Research Paper

International Security Programme

August 2024

The internet under attack

Insights from Afghanistan and Ukraine on maintaining a resilient internet in conflict and crisis

James Shires and Isabella Wilkinson

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

	Summary	2
01	Introduction	4
02	Rethinking resilience	10
03	Internet resilience in Afghanistan	15
04	Internet resilience in Ukraine	24
05	Conclusion	37
	About the authors	40
	Acknowledgments	40

Summary

- Many aspects of modern conflict are defined by the internet and digital technologies. The concept of resilience is essential to understanding the complex web of incentives, interests and dependencies that determine how the internet and these technologies work – and, often, do not work – in conflict and crisis situations.
- This research paper distinguishes between two types of resilience – *technical* and *sociopolitical*. *Technical* resilience focuses primarily on technological systems constituting the internet, while *sociopolitical* resilience refers to the human networks and groups that both maintain those technological systems and ensure they are available to use. Considering how these two types of resilience interact helps develop a deeper understanding of how different actors use the internet and digital technologies in complex scenarios, from invasions to military takeovers. The value of distinguishing between types of resilience applies especially when assessing the roles of the private sector; these roles are rewritten, enabled and constrained by a range of incentives and pressures unique to commercially driven actors.
- The paper is built on two case studies, with almost opposing characteristics in key areas such as internet infrastructure, conflict dynamics and policy priorities. The first discusses events before, during and after the Western coalition's withdrawal from Afghanistan in August 2021. The second examines internet resilience before and during Russia's full-scale invasion of Ukraine in February 2022. Each is a powerful demonstration of how internet resilience is crafted, contested and reconstituted in unstable situations, and of the interplay between global and local internet resilience – where decisions adopted by actors operating at the local level have global implications, and vice versa. Both case studies highlight the varied roles the private sector plays when it withdraws from and steps into these settings.
- These case studies make clear that *technical* and *sociopolitical* resilience are inextricably linked, particularly when it comes to the reaction of people and organizations to disruption. The distinction between resilience types raises questions such as: how agile are the responses of various individuals and their communities to recovering data and replacing lost connections? What are the processes and mechanisms in place for doing so, and how effective are they? As the case studies demonstrate, interdependence between the technical and sociopolitical is amplified in conflict and crisis settings.

- The resilience of the internet is fundamentally implicated with that of individuals, organizations and even countries. Adversaries incorporate resilience thinking into their offensive tactics as much as defenders incorporate it into theirs. The most visible manifestation of this idea is the rise in cyberattacks to accompany – and, in some cases, exacerbate – conventional military attacks on critical infrastructure. But threats to, and drivers of, internet resilience extend far beyond cyber defence to involve everything from the people, processes and measures involved in the technical repair of damaged cables to the measures adopted by civil society groups to weather or circumvent internet shutdowns.
- Afghanistan and Ukraine also show that the private sector plays crucial and rapidly evolving roles in maintaining internet resilience in conflict and crisis. These roles are also highly dependent on context. The private sector is not a monolith; even a single entity can often occupy multiple, sometimes even contradictory, roles. To better delineate, untangle and identify those roles, this research paper concludes by proposing a typology of four main role categories:
  - **Providers** that supply and maintain parts of internet infrastructure at distinct or multiple layers of the stack (e.g. a telecommunications company supplying hardware such as cables or providing satellite internet services);
  - **Shapers** that seek to impact policies, strategies and processes concerning internet resilience on the national or international levels (e.g. a major technology company active in the multi-stakeholder community, sharing input in UN-level meetings on cyber governance);
  - **Entrepreneurs** that innovate technologies at distinct or multiple levels of the stack, with direct bearing on resilience (e.g. a hardware- or software-focused quantum computing and communications company); and
  - **Challengers** that provide enabling technology, resources or personnel to challenge internet resilience (e.g. a commercial hacking company contracted by an intelligence or military agency to mount cyberattacks targeting internet infrastructure).
- This paper seeks to challenge existing approaches to resilience and apply a new approach to its case studies, merging the technical and sociopolitical dimensions of resilience and considering the interplay between them. For private sector stakeholders (for example, those involved in the provision of connectivity), the paper seeks to present novel characterizations of their own complex roles in resilience, thereby encouraging more comprehensive mapping of their web of interests and incentives in providing, maintaining or even damaging both types of internet resilience. For public sector and policymaking stakeholders (for example, those involved in developing and shaping a strategic approach to engagement in international conflicts), the paper carries lessons, best practices and, in some cases, cautionary tales for providing resilience and for their engagement with private sector stakeholders – whether through procurement of services, information-sharing or in consultation.

01 Introduction

Rethinking what constitutes resilience is essential for understanding the complex web of incentives, interests and dependencies that have come to define how the internet works – and, often, does not work – in conflict.

As part of their invasion of Gaza in October 2023, Israeli armed forces cut off all telephone and internet communications to the territory on several occasions, for multiple hours each time. The effect on media reporting of the conflict was immediate – a previously constant stream of images, videos and live updates virtually ceased for the duration of the outage. In a thread on X (formerly Twitter), Elon Musk responded to demands for his platform to facilitate internet access through the Starlink satellite network (which Musk also owns) by stating that 'Starlink will support connectivity to internationally recognized aid organizations in Gaza'.[1] Musk had reacted similarly in Ukraine, where Starlink terminals and connections had enabled the Ukrainian military in its operations in early 2022.[2]

In some ways, the two events – armed forces' severing of telephone and internet communications and the offer by a private company to fill gaps in service – are neither new nor surprising. Information channels have always been a crucial aspect of any conflict, and states have long targeted the strategic communications routes of their adversaries to gain a military advantage, while also developing and reinforcing their own communications technologies and processes. In the digital era, intentional internet shutdowns are frequent occurrences, both to facilitate military manoeuvres and to enable authoritarian states to dampen

1 Shankar, P. (2023), 'Can Elon Musk's Starlink provide internet service to Gaza?', Al Jazeera, 29 October 2023, https://www.aljazeera.com/news/2023/10/29/can-elon-musks-starlink-provide-internet-service-to-gaza.
2 In the biography of Musk by Walter Isaacson, it was claimed that Starlink received an emergency request to activate satellite internet over Crimea, which was refused to avoid 'be[ing] explicitly complicit in a major act of war'. See Isaacson, W. (2023), *Elon Musk*, London: Simon & Schuster. However, in September 2023, Isaacson clarified the record and admitted that he had misinterpreted the events discussed. The *Washington Post*, which had published excerpts of Isaacson's book, subsequently added a correction stating that the book had 'mischaracterized the attempted attack by Ukrainian drones on the Russian fleet in Crimea. Musk had already disabled ('geofenced') coverage within 100 km of the Crimean coast before the attack began, and when the Ukrainians discovered this, they asked him to activate the coverage, and he refused.' See Isaacson, W. (2023), "How am I in this war?': The untold story of Elon Musk's support for Ukraine', *Washington Post*, 7 September 2023, https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion.

and repress popular dissent or protest.[3] Likewise, private companies have been important actors in conflict for centuries, providing logistical support, arms and other advanced technological equipment to one party or another, and quickly becoming entangled in the geopolitical ramifications of their actions.

However, in the 'internet era', there are qualitative differences in the extent to which non-state actors – such as technology companies and non-profit internet governance organizations – can directly or indirectly influence conflict dynamics. For example, the large-scale transfer of Ukrainian government data to cloud-based infrastructure in February 2022 – facilitated technologically by major Western companies, legally by swift action on the part of Ukrainian legislators, and diplomatically by NATO states – would have been unthinkable only a few years ago.[4] The decision by the non-profit Internet Corporation for Assigned Names and Numbers (ICANN) in March 2022 to maintain Russia's access to core internet services (namely, the domain name system – DNS) was another striking novel development. This example was notable not only because ICANN resisted strong pressure to restrict these services (in contrast with a decision by the Swift international banking network to cut Russia off from its services two months later),[5] but because the power to decide a nation's relationship with the global internet sat with a multi-stakeholder and largely technocratic organization, rather than with states or private companies. Questions remain regarding the power of other non-state actors in 'internet era' conflicts, particularly when such actors directly supply military or dual-use technologies, such as software used for tracking troop movements or facilitating targeting decisions.[6]

Defining internet resilience

Significant parts of modern conflict are increasingly defined by the internet and digital technologies. Seeking to untangle and understand the rapidly changing roles of technology and private sector actors in these settings, policymakers and experts alike increasingly turn to the idea of *resilience*. The concept of resilience is essential for understanding the complex web of incentives, interests and dependencies that have come to define how the internet works – and, often, does not work – in conflict.

However, as a term and concept, resilience is inclusive of a wide variety of issues. In the case of Starlink in Ukraine, the issue is the *technical* resilience of telecommunications networks and their effect on the resilience of the Ukrainian military. In Gaza, urgent questions revolve around the implications of the resilience of internet and telecommunications infrastructure for social and medical infrastructure, in a rapidly worsening humanitarian crisis. While both cases

3 Gohdes, A. (2023), 'Digital infrastructure is strategic terrain', Binding Hook blog, 21 November 2023, https://bindinghook.com/articles-hooked-on-trends/digital-infrastructure-is-strategic-terrain.
4 However, this was by no means the first event of its kind, although the speed and scale of movement, and international attention, was unprecedented. For example, during the Russia–Georgia war in 2008, the Georgian government used a Google-run blogging website to post news after deliberate denial of service (DDOS) cyberattacks against government websites.
5 Swift (2022), 'An update to our message for the Swift Community', article, 20 March 2022, https://www.swift.com/news-events/news/message-swift-community.
6 Bertuca, T. (2022), 'Next phase of Army's TITAN AI program pits Palantir against Raytheon', Inside Defense, 29 June 2022, https://insidedefense.com/insider/next-phase-armys-titan-ai-program-pits-palantir-against-raytheon.

revolved around the availability of the internet in a particular location – and hence Starlink was proposed as a solution in both instances – the state and social functions that internet connectivity sought to enable were vastly different. In the ICANN case, pertinent questions arose around the resilience of the global internet governance architecture, and its vulnerability to future politically motivated intervention.

The key question is then how the concept of resilience can be refined in order to understand the changing role of the internet in conflict. This research paper's starting point is that internet resilience should be thought of in two distinct types: *technical* and *sociopolitical*. While, in both cases, resilience concerns the ability of a system (for the purposes of this paper, the internet) to recover from a shock or incident, *technical* resilience focuses primarily on technological systems constituting the internet. *Sociopolitical* resilience meanwhile refers mainly to the human networks and groups that maintain and uphold those technological systems, enabling their continued availability and use.

Technical resilience focuses primarily on technological systems constituting the internet. _Sociopolitical_ resilience refers mainly to the human networks and groups that maintain and uphold those technological systems, enabling their continued availability and use.

The distinction is not clear-cut. Technological systems are never purely technological, while sociopolitical processes are more technological than they may seem at first. More precisely, technological systems depend on practices developed in specific social settings and modern sociopolitical processes rely on the affordances of extensive technological infrastructure to function smoothly. Nonetheless, viewing internet resilience through either a *primarily* technical or sociopolitical lens helps to distinguish the roles and responsibilities of various stakeholders, and the kinds of impact that these stakeholders might mitigate or repair. This paper argues that the interplay between the two forms of internet resilience reveals significant (and, in some cases, surprising) dynamics around the use of internet and digital technologies in conflict.

To make its argument, the paper draws on two case studies. The first examines internet architecture and use before, during and after the US-led military coalition's withdrawal from Afghanistan in August 2021. The second case study highlights the connections between global and local internet resilience and the resilience of internet architecture in Ukraine before, during and after the Russian invasion that began in February 2022.

This second study is chosen as the inverse of the first. In demographic terms, Afghanistan is a poor, developing country with low levels of internet penetration and other, more pressing infrastructural priorities. By contrast, pre-war

Ukraine had a booming IT sector closely tied to European and US markets. In addition, Ukraine continues to receive extensive policy and media attention, with overlapping and mutually reinforcing incentives for private sector actors to contribute, although significant gaps remain. After the chaos and political fallout of the hasty withdrawal of forces after over 20 years of fighting and reconstruction, issues of internet resilience in Afghanistan have received less international attention.

Most commentators examining internet and cybersecurity issues in the context of Russia's 2022 invasion of Ukraine have focused on the role (or lack thereof) of Russian offensive cyber operations, with some seeing a surprising lack of effect from 'wiping'[7] and other disruptive operations, and others identifying a concerning 'civilianization' of cyber operations towards cybercriminal groups, hacktivists and 'cyber militias' such as the Ukraine IT Army.[8] In contrast, an analysis in terms of resilience highlights a more central role for early decisions by private companies and non-state actors to provide cloud infrastructure in support of Ukraine, and for broader efforts to build Ukrainian cyber defence capabilities to prevent complete internet shutdowns or loss of communications. While these efforts are usually discussed in terms of cybersecurity capacity-building,[9] this paper argues that a framing in terms of resilience helps to connect technical cybersecurity protections with their broader sociopolitical purpose in resisting occupation. Such a frame also provides a clearer understanding of the motivations for different actors – especially those in the private sector – to contribute to such efforts.

Investigating internet resilience in Afghanistan provides an equally important insight into the motivations and roles of similar stakeholders to those in Ukraine (for example, government contractors, IT companies or telecoms providers), but in a situation where the priorities are almost reversed. Dividing the Afghanistan case study into pre-, during and post-crisis environments also reveals a landscape (including the internet and digital technologies themselves, and the variety of actors interacting with and impacting the internet and digital technologies in different ways) that shifts over time. More generally, the case of Afghanistan is important not just in its own right, but because it offers indications for current or potential future scenarios (e.g. Gaza or Taiwan) where international support may be more ambiguous, as well as the dangers of what might be termed 'support fatigue' as Russia's war on Ukraine continues.

---

7 'Wiper' malware refers to malware that can corrupt or delete data beyond recoverability. Actors may deploy wiper malware to make computer networks unusable by preventing an organization from accessing its data or to obfuscate evidence of a cyber intrusion. For more, see Zieniūtė, U. (2024), 'Wiper malware: What is it, history, and prevention', Nord VPN blog, 28 March 2024, https://nordvpn.com/blog/wiper-malware.
8 See Wilde, G. (2022), *Cyber Operations in Ukraine: Russia's unmet expectations*, working paper, Washington, DC: Carnegie Endowment for International Peace, https://carnegieendowment.org/files/202212-Wilde_Russia Hypotheses-v2.pdf; Kostyuk, N. and Gartske, E. (2022), 'Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine', *Texas National Security Review*, 5(3), pp. 113–26, https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of-ukraine.
9 Brantly, A. (2022), 'Battling the bear: Ukraine's approach to national cyber and information security', in Dunn Cavelty, M. and Wenger, A. (eds) (2022), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, Abingdon: Routledge, pp. 157–71.

Methodology

The paper relies empirically on extensive research from a range of primary and secondary sources, including documents from government and international organizations, private sector statements, media and news reports, commentary and analysis prepared by civil society organizations, and research reports. It also builds on Chatham House's research on the changing dynamics of the cyber policy threat landscape.

The paper – and especially the featured case study on Ukraine – also draws on 11 interviews conducted with UK-based stakeholders (from government, the private sector and civil society) in May and June 2023. Interviewees were selected from among the participants[10] in a Chatham House event on 'Internet in Conflict: Trends and Future Challenges', held in May 2023 under the Chatham House Rule.[11] The interviews shed light on how key stakeholders from government, the private sector and academia are tackling the notion of resilience, particularly in response to Russia's war on Ukraine.

Notwithstanding this, the interviewees were mainly UK-based and, in most cases, offered UK- or Western-centric perspectives. Consequently, while attempts to balance this with a wider range of interviews were regrettably beyond the scope of the work conducted for this paper, each chapter seeks to ensure interview insights are critically accompanied by other sources.

Gathering primary data on Afghanistan was also a challenge, in part due to the interviewees' primary focus and expertise on Ukraine, and the research team's existing expertise on Ukraine, but also partly to the operational challenges of interviewing in-country experts. To compensate for these deficiencies, the authors sought additional research assistance focused solely on internet resilience in Afghanistan, and convened several evidence-based reviews and discussions of secondary research.[12] Their work also benefited from an informal conversation with a regional digital policy expert, whose experience underlined the difficulties of conducting research interviews with Afghanistan-based experts.

---

10 These participants, in turn, were selected due to their expertise and/or involvement in the UK's approach to internet resilience and technology policymaking, with a focus on Ukraine and Afghanistan. Among the participants, there were more with experience and/or involvement surrounding Ukraine. As a result, the Afghanistan case study draws further on secondary sources than the study on Ukraine.

11 'When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.' See Chatham House (undated), 'Chatham House Rule', https://www.chathamhouse.org/about-us/chatham-house-rule. Interviews were conducted online, lasted around 30 minutes and were transcribed by the authors. Interviewees were asked a series of open-ended guiding questions (shared in advance) on internet resilience, the UK's role in internet governance, private sector actors in conflict and their roles, responsibilities and relationships. During the interviews, in the interests of time and according to the interviewee's experience and expertise, the interviewer(s) prioritized certain questions over others. Data from the interviews were all anonymized. To analyse the interview data, the authors employed qualitative coding – in particular, thematic coding based on themes identified in the guiding questions, with space for inductive, open coding for remaining data and any significant gaps). Insights and quotations from these interviews are attributed to role and organization description, which most interviewees offered. In the event interviewees did not offer this information, the authors created an anonymized, representative description.

12 The authors thank Beth Whittaker (a former intern in the International Security Programme at Chatham House) for her support.

Both case studies would undoubtedly have been strengthened by interviews with individuals and organizations on-the-ground. Nonetheless, the authors are confident that the content of both case studies presents others with potential avenues for further research.

About this paper

The paper is structured as follows. Chapter 2 sets out the background in more detail, outlining the relationship between technical and sociopolitical resilience; the role of private sector technology companies in conflict; and how internet resilience may change in these settings. Chapters 3 and 4 then address the case studies of Afghanistan and Ukraine, applying the conceptual approach and drawing on the data sources above to unpack the roles and responsibilities of different stakeholders in maintaining or improving internet resilience in each setting. Chapter 5 highlights some preliminary conclusions and proposes a typology for characterizing the roles of private sector stakeholders in internet resilience.

This paper encourages readers to apply a holistic approach to internet resilience. For state stakeholders (e.g. those involved in developing and shaping a strategic approach to engagement in international conflicts), the paper carries lessons, best practice and, in some cases, cautionary tales for providing resilience and in their engagement with private sector stakeholders – whether through procurement of services, information-sharing or in consultation. For private sector stakeholders (e.g. technology and telecommunications companies involved in the provision of connectivity in conflict areas), the paper may include familiar and novel characterizations of their own complex roles in ensuring resilience, encouraging them to map more comprehensively their web of interests and incentives in recognition of the fact that, in conflict and crisis settings, this web will face severe and unpredictable disruption.

02 Rethinking resilience

Examining both the technical and sociopolitical types of internet resilience helps develop a deeper understanding of threats to, and drivers of, resilience.

In the context of internet governance, resilience is by no means a new concern. The goal of building and maintaining resilient systems has driven the development of standards, protocols and cybersecurity measures since the internet was in its infancy.[13] However, in recent years, the notion of resilience has gained traction in security discourse, research and practice.[14] In the field of cyber policy and governance, resilience thinking is at least partial evidence of a shift towards a human-centric, whole-of-society approach to security.

For those involved in technical aspects of the internet, resilience often simply means the internet's capacity to 'bounce back' from disruptive incidents, ranging from outages to malicious cyberattacks.[15] Several experts interviewed for this paper – from a variety of sectors, including industry and the technical community[16] – described resilience as a measure of a network's ability to recover through the repair of impaired or impacted systems, patching of vulnerabilities and restoration of reliable access to the end user. The Internet Society, an internet governance and technical body, defines resilience as an 'acceptable level of service… in the

13 Leiner, B. et al. (1997), 'A Brief History of the Internet', *ACM SIGCOMM Computer Communication Review*, 39(5), pp. 22–31, https://doi.org/10.1145/1629607.1629613.
14 For further reading, see Dunn Cavelty, M., Kaufmann, M. and Kristensen, K. (2015), 'Resilience and (In)security: Practices, Subjects, Temporalities', *Security Dialogue*, 46(1), https://doi.org/10.1177/0967010614559637.
15 Research interview with an employee at a large threat intelligence and incident response company, May 2023. For further reading, see Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015), 'Cyber Resilience – Fundamentals for a Definition', in Rocha, A., Correia, A., Costanzo, S. and Reis, L. (eds) (2015), *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, Springer: Cham, https://doi.org/10.1007/978-3-319-16486-1_31.
16 The technical community refers to the diverse range of global technical stakeholders involved in the development, provision and standardization of the internet and digital technologies. A prime example is that of stakeholders involved in the Internet Engineering Task Force set up to oversee parts of the technical management and operation of the global internet.

face of faults and challenges to normal operations'.[17] In this sense, resilience is contingent on perceived, predicted and actual (cyber)security risks and unintentional accidents.[18]

But analysts have become increasingly concerned by the non-technical side of resilience, seeking a fuller picture of risks to the internet, its applications and users. Some analysts have sought to gauge resilience by looking at market dynamics (such as traffic localization) and technical performance (such as the performance of internet service providers).[19] These wider notions of resilience often aim to be human-centric and subject-driven, rooted in an individual's experience of internet access and use.[20] These notions are therefore dependent on perspective. Perceptions of resilience also have a degree of 'complex temporality', in that benchmarks are responsive to, and defined by, both past and future incidents.[21]

Wider notions of resilience aim to be human-centric and subject-driven, rooted in an individual's experience of internet access and use.

Conceptual flexibility – and the idea that resilience can mean different things in different settings – is not necessarily an analytical shortcoming. Careful and strategic merging of technical and non-technical approaches gives rise to ecosystem-level thinking, and demands the consideration of resilience for whom, where, why and when. For example, an incident responder at a national cyber agency may define resilience in terms of technical benchmarks such as availability and recoverability. However, if that responder is also partially responsible for developing their country's national cybersecurity strategy, their approach to resilience may then focus more on improving the experience of individuals online. If said responder then becomes a contributor to an international standards development organization, the same individual may instead define a resilient internet in terms of the strength of processes and mechanisms required to ensure the interoperability of the global internet.

---

17 Phokeer, A. et al. (2021), *Measuring Internet Resilience in Africa (MIRA)*, Internet Society, https://pulse.internetsociety.org/wp-content/uploads/2021/05/Measuring-Internet-Resilience-in-Africa-EN-May2021.pdf.
18 Shires, J. and Hakmeh, J. (2020), *Is the GCC Cyber Resilient?*, Briefing Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/2020/03/gcc-cyber-resilient-0/state-cybersecurity-gcc-overview.
19 The Internet Society's measures for internet resilience includes four pillars: infrastructure (i.e. the existence and availability of physical infrastructure that provides internet connectivity); security (the ability of the network to resist intentional or unintentional disruptions through the adoption of security technologies and best practices); performance (the ability of the network to provide end users with seamless and reliable access to internet services); and market readiness (the ability of the market to self-regulate and provide affordable prices to end users by maintaining a diverse and competitive market). See Internet Society (undated), 'Internet Resilience', https://pulse.internetsociety.org/resilience.
20 An important example is the concept of 'meaningful connectivity', authored by the Alliance for Affordable Internet, which asks: 'Can different individuals access the internet regularly? Can they do so affordably and from an appropriate device?' See Woodhouse, T. (2022), 'Meaningful Connectivity: A new measure for internet access', World Wide Web Foundation blog, 28 February 2022. https://webfoundation.org/2022/02/meaningful-connectivity-a-new-measure-for-internet-access.
21 Dunn Cavelty, Kaufmann and Kristensen (2015), 'Special Issue: Resilience and (in)security', p. 7.

This paper therefore distinguishes between two types of internet resilience:

— *Technical* resilience refers to the continued, reliable operation of internet infrastructure and architecture at all levels, including the ability to recover from incidents.

— *Sociopolitical* resilience refers to the local, organizational, national and/or international processes, policies, and non-technical systems and responses in place to ensure continued availability and meaningful use of the internet. While technological innovations increase internet resilience (for example, cloud data storage or secure transmission protocols), they do so within a particular sociopolitical context, and their impact is neither uniform nor determined solely by the technology itself.[22]

In addition, this paper suggests two scope conditions that can aid understanding of internet resilience in any given case. First, internet resilience depends on *setting*, defined in geospatial or contextual terms. This includes locations (e.g. a certain country) and contextual environments (e.g. an active military conflict). For the purposes of this paper, conflict and crisis are considered as settings. Internet resilience in a particular setting and internet resilience at a global or holistic network level are closely interrelated, as demonstrated by the discussion of Ukraine in Chapter 4. Crucially, while all layers of the stack are interdependent, it is possible for some layers to demonstrate resilience while others do not.[23] This underlines the need for a contextual approach to defining resilience, in addition to one that considers both global and local resilience.

Second, internet resilience is dependent on the relevant *stakeholders*. This paper defines stakeholders as those involved in the construction, maintenance and challenging of internet resilience, as opposed to those experiencing resilience (or lack thereof). Stakeholders can be loosely defined by sector or more specifically defined at the individual or organizational level.

These two distinctions provide an overall structure for the paper, as follows:

— There are two **types** of resilience within the scope of this paper: *technical* and *sociopolitical*.

— The **settings** considered in this paper are conflict and crisis settings at the national or immediate cross-border level, detailed below. Although outside of the scope of this paper, other settings could vary in levels of political and economic stability and security (e.g. peacetime, post-conflict or post-disaster, transitional).

---

22 'Forensics and incident response are drivers of internet resilience. So is access to cloud architecture… if you get wiper malware, you can reset your systems almost instantaneously.' Research interview with an employee at a large threat-intelligence and incident response company, May 2023.
23 A useful way to visualize the internet's different layers (often called 'the stack') are the OSI (seven-layer) and TCP/IP (four-layer) models. See Frenzel, L. (2013), 'What's The Difference Between The OSI Seven-Layer Network Model And TCP/IP?', Electronic Design, 3 October 2013, https://www.electronicdesign.com/technologies/communications/article/21800810/electronic-design-whats-the-difference-between-the-osi-seven-layer-network-model-and-tcp-ip.

— As explored in this section, the internet resilience landscape involves a diverse variety of **stakeholders**. While this paper broadly considers the private sector, others may include armed groups, militaries, international organizations, civil society organizations and others.

As described above, this paper considers internet resilience *only* during conflict and crisis. Conflict is defined as a setting with sustained, antagonistic military or security engagement between two or more parties with misaligned strategic objectives at the local, national or cross-border level. Conceptually, conflict is closely related to crisis. Crisis settings are more ambiguous – and can include political, military and/or other security turbulence, turnover and takeovers at the local, national or cross-border level, as well as post-conflict settings. Perhaps most importantly, both conflict and crisis settings are ones in which security risks – including risks to internet resilience – are usually heightened.

Conflicts around the world often have a direct impact on the continued, reliable operation of internet infrastructure and architecture. A violent military takeover, for instance, could lead to the physical disruption of internet infrastructure. As a representative from a major technology company commented, 'conflict changes how [internet] infrastructure works', but it 'doesn't necessarily mean it's less resilient'.[24] A commonly cited example of technical internet resilience is the ability of internet service providers (ISPs) to recover from localized disruptions, whether these are outages or direct attacks.[25] However, while conflict poses severe threats to resilience, it may also provide the opportunity for demonstrating resilience. The same interviewee above commented that 'you would assume that, during conflict, of course the internet is less resilient. But what we've found is that conflict teaches us lessons about resilience'.[26]

Conflicts around the world often have a direct impact on the continued, reliable operation of internet infrastructure and architecture.

Sociopolitical internet resilience has increased salience during conflict. For instance, an ISP's operations may be considered technically resilient if it can resume service provision to end users in the event of disruption. However, from the perspective of sociopolitical internet resilience, resumption of service must lead to the resumption of the meaningful use of everyday services for those end users. From the end user's perspective, resilience hinges on basic functioning. As an academic researcher specializing in Ukraine noted, this means that the end user is not 'thinking about whether [the internet] will be there the next day'.[27]

---

24 Research interview with a representative from a major technology company, May 2023.
25 Experts at Cloudflare, a connectivity cloud platform, note the spike in 'localized disruptions in certain regions' in the first few months of Russia's war in Ukraine. See Tomé, J., Belson, D. and Berdan, K. (2023), 'One year of war in Ukraine: Internet trends, attacks, and resilience', Cloudflare blog, 23 February 2023, https://blog.cloudflare.com/one-year-of-war-in-ukraine.
26 Research interview with a representative from a major technology company, May 2023.
27 Research interview with an academic researcher, May 2023.

By examining these two kinds of internet resilience in conflict and crisis, this paper can help policymakers, practitioners and researchers better understand the threats and drivers of resilience under stress. Conversely, analysing internet resilience in these settings can also reveal economic, security, political and military dynamics about the conflict or crisis itself. For instance, activists and researchers have long used open-source methodologies to track network shutdowns, bandwidth-throttling and service-based blocking of communication platforms. But this practice can also enable them to raise the necessary alerts about the use (or abuse) of internet shutdowns by repressive states to curb social upheaval.[28]

This paper focuses on one particular set of stakeholders in the internet resilience ecosystem: the private sector. Private sector actors are individuals operating on behalf of a privately owned or publicly listed company, a company acting as a consolidated entity or several entities operating together. There are no definitional limits on organizational size, scope or remit. Indeed, the diversity of private sector actors is a key consideration in both case studies. In some cases – including that of Ukraine – whether an individual is acting on behalf of a company is not always easy to ascertain, as many initial contributions to Ukrainian cyber defence were made by individuals outside their corporate commitments. While this paper focuses on private sector stakeholders, it also considers, where relevant, the role that other non-state stakeholders may play in internet resilience. These 'others' range from representatives of non-profit internet governance organizations, 'white hat' hackers and cybercriminals, to digital rights activists and civil society advocates.

The private sector's perceived and actual roles and responsibilities differ from 'business-as-usual' in two ways. First, conflict and crisis settings disrupt private sector activities due to newly created or amplified barriers to operation and risks faced in service provision on the one hand, and direct attacks, complicity[29] or implication in conflict dynamics on the other. For instance, as an employee at a large threat-intelligence and incident-response company commented, private sector companies 'are in the crosshairs of government operations' and may 'already be an intelligence target'.[30] This new reality is encouraging private sector actors to change or adapt their posture to maintain operations.

Second, notions of duty and responsibility may also expand in such settings. Multiple interviewees from the private sector commented that in conflict environments, private sector actors will take additional steps to protect both their commercial interests and the physical security of their staff.[31] Other interviewees commented on new modes of communication, collaboration and information sharing between the UK government and technology companies that was prompted by the Ukraine conflict (although at least two noted that similar arrangements were worryingly 'ad hoc').[32] The extent of these expanded roles depends on the context of specific cases, such as those discussed in the following chapters.

---

28 Access Now (2023), 'Shutdown Tracker Optimization Project (STOP)', https://www.accessnow.org/wp-content/uploads/2023/03/Read-Me_STOP_data_methodology.pdf. For further information on the #KeepItOn coalition and campaign, see Access Now (2023), '#KeepItOn: fighting internet shutdowns around the world', https://www.accessnow.org/campaign/keepiton.
29 Research interview with a senior defence and technology advisor working in the UK government, May 2023.
30 Research interview with an employee at a large threat-intelligence and incident-response company, May 2023.
31 Research interview with a senior representative from a technology company, May 2023; research interview with representatives from a technology/cybersecurity company, June 2023.
32 Research interview with a representative from a major technology company, May 2023; research interview with a member of the internet governance technical community, May 2023.

03
Internet resilience in Afghanistan

Studying the state of internet resilience in Afghanistan reveals the interplay between technical and sociopolitical internet resilience and how it unfolds in a crisis environment.

This case study considers the interplay between technical and sociopolitical internet resilience and how this interplay unfolds in a crisis environment, namely Afghanistan, with a focus on how the private sector was engaged in constructing – and challenging – resilience.

Definitions of what (and when) constitutes a crisis are highly subjective and driven by context. Some Afghan regions suffered sustained military action for the duration of the international coalition's presence in the country, while others enjoyed periods of relative calm. For ease of analysis, this chapter splits the withdrawal period into three separate phases.

- First, the period before US president Joe Biden's announcement of the full and unconditional troop withdrawal in April 2021 is regarded as 'pre-crisis' for the purposes of this paper. Although withdrawal itself was prolonged and politically controversial well before this point, it did not become an acute or active crisis until this moment. Hostilities – for instance, between the Taliban and (former) government forces in the Helmand province – occurred just days after NATO forces commenced their final withdrawal of their Afghanistan mission.[33]
- Second, the period between the April 2021 announcement and early to mid-September 2021 is treated as a state of 'active crisis'. Between May and August, Taliban forces swept through the country, taking Kabul on 15 August.

33 Agence France-Presse via *Guardian* (2021), 'Timeline: the Taliban's sweeping offensive in Afghanistan', 16 August 2021, https://www.theguardian.com/world/2021/aug/16/timeline-the-talibans-sweeping-offensive-in-afghanistan.

But the state of active crisis is not considered to have ended until Taliban forces claimed victory in the Panjshir province, which was regarded as the final holdout of substantial anti-Taliban resistance.[34]

— Finally, the period from the announcement of the Taliban's interim administration to 30 November 2023 (the cut-off date for research conducted for this paper) is considered 'post-crisis'. The establishment of the Taliban's 'Islamic Emirate' was announced on 7 September 2021,[35] and since its takeover, the Taliban has sought to normalize its relations with foreign governments and establish itself as the legitimate representative of the Afghan nation. But hopes for a slightly more moderate 'Taliban 2.0' at the domestic level were rapidly dashed. Indeed, Amnesty International characterized the Taliban's first year in power as a year of 'violence, impunity and false promises', with oppressive and violent measures undertaken to consolidate power, quell resistance and curb political freedoms and civil rights.[36]

Internet resilience pre-crisis

In Afghanistan, there are long-standing structural, political and economic barriers to internet connectivity, in addition to the continued disruptions posed by localized conflicts. These barriers have served to undermine the country's overall internet resilience. Although over 90 per cent of the country receives 2G mobile network coverage,[37] internet penetration rates in January 2021 were only around 22 per cent,[38] compared to around 80 per cent in a country like Ukraine.[39] Other surveys report that just 15 per cent of all Afghans have access to the internet, a figure unchanged since 2016.[40] Several civil society organizations and research institutes have mapped the barriers to internet access in Afghanistan. These barriers are technical (such as destroyed or absent digital infrastructure); socio-economic (such as the affordability of, and access to, devices and internet connectivity); and cultural (such as social norms).[41]

From 2001 onwards, multiple national initiatives, partnerships and foreign development projects were launched, seeking to improve Afghanistan's internet infrastructure and put in place building blocks for both technical and sociopolitical

---

34 Blue, V. J. and Huylebroek, J. (2021), 'In Panjshir, Few Signs of an Active Resistance, or Any Fight at All', *New York Times*, 17 September 2021, https://www.nytimes.com/2021/09/17/world/asia/panjshir-resistance-taliban-massoud.html.
35 BBC News (2021), 'Hardliners get key posts in new Taliban government', 7 September 2021, https://www.bbc.co.uk/news/world-asia-58479750.
36 Amnesty International (2022), 'Afghanistan: One year of the Taliban's broken promises, draconian restrictions and violence', 15 August 2022, https://www.amnesty.org/en/latest/news/2022/08/afghanistan-one-year-of-the-talibans-broken-promises-draconian-restrictions-and-violence.
37 Barton, J. (2022), 'Afghanistan telecom sector's progress threatened by return of Taliban regime', Developing Telecoms, 9 June 2022, https://developingtelecoms.com/telecom-business/market-reports-with-buddecom/13589-afghanistan-telecom-sector-s-progress-threatened-by-the-return-of-the-taliban-regime.html.
38 Kemp, S. (2021), 'Digital 2021: Afghanistan', Data Reportal, 11 February 2021, https://datareportal.com/reports/digital-2021-afghanistan.
39 Statista (2024), 'Share of daily internet users in Ukraine from 2015 to 2023', https://www.statista.com/statistics/1023197/ukraine-internet-penetration.
40 Nusratty, K. and Crabtree, S. (2023), 'Digital Freedom Out of Reach for Most Afghan Women', Gallup blog, 8 March 2023, https://news.gallup.com/opinion/gallup/471209/digital-freedom-reach-afghan-women.aspx.
41 Ibid. Nusratty and Crabtree (2023) estimate that of the approximately 15 per cent of Afghans with internet access, the majority are men.

resilience. International partners including the World Bank[42] and NATO[43] funded various schemes to develop the country's ICT sector, expand internet connectivity and build cybersecurity capacity. Foreign partners including the US and UN agencies also developed, and helped to deploy, biometric data systems used for public administration.[44] Relevant Afghan authorities – including the National Statistics and Information Authority and the Ministry of Communication and Information Technology (MCIT) – established as national priorities the building of infrastructure for digital transformation and empowering digital capabilities.[45] Various public-private partnerships (PPPs) were also created to build and bolster internet availability. For example, state-owned Afghan Telecom struck major 2G and 3G network rollout deals with a Chinese company, ZTE.[46] Meanwhile, the predecessor of Afghan Wireless – currently Afghanistan's best-connected autonomous system – was formed as a joint venture between the MCIT and Telephone Systems International Ltd in 2002.[47]

From 2001 onwards, multiple national initiatives, partnerships and foreign development projects were launched, seeking to improve Afghanistan's internet infrastructure and put in place building blocks for both technical and sociopolitical resilience.

In the years immediately prior to the Taliban's takeover in 2021, the country experienced direct attacks on its internet infrastructure. In 2019 alone, the Afghanistan Telecom Regulatory Authority (ATRA) reported the destruction or disruption of 220 towers by the Taliban and other groups.[48] Targeting telecommunications infrastructure is a decades-old Taliban strategy. (In the 1990s, there were reports of the Taliban cutting internet cables.)[49] These activities reportedly intensified in the lead-up to the 2021 takeover.[50] According to the MCIT

---

42 For an overview of the World Bank's support for Afghanistan's connectivity, see Crouch, G. (2014), 'Afghanistan Moves to Connect Afghans with Each Other and with the World', World Bank blog, 10 January 2014, https://www.worldbank.org/en/news/feature/2014/01/09/afghanistan-connects-each-other-world.
43 NATO supported a range of cyber defence and connectivity projects. See North Atlantic Treaty Organization (2010), 'NATO to expand Internet connectivity in Afghanistan', press release, updated 13 January 2010, https://www.nato.int/cps/en/natohq/news_60259.htm?selectedLocale=en; North Atlantic Treaty Organization (2012), 'Afghan managers train in cyber defence', updated 23 May 2012, https://www.nato.int/cps/en/natohq/news_86990.htm?selectedLocale=en.
44 Many systems were left behind in 2021; today, the Taliban's control over them has sparked concerns from human rights organizations. Human Rights Watch (2022), 'New Evidence that Biometric Data Systems Imperil Afghans', 30 March 2022, https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans.
45 For an overview and analysis of Afghanistan's science, technology and innovation ('STI') policy initiatives and ministerial leadership of said initiatives (up to 2020), see Mohsen, A. (2020), *Science, Technology, and Innovation (STI) Gap Analysis of Afghanistan*, United Nations Economic Commission for Europe, August 2020, https://unece.org/sites/default/files/2021-03/STI%20gap%20analysis_Afghanistan%20Report_%20Ahsanullah%20Mohsen.pdf.
46 Cerulus, L. (2021), 'Fears loom over Afghanistan's internet', Politico, 25 August 2021, https://www.politico.eu/article/afghanistan-braces-for-fight-over-taliban-internet-information-control.
47 Netcraft (2021), 'Afghanistan's Internet: who has control of what?', Netcraft blog, 30 August 2021, https://www.netcraft.com/blog/afghanistan.
48 Nikzad, K. (2019), '220 Telecom Towers Destroyed in Eight Months: ATRA', TOLO News, 26 November 2019, https://tolonews.com/afghanistan/220-telecom-towers-destroyed-eight-months-atra.
49 Cerulus (2021), 'Fears loom over Afghanistan's internet'.
50 However, there is a lack of publicly available information about the recoverability and rebuilding of telecommunications infrastructure following disruption or destruction.

in 2015, 'security issues' were the 'main obstacle' for completing the country's optical fibre network 'backbone ring' project, which aimed to bring broadband connection to provincial capitals.[51] The cases of two specific telecommunications companies – Roshan and MTN – demonstrate the challenges of building internet resilience in this context.

As of 2019, Roshan was one of Afghanistan's biggest employers.[52] Its GSM network reaches 91 per cent of Afghanistan's population, including remote rural areas.[53] Roshan's initial funding came from the Aga Khan Fund for Economic Development in 2003. Its mission to improve connectivity was motivated by both commercial incentives and philanthropic motivations. But from its launch, Roshan faced severe operational risks. For instance, Taliban forces targeted the company's cell towers (as well as those owned by other operators) from as early as 2008,[54] leading to significant costs incurred for repairing and replacing infrastructure.[55] Roshan's founder even claimed that competitors were paying protection money to avoid their towers being targeted, accusations that were denied by Afghan Wireless, Etisalat and Afghan Telecom.[56] In 2017, a deadly truck bombing took place directly outside Roshan's offices in Kabul, with at least 30 of its staff members reported to have been killed.[57] This bombing took place just months after one of the company's employees had been killed in another attack in Kabul.[58]

MTN Afghanistan, a subsidiary of the South African telecommunications company MTN, presents a different balance of incentives and interests. The company was formerly a major guarantor of mobile connectivity in Afghanistan, but in August 2020 MTN's leadership announced a planned exit from the Afghan market, citing reasons including 'tough macro conditions'[59] and the region's 'increasingly complex' situation.[60] MTN's rapid exit from the Afghan market – which concluded in November 2020, when Lebanon's M1 New Ventures bought its Afghan subsidiary

---

51 Ministry of Communications and Information Technology (2015), 'Presentation by MCIT on Fiber Connectivity in Afghanistan', https://www.unescap.org/sites/default/files/Presentation%20by%20MCIT%20On%20fiber%20connectivity%20in%20Afghanistan.pdf.
52 Weber, C. (2019), 'The extraordinary story of the only B Corp in Afghanistan', Quartz, 12 December 2019, https://qz.com/work/1765329/roshan-the-extraordinary-story-of-the-only-b-corp-in-afghanistan.
53 For further information about the company, see Roshan (undated), 'About Us', https://roshan.af/about-us (accessed 4 July 2024).
54 ITP Staff via Edge Middle East (2008), 'Roshan CEO says competitors are paying off the Taliban', 10 June 2008, https://www.edgemiddleeast.com/news/521702-roshan-ceo-says-competitors-are-paying-off-the-taliban.
55 Barton (2022), 'Afghanistan's telecom sector's progress threatened by return of Taliban regime'.
56 Boone, J. (2008), 'Telecom chief says rivals pay Taliban protection', *Financial Times*, 9 June 2008, https://www.ft.com/content/f9f8b610-363b-11dd-8bb8-0000779fd2ac. The *FT* article states that MTN was unavailable for comment.
57 Jhanmal, Z. (2017), 'Roshan Telecoms Suffers Enormous Loss in Truck Bombing', TOLO News, 5 June 2017, https://tolonews.com/business/roshan-telecoms-suffers-enormous-loss-truck-bombing.
58 Radio Free Europe/Radio Liberty (2017), 'Attack On Bus In Kabul Kills Employee Of Afghan Telecom Company', 14 March 2017, https://www.rferl.org/a/afghanistan-kabul-bombing-telecom-company/28368154.html.
59 Gilbert, P. (2022), 'MTN offered $35m for Afghanistan operation', *Connecting Africa*, 8 November 2022, https://www.connectingafrica.com/author.asp?section_id=761&doc_id=779636.
60 Barton, J. (2020), 'MTN lining up sales of Afghan, Syrian and Yemeni operations', Developing Telecoms, 20 August 2020, https://developingtelecoms.com/telecom-business/operator-news/9903-mtn-lining-up-sales-of-afghan-syrian-and-yemeni-operations.html.

for approximately $35 million[61] – may reflect the difficulties of balancing commercial incentives with on-the-ground barriers to operation (for example, navigating service provision in areas with an increasingly deteriorating security situation).

Overall, while Afghanistan's internet ecosystem certainly contained some of the building blocks for resilience (for instance, improved accessibility, national policy buy-in and mechanisms for enhancing technical and sociopolitical drivers of resilience), substantial barriers to the internet's continued availability for the majority of end users remained throughout the pre-crisis period, exacerbated by continual background or localized targeting of telecommunications and internet services.

Internet resilience during active crisis

According to one interviewee, the Taliban takeover '100 per cent' made Afghanistan's internet less resilient.[62] During this period, internet resilience in Afghanistan faced heightened (and, in some cases, unprecedented) threats on both the technical and sociopolitical levels, ranging from (continued) direct disruptions to internet infrastructure at multiple levels of the stack to the disruptions of policies, processes and responses in place to ensure the internet's continued operation and recoverability.

As noted above, telecommunications infrastructure was a long-standing target for Taliban attacks, resulting in severe service disruptions to end users as the country plunged into crisis. Often, targets appeared to be selected as measures to realize the group's strategic military objectives and support ongoing operations in targeted regions.[63] In early July 2021, Taliban fighters attacked optical fibre devices and systems equipment in the Herat province, leaving residents of Islam Qala without any internet connection. Then, on 9 July, Taliban fighters seized control of both Islam Qala and Torghundi.[64]

As the Taliban aimed to consolidate power in Kabul and the country's various regions, its members orchestrated internet shutdowns to quell resistance and dissent, thus posing a direct threat to connectivity and access. In September 2021, there were reports of a shutdown of internet and phone services provided by both

---

61 Barton, J. (2022), 'MTN exits Afghanistan with sale to M1', Developing Telecoms, 4 November 2022, https://developingtelecoms.com/telecom-business/operator-news/14180-mtn-exits-afghanistan-with-sale-to-m1.html. In June 2023, MTN and Afghan Wireless were reportedly selected by MCIT to provide telecommunication services to remote areas. MCIT (2023), 'The signing of a contract worth 365 Million Afghanis between the MCIT and telecommunication companies for providing telecommunication services to remote areas', MCIT press release, 5 June 2023, https://mcit.gov.af/en/signing-contract-worth-365-million-afghanis-between-mcit-and-telecommunication-companies-providing.
62 Research interview with a senior analyst at an open-source human rights monitoring project, May 2023.
63 For reporting on the Taliban's targeting of IT infrastructure, see Kumar, R. (2021), 'Taliban targeting Afghanistan's crucial power, IT infrastructure', Al Jazeera, 15 July 2021, https://www.aljazeera.com/news/2021/7/15/taliban-afghanistan-it-electricity-power.
64 BBC News (2021), 'Taliban capture key Afghanistan border crossings', 9 July 2021, https://www.bbc.co.uk/news/world-asia-57773120.

Roshan and Etisalat in the Panjshir valley, one of the last remaining strongholds of anti-Taliban resistance.[65] Also in September, in response to rising anti-Taliban protests, the group suspended internet access in Kabul.[66]

This example, among others, serves as a stark reminder of how the internet is controlled and weaponized in different ways in conflict – through physical destruction and disruption in some cases, and appropriation and shutdown in others.

While there is a lack of open-source reporting on the Taliban's takeover of MCIT and ATRA, it appears that high-level directives for partial or full internet outages in Kabul and elsewhere were ad-hoc decisions – perhaps new ministerial or extra-ministerial processes – setting a dangerous precedent for the weaponization of Afghanistan's internet infrastructure. A similar precedent was set higher up the stack, with the Taliban implementing a repressive content-moderation policy for news and media, such as the blocking of access to certain websites – according to their own estimate in August 2022, this included up to 23 million 'immoral' websites.[67]

The coexistence of the Taliban's dependence on a resilient internet and its actions to threaten it adds a layer of complication to the picture of deteriorated internet resilience in post-takeover Afghanistan.

However, Afghanistan's previous government did not necessarily have sufficient policies, processes and responses in place to ensure internet resilience and safeguard digital rights. As explained in the previous section, there were substantial pre-existing gaps. Nevertheless, the scale of the Taliban's abuse of the internet (ranging from disruptions of physical infrastructure to content moderation at the application layer) is a significant, and unprecedented, development.

While some of the Taliban's actions directly threatened internet resilience, others demonstrated the group's dependence on internet infrastructure to deliver on its propaganda objectives. This was a substantial step-change from the Taliban's reluctance to use digital technology during its first period of rule. In the lead-up to 15 August 2021, it was reported that the Taliban insurgents' 'smartphones proved just as handy as rifles'.[68] The group's access to and use of social media platforms played an important role in their takeover of power. These uses included amplifying mis- and disinformation (including premature declarations of military

65 BBC News (2021), 'Afghanistan: Fresh fighting in final anti-Taliban stronghold', 4 September 2021, https://www.bbc.co.uk/news/world-asia-58443679.
66 Tarabay, J. and Najafizada, E. (2022), 'Taliban Continues Censorship, Web Blocks As It Promises 4G', Bloomberg, 31 August 2022, https://www.bloomberg.com/news/newsletters/2022-08-31/taliban-continues-censorship-web-blocks-as-it-promises-4g.
67 Ibid; Shahir, T. (2022), 'Over 23 Million 'Immoral' Websites Blocked in Afghanistan: Minister', TOLO News, 25 August 2022, https://tolonews.com/index.php/afghanistan-179554.
68 Brooking, E. T. (2021), 'Before the Taliban took Afghanistan, it took the internet', Atlantic Council blog, 26 August 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/before-the-taliban-took-afghanistan-it-took-the-internet.

victory)[69] on X (formerly known as Twitter)[70] and using WhatsApp for official communications. The coexistence of the Taliban's dependence on a resilient internet and access to platforms, and its actions to threaten it, adds a layer of complication to the picture of deteriorated internet resilience in post-takeover Afghanistan.

Additionally, the instability of the crisis environment itself may have provided an opening for other actors to advance threats to resilience and impeded the capacity of targeted systems and organizations to recover. For instance, Insikt Group reports that a Chinese state-sponsored advanced persistent threat (APT) targeted telecommunications provider Roshan in 2020 and 2021. Insikt claimed that the APT was used for intelligence-gathering operations,[71] perhaps driven by China's strategic interest in expanding its influence in a future Taliban-led Afghanistan.

Internet resilience post-crisis

After consolidating power, the Taliban government has taken steps to rebuild internet resilience to serve strategic ends, including domestic content control. Former ATRA chairman Mohammad Najeeb Azizi noted that the Taliban 'is eager to use the internet in their own favour'.[72] In October 2021, the new ATRA leadership announced that telecommunication services had returned to pre-crisis levels,[73] although there is a lack of public reporting on the repair of damaged internet infrastructure. In August 2022, acting MCIT head Najibullah Haqqani outlined aspirations to secure 4G coverage for the country.[74]

The Taliban has also announced a set of policies and initiatives for the use of the internet and technology for governance and public administration. Despite US sanctions and constant action from Meta to close known Taliban accounts, WhatsApp is still the preferred mode of official communication for the new regime.[75] The 'delicate dance'[76] between the Taliban government and social media platforms like WhatsApp presents a unique challenge, as instead of simply blocking all access to social media, the Taliban are trying to use it to their advantage – whether for public administration and official communiques or seeking to spread and control narratives. One local government spokesperson noted that 'if there were no WhatsApp, all our administrative and non-administrative work would be paralyzed'.[77]

---

69 Ibid.
70 DFRLab via Medium (2021), 'As the Taliban offensive gained momentum, so did its Twitter propaganda campaign', 20 August 2021, https://medium.com/dfrlab/as-the-taliban-offensive-gained-momentum-so-did-its-twitter-propaganda-campaign-75021ba3082.
71 Insikt Group (2021), '4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan', Recorded Future blog, 28 September 2021, https://www.recordedfuture.com/chinese-apt-groups-target-afghan-telecommunications-firm.
72 Cerulus (2021), 'Fears loom over Afghanistan's internet'.
73 Moss, S. (2021), 'Afghanistan claims telecoms sites are fully operational following Taliban takeover', Data Center Dynamics, 20 October 2021, https://www.datacenterdynamics.com/en/news/afghanistan-claims-telecoms-sites-are-fully-operational-following-taliban-takeover.
74 Tarabay and Najafizada (2022), 'Taliban Continues Censorship, Web Blocks As It Promises 4G'.
75 Goldbaum, C. and Padshah, S. (2023), 'Taliban Rely on WhatsApp, but Keep Getting Kicked Off', *New York Times*, 17 June 2023, https://www.nytimes.com/2023/06/17/world/asia/taliban-whatsapp-afghanistan.html.
76 Ibid.
77 Shead, S. (2021), 'Facebook, TikTok won't lift ban on posts that promote Taliban after the fall of Afghanistan', CNBC, 17 August 2023, https://www.cnbc.com/2021/08/17/taliban-content-banned-on-facebook-instagram-whatsapp.html.

In the post-crisis period, however, the state of Afghanistan's internet has been defined both by long-standing barriers to availability, connectivity and recoverability, and by new challenges. According to one interviewee, the resumption of internet services after the takeover was 'particularly slow'.[78] Open access data suggest that internet penetration and usage rates in Afghanistan have remained relatively unchanged since 2021.[79] This is despite the Taliban raising taxes on internet and mobile phone operators during that time, in addition to ordering those companies to decrease prices for end users.[80]

The case of Afghanistan's internet exchange point (IXP)[81] and the .af domain name – which (to date) remains operational – provides some insight into the new regime's continued reliance on international mechanisms and processes to ensure technical resilience. The US-based Packet Clearing House (PCH) is a non-profit, intergovernmental treaty organization that provides operational support to internet infrastructure, namely through technological support to IXPs and the core of the DNS. Since July 2018, PCH has served the National Internet Exchange of Afghanistan (NIXA) in Kabul and reportedly continues to provide support.[82] Similarly, Gransy, a Czechia-based registrar and registry services provider, also provides Anycast, which the .af country code top-level domain (ccTLD) reportedly relies on. During the Taliban takeover, in response to 'political questions' about the future of the .af ccTLD, Gransy emphasized its political neutrality and 'social responsibility' as part of its daily work, stating that any change to the ccTLD operator 'is not our decision', and is instead defined by strict guidelines set by ICANN and the Internet Assigned Numbers Authority (IANA) function.[83]

At the telecommunications level, Voice of America (VoA) reported in February 2023 that Etisalat was among the carriers affected by Taliban orders to block access to certain websites. VoA claimed that the Afghan Media Violation Commission had not received any order to restrict access,[84] which might imply that other parts of the Taliban government had acted unilaterally.

In 2023, meanwhile, media reports suggested that Huawei had reached a 'verbal agreement' with the Taliban to install surveillance systems across Afghanistan,[85] although comprehensive, sophisticated surveillance systems are likely

---

78 Research interview with a programme manager and a senior analyst at an open-source human rights monitoring project, May 2023.
79 Kemp, S. (2023), 'Digital 2023: Afghanistan', Data Reportal, 13 February 2023, https://datareportal.com/reports/digital-2023-afghanistan.
80 Tarabay and Najafizada (2022), 'Taliban Continues Censorship, Web Blocks As It Promises 4G'.
81 An IXP is a location where ISPs can connect their networks to other ISPs. This is essential for the exchange of internet traffic.
82 Afghanistan Ministry of Communications and Information Technology (undated), 'NIXA (National Internet Exchange Of Afghanistan)', https://mcit.gov.af/en/nixa-national-internet-exchange-afghanistan-8; Packet Clearing House (undated), 'Internet Exchange Directory', https://www.pch.net/ixp/dir.
83 Stojičević, D. (2021), 'Gransy and Afghanistan's .af Top Level Domain – political questions to apolitical organization', Gransy blog, 30 August 2021, https://gransy.blog/gransy-and-afghanistans-af-top-level-domain-political-questions-to-apolitical-organization.
84 Voice of America News (2023), 'Access to Some News Websites Restricted in Afghanistan', 9 February 2023, https://www.voanews.com/a/access-to-some-news-websites-restricted-in-afghanistan-/6955980.html.
85 Tarabay, J. and Najafizada, E. (2023), 'Taliban Says Huawei to Install Cameras to Locate Militants', Bloomberg, 25 August 2023, https://www.bloomberg.com/news/articles/2023-08-25/taliban-says-huawei-to-install-cameras-to-locate-militants; Yawar, M. Y. and Greenfield, C. (2023), 'Taliban weighs using US mass surveillance plan, met with China's Huawei', Reuters, 25 September 2023, https://www.reuters.com/world/taliban-weighs-using-us-mass-surveillance-plan-met-with-chinas-huawei-2023-09-25. The authors contacted Huawei for comment on 18 April 2024; at the time of publication, Huawei had yet to respond.

out of reach.[86] Several civil society organizations have voiced concerns about the misuse of biometric and digital ID data for the surveillance and targeting of human rights defenders, dissidents, journalists, activists and other Taliban opponents.[87]

Interviewees for this paper underlined the physical dimension of threats to resilience in post-crisis Afghanistan. While the new regime is taking steps to sharpen technical and regulatory measures to control the internet, personal devices are also just arbitrarily 'seized' at checkpoints, while individuals are subject to police 'swiping through [their] apps'.[88] As the Taliban takeover became an inevitability in 2021, many human rights defenders, activists and others took steps to bolster their online safety from emerging threats, including measures like deleting their search history and minimizing their online presence.[89] In post-takeover Afghanistan, the threat of punitive measures may discourage end users from internet usage and pushes them towards self-censorship. In other words, even when there is no direct technical barrier to internet availability at the application layer, sociopolitical barriers manifest in the actual and perceived safety risks to the end user.

Overall, the state of internet resilience in post-crisis Afghanistan is opaque and evolving. A new network of interests, incentives and actors has emerged since the Taliban takeover, each exerting some impact on resilience. The Taliban both amplifies threats to resilience (i.e. through institutionalizing repressive measures and limiting accessibility) and pioneers or supports technical efforts to secure resilience (i.e. through the development of 4G network infrastructure). Several pertinent questions remain, which may present avenues for further research: namely, investigating the Taliban's strategic motivations in both actively disrupting (or, in some cases, preventing via physical destruction) access to networks in some cases and enabling it in others.

The role of private sector actors is equally nuanced. Many played a proactive role in internet infrastructural development and improving connectivity in Afghanistan pre-2021, despite facing barriers and direct risks to their operations. These challenges were exacerbated and amplified during active conflict. In post-crisis Afghanistan, private sector stakeholders have carved out new roles (e.g. through blocking the Taliban's use of platforms, as in the case of WhatsApp), pursued new opportunities (e.g. the successful bid of two telecommunications companies to roll out 4G nationwide),[90] and continued to provide services despite new barriers to operations (e.g. due to new content moderation requirements imposed by the Taliban).

---

86 Cerulus (2021), 'Fears loom over Afghanistan's internet'.
87 Access Now (2021), 'Civil society calls on international actors in Afghanistan to secure digital identity and biometric data immediately', open letter, 25 August 2021, https://www.accessnow.org/wp-content/uploads/2021/09/Civil_Society_Afghanistan_Biometrics_Open_Statement.pdf.
88 Research interview with a programme manager and a senior analyst at an open-source human rights monitoring project, May 2023.
89 Access Now (2021), 'Online safety resources for Afghanistan's human rights defenders', 17 August 2021, https://www.accessnow.org/online-safety-resources-afghanistan.
90 MCIT (2023), 'The signing of a contract worth 365 Million Afghanis between the MCIT and telecommunication companies for providing telecommunication services to remote areas', https://mcit.gov.af/en/signing-contract-worth-365-million-afghanis-between-mcit-and-telecommunication-companies-providing.

04
Internet resilience in Ukraine

A combined resilience frame – considering both technical and sociopolitical internet resilience – highlights underappreciated aspects of Russia's war on Ukraine.

Russia's war on Ukraine has occupied far more global media and policy attention than Afghanistan, at least since the withdrawal of US troops from the latter – with two consequences for this research paper. First, attendees at the Chatham House event and subsequent interviewees spoke far more about Ukraine than Afghanistan or any other conflict, demonstrating Ukraine's presence on the top tier of cyber policy issues. Second, far more research and analysis is available in the public domain on Ukraine than Afghanistan, including high-profile incidents relating to cyber resilience. For these reasons, this chapter is organized differently to that on Afghanistan.

The section on global resilience focuses largely on the impact of international actors on the Russian internet, while the section on local resilience examines the impact of Russia's invasion on Ukrainian networks and people. It is crucial to underline the fact that any impact on Russian networks ultimately stems from the invasion itself, and that the devastation experienced by Ukraine is much greater than the limited impact on internet connectivity in Russia – which was already constrained by repressive domestic internet policies.

This chapter draws on interviews throughout to examine how a combined resilience frame helps to highlight underappreciated aspects of Russia's war on Ukraine, especially from the point of view of private sector actors, whose roles and responsibilities shift, disrupt and change.

Ukraine's internet resilience pre-war

Prior to 2022, Ukraine had developed a large technology sector, with close links to both Russia and Europe. Many US and European companies outsourced IT services to Ukraine, and Ukraine enjoyed a high level of technical and computer engineering education among young graduates. Ukraine also had an unusually complex and decentralized internet architecture, with a relatively high number of autonomous systems – which are the building blocks of the global internet – to population size compared to Western Europe. Frédérick Douzet et al. trace this structure to the uncoordinated development of the internet in the former Soviet states, where many small ISPs emerged independently, as opposed to the more centralized pattern common in Western European countries that results from internet adoption by national telecoms companies.[91] A high number of autonomous systems is usually associated with increased resilience, as failure in one lessens the impact on others. However, given that many of the autonomous systems in Ukraine only serve small, separate regions, this conclusion is less warranted. Failure of those systems would still result in an internet outage, but in a smaller geographical area.

The 2014 occupation reshaped Ukraine's internet connectivity, with Russia building two new cables to Crimea in an attempt to integrate that territory firmly into its national networks.

Russia's full-scale invasion of Ukraine in February 2022 was preceded by eight years of partial occupation from 2014. In that year, Russia annexed Crimea and engaged in a relatively low-intensity conflict in the eastern Donbas region, which then became partly occupied by separatists and covert Russian troops. The annexation of Crimea and conflict in Donbas are crucial to understanding the lead-up to, and outcome of, the 2022 invasion.

The 2014 annexation and separatist seizure of territory were also decisive for Ukraine's internet connectivity. Prior to 2014, Ukrainian internet connections were broadly split between Russia and Europe, with traffic in both directions approximately equal. But Douzet et al. show that the 2014 occupation reshaped Ukraine's internet connectivity, with Russia building two new cables to Crimea in an attempt to integrate that territory firmly into its national networks.[92] Local ISPs were re-registered as Russian, while the Russian national telecoms company Rostelcom made a major investment in a local branch to expand connectivity.[93] Conversely, Ukraine placed sanctions on those ISPs that continued to supply Crimea, leading to further divergence. Similar effects occurred in Donbas, although the

91 Douzet, F. et al. (2020), 'Measuring the Fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis', in Jančárková, T. et al. (eds) (2020), *20/20 Vision: The Next Decade – the 2020 12th International Conference on Cyber Conflict*, Tallinn: NATO CCDCOE.
92 Ibid.
93 Fontugne, R., Ermoshina, K. and Aben, E. (2020), 'The Internet in Crimea: a Case Study on Routing Interregnum', 2020 IFIP Networking Conference, June 2020, Paris, France, https://hal.science/hal-03100247/document.

divergence was less pronounced. Local ISPs deepened their Russian connections and reduced their Ukrainian ones, amid pressure from both sides. A trace-route test conducted by Douzet et al. identified a packet travelling from Dnipro in eastern Ukraine to Moscow via Germany, Poland and Belarus, rather than directly across the Ukraine–Russia border.[94]

This separation has important implications for internet resilience, as the number of routes available to internet packets increases the ability for communications to continue in case of disruption. But conversely, the length of the route taken by packets also increases the likelihood of disruption, as well as latency and consequent economic cost. In both cases, decisions are made by private sector actors such as ISPs responding to government regulation or intervention, as well as geopolitical factors and ideological leanings. These decisions are then actioned through commercial agreements in technical routing protocols, as well as being enforced by changes in the physical infrastructure available to specific regions. In this way, the 2014 occupation of Crimea and Donbas not only foreshadowed a much larger rerouting of internet traffic after February 2022, but highlighted the complexity of factors that feed into private sector decisions on where and how to provide internet access. Private sector actors are far from purely commercial entities, as they need to respond to, and integrate, geopolitical and personal relationships into strategies for infrastructure provision.

The war and global internet resilience

In February 2022, immediately after the full-scale Russian invasion, the Ukrainian deputy prime minister asked ICANN to revoke the security certificates of Russian top-level domains such as .ru, and to shut down two DNS servers in Moscow and St Petersburg.[95] This request also involved asking the European internet registry (RIPE NCC), which allocates IP address space, to withdraw IP address rights from Russian internet registries and to block any DNS servers operated by those registries. This request would have effectively prevented Russian internet users from accessing the global internet, creating a precedent of politically motivated decisions on country-level internet access by the multi-stakeholder internet governance community. It would thereby have contributed to already growing fears of internet fragmentation, and suspicion of bias inherent in multi-stakeholder processes.

However, ICANN resisted the Ukrainian request on these grounds, drawing on both technical and sociopolitical arguments in support of the organization's pivotal role in upholding a global, resilient internet. ICANN's response noted the distributed technical characteristics of internet security, including the production of security certificates by third parties.[96] Observers also questioned the feasibility of 'revoking' Russian TLDs (i.e. removing them from the DNS master root zone

---

94 Douzet et al. (2020), 'Measuring the Fragmentation'. For further reading, see also Limonier, K. et al. (2021), 'Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine', *First Monday*, 26(5), https://dx.doi.org/10.5210/fm.v26i5.11700.
95 Ministry of Digital Transformation of Ukraine and Mykhailo Fedorov (2022), *Letter to Goran Marby, President and CEO, ICANN*, 28 February 2022, https://eump.org/media/2022/Goran-Marby.pdf.
96 Brodkin, J. (2022), 'ICANN won't revoke Russian Internet domains, says effect would be "devastating"', Ars Technica, 4 March 2022, https://arstechnica.com/tech-policy/2022/03/icann-wont-revoke-russian-internet-domains-says-effect-would-be-devastating.

file), arguing that this measure would not in fact cut Russia off from the global internet as intended. Rather, its effect on which paths Russian traffic took, and how, were unpredictable.[97] Such unpredictability arises because managers of a DNS resolver[98] can independently configure their servers to direct traffic for particular domains (such as .ru) to other 'authoritative' servers, rather than to the root.[99] ICANN's response to Ukraine's request – along with that of many of Ukraine's supporters[100] – also cited the importance of neutrality to the multi-stakeholder model of internet governance.

This was not the first time that ICANN had become entangled in Russia's war on Ukraine. ICANN's role as allocator of time zones for many software applications meant that its decision to locate Crimea in the Russian time zone after 2014, when Russia switched Crimea to Russian time, attracted some criticism.[101] Some US registrars reportedly prevented Crimean registrants from accessing US domains.[102] More generally, Russia does not recognize ICANN's domain name dispute procedures,[103] and has repeatedly sought to transfer ICANN's responsibilities to the International Telecommunication Union (ITU) – most notably at the World Summit on the Information Society Forum in Dubai in 2012. This confrontation continued after the 2022 invasion of Ukraine, as Russia was unable to appoint preferred candidates to key ITU positions, including that of secretary-general,

---

97 Bortzmeyer, S. (2022), 'Internet Network Shutdowns in Russia', RIPE Labs (blog), 9 March 2022, https://labs.ripe.net/author/stephane_bortzmeyer/internet-network-shutdowns-in-russia.
98 An online server that converts domain names into IP addresses.
99 Ibid.
100 Article 19 (2022), 'ICANN: Human rights law calls for an open Internet at a time of war', 4 March 2022, https://www.article19.org/resources/icann-human-rights-law-calls-for-an-open-internet-at-a-time-of-war; Campbell, N. and Gahnberg, C. (2022), *Internet Impact Brief: Impact of Ukraine's Requests to Block Russia's Access to the Internet*, Internet Society, https://www.internetsociety.org/resources/2022/impact-of-ukraines-requests-to-block-russias-access-to-the-internet.
101 Murphy, K. (2019), 'What time is it? For ICANN, even that can be a controversial question', Domain Incite (blog), 21 June 2019, https://domainincite.com/24428-what-time-is-it-for-icann-even-that-can-be-a-controversial-question. The administrator argued that 'when people use time-zone data, they typically want to know the facts on the ground even when these are not the facts as they ought to be.' See Eggert, P. (2018), 'Error in the Time Zone Database', ICANN Pipermail mailing list, 6 December 2018, https://mm.icann.org/pipermail/tz/2018-December/027304.html.
102 Badii, F. (2017), 'ICANN's jurisdiction: sanctions and domain names', GT School of Public Policy Internet Governance Project (blog), 13 January 2017, https://www.internetgovernance.org/2017/01/13/icanns-jurisdiction-sanctions-and-domain-names. For information on the 2014 sanctions, see Office of Foreign Assets Control, 'Sanctions Programs and Country Information', https://ofac.treasury.gov/sanctions-programs-and-country-information. For the impact of the sanctions, see: Interfax-Ukraine (2015), 'Domain name registrar Go Daddy ceases Crimean operations over sanctions', *Kyiv Post*, 30 January 2015, https://archive.kyivpost.com/article/content/war-against-ukraine/domain-name-registrar-go-daddy-ceases-crimean-operations-over-sanctions-378926.html. Following some pressure (including from NGOs) the US government granted an exemption: see Access Now, Electronic Frontiers Foundation, Global Voices Advocacy, New America's Open Technology Institute, Cutler, S. and Ferrari, E. C. (2015), *Letter to OFAC on Crimea and Personal Communications*, 12 February 2015, https://www.accessnow.org/wp-content/uploads/archive/LettertoOFAConCrimeaandPersonalCommunications.pdf; Federal Register (2015), 'Russian Sanctions: Revisions and Clarifications for Licensing Policy for the Crimea Region of Ukraine' (Final Rule), Bureau of Industry and Security, Commerce, 22 May 2015, https://www.federalregister.gov/documents/2015/05/22/2015-12267/russian-sanctions-revisions-and-clarifications-for-licensing-policy-for-the-crimea-region-of-ukraine. For further reading and a perspective from an internet services company about the difficulties of sanctioning internet services and infrastructure, see, Klick, L. (2022), 'The challenges of sanctioning the Internet', Cloudflare blog, 12 December 2022, https://blog.cloudflare.com/the-challenges-of-sanctioning-the-internet.
103 Goryachev, I. and Medvedev, S. (2022), 'At a glance: transferring or cancelling a domain in Russia', Lexology, 18 March 2022, https://www.lexology.com/library/detail.aspx?g=7f28fa74-4170-4888-b86a-5e86175b6166.

owing to opposition from various parties including ICANN.[104] Following these controversies, and ICANN donations to Ukraine, Russia stopped its nominal payment to ICANN's budget in October 2023.[105]

ICANN's decision to refuse the Ukrainian request regarding Russian domains must be seen in the light of this longer history of Russian unease at its role. ICANN was already sensitive to accusations of pro-Western and pro-Ukrainian bias. Technical inaccuracies in the Ukrainian request were therefore useful in ICANN's attempt to establish a principled stance in favour of neutrality. ICANN also included malicious domain-monitoring services across multiple languages – including Russian – at the same time, to reinforce its position.[106] Ultimately in this case, the desire for ICANN to uphold not just neutrality but global internet resilience outweighed the pressure to act in ways that could undermine global resilience. It is worth noting that ICANN's decision did not receive strong public criticism from the Ukrainian government. This reticence on Ukraine's part perhaps points to acceptance of the technical infeasibility of parts of its request, and potentially even to the desire among Ukraine's allies to uphold the norm of a global, resilient internet.

The desire for ICANN to uphold not just neutrality but global internet resilience outweighed the pressure to act in ways that could undermine global resilience.

Even so, the multi-stakeholder nature of internet architecture meant that other parties were able to take independent action. Russia had already taken preventative actions to avoid foreign web-hosting services and use DNS servers located in Russia, in anticipation of requests such as that from the Ukrainian government.[107] These actions were also part of a broader ongoing attempt to increase the Russian government's ability to control and redirect domestic internet traffic.[108] Despite ICANN's dismissal of Ukraine's request to revoke security certificates, in March 2022, Russia created a domestic certificate authority, which from its perspective, confers several advantages such as developing a government-controlled means to create certificates that then could be used either legitimately or maliciously

---

104 Ling, J. (2022), 'The election that saved the internet from Russia and China', Wired, 30 October 2022, https://www.wired.co.uk/article/itu-2022-vote-russia-china-open-internet; Murphy, K. (2022), 'ICANN to "stand up" to Russia at the ITU', Domain Incite, 20 September 2022, https://domainincite.com/28260-icann-to-stand-up-to-russia-at-the-itu.
105 Murphy, K. (2022), 'Russia cuts off ICANN funding after pro-Ukraine stance', Domain Incite, 4 October 2022, https://domainincite.com/29107-russia-cuts-off-icann-funding-after-pro-ukraine-stance.
106 ICANN (2022), 'ICANN Expands DNSTICR to Monitor Terms Related to Russia-Ukraine War', press release, 9 March 2022, https://www.icann.org/en/announcements/details/icann-expands-dnsticr-to-monitor-terms-related-to-russia-ukraine-war-09-03-2022-en.
107 DigWatch (2022), 'Russian government instructs state-owned websites and services to switch to Russian DNS servers', *DigWatch Geneva Internet Platform*, 6 March 2022, https://dig.watch/updates/russian-government-instructs-state-owned-websites-and-services-to-switch-to-russian-dns-servers.
108 Meinel, C. and Hagebölling, D. (2023), 'Russia's War Against Ukraine is Catalyzing Internet Fragmentation', Council on Foreign Relations Net Politics, 13 March 2023, https://www.cfr.org/blog/russias-war-against-ukraine-catalyzing-internet-fragmentation.

and to avoid action by others to prevent certificate use.[109] But in terms of Russian internet resilience, this development is double-edged: on one hand, it reduces Russia's dependence on foreign companies. But on the other, it creates a point of failure (and therefore a clear target) in Russia's domestic internet ecosystem.

In response to the 2022 invasion, US internet provider Cogent unilaterally decided to terminate service to Russian ISPs.[110] Lumen, the top transit provider for Russia, partially disconnected shortly afterwards.[111] As one interviewee noted: '[T]here's a real conflict for back-bone internet providers. I do believe that a lot of these companies genuinely believe in the provision of free, open, interoperable internet as a benchmark principle.'[112] But the desire and pressure to counter the Russian invasion was similarly strong – as were security and personnel concerns. Nevertheless, the Internet Society assessed that actions to deny service to Russian ISPs reduced the overall resilience of the global internet.[113]

Finally, a separate risk comes from unintentional disruption or intentional sabotage of undersea communications cables.[114] In October 2023, two cables connecting Estonia, Finland and Sweden were damaged, with initial attribution by these states focusing on a Hong-Kong registered ship operated by a Russian company that was located above the two cables when they were cut, along with a Russian state-owned cargo ship.[115] It is unclear whether the damage was deliberate or accidental – although former Russian president Dimitry Medvedev had hinted at the possibility of deliberate sabotage of undersea internet cables in June 2023.[116] Other observers have speculated that damage to cables next to the Shetland Islands in October 2022 could also have been due to Russian activity.[117]

---

109 Fadilpašić, S. (2022), 'Russia creates its own TLS certificate authority to bypass sanctions', TechRadar, 11 March 2022, https://www.techradar.com/news/russia-creates-its-own-tls-certificate-authority-to-bypass-sanctions. Another contributing factor could have been the decision from multiple companies to withdraw their antivirus and website certification services from Russia. See Brewster, T. (2022), 'Big Web Security Firms Ditch Russia, Leaving Internet Users Open To More Kremlin Snooping', Forbes, 11 March 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/11/russians-exposed-to-more-surveillance-and-cybercrime-as-web-security-giants-leave-over-ukraine-invasion.

110 DigWatch (2022), 'Major Internet bandwidth provider terminated services to Russia', *DigWatch Geneva Internet Platform*, 5 March 2022, https://dig.watch/updates/major-internet-bandwidth-provider-terminated-services-to-russia.

111 Moss, S. (2022), 'Telco Lumen disconnects from Russia, ends business relationships', *Data Center Dynamics*, 8 March 2022, https://www.datacenterdynamics.com/en/news/telco-lumen-partially-disconnects-from-russia-ends-business-relationships.

112 Research interview with an academic researcher, May 2023

113 Campbell, N. and Gahnberg, C. (2022), *Internet Impact Brief: How Refusing Russian Networks Will Impact the Internet*, briefing, Internet Society, https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-how-refusing-russian-networks-will-impact-the-internet.

114 Kavanaugh, C. (2023), *Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour*, Geneva: UN Institute for Disarmament Research, https://unidir.org/publication/wading-murky-waters-subsea-communications-cables-and-responsible-state-behaviour.

115 Page, M. (2023), 'Russia, a Chinese cargo ship and the sabotage of subsea cables in the Baltic Sea', Australian Strategic Policy Institute The Strategist blog, 31 October 2023, https://www.aspistrategist.org.au/russia-a-chinese-cargo-ship-and-the-sabotage-of-subsea-cables-in-the-baltic-sea; Braw, E. (2023), 'A Pipeline Mystery Has a $53 Million Solution', *Foreign Policy*, 6 November 2023, https://foreignpolicy.com/2023/11/06/finland-pipeline-sabotage-balticconnector-china-russia; Staalesen, A. (2023), 'Runaway ship Newnew Polar Bear, suspected of sabotage in Baltic Sea, is sailing into Russian Arctic waters', The Barents Observer, 26 October 2023, https://thebarentsobserver.com/en/security/2023/10/runaway-ship-newnew-polar-bear-suspected-sabotage-baltic-sea-sailing-russian-arctic.

116 Faulconbridge, G. (2023), 'Russia now has free hand to destroy undersea communications cables, Putin ally says', Reuters, 14 June 2023, https://www.reuters.com/world/europe/russias-medvedev-says-moscow-now-has-free-hand-destroy-enemies-undersea-2023-06-14.

117 Stringer, E. (2022), 'Putin knows that undersea cables are the west's Achilles heel', *Financial Times*, 4 November 2022, https://www.ft.com/content/0ddc5b48-b255-401b-8e9f-8660f4eab37b.

These incidents highlight the potential for Russia's war on Ukraine to impact global internet connections beyond governance and protocol-level decisions. Technical internet resilience is at risk during conflict at the physical layer of international cable traffic, because removing or disrupting subsea cables (especially when co-located) increase traffic through other suboceanic or subsea cables, increasing the likelihood of outages and making them harder to repair.

Local internet resilience since February 2022

The main cause of internet disruption in Ukraine since February 2022 has been Russian military action, including air strikes, drone strikes and artillery. These attacks have destroyed towns and cities across Ukraine and killed thousands of people. In some cases, destruction to telecoms infrastructure was the primary aim of Russian attacks, rather than a side effect – and telecoms infrastructure has also been targeted by Russian cyberattacks.[118] The EU estimated that, by July 2022, 20 per cent of Ukraine's telecoms infrastructure had been destroyed, rising to 25 per cent in August 2023,[119] with the World Bank estimating the total cost of damage by February 2023 at $1.6 billion.[120]

The 2022 invasion also changed Ukraine's local internet architecture through less violent physical and logical reconstitution. In April and May 2022, the subsidiary of Rostelcom providing internet services to Crimea also began to receive traffic from local telecoms providers in Kherson, which had recently suffered an internet outage. Ukrainian officials argued that this was due to the disconnection and reconnection of fibre-optic cables, and independent analysis suggests this continued into 2023 for some Kherson-based ISPs.[121] Separate investigations highlighted the increased route length for packets travelling from Kyiv to Kherson and Donbas, aligning with the findings pre-2022 discussed earlier – and likely in order to direct traffic through Russian territory to enable surveillance.[122] Similarly, Kyiv-based servers were able to connect to Russian servers, but only for transit, not as a packet destination.[123] More broadly, Ukraine-wide data indicate that many Ukrainian autonomous systems stopped functioning after the onset

---

118 Antoniuk, D. (2023), 'Russia's Sandworm hacking unit targets Ukrainian telecom providers', The Record, 17 October 2023, https://therecord.media/russia-sandworm-hacking-ukraine-telecom-internet-providers; Bing, C. and Satter, R. (2022), 'Ukrainian telecom company's internet service disrupted by 'powerful' cyberattack', Reuters, 28 March 2022, https://www.reuters.com/business/media-telecom/ukrainian-telecom-companys-internet-service-disrupted-by-powerful-cyberattack-2022-03-28.
119 Pollet, M. (2023), 'Ukraine walks telecoms tightrope between China and the West', Politico, 29 August 2023, https://www.politico.eu/article/ukraine-reconstruction-digital-infrastructure-contemplate-ban-china-suppliers-telecom.
120 World Bank, Government of Ukraine, European Union and United Nations (2023), *Ukraine Rapid Damage and Needs Assessment, February 2022-February 2023*, report, Washington, DC: World Bank Group, https://documents.worldbank.org/curated/en/099184503212328877/P1801740d1177f03c0ab180057556615497; International Telecommunications Union (2022), *Interim assessment on damages to telecommunications infrastructure and resilience of the ICT ecosystem in Ukraine*, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2022/Interim%20report_Ukraine/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf.
121 Tomé, J., Belson, D. and Berdan, K. (2023), 'One year of war in Ukraine: Internet trends, attacks, and resilience', Cloudflare blog, 23 February 2023, https://blog.cloudflare.com/one-year-of-war-in-ukraine.
122 Madory, D. (2023), 'Ukraine's wartime internet from the inside', Kentik, 11 April 2023, https://www.kentik.com/blog/ukraines-wartime-internet-from-the-inside.
123 Ibid.

of conflict,[124] indicating an overall drop in internet connectivity across the country. Some areas under heavy bombardment from Russian forces – such as Mariupol – either disappeared altogether or reduced their footprint significantly.[125] Importantly, disruptions to internet connectivity connected to the war are nearly all inflicted on Ukraine by Russia, with only isolated incidents of Ukrainian cyber militias like the IT Army conducting DDOS operations on ISPs in occupied regions.[126] Such logical rerouting and connectivity disruptions enable the Russian military to weaponize the control of internet traffic patterns to aid their war aims of population surveillance and information control.

On one hand, greater connectivity restores meaningful use to local populations. On the other hand, internet connectivity is now a crucial element of state sovereignty.

It is worth highlighting the contradictory elements of sociopolitical internet resilience involved in the rerouting of internet traffic through and around Ukraine during the conflict. On one hand, greater connectivity restores meaningful use to local populations: the owner of a Kherson telecom provider who switched to Russian-controlled connections justified that decision as a way to get individual end users back online.[127] On the other hand, internet connectivity is now a crucial element of state sovereignty. Controlling the information space in addition to physical internet infrastructure gives a state the powers of surveillance and censorship, ensuring that connected populations are exposed to the state's choice of media and information, and that information extracted from communications networks can be used for that state's advantage.[128] Reports have emerged of people in occupied towns receiving blank SIM cards to connect to Russian telecoms networks – thereby restoring their online presence, but at the cost of increased surveillance and censorship.[129] Finally, in some cases, disconnection itself may have been intended an act of resilience. One analysis speculated

---

124 Trusin, C., Bertholdo, L. and Santanna, J. J. (2022), 'The Effect of the Russian-Ukrainian Conflict from the Perspective of Internet eXchanges', paper presented at the 18th International Conference on Network and Service Management, 2 December 2022, https://ieeexplore.ieee.org/document/9964765.
125 Siddiqui, A. (2023), 'Ukraine War: How has the Internet Changed in Ukraine 12 Months on', Internet Society Pulse, 23 February 2023, https://pulse.internetsociety.org/blog/ukraine-war-how-has-the-internet-changed-in-ukraine-12-months-on. As one interviewee explained, in Malitopol, ' … people filmed things, then physically passed to a person… when you don't have connectivity you essentially go back in time'. Research interviewee with an academic researcher, May 2023.
126 Paganini, P. (2023), 'IT Army of Ukraine disrupted Internet providers in territories occupied by Russia', Security Affairs, 29 October 2023, https://securityaffairs.com/153192/hacktivism/it-army-of-ukraine-hit-russia-isp.html.
127 Burgess, M. (2022), 'Russia is taking over Ukraine's Internet', Wired, 15 June 2022, https://www.wired.com/story/ukraine-russia-internet-takeover.
128 Horbyk, R. (2022), '"The war phone": mobile communication on the frontline in Eastern Ukraine', *Digital War*, 3, pp. 9–24, https://doi.org/10.1057/s42984-022-00049-2.
129 Burgess (2022), 'Russia is taking over Ukraine's Internet'. In addition, as one interviewee for this paper noted, there is a crucial 'physical side' to resilience: '… pulling people aside, demanding access to the device, swiping through people's apps. Real-world human impact, implications for self-censorship, freedom of communications, political expression, etc. Let's not just focus on the technical side.' Research interview with a programme manager at an open-source human rights monitoring project, May 2023.

that data indicating the severing of connections between Donbas and Russia may have been a way to reduce the likelihood of hostile cyber operations being conducted from Russia.[130]

Disconnection and surveillance extends to the media sphere, too. Reporters Without Borders also reports that the Kremlin seeks to extend 'systematic control… over Ukrainian media in the illegally annexed territories', noting the closure of independent media outlets ('only media that toe the Kremlin line can operate in the occupied territories') and disappearance and arrests of independent journalists.[131] For people living in the occupied territories, accessing Ukrainian media sources is both a technical challenge and comes at great personal risk.

Setting aside the long-term cost of reconstruction,[132] Russia's bombardment of Ukraine created an immediate need for physical repairs to cables, data centres and telecoms towers. As a result, the three Ukrainian mobile companies were forced to set aside their usual commercial rivalry to share infrastructure and permit individuals to move between networks easily,[133] as well as repurposing other parts of the radio spectrum for increased resilience (a technique also adopted by militaries to avoid jamming of frequencies by opponents).[134] While repair teams are usually made up of employed or contracted engineers, reports have also emerged of volunteer networks carrying out such tasks in Ukraine.[135]

The role of emergency repair in internet resilience was stressed repeatedly by interviewees. It highlights the complexity of private sector actors' role – and responsibilities to various stakeholders – as service providers during conflict. As one interviewee noted, 'there's been an empowerment of civil society organizations to step in [to] voluntarily replace public services that go down [and] replace government functions if they've been interrupted,' meaning these networks are 'really resilient'.[136] Another highlighted the 'physical security risks' to cable technicians, asking 'who is responsible if someone fixing a cable on the ground is injured?'.[137] Consequently, interviewees noted companies' 'duty of care to… staff on both sides of the conflict',[138] including 'a real concern about protecting their people on the ground', which could lead multinational companies to withdraw specialized staff. As one interviewee put it, 'they can't put their people in danger for the public good'.[139]

---

130 Madory (2023), 'Ukraine's wartime internet from the inside'.
131 Reporters Without Borders (2023), 'Occupied Territories of Ukraine: Russia propaganda machine continues to absorb local media', Reporters Without Borders News, 6 December 2023, https://rsf.org/en/occupied-territories-ukraine-russia-propaganda-machine-continues-absorb-local-media.
132 Bandura, R., Staguhn, J. and McLean, M. (2023), 'Rebuilding and Modernizing Ukraine's ICT Infrastructure Will Be Essential to Attract Private Investment', Center for Strategic and International Studies, 2 October 2023, https://www.csis.org/analysis/rebuilding-and-modernizing-ukraines-ict-infrastructure-will-be-essential-attract-private.
133 Brewster, T. (2022), 'Ukraine's Engineers Battle To Keep The Internet Running While Russian Bombs Fall Around Them', *Forbes*, 22 March 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running.
134 Moskaliuk, T. and Malatest, B. (2023), 'Russia Versus Ukraine and the Role of Software-Defined Radios', The Cyber Edge, 1 February 2023, https://www.afcea.org/signal-media/cyber-edge/russia-versus-ukraine-and-role-software-defined-radios.
135 Strachan, M. (2022), 'DIY Volunteers Are Repairing Ukraine's Destroyed Internet Infrastructure', Vice News, 23 March 2022, https://www.vice.com/en/article/qjbapv/diy-volunteers-are-repairing-ukraines-destroyed-internet-infrastructure.
136 Research interview with a senior defence and technology advisor working in the UK government, May 2023.
137 Research interview with representatives from a technology/cybersecurity company, June 2023.
138 Research interview with a representative from a major technology company, May 2023.
139 Research interview with a member of the internet governance technical community, May 2023.

These threats to local internet infrastructure have led to one of the most publicized aspects of the conflict: Elon Musk's decision to provide Starlink to Ukraine (other than Crimea).[140] Although this was originally a pro bono arrangement, as of June 2024 Starlink is contracted by the US Department of Defense.[141] While access to Starlink increases the resilience of Ukraine's internet communications, removing the necessity for ground infrastructure and replacing it with low-orbit satellites that are difficult to target, the overall impact of Starlink on the conflict should not be overestimated. Analysis suggests that no more than 0.3 per cent of Ukrainian internet traffic has ever travelled via Starlink satellites at any one time,[142] meaning that even if that small percentage is crucial for frontline military activities, it does not represent a realistic option to increase the resilience of the Ukrainian internet overall. Interviewees went further than this, highlighting the 'fragility of allowing a company like that [Starlink] to be a central node' in internet provision. According to the same interviewee, such dependence on a single supplier 'goes against decentralization and resilience', as loyalties and preferences 'could switch very quickly'.[143] Furthermore, the Russia-attributed hack of satellite communications company Viasat at the start of the invasion suggests that Russia was aware of the potential for satellite communications to increase Ukrainian internet resilience, and actively worked to counter this possibility – although with limited success and an extensive collateral impact beyond Ukraine.[144]

The Ukraine conflict is a live example of the interplay between technical and sociopolitical resilience – internet infrastructures contribute to the overall morale and war effort of Ukrainian society, while strong social relationships and political prioritization in turn help to defend those infrastructures.

The Ukraine conflict is a live example of the interplay between technical and sociopolitical resilience – internet infrastructures contribute to the overall morale and war effort of Ukrainian society, while strong social relationships and political prioritization in turn help to defend those infrastructures. But the conflict also highlights the interplay between global and local internet resilience, as decisions and actions taken at one level have direct effects on – and lead to responses at – the other level.

---

140 Copp, T. (2023), 'Elon Musk's refusal to have Starlink support Ukraine attack in Crimea raises questions for Pentagon', Associated Press, 11 September 2023, https://apnews.com/article/spacex-ukraine-starlink-russia-air-force-fde93d9a69d7dbd1326022ecfdbc53c2.
141 Capaccio, T. (2024), 'Pentagon Deal With Musk's Starlink in Ukraine Extended Six Months for $14 Million', Bloomberg via MSN, 14 June 2024, https://www.msn.com/en-us/news/technology/pentagon-deal-with-musk-s-starlink-in-ukraine-extended-six-months-for-14-million/ar-BB1oaO2Q?ocid=BingNewsSerp.
142 Tomé, Belson and Berdan (2023), 'One year of war in Ukraine'.
143 Research interview with an academic researcher, May 2023. This assessment is supported by anonymous US military officials, stating that the US military contract with Starlink 'has language that would prevent Elon Musk from turning the service off on a whim'. See Erwin, S. (2023), 'SpaceX providing Starlink services to DoD under 'unique terms and conditions'', Spacenews, 3 October 2023, https://spacenews.com/spacex-providing-starlink-services-to-dod-under-unique-terms-and-conditions.
144 Google Threat Analysis Group (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape', 16 February 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape.

Private sector involvement in Ukraine's cyber defence

Although cyber operations are not the main threat to internet resilience in Ukraine, the telecoms and satellite examples mentioned previously in this chapter demonstrate their potential to negatively affect internet resilience at both local and global levels. This aspect also reveals the shifting roles of private sector actors involved in providing resilience.

In both academic and industry treatments of Russia's war on Ukraine to date, there has been significant discussion of the relevance of cyber operations to the overall conflict dynamics.[145] Some observers argue that Russia's expectations of their impact were overly high – and overstated by Western analysts.[146] Others point to the novelty and cumulative impact of Russian tactics.[147] Despite these differences in opinion, scholars and industry observers agree that the scale and success of Ukrainian cyber defence have been higher than expected, thanks in part to the role of Western private sector actors in providing both immediate capabilities and longer-term capacity-building before, during and after the 2022 invasion.[148]

These efforts include rapid action by the Ukrainian government and its private sector partners to migrate government data to the cloud. The risks to data from physical invasion were shared by both stakeholders, as an interviewee explained: 'We were very concerned that… Russia would take over… data centres. What happens if they have access to this? How do you make sure this is safeguarded technically?'[149] Other interviewees also framed mass cloud migration in terms of resilience, arguing that 'Ukraine's infrastructure was resilient *because* it had the capacity to store, secure, transfer people's data effectively',[150] and that 'the ability to [migrate data to the cloud] is incredibly important for resilience in a time of conflict'.[151]

Interviews conducted for this paper highlighted a range of considerations at play in private sector contributions to Ukrainian cyber defence. Most obviously, interviewees expressed a clear normative motivation with wider Western political orientations, seeing assistance to Ukraine as 'the right thing to do in important

---

145 Smith, B. (2022), 'Defending Ukraine: Early Lessons from the Cyber War', Microsoft, 22 June 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war; Bateman, J. (2022), *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Washington, DC: Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en.
146 Wilde (2022), *Cyber Operations in Ukraine*.
147 Fischerkeller, M., Goldman, E. O. and Harknett, R. J. (2023), 'Cyber Persistence Theory in the Russo-Ukrainian war', Binding Hook, 7 November 2023, https://bindinghook.com/articles-book-binder/cyber-persistence-theory-in-the-russo-ukrainian-war.
148 Kostyuk, N. and Brantly, A. (2022), 'War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation', *Contemporary Security Policy*, 43(3), pp. 498–515, https://doi.org/10.1080/13523260.2022.2093587; Brantly, A. (2022), 'From the Foxhole: Cyber and Kinetic Conflict in Ukraine', *Cyber Defense Review*, pp. 1–5, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_spring_special_edition/CDR_V7N2_SPRING_2022_Brantly_From_the_Foxhole_r6.pdf?ver=lNO3pZmxwb2pTplTIqDtyA%3d%3d; Beecroft, N. (2022), *Evaluating the International Support to Ukrainian Cyber Defense*, Washington, DC: Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en&center=global.
149 Research interview with representatives from a technology/cybersecurity company, June 2023.
150 Research interview with a representative from a major technology company, May 2023.
151 Research interview with representatives from a technology/cybersecurity company, June 2023.

circumstances'.[152] In the words of another interviewee, 'their duty of care moved from customer to a full country and economy very rapidly'.[153] This 'ad hoc' emergency response attitude changed the relationship not only between private companies and Ukraine, but also between the companies themselves. Interviewees viewed their interactions as 'not competitive, as it would be competing to do things for free',[154] instead highlighting instances of 'good collaboration', especially in commercial threat intelligence and incident response. Such collaboration was also likely incentivized by the global cybersecurity advantages afforded to companies collecting threat intelligence in Ukraine, enabling them to identify and mitigate threats early that could affect their clients worldwide.

However, interviewees also voiced uncertainty about the longevity and generalization of this commitment. One claimed that 'it's not a viable financial model… [we] can't spend [millions] on each conflict',[155] with another agreeing that this work incurs 'massive financial costs'.[156] In contrast, one interviewee argued 'our principles wouldn't stand up if we had different approaches in different contexts', applied in Ukraine conflict [but] not elsewhere.[157] Others were concerned about the time horizons for voluntary aid, noting that 'everyone is going in to do good – but they also recognize that it's not easy to hop into a conflict and then hop out again.'[158] More generally, concerns were raised over financial viability:

> How much responsibility would there be for [us] to do that for free, for reasons of serving the Ukrainian population? Some work does fall out of a normative responsibility [but] to continuously run new services for free – or to guarantee them – is a big departure from [our] structure.[159]

As well as these concerns, interviewees highlighted risks arising from further involvement in the conflict (a topic discussed more widely in work by the International Committee of the Red Cross on the 'civilianization' of armed conflict).[160] Several interviewees for this paper asked themselves variations of the questions 'when do you become a party to the conflict by virtue of providing services?', and 'who are legitimate targets under international law?'.[161] One interviewee accepted that such issues were 'the reality of being in a conflict zone'. Going further, one interviewee remembered how 'companies have rushed in to provide services, [including] attempts to get Ukrainians involved in documenting war crimes, with potential consequences of exposing users to risk, breaking the law, potentially becoming complicit in war crime violations'.[162]

Given these concerns, some interviewees took a far more limited view of the responsibility of private sector actors in conflict, one tied more closely to the commercial benefit for their involvement. Most starkly, an interviewee stated

---

152 Research interview with a representative from a major technology company, May 2023.
153 Research interview with a representative from a major technology company, May 2023.
154 Research interview with a representative from a major technology company, May 2023.
155 Research interview with a representative from a major technology company, May 2023.
156 Research interview with an academic researcher, May 2023.
157 Research interview with a member of the UK government, May 2023.
158 Research interview with a senior academic researcher, May 2023.
159 Research interview with an employee at a large threat intelligence and incident response company.
160 International Committee of the Red Cross (2023), 'Global Advisory Board on digital threats during conflict', blog post, ICRC, 9 October 2023, https://www.icrc.org/en/document/global-advisory-board-digital-threats.
161 Research interview with representatives from a technology/cybersecurity company, June 2023.
162 Research interview with a senior defence and technology advisor working in government, May 2023.

that 'our responsibility is to our shareholders. It's zero unless we're being paid for it. We shouldn't spend our money building resilience for the government… or do the government's job for them'.[163]

Despite these reservations, others considered that there were commercial reasons for intervention, as 'there's a reputational angle and a self-interest angle – we don't want our services to be undermined'.[164] Reputation and self-interest were seen as potentially positive influences on decision-making. For example, one interviewee saw contributing to Ukraine cyber defence as representing '[b]rand value for later. Costs today, profits tomorrow – that can be a good balance struck'.[165]

However, the reputational aspects of contribution were not clear-cut. From one perspective, an interviewee explained that 'for the general public … contributing to a war might be difficult for them to get their heads around.'[166] In contrast, other interviewees saw a public perception of their company as 'providing critical digital services in conflict situations… [as] in our interest, it's market-forming, we're all about providing services – if you don't do that, you won't be in business for very long'.[167]

These remarks and insights demonstrate that the private sector is far from a single entity with a single mind. Conflicting approaches co-exist among – and even within – large multinational companies. Responsibility for internet resilience is widely distributed. At operational and senior levels, private sector companies grappled with complex moral, legal and commercial questions to decide the extent of their involvement in Ukrainian cyber defence, and thereby Ukraine's internet resilience overall. Ultimately, internet resilience in Ukraine turned on such considerations, but this aspect of the conflict has been underexplored in public and policy discourse.

163 Research interview with a senior representative from a technology company, May 2023.
164 Research interview with a senior representative from a technology company, May 2023.
165 Research interview with a senior defence and technology advisor working in government, May 2023.
166 Research interview with a representative from a major technology company, May 2023.
167 Research interview with a senior representative from a technology company, May 2023.

05 Conclusion

In conflict and crisis situations, technical repair, recovery and reconstruction of internet infrastructure relies on human and social networks and expertise. Private sector choices matter, both for the state of internet resilience but also for the individuals and communities dependent on it.

At the event from which this research paper originated, an attendee posed a deceptively simple question: *What is the internet?* Among the polite (and nervous) laughter in response, another attendee provided a simple and poignant answer:

> It's the babushka in eastern Ukraine trying to keep in touch with her granddaughter in Germany. We [at this event] have so much technical knowledge on what the internet is, but for the majority of people, it is connection with other humans… just a medium to get to other people.[168]

This idea has served as a guiding thread for the approach to internet resilience adopted in this research paper. It is a reminder of the fundamentally human dimension of what a resilient internet could – and, indeed, should – look like. It also shows that the technical and sociopolitical aspects of how a resilient, reliable internet works, while often separated for the purposes of analysis, are in practice intertwined.

This paper has advanced three core arguments about the nature of internet resilience, using two case studies to reveal underexplored dimensions of resilience in conflict and crisis settings. It has also used discussion of private sector actors' shifting roles in said landscape to provide not only a greater understanding of resilience, but also of the use of technologies in modern conflict more broadly.

The first argument is that there is a clear, understudied and revealing interplay between technical and sociopolitical resilience of the internet. Technical repair, recovery and reconstruction relies on humans, their social networks and their expertise, as much as the provision of suitable technology. In part, this is an issue of numbers: the greater the level of connectivity in a given country, the greater

168 Remarks made at a private dinner event, hosted at Chatham House, in May 2023.

the resilience of its internet. This resilience is in part due to alternative routes, infrastructure and connections beyond its borders. But technical and sociopolitical internet resilience are also combined, in the sense that resilience depends on the preparation and reaction of *people* to disruption. This is precisely why the relationship between technical and sociopolitical internet resilience is amplified (in depth, complexity and consequences) in a conflict or crisis environment.

Second, the technical and sociopolitical resilience of the internet is closely connected to the lives and livelihoods of individuals, and to countries and regions. In places as diverse as Afghanistan and Ukraine, with vastly different levels of internet use and infrastructure, the resilience of the internet – or lack thereof – played a key part in conflict dynamics. Adversaries recognize the strategic benefit of targeting different parts of the internet, incorporating (anti-)resilience thinking into their offensive tactics, as much as defenders incorporate strategic, resilience-based thinking into theirs. Put simply, the internet is increasingly central to modern conflict. One of the most visible manifestations of this centrality is the rise in cyberattacks to accompany – and, in some cases, exacerbate[169] – attacks[170] on energy, telecommunications and other national critical infrastructure in Ukraine. But, as this paper has demonstrated, internet resilience extends far beyond cyber defence to decisions made in global multi-stakeholder governance forums and networks of cable engineers rushing to repair bombed-out connection points.

Third, and finally, the private sector has a crucial but complex role in maintaining internet resilience at all levels of the stack, between and among both types of resilience and from the local to the global levels. The private sector is increasingly implicated in the continued operation of the internet itself and the lives of those using it. The interviews conducted for this paper in particular give insights into the complex considerations private sector entities face in maintaining, withdrawing or increasing their service and operational delivery in a conflict or crisis zone. Some considerations are reputational: will the continued or resumed delivery of service in a conflict zone jeopardize the company's local, national or global reputation? Others are commercial, rooted in the (often, overriding) incentive to protect against significant revenue disruption on the one hand, or to seek novel opportunities for increasing revenue on the other. Interviewees also highlighted the power of welfare considerations, asking: where are the main risks to the safety of company staff and their local networks? Another consideration relates to political and legal factors, associated with the potential risk of being identified as a party to conflict or the political and diplomatic pressure applied to act or withdraw services to different groups and in different locations.

A simple categorization of private sector roles in internet resilience is impractical, particularly as their roles are constituted and reconstituted along with the shifting realities of conflict and crisis environments. In any case, private sector entities are diverse, and members of the same organization do not act as one unified body with fully aligned incentives and considerations. However, for the purpose of future analysis, this paper identifies a typology of private sector and non-state

169 Black, D. (2023), 'Russia ushers in a new era of cyber-physical attack', Binding Hook (blog), 14 November 2023, https://bindinghook.com/articles-hooked-on-trends/russia-ushers-in-a-new-era-of-cyber-physical-attack.
170 Kinetic attacks are physical, non-cyberattacks.

roles, comprising the following four proposed categories. This typology is intended as a starting point from which to better delineate, untangle and identify private sector and non-state roles in providing internet resilience in conflict or crisis.

- **Providers** are private sector stakeholders that supply and maintain various parts of internet infrastructure at distinct or multiple layers of the stack (e.g. a telecommunications company supplying hardware such as cables).
- **Shapers** are those that endeavour to impact policies, strategies and processes concerning internet resilience on the national or international levels (e.g. a major technology company active in the multi-stakeholder community, sharing input in UN-level meetings on cyber governance).
- **Entrepreneurs** are those that innovate technologies at distinct or multiple levels of the stack with direct bearing on resilience (e.g. a hardware- or software-focused quantum computing and communications company).
- **Challengers** are those that provide enabling technology, resources or personnel to challenge internet resilience (e.g. a commercial hacking company contracted by an intelligence or military agency to mount cyberattacks targeting internet infrastructure).

The design and deployment of digital technologies, and the resilience of global and local internet, will continue to define the contours and, in some cases, the outcomes of modern conflict. Looking ahead, the nature and impact of future conflicts will become even more contingent on the state of the internet. Emerging technologies like artificial intelligence, which are increasingly prevalent tools in modern warfare,[171] are themselves reliant on stable cloud-data computing and fast global connectivity – all of which are significantly mediated by private sector actors.

For private sector actors operating in existing and future conflicts, progressively harder choices lie ahead, balancing political pressures with shareholder interests and profit-making duties, and maximizing voluntary contributions to provide and safeguard resilience, while minimizing legal and physical risks to staff. This paper has offered two contrasting examples of how and why these choices might be made – and, more importantly, why they matter, both for the state of internet resilience but also for the individuals and communities dependent on it.

This paper has challenged siloed approaches to internet resilience, advocating a more holistic approach that presents a clearer and more informative view on the state of resilience in conflict and crisis environments. The paper's conceptual approach, case studies and proposed typology ultimately aim to encourage and challenge stakeholders from the public and private sectors to continually reassess and strengthen their own strategic and operational approach to internet resilience.

171 Del Valle, G. (2024), 'Report: Israel used AI to identify bombing targets in Gaza', The Verge, 4 April 2024, https://www.theverge.com/2024/4/4/24120352/israel-lavender-artificial-intelligence-gaza-ai.

About the authors

James Shires is the co-director of both the European Cyber Conflict Research Incubator (ECCRI CIC) and the European Cyber Conflict Research Initiative. With ECCRI CIC, James leads the Google.org European Cybersecurity Seminars programme, a multi-year initiative to expand AI and cybersecurity education across Europe.

Isabella Wilkinson is a research fellow in the Digital Society Initiative at Chatham House and formerly a research associate in the International Security Programme. Isabella's work covers international cyber and technology governance, the online information environment and advancing responsibility and gender inclusivity.

Acknowledgments

This research paper was produced as part of a Chatham House project on trends in technology, generously supported by DXC Technology, whom we thank sincerely for enabling this project.

The authors extend their gratitude to participants of a May 2023 event on 'The Internet in Conflict', which served as inspiration for this paper, and to the interviewees and their organizations for sharing their anonymized insights, expertise and suggestions.

The authors also received valuable research assistance from Beth Whittaker (a former intern in Chatham House's International Security Programme). Feedback from Chatham House staff (in particular, Joyce Hakmeh of the International Security Programme) and fellows (most notably, Hameed Hakimi of the Asia-Pacific Programme and Olga Tokariuk of the Russia and Eurasia Programme) was particularly helpful. Thank you also to the anonymous peer reviewers, whose recommendations were incredibly constructive.

Finally, support from the institute's Communications and Publishing department has been essential. Thank you to Chris Matthews and Jake Statham, in particular, for their guidance.

Cover image: A man watches video footage featuring Taliban fighters, Khost, Afghanistan, 28 October 2021.
Photo credit: Copyright © Sardar Shafaq/Anadolu Agency/Getty Images

ISBN 978 1 78413 612 3
DOI 10.55317/9781784136123

Cite this paper: Shires, J. and Wilkinson, I. (2024), *The internet under attack: Insights from Afghanistan and Ukraine on maintaining a resilient internet in conflict and crisis*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136123.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223