**Submission to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression on Challenges to freedom of opinion and expression in times of conflicts and disturbances for the Special Rapporteur’s U.N. General Assembly 77th Session Report**

18 July 2022

**Introduction**

Access Now welcomes this opportunity to provide relevant information to the United Nations (U.N.) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur) to inform the Special Rapporteur’s report to be presented to the U.N. General Assembly at its seventy-seventh session.[[1]](#footnote-1) As an ECOSOC accredited organization, Access Now routinely engages with U.N. Special Procedures in support of our mission to extend and defend digital rights of users at risk around the world.[[2]](#footnote-2)

This submission examines the challenges to the right to freedom of opinion and expression in the context of conflict in the digital age. It specifically addresses situations where internet shutdowns, disinformation, misinformation, propaganda, or online censorship have been used to instigate, aggravate, or sustain conflict. This submission also addresses the intersecting impact of cyberattacks and surveillance amid times of conflict that disproportionately impact human rights defenders, journalists, activists, and civil society. It also explores the growing intersection between sanctions and digital rights. Finally, this submission concludes with recommendations for States, the private sector — including investors — and international organizations.

There are two caveats regarding this submission. First, we refer to “conflict” as described under the definition of armed conflict within the current interpretation of international humanitarian law.[[3]](#footnote-3) It is therefore beyond the scope of this submission to capture lower incidents of violence such as state repression during protests. However, we note that such incidents of violence can evolve into greater forms of conflict, and thus eventually fall under the ambit of international humanitarian law. Second, while this submission draws upon examples from various regions worldwide, these examples are non-exhaustive, and do not represent the lived experiences of all persons at risk. More information is required to take into full account the intersecting forms of oppression of those who are directly targeted.

***Internet shutdowns***

1. As five years of data in Access Now’s STOP database show, during times of conflict, internet infrastructure becomes a target in order to control the flow of information and gain or maintain power. Internet shutdowns also prevent the documentation of atrocities.In 2021, Access Now and the #KeepItOn Coalition continued to witness shutdowns in conflict zones, and as a form of attack in conflicts, including before, during, and after two coups (Myanmar and Sudan). The shutdowns in Eastern Europe and Central Asia, including in Russia, point to the increased geopolitical tensions that we see exploding today. The continued trend of long shutdowns is an agonizing indicator of the willingness of government authorities to disconnect and deepen the suffering of their own people.[[4]](#footnote-4)
	1. In 2021, we saw a continuation of the shutdown in **Ethiopia’s Tigray region**, which began in November 2020, in a context of ongoing civil war, crimes against humanity, and ethnic cleansing. The shutdown impacted the neighboring Amhara and Afar regions following a spillover of the conflict to those areas.
	2. On 1 February 2021, as the military launched a coup in **Myanmar**, the junta shut down multiple communications channels for a half day across the nation, in an apparent attempt to control spread of news about the coup and facilitate arrests of key members of the political opposition and civil society.[[5]](#footnote-5) This included cutting internet access, mobile phone networks, radio channels, and television channels — except for the military owned Myawaddy television channel.[[6]](#footnote-6)
		1. On February 3, the military restored 4G mobile access in some townships of Rakhine state, where the internet had long been suspended to conceal human rights abuses – presumably to distract attention from the coup.
		2. The blackouts resumed on February 6 and 7, when the junta cut access to the internet nationwide for the second time, for about 30 hours, blocking citizens’ attempts to get accurate information about the unfolding events.
		3. Military authorities imposed yet another nationwide shutdown on February 15, impacting fiber internet, wireless, and mobile networks. After that, the junta imposed nightly curfew-style shutdowns between 01:00 and 09:00 local time. These nightly disruptions lasted until April 28.

In addition, on March 15, the junta shut down mobile internet services, an action that had a deep impact because the majority of internet users in Myanmar rely on their mobile phones for that access.

* + 1. By April 1, the Ministry of Transport and Communications had ordered internet service providers to suspend wireless broadband services[[7]](#footnote-7) as well, increasing the military’s control of the internet. It would be two and a half months before the junta restored fiber optic and fixed cable connectivity, and even then, it did so by “allow-listing” organizations, corporations, and individuals for whom internet connectivity would remain specifically uninterrupted.[[8]](#footnote-8) Allowlisting effectively flips the concept of a free and open internet on its head, making blocking the norm and access the exception, in a discriminatory manner that exacerbates inequality, especially in the context of a coup and humanitarian crisis.
		2. While the military gradually restored internet access across the country in 2021, it is still imposing regional internet shutdowns to this day, particularly in places where the military is meeting resistance.[[9]](#footnote-9) These shutdowns are blatant attempts to shroud serious human rights violations, including those potentially amounting to international crimes.[[10]](#footnote-10)
		3. It is evident that regional shutdowns are continuously and aggressively imposed in regions where conflict between the military and the resistance movement is most intense, and where arson attacks by the junta have been most widespread and killings, assault, destruction of property and looting widely reported.[[11]](#footnote-11) As of May 2022, at least 54 townships across Myanmar are suffering from recurring regional shutdowns.[[12]](#footnote-12)
		4. In addition, the junta has proceeded to ban websites, including widely used social media and messaging platforms, forcing people in Myanmar to use VPNs to gain access. If the junta pushes through a recently resurrected cybersecurity bill, use of VPNs will be criminalized.[[13]](#footnote-13)
		5. The military is also throttling internet access where it is not shutting down the internet. The junta is pricing people out of telecommunications access by imposing a 10% tax hike on mobile data service providers that in turn, increases what customers need to pay every month, and an US$11 commercial tax on new SIM card activation. Regulations have also been introduced to exacerbate already-onerous requirements for SIM card registration.[[14]](#footnote-14) In particular, individuals needing to change SIM cards for security reasons – namely activists and other at-risk individuals targeted by the military – have been affected by these new regulations.
		6. On 29 June 2022, Access Now addressed the U.N. Human Rights Council regarding the escalating digital threats faced by the people in Myanmar during the Interactive Dialogue with the U.N. Special Rapporteur on the human rights situation in Myanmar.[[15]](#footnote-15) We highlighted how targeted communications blackouts are being used by the military junta in regions where people’s resistance has been most intense. We illustrated why losing connectivity in Myanmar is life-threatening - because people cannot get critical information for their safety, contact their families, or expose serious human rights violations. We also raised the alarm that the military could be requiring the International Mobile Equipment Identity (IMEI) number of phones to be registered. Linking data from IMEI number and SIM card registration will potentially give the military the power to collect data needed to track and locate people anytime they want.[[16]](#footnote-16) If the people of Myanmar refuse to use phones with registered IMEI numbers in order to evade surveillance, they will lose access to critical mobile communications services.
		7. This built on our earlier statement to the U.N. Human Rights Council of 23 March 2022, which detailed our concerns regarding the digital coup in Myanmar.[[17]](#footnote-17)
		8. Freedom of expression and opinion in Myanmar are under attack and the tools are diverse and multifaceted. These include total and partial shutdowns; communications blackouts; financial obstacles on access to vital communications services; surveillance tools including the activation of intercept technologies in telecom infrastructure; the plan to require mandatory registration of IMEI numbers; and the roll-out of abusive legal measures to curtail internet access and the rights to free expression, association, information, privacy and security – amongst others – including through potential criminalisation of the use of VPNs through the proposed cybersecurity law.
	1. In May 2021, Israeli military forces bombed and destroyed or damaged telecommunications infrastructure, causing full and partial shutdowns in the **Gaza Strip**. The bombing also led to electricity outages that further compromised connectivity. The bombings struck Al-Jawahra tower on May 12, impacting telecommunications infrastructure housed in the building. On May 15, the strikes toppled the Al-Jalaa tower,[[18]](#footnote-18) which houses the offices of some telecommunications providers and media organizations including the Associated Press and Al Jazeera. Fusion, a local telecommunications company, reported disruption of its services due to bombings on May 12, 14, and 18.[[19]](#footnote-19)
	2. In **Afghanistan**, also an active conflict zone in 2021, the Taliban shut down internet access along with phone connections and other forms of communication in the province of Panjshir, in order to curtail resistance from the area.[[20]](#footnote-20)
	3. In 2021, **Russia** was the only country to block access to communications platforms in Eastern Europe in 2021.[[21]](#footnote-21) It is however also notable that the **Belarus** government, which cut access to the internet[[22]](#footnote-22) surrounding disputed elections in 2020 and is now helping Russia wage war in Ukraine,[[23]](#footnote-23) took steps in 2021 to institutionalize its power to hit the “kill switch” and block internet access at its discretion.[[24]](#footnote-24)
		1. In March 2022, Russia wielded internet disruptions as part of its escalating attacks on Ukraine:[[25]](#footnote-25)
			1. Russian troops deliberately cut the residents of **Mariupol** off from the world when they shelled the area’s last cell tower;[[26]](#footnote-26)
			2. The invading army also plunged the cities of **Bucha**[[27]](#footnote-27) and **Irpen**[[28]](#footnote-28) into darkness as part of its occupation;
			3. Ukrainian authorities and residents also reported interruptions to Vodafone’s mobile and internet services in the cities of **Berdyansk**[[29]](#footnote-29) and **Energodar**[[30]](#footnote-30), as well as in the **Donetsk[[31]](#footnote-31)** and **Luhansk**[[32]](#footnote-32) regions;
			4. Ukrainians have also temporarily **lost internet connection**[[33]](#footnote-33) in the Zaporizhzhia, Kherson, Mykolaiv, Chernihiv, and Kyiv regions;
			5. In March 2022, to mitigate the impacts of targeted network shutdowns, mobile operators Kyivstar, Vodafone Ukraine, and lifecell, together with the Ministry of Digital Transformation of Ukraine, **launched**[[34]](#footnote-34) a national roaming service that allows subscribers to switch to other operators’ networks if they are unable to access their own operator’s. Access Now **welcomes**[[35]](#footnote-35) this swift approach to #KeepItOn throughout military aggression.
			6. On 7 June 2022, **the city of** **Kherson and Kherson region** were plunged into darkness through ongoing internet shutdowns.[[36]](#footnote-36) Russian authorities have also re-routed internet traffic to connect Ukrainians to the Russian network[[37]](#footnote-37), which seeks to exert control over Ukraine’s internet space, and make social networks like Instagram, YouTube, and Viber[[38]](#footnote-38), unavailable in these areas.
			7. However, in a July 1, 2022 press release,[[39]](#footnote-39) the **Ukrainian** authorities confirmed that they are also responsible for periodically disabling the fiber optic cable in the Russia-occupied Kherson region that might result in an unstable internet connection. In order to stay online, residents of Kherson are forced to use unbranded mobile phone SIM cards with Russian numbers that are circulated in the region by the occupying authorities, putting them and their contacts at great risk.
			8. Ukrainian media outlets report[[40]](#footnote-40) that people were targeted and attacked by long-distance artillery shelling for attempts to call their relatives via Ukrainian mobile operators in occupied **Izyum**. Russian forces usually present at the site were absent on the day of the attack, suggesting pre-meditation. The total number of victims is unknown due to the loss of the connection in the city.
	4. On 21 January 2022, Saudi-led airstrikes that damaged **Yemen’s** telecom infrastructure plunged the whole country into darkness, with the exception of those in the region of Aden.[[41]](#footnote-41) The strike targeted a facility which houses the only internet cable landing point, the FALCON international cable, which connects Yemen to global networks. Also, in 2020, damage to a submarine fiber optic cable cut nearly 80 percent of internet capacity in Yemen, with many sources attributing the shutdown to sabotage by the Houthis, a rebel group involved in the conflict.[[42]](#footnote-42)

***Impact on human rights defenders, journalists, and civil society: internet shutdowns, cyberattacks and surveillance***

1. Internet shutdowns during times of conflict make it particularly difficult for journalists and human rights defenders to get vital information in and out of these regions and for people to access crucial information that can impact their safety.
	1. Since the beginning of 2022, individuals, organizations, and a variety of institutions in **Ukraine** have faced 1350 incidents[[43]](#footnote-43) of organized and persistent cyberattacks. Civil society, public service institutions, and other services relied upon by countless individuals at risk in an active conflict zone have been regularly subject to cyberattacks, a form of cyber ‘shelling’ that often goes unnoticed while attention focuses on the more sophisticated cyber weapons that some expected to be deployed in a major geopolitical conflict. We also see a persistent trend of kinetic and cyber attacks against broadcast and telecommunications service providers, resulting in disruption and shutdown of internet access for individuals and critical infrastructure.
	2. In **Myanmar**, as noted above, internet shutdowns are currently being deployed to expand a scorched-earth military campaign, where entire villages are torched and wiped out amidst communications blackholes. Transport of essential supplies is blocked to villages, as drivers are unable to discern safe routes for travel. People are unable to [transfer or receive funds](https://www.myanmar-responsiblebusiness.org/news/return-full-mobile-internet.html) as they are cut off from [mobile payment services](https://www.voanews.com/a/myanmar-junta-hits-opposition-forces-with-communications-blackouts-/6550158.html). Amidst a pandemic, people have no way to share health information or receive medical attention, in [violation](https://www.icj.org/wp-content/uploads/2020/04/Myanmar-COVID19-Briefing-Paper-2020-ENG.pdf) of their right to health, and risks of gender-based violence are [exacerbated](https://reliefweb.int/report/myanmar/covid-19-and-coup-blockage-internet-and-social-media-access-further-exacerbate-gender). Meanwhile, children who were already unable to receive in-school education because of ongoing school boycotts and burnt down schools are now cut out of online means of learning, leading to an increasing number of school dropout cases and reported cases of  [child marriages](https://drive.google.com/drive/u/1/folders/1wwUFrhqUUtmGLzgwxSBycHxqM8SzazMF?fbclid=IwAR1RXvSC1TA7mc115L4mmDQnT_-VIgXduwJFpiK4W2H8mqu8Wuxx_4W7wLQ). Humanitarian actors and many journalists who remain in the country [struggle](https://restofworld.org/2022/blackouts-myanmar-atrocities/) to monitor and report on the ongoing human rights violations and provide [essential aid](https://www.ohchr.org/en/statements/2022/06/50th-session-human-rights-council-oral-update-myanmar), while UN experts have [highlighted](https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship) challenges to their gathering of evidence of human rights violations.[[44]](#footnote-44) Journalists, human rights defenders and monitors particularly struggle to document or verify reports of killings, arrests, ill-treatment or torture.
2. The use of cyberattacks, as evidenced in the Russia-Ukraine conflict, to shut down the internet and impede the communications infrastructure that global networks depend upon is unacceptable. It is a direct affront to protected human rights and increases global cyber insecurity. It represents irresponsible state cyber behavior at its worst if such actions have been directly perpetrated or allowed to be perpetrated by any government, which requires accountability and consequences under international law.

1. In addition to cyberattacks, in times of conflict, journalists, activists, and civil society—especially women and LGBTQI persons—face threats, like being tracked, surveilled, questioned, and detained. Rapidly building online security is vital to ensure their safety.
2. Telecommunications services are a lifeline for activists and vulnerable communities operating within conflict contexts, and global human rights organisations and digital security aid groups currently assisting them. Telecommunications providers also have access to sensitive user data — including biometric data — and communications records which can be used to identify human rights defenders and others who face hostility from armed actors. These telecom networks may also be used to both surveil activists and vulnerable communities, as well as be made complicit with internet shutdowns. Activists on ground are already deeply concerned about public and private information regarding them available via the internet and electronic communications links being used to bring them to harm.
	1. As the Taliban seized control of **Afghanistan** and with citizens trying to flee, uncertainty ensued about if and to what extent Taliban forces were surveilling people, notably human rights defenders and journalists, online, and the data they could potentially collect.[[45]](#footnote-45) For instance, the Taliban could [access various biometric databases](https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/) and equipment in Afghanistan, including some left behind by military forces.[[46]](#footnote-46) This technology is likely to include access to a database with fingerprints and iris scans, and include facial recognition technology.[[47]](#footnote-47)
	2. In **Myanmar**, Telenor itself confirmed that telcos have received orders from the military to activate intercept equipment and capabilities in its infrastructure[[48]](#footnote-48) and that the sale of its Myanmar operations includes “transfer of all call data records.”[[49]](#footnote-49) It appears all telecommunications service providers in Myanmar have been ordered by the military to activate intercept equipment, with Telenor being the only operator to publicly confirm the same. With Telenor leaving the market, three telecommunications service providers remain in the country, two biggest ones of whom are military-owned Myanmar Posts and Telecommunications (MPT) and Telecom International Myanmar Company Limited (MyTel). Qatar’s Ooredoo is the fourth telecommunications service provider in-country, with the smallest share of approximately 15% of the market, and can be reasonably assumed to be complying with intercept activation orders from the military.[[50]](#footnote-50)
	3. When the military or military-linked companies have access to massive amounts of data, the people become more vulnerable to surveillance and to other forms of harassment. In Myanmar, this is life-threatening as protesters and activists are being forced into hiding amidst mass killings, detention, and torture aimed at crushing all forms of resistance against the junta.[[51]](#footnote-51)
3. The expansion of mass surveillance systems to widely monitor and target individuals in a region of conflict is also evident – through purchase and deployment of surveillance technologies and tools from companies which have apparently failed to uphold their obligations to protect human rights or conduct relevant human rights due diligence.
	1. In **Myanmar**, the military has expanded CCTV surveillance systems across ten cities in Myanmar - with an aim to reportedly ensure roll-out across each of Myanmar’s seven states and seven regions.[[52]](#footnote-52) Purchase of surveillance equipment are reportedly from Chinese surveillance companies, Zhejiang Dahua Technology (Dahua), Huawei Technologies Co Ltd and Hikvision, and the local procurement firms which have won tenders are Fisca Security & Communication and Naung Yoe Technologies Co – both companies with strong links to the Myanmar military.[[53]](#footnote-53)
4. Access Now’s Digital Security Helpline has issued a series of digital security guidance for human rights defenders, journalists, activists, and civil society in the context of conflicts, including **Afghanistan[[54]](#footnote-54)** and **Ukraine**.[[55]](#footnote-55) Such resources aim to support human rights defenders, journalists, activists and civil society in defending against digital attacks and maintaining access to essential information during conflict.

***Disinformation, misinformation, or propaganda***

1. Social media platforms have a responsibility to keep their users safe and identify and respond to any campaigns of disinformation that may result in violence and abuse. In the context of conflict, tech companies should take swift action to enable users to easily lock down or delete their accounts and data, and enhance the security and resilience of networks, apps and services, while keeping watch for campaigns of disinformation and abuse.
2. As the primary duty bearers, States should encourage and enable companies to adopt rights-respecting practices and together ensure that incitement to violence has no place on the platform. Yet, instead we have witnessed States abusing these systems. So-called internet referral units are gaming community standards to limit speech and pressure companies to act as their censoring proxies. Communications ministries are forcing telcos to shut down services for the population while preserving access to the internet for their elites.[[56]](#footnote-56)
	1. In the **Russia-Ukraine conflict,** misinformation has been rampant across all social media platforms, but TikTok has done even less than Facebook, Instagram or Twitter to combat it. Evidence suggests that TikTok is perpetuating misinformation.
		1. In March 2022, in light of Russia’s “fake news laws” TikTok announced that it will cease live streaming and new content to video functions in Russia and will prioritize combating misinformation.[[57]](#footnote-57) Nonetheless, evidence suggests that TikTok has actually become a tool for propaganda and one of the main sources of misinformation in the Russia-Ukraine conflict.
		2. In April 2022, TikTok created an alternate universe just for Russia.[[58]](#footnote-58) TikTok specifically blocked people in Russia from seeing any posts from outside the country, including Ukraine. Such a ban on outside content violates an individual's rights to access information.
		3. TikTok algorithms continue to feed Kremlin propaganda to users, regardless of preferences and subscriptions.[[59]](#footnote-59) Even newcomers to the service receive falsified information about the war in Ukraine in their lists of recommendations within 40 minutes after registration. While TikTok claims they are independent, the platform is being used as a tool for pro-war propaganda. For instance, we have seen them implementing censorship of pro-opposition content[[60]](#footnote-60), protest-related content in Russia, and anti-government content.[[61]](#footnote-61) The Russia-Ukraine conflict has been escalating since 2014. The problems of Kremlin propaganda and misinformation have been raised with TikTok long before the invasion. While TikTok has promoted to double down on their efforts and partner with content checkers, it is evident that they are not taking this obligation seriously.
	2. In **Myanmar**, hate speech and incitement to violence online is rampant across social media platforms and messaging services, including Facebook, TikTok, LINE, Viber and Telegram. In particular, military-linked social media accounts dox activists, and pro-democracy police or soldiers on Telegram, and call for assassinations and bounty killings of these actors.[[62]](#footnote-62) Incitement to violence by non-military actors is also rampant across these social media platforms and messaging services. Meanwhile, hate speech, incitement to violence and disinformation continues to proliferate on YouTube – a problem which, as with other platforms and services, was already evident before but is now accentuated by the coup.[[63]](#footnote-63) Access Now has also been in touch with partners documenting increasing incitement to gender-based violence against women – particularly women human rights defenders – within Myanmar. In private engagement with actors documenting violations across Telegram, Facebook, YouTube, TikTok, LINE and Viber, it is evident all platforms and services are struggling with the scale and rampancy of proliferation of incitement by military-linked or pro-military actors. Telegram in particular has been woefully inadequate in its responses or engagement with civil society on its obligations to protect its users against serious harm.[[64]](#footnote-64)
	3. On 2 March 2022, Canada, as Chair of the Freedom Online Coalition, issued a statement for a call to action on state-sponsored disinformation in **Ukraine**.[[65]](#footnote-65) The statement called for the “cessation of the conducting and sponsoring of disinformation campaigns, and urge[d] all stakeholders to take active steps to address the issue in a manner that respects human rights, democracy and the rule of law.” The statement also called for “the end of Internet shutdowns and the blocking or filtering of services” and for the “Russian Federation to refrain from content restrictions on the Internet that violate international human rights laws.” It noted that “States must not unduly restrict, moderate or manipulate online content or disrupt networks to deny users access to information, contrary to their international obligations” and underscored the powerful role of social media platforms in the health of democracies and global stability. The statement was endorsed by Australia, Austria, the Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Italy, Latvia, Lithuania, Luxembourg, New Zealand, the Netherlands, Norway, Poland, Sweden, the United Kingdom, and the United States.

***Online censorship***

1. Online censorship in times of conflicts has debilitating effects. Aside from preventing the documentation of the situation as it unfolds, it also blocks the exposure of human rights violations. Online censorship prevents people from accessing information that is critical for their safety and survival. Around the world, we have seen that online censorship takes many forms:
2. Social media algorithms dictate what people can and cannot see in times of conflict. Such platforms hold evidence of atrocities — from documented killings of civilians, traces of torture, pillaging of civilian property and possessions — ultimately shining the international spotlight on the horrors unfolding in situations of conflict.
3. Bad hate speech laws often pressure companies to over-censor, and to remove content unreasonably fast or face penalty. This privatizes enforcement, misplacing what should be the role of an independent judge. Meanwhile, these policies and the tools companies deploy in response do not stop hate speech, but instead silence those who should be most protected — including women, girls, the LGBTQI community, immigrants, journalists, and activists. Governments should be on the lookout for when social media companies are abusing the power to remove content.[[66]](#footnote-66)
4. **Russia’s** escalated censorship in 2021 set the stage for what the world continues to witness in 2022.[[67]](#footnote-67) From censorship of particular websites or organizations, to takedown orders for major online communications platforms, to the throttling (slowing) of these platforms, to full platform blocks.
5. In March 2021, Roskomnadzor, the Russian agency responsible for ensuring compliance with media and telecommunications laws, responded to Twitter’s refusal to take down content it flagged by ordering telcos to throttle access to the widely used platform. The decision had unintended consequences,[[68]](#footnote-68) slowing down access to over 40,000 domains containing t.co (Twitter’s shortened domain name). That included the websites of key government institutions in Russia, as well as major platforms Google and Yandex.[[69]](#footnote-69)
6. Throttling is among many tactics the Russian government has pursued to force foreign tech companies to do its bidding. After Google and Meta refused to take down content the state deemed unlawful, Russian authorities filed lawsuits against them.[[70]](#footnote-70) They also threatened staff at Google and Apple, succeeding in convincing these companies to take down opposition leader Alexey Navalny’s Smart Voting app from their stores and platforms on election day.[[71]](#footnote-71) Authorities also blocked VPNs to stop the Russian people from circumventing this censorship.[[72]](#footnote-72)
7. After Russia invaded Ukraine in February 2022, we have seen an even more extensive crackdown on free expression as the government seeks to suppress dissent and gain control of the narrative about the conflict. Authorities have passed new laws restricting speech about the war,[[73]](#footnote-73) and banned digital and media platforms, as well as accelerated blocking circumvention tools such as VPNs. After Facebook decided to temporarily allow people in Ukraine to call for violence against the Russian heads of state and military invading their country, a Russian court declared parent company Meta “extremist,” effectively banning use of the Facebook and Instagram platforms in Russia.
	1. In April 2022, Instagram began blocking content related to the **Russia-Ukraine conflict** as evidence of atrocities committed in Bucha and Ipren shook the international community.[[74]](#footnote-74) Instagram algorithms specifically hid several hashtags such as #Bucha, #BuchaMassac, #GenocideOfUkrainians, #RussianWarCrime, and the popular #StandWithUkraine, out of supposed concerns that corresponding content might breach Community Standards.[[75]](#footnote-75) The temporary restrictions were soon lifted, making all the hashtags active again, but many users’ posts were not recovered.
8. The May 2021 Israeli bombing and destruction of telecommunications infrastructure resulting in partial shutdowns in the **Gaza Strip** particularly silenced Palestinian voices. When Palestinians were able to re-connect, major platforms like Facebook and Instagram removed hundreds of posts and suspended their accounts, disabled hashtags and live-streaming features, under biased policies and algorithms that effectively, if not intentionally, censored them.[[76]](#footnote-76)
9. In **Myanmar**, the military junta is implementing a coordinated attack to crush the resistance against it. Apart from shutdowns and surveillance, it has also used online censorship to attack the people’s exercise of their freedom of expression and opinion.
10. On 3 February 2021, the military ordered telcos to block Facebook, Instagram, Whatsapp, and Messenger, until February 7, essentially cutting off major communication platforms for millions of people in Myanmar.[[77]](#footnote-77)
11. On 13 February 13 2021, the websites of thirty Myanmar news outlets, a human rights website, and even an app providing information on the coronavirus were blocked.
12. By 17 March 2021, five independent newspapers had their publishing licences revoked and shut down operations following military threats to the Myanmar Press Council and arrests of multiple journalists from independent media outlets in February 2021.[[78]](#footnote-78)
13. In January 2022, leaked documents of the proposed Cybersecurity Law revealed sweeping definitions that would allow paralyzing censorship in violation of the rights to free expression and privacy.[[79]](#footnote-79) This includes an overbroad definition of “cybercrime” which would allow the military to easily suspend, block, take over, or ban websites, digital platform services, and providers that threaten the power of the junta.[[80]](#footnote-80)

**Sanctions and Digital Rights**

1. Sanctions are becoming a primary tool for states to achieve foreign policy goals. Their use is “accelerating enormously”[[81]](#footnote-81); the U.S. alone lists more than 10,000 people and entities.[[82]](#footnote-82) States are citing digital rights violations like internet shutdowns and spyware invasions as justifications for targeted sanctions[[83]](#footnote-83) and “block-listing” of individuals and companies.[[84]](#footnote-84)
2. Civil society increasingly calls for targeted sanctions to curtail a regime’s ability to wage illegal wars, fight corruption and retake assets, punish torturers,[[85]](#footnote-85) and affirm human rights after public or even private sector abuses. For example, human rights advocates support sanctions to prevent the transfer of surveillance equipment[[86]](#footnote-86) and sensitive data[[87]](#footnote-87) in **Myanmar** and the spyware sold by NSO Group in the **EU**.[[88]](#footnote-88)
3. However, sanctions regimes often adversely impact human rights, including digital rights. Currently, processes to develop, publicize, implement, monitor, and withdraw sanctions do not adequately integrate human rights considerations. Sanctions often fail to meet the tests of necessity and proportionality, and facilitate human rights harms that compound as third parties like tech companies and banks attempt to navigate the growing databases.
4. Overly broad sanctions, and excessive measures by companies in response – dubbed “overcompliance” – have interfered with access to information and freedom of expression in **Iran**,[[89]](#footnote-89) **Sudan**,[[90]](#footnote-90) and **Syria**.[[91]](#footnote-91) In Iran, many paid and free applications and services remain unavailable despite multiple rounds of clarification and sanctions relief by the U.S. government.[[92]](#footnote-92) While successive U.S. administrations may intend to allow humanitarian and human rights-affirming goods and services, banks and credit card companies remain reticent to support the transactions.[[93]](#footnote-93) After withdrawing services there in 2019,[[94]](#footnote-94) Microsoft-owned tech firm GitHub applied and received a specific license to again serve Iran, a “lengthy and intensive” – and likely expensive – process.[[95]](#footnote-95)
5. Lacking access to paid, licensed, upgraded, global, and secure versions of software, applications and services, people often resort to counterfeit, unlicensed, or local applications and technologies that leave them less secure and more vulnerable to cyberattack, shutdowns, and privacy invasions.[[96]](#footnote-96)
6. Overcompliance can mean the adverse impact of state sanctions lasts long beyond the sanctions themselves. In Sudan, U.S. sanctions were largely withdrawn in 2017, yet access to the Google Play Store and Apple App Store remain difficult and paid applications and services are largely out of reach.

**Russia, Belarus, and the War on Ukraine**

1. Sanctions are often counterproductive. The growing calls[[97]](#footnote-97) to interfere with the Russian and Belarusian people’s access to the internet – and actions by some companies to disable essential digital services for Russian and Belarusian users – are hurting individuals attempting to organize in opposition to the war, report openly and honestly on events in their countries, and access information about what is happening in Ukraine and abroad. These measures are facilitating further repression by the Russian and Belarusian governments.
2. In April, 2022, the U.S. Department of Treasury answered civil society’s call[[98]](#footnote-98) to protect Russian people’s access to the internet, issuing General License 25.A[[99]](#footnote-99) to exempt internet communications services, and related software, hardware, or technologies, from U.S. sanctions against Russia. A White House statement[[100]](#footnote-100) noted its commitment to exempting essential humanitarian and related activities from U.S. sanctions against Russia, including those “enabling telecommunications services to support the flow of information and access to the internet which provides outside perspectives to the Russian people.” U.S. Dept of Treasury then followed with General License No. 27[[101]](#footnote-101) exempting transactions supporting NGOs and democracy advocates.[[102]](#footnote-102) The U.K. government also responded with similar measures.[[103]](#footnote-103)
3. However, despite these carve-outs and exemptions, tech and financial companies continue to cut off and disconnect services in Russia and Belarus affecting the work of human rights defenders, independent media, and anti-war voices. For example:
4. **Google** cut off ads and all paid services in Russia, such as YouTube ads, AdSense, GSuite, paid apps, additional email storage, etc. Civil society groups are unable to prolong their subscriptions, even if they are no longer in Russia or have credit cards from foreign banks, as Google makes it difficult to update their country across the different services and devices, forcing individuals to open new accounts and losing access to their existing accounts and data.
5. **Facebook** and **Instagram** also disabled ads inRussia, which hurts the ability of anti-war voices to reach the Russian public.[[104]](#footnote-104)
6. Other tech companies, like **Slack[[105]](#footnote-105)** and **Sectigo[[106]](#footnote-106), Mailchimp**[[107]](#footnote-107) have disconnected Russian and Belarusian users, including Russian civil society organizations like OVD-Info, GOLOS, and Committee against Torture. These platforms are key for soliciting funding, keeping websites secure, and communicating with the public and internally.
7. **Visa, Mastercard, American Express,** and **Paypal,** along with other online payment services have left Russia, which makes it impossible for Russian independent media who provide daily independent reporting on the war in Ukraine, such as **Meduza, Mediazona, Holod, DOXA,** and others to receive donations from their readers on which they depend on survival.
8. Restricting access to foreign technology and communications platforms could further isolate the region and force users to rely on alternative and available services provided by Russian and Belarusian companies. These services are highly controlled by authorities and have actively stifled independent channels of information through aggressive censorship and surveillance. In addition, these steps can drive individuals toward unauthorized or pirated versions of software and services that are likely to be vulnerable to hacking and surveillance.

**Conclusion**

1. Overall, in times of conflict, measures such as knee-jerk content removals, holding tech company executives personally liable, or shutting down the internet, treat symptoms — not the cause — and are often abused by those in power to maintain political control. Social media must de-escalate conflict and empower marginalized communities, rather than enhancing inequity and division. Anything short is a roadblock to peace and security. States must stop calls for violence and hatred at their roots, and build constructive relationships with companies and civil society that regulate human rights and affected communities at the center.

**Recommendations**

1. **States**
	1. Ensure that telecom access continues while mitigating against likely surveillance and data collection risks that may facilitate reprisal and attacks against human rights defenders, civil society, journalists, and vulnerable communities;
	2. Any restriction on social media must reflect the U.N. Strategy and Plan of Action on Hate Speech and the excellent [Rabat Plan of Action](https://www.ohchr.org/en/issues/freedomopinion/articles19-20/pages/index.aspx);
	3. Act to contain and mitigate digital identification programs, biometric databases, and sensitive information that can place the people, including human rights defenders, women's groups, and others, at risk;
	4. States considering steps that would limit internet access for the nationals or individuals under the de facto or de jure jurisdiction of the aggressor and/or occupier state to carefully consider the full impact of such measures and their possible unintended consequences, and to act in a targeted, open, and strategic manner, consistent with international human rights principles of legality, legitimacy, necessity and proportionality;
	5. Continue to prioritize advocacy and push back against states’ violations of the rights to freedom of expression and information, and maintain support, including funding, for civil society advocating for human rights protections on the ground;
	6. Ensure sanctions comply with human rights law and are necessary and proportionate to achieving a legitimate aim;
	7. Avoid sanctions and related measures that broadly punish entire populations, obstruct access to devices and services that enable open and secure access to the internet, restrict civic space and humanitarian initiatives, or encourage companies to over-comply with sanctions regimes, whether current or past; and
	8. Explain the justifications for sanctions and clarify how they are developed; consult civil society actors and technologists to understand the digital and cyber impacts of potential sanctions; and enable stakeholders to provide evidence on current and potential targets and measures and their impacts on human rights.
2. **Private Sector**
	1. Platform must invest in non-English speaking countries and regions, particularly in conflict-affected or high risk areas. Platforms' investments in policy, safety, and integrity must be determined by the level of risk they pose to human rights, not just by the commercial value of a particular country or whether they are located in jurisdictions with enforceable regulatory powers. This includes linguistic equity in content moderation through hiring adequate content reviewers and skilled staff;
	2. Develop partnerships with fact-checking organizations and engage in ongoing and meaningful human rights due diligence while dealing with harmful disinformation, propaganda of war, hatred, or promotion of violence;
	3. Take swift action enabling users to easily lock down or delete their accounts and data — particularly biometric data — and enhance the security and resilience of networks, apps and services, while keeping watch for campaigns of disinformation and abuse;
	4. Tech companies, nonprofits, and funders to provide direct support to journalists, civil society, and human rights defenders in strengthening their resilience against cyber threats;
	5. Conduct heightened human rights due diligence on the situation in line with their obligations to respect human rights, including under the U.N. Guiding Principles on Business and Human Rights, and provide accessible and effective remedy to risks and damages identified in the process of conducting human rights due diligence and in engaging with stakeholders in conflict areas where they are operating;
	6. Telecommunications and technology companies must conduct due diligence and pursue genuine public engagement when creating or changing their policies on data protection, content moderation, and others, pursuant to international human rights standards;
	7. Transparency and regular and secure communication with civil society about requests they receive from government and any directives that do not comply with human rights; and
	8. Investors should conduct ongoing, enhanced human rights due diligence and check for any direct equity or fixed-income investments in conflict affected areas involving the state(s) or any of their agencies, state-affiliated entities, or separatists in occupied areas and understand their potential risks, whether these are direct or indirect risks occurring through your potential investment.
3. **International Organizations**
	1. U.N. bodies and other international organizations should establish and uphold clear, people-first cybersecurity standards;
	2. Oppose and condemn any calls or measures by states or companies to disconnect individuals from the internet or essential online services no matter their location, jurisdiction, or nationality;
	3. Provide technical assistance, support, and assistance in rebuilding infrastructure in conflict affected areas, as well as ensuring the supply of telecommunications equipment within the mandate of the International Telecommunication Union (ITU);
	4. Aid agencies, humanitarian organizations, and other international actors operating within conflict zones should:
		1. Carefully control and audit which parties have access to data of beneficiaries and staff, including checks to see patterns of access revealing efforts to surveil and profile individuals and vulnerable communities;
		2. Impose a moratorium on any continued usage of biometrics in context of conflicts without prior human rights assessments that can ensure that any such systems are safe, inclusive, not prone to error, and are the least intrusive means of authentication available;
		3. Move data off computer infrastructure physically located in conflict areas to infrastructure outside of the influence of militants and other actors seeking to intimidate vulnerable communities and at-risk individuals;
		4. Take remedial steps to inform anyone whose data has been compromised or who may be at risk, to support individuals who have been harmed by misuse of their data, and to ensure unintended access to an individual’s data does not cause further harm;
		5. Make public announcements of detected or known breaches of data, and provide authenticated mechanisms for individuals to verify if their personal data was included in the breach;
	5. Ensure that the International Criminal Court and other relevant courtsinvestigate any credible allegations of war crimes, crimes against humanity, or the crime of genocide committed in conflict areas, including crimes perpetrated online or through digital and cyber activities; and
	6. Invite civil society to collaborate in investigations, including through witness and victim support, and digital evidence collection and preservation.

##### **Access Now (**[**https://www.accessnow.org**](https://www.accessnow.org)**)** defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact:* ***un@accessnow.org***

1. United Nations Human Rights Office of the High Commissioner Special Procedures (2022, July). Call for submissions: Challenges to freedom of opinion and expression in times of conflicts and disturbances (2022, July ). Available at: <https://www.ohchr.org/en/calls-for-input/2022/call-submissions-challenges-freedom-opinion-and-expression-times-conflicts-and>. [↑](#footnote-ref-1)
2. Access Now, About Us (2022). Available at <https://www.accessnow.org/>. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. Access Now works to defend and extend the digital rights of users at risk around the world through policy, advocacy, technology support, grants, legal interventions, and global convenings like RightsCon. [↑](#footnote-ref-2)
3. There are two categories of conflict “international” as per Article 2 of the 1949 Geneva Convention (<https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf>) and “non-international” as per Protocol II of the Geneva Convention (<https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/475>). [↑](#footnote-ref-3)
4. Access Now (2022, April). The Return Of Digital Authoritarianism. Available on Page 3 at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-4)
5. Access Now (2022, April). The Return Of Digital Authoritarianism. Available on Page 3 at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-5)
6. Radio Free Asia (2021, February). News Stations Still Closed in Myanmar, Some Other Channels Reopen. Retrieved February 18, 2022, from <https://www.rfa.org/english/news/myanmar/stations-02022021181731.html>. [↑](#footnote-ref-6)
7. Reuters (2021, April). Myanmar orders wireless internet shutdown until further notice: telecoms sources. Retrieved April 26, 2022, from <https://www.reuters.com/article/us-myanmar-politics-internet/myanmar-orders-wireless-internetshutdown-until-further-notice-telecoms-sources-idUSKBN2BO5H2>. Cited in Access Now (2022, April). The Return Of Digital Authoritarianism. Available at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-7)
8. Access Now (2021, September). [#KeepItOn: Immediately reinstate internet access for all in Myanmar.](https://freedomhouse.org/article/coalition-calls-myanmar-immediately-reinstate-internet-access-all) Retrieved February 23, 2022, from <https://www.accessnow.org/cms/assets/uploads/2021/05/KeepItOn_-Immediately-reinstate-internetaccess-for-all-in-Myanmar_31-May-2021.pdf>. Cited in Access Now (2022, April). The Return Of Digital Authoritarianism. Available at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-8)
9. VOA (2021, September). In Post-Coup Myanmar, Citizens Fight to Get Online. Retrieved February 22, 2022, from <https://www.voanews.com/a/myanmar-citizens-fight-to-get-online/6250855.html> cited in Access Now (2022, April). The Return Of Digital Authoritarianism. Available at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-9)
10. BBC News (2022, March). Myanmar Rohingya violence is genocide, US says. Retrieved March 28, 2022, from <https://www.bbc.com/news/world-asia-60820215> cited in Access Now (2022, April). The Return Of Digital Authoritarianism. Available at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-10)
11. Access Now (2022, June).Open call to all international actors: do more to stop internet shutdowns shrouding torchings and killings in Myanmar. Available at: <https://www.accessnow.org/statement-against-myanmar-shutdowns/> [↑](#footnote-ref-11)
12. Athan (2022, May). Internet Access Amid Darkness and Lives Amid Threats. Available at <https://progressivevoicemyanmar.org/wp-content/uploads/2022/06/Internet-Shutdown-Athan-May-2022-Eng.pdf> [↑](#footnote-ref-12)
13. Access Now (2022, January). Analysis: the Myanmar junta’s Cybersecurity Law would be a disaster for human rights. Retrieved January 27, 2022, from <https://www.accessnow.org/analysis-myanmar-cybersecurity-law/> cited in Access Now (2022, April). The Return Of Digital Authoritarianism. Available at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-13)
14. Access Now and others (2022, February). Resist Myanmar’s digital coup: stop the military consolidating digital control. Retrieved July 18, 2022 from <https://www.accessnow.org/myanmars-digital-coup-statement/> [↑](#footnote-ref-14)
15. Access Now (2022, July). Access Now’s statement on Myanmar during the UN Special Rapporteur on the situation of human rights in Myanmar’s Oral Progress Report. Available at <https://www.accessnow.org/access-now-un-statement-on-myanmar/> [↑](#footnote-ref-15)
16. Access Now (2022, July). Myanmar IMEI FAQ: how the junta could disconnect the resistance. Retrieved July 18, 2022, from <https://www.accessnow.org/myanmar-imei/> [↑](#footnote-ref-16)
17. Access Now (2022, March). Access Now’s statement on Myanmar at the U.N. Human Rights Council.. Available at <https://www.accessnow.org/united-nations-on-myanmar/> [↑](#footnote-ref-17)
18. SMEX (2021, May). Israeli Airstrikes Destroyed Internet Infrastructure In Gaza [Report]. Retrieved February 28, 2022, from <https://smex.org/israeli-airstrikes-destroyed-internet-infrastructure-in-gaza-report/> Internet Outage Alerts (@gatech\_ioda). Twitter post. 3:59 pm. May 16, 2021. Retrieved February 28, 2022, from https://twitter.com/caida\_ ioda/status/1393959216595959810. Cited in Access Now (2022, April). The Return Of Digital Authoritarianism. Available at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-18)
19. Facebook post (2021, May 12). Fusion Internet and Communications Services (@FusionGaza). Retrieved February 23, 2022, from <https://www.facebook.com/FusionGaza/posts/4399068443459303?_rdc=1&_rdr>. Cited in Access Now (2022, April). The Return Of Digital Authoritarianism. Available at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-19)
20. Access Now (2022, April). The Return Of Digital Authoritarianism. Available on Page 3 at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-20)
21. Access Now (2022, April). The Return Of Digital Authoritarianism. Available on Page 10 at <https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf> [↑](#footnote-ref-21)
22. Access Now (2020, August). Belarusian election tainted by internet shutdown and state-sponsored violence. Retrieved July 14, 2022, from <https://www.accessnow.org/belarusian-election-tainted-by-internet-shutdown-and-state-sponsored-violence/> [↑](#footnote-ref-22)
23. The Conversation (2022, March). 3 reasons Belarus is helping Russia wage war against Ukraine. Retrieved July 14, 2022, from <https://theconversation.com/3-reasons-belarus-is-helping-russia-wage-war-against-ukraine-177984> [↑](#footnote-ref-23)
24. Freedom House (2021). Belarus: Freedom on the Net 2021 Country Report. RetrievedJuly 14, 2022, from <https://freedomhouse.org/country/belarus/freedom-net/2021> [↑](#footnote-ref-24)
25. Access Now (2022, July). Updates: Digital rights in the Russia-Ukraine conflict. Available at <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/> [↑](#footnote-ref-25)
26. Human Rights Watch (2022, March). Ukraine: Mariupol Residents Trapped by Russian Assault. Available at <https://www.hrw.org/news/2022/03/07/ukraine-mariupol-residents-trapped-russian-assault> [↑](#footnote-ref-26)
27. Facebook post (2022, March). Bucharada.gov.ua. Available at <https://www.facebook.com/bucharada.gov.ua/posts/1822668304606232> [↑](#footnote-ref-27)
28. UNIAN (2022, March). Russian troops fired on civilians during the evacuation from Irpen, there are victims. Available at <https://www.unian.net/war/voyska-rf-obstrelyali-grazhdanskih-vo-vremya-evakuacii-iz-irpenya-est-zhertvy-smi-novosti-kieva-11731258.html> [↑](#footnote-ref-28)
29. Telegram post (2022, March). Available at <https://t.me/zoda_gov_ua/4999> [↑](#footnote-ref-29)
30. UNIAN (2022, March). Vodafone does not work in Berdyansk, Energodar and the surrounding area. Available at <https://www.unian.net/economics/telecom/v-energodare-i-okrestnostyah-ne-rabotaet-vodafone-novosti-11731165.html> [↑](#footnote-ref-30)
31. Radio Free Europe/Radio Liberty (2022, February). Vodafone has not been in Donetsk for three days already. "Must wait". Available at <https://www.radiosvoboda.org/a/donetsk-vodafone/31728183.html> [↑](#footnote-ref-31)
32. The Economist (2022, March). Ukrainian cities are suffering internet blackouts. Available at <https://www.economist.com/graphic-detail/2022/02/26/ukrainian-cities-are-suffering-internet-blackouts> [↑](#footnote-ref-32)
33. The Sovereign Service of the Special Contact and Protection of Information of Ukraine (July, 2022). Operational information of the State Special Service about the work of mobile networks at 09:00 on 11 March 2022. Available at <https://cip.gov.ua/ua> [↑](#footnote-ref-33)
34. Interfax-Ukraine (2022, March). Ukrainian mobile operators unite, launch national roaming. Available at <https://ua.interfax.com.ua/news/general/808856.html> [↑](#footnote-ref-34)
35. Twitter thread (2022, March). Access Now. Available at <https://twitter.com/accessnow/status/1500859631652020232> [↑](#footnote-ref-35)
36. Novaya Gazeta (2022, June). The Russian military "cut off" the occupied Kherson from Ukrainian networks, and the residents of the city were forced to stand in line for unmarked SIM cards. Available at <https://novayagazeta.eu/articles/2022/06/06/driannaia-sviaz?utm_source=tg.me&utm_medium=social&utm_campaign=-zhiteley-okkupirovannogo-yuga-ukrainy-li> [↑](#footnote-ref-36)
37. The Cloudflare Blog (2022, May). Tracking shifts in internet connectivity in Kherson, Ukraine. Available at <https://blog.cloudflare.com/tracking-shifts-in-internet-connectivity-in-kherson-ukraine/> [↑](#footnote-ref-37)
38. The Moscow Times (2022, July). YouTube Blocked in Ukraine's Russian-Occupied Kherson. Available at <https://www.themoscowtimes.com/2022/07/06/youtube-blocked-in-russia-occupied-kherson-a78220> [↑](#footnote-ref-38)
39. State Service of Special Communications and Information Protection of Ukraine (2022, July). Зв’язок на тимчасово окупованих територіях відновимо після їх звільнення. Available at <https://cip.gov.ua/ua/news/zv-yazok-na-timchasovo-okupovanikh-teritoriyakh-vidnovimo-pislya-yikh-zvilnennya>. [↑](#footnote-ref-39)
40. Ukraine Today (2022, July). In Izyum, the invaders shot people who were looking for a mobile connection on the mountain – media. Available at <https://ukrainetoday.org/2022/07/12/in-izyum-the-invaders-shot-people-who-were-looking-for-a-mobile-connection-on-the-mountain-media/>. See also Kharviv Today, Россияне обстреляли Изюм: сообщают о множестве раненых и убитых (2022, July)

 available at https://2day.kh.ua/ru/kharkow/rossiyane-obstrelyali-izyum-soobschayut-o-mnozhestve-ranenykh-i-ubitykh [↑](#footnote-ref-40)
41. Access Now (2022, January). Internet shutdowns in Yemen: telecommunications structure is not a military target. Available at <https://www.accessnow.org/yemen-internet-shutdown-statement/>. Cited in Access Now (2022, May). #KeepItOn for peace and democracy in Sudan, Yemen, and Tajikistan. Available at <https://www.accessnow.org/keepiton-for-peace-and-democracy-in-sudan-yemen-and-tajikistan/> [↑](#footnote-ref-41)
42. Wired (2020, January). Cut undersea cable plunges Yemen into days-long internet outage. Available at <https://www.wired.com/story/yemen-internet-blackout-undersea-cable/> [↑](#footnote-ref-42)
43. State Service of Special Communications and Information Protection of Ukraine (2022, July). Russian hackers keep attacking the Ukrainian infrastructure and descending to civilian targets. Available at <https://cip.gov.ua/en/news/rosiiski-khakeri-prodovzhuyut-atakuvati-ukrayinsku-infrastrukturu-ne-grebuyuchi-civilnimi-cilyami> [↑](#footnote-ref-43)
44. Access Now (2022, June). Open call to all international actors: do more to stop internet shutdowns shrouding torchings and killings in Myanmar. Available at <https://www.accessnow.org/statement-against-myanmar-shutdowns/> [↑](#footnote-ref-44)
45. MIT Technology Review (2021, August). This is the real story of the Afghan biometric databases abandoned to the Taliban. Available at

 <https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/> [↑](#footnote-ref-45)
46. Access Now (2021, August). #WhyID: international actors in Afghanistan must clean up, restrict dangerous biometric trail. Available at <https://www.accessnow.org/whyid-afghanistan-biometrics/> [↑](#footnote-ref-46)
47. Human Rights Watch (2022, March). New Evidence that Biometric Data Systems Imperil Afghans. Available at <https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans> [↑](#footnote-ref-47)
48. Telenor (2021, Sept), Continued presence in Myanmar not possible for Telenor, available at <https://www.telenor.com/media/announcement/continued-presence-in-myanmar-not-possible-for-telenor> [↑](#footnote-ref-48)
49. Myanmar Now, Telenor will transfer call data records for 18m subscribers to junta-linked company, 26 July 2021, available at <https://www.myanmar-now.org/en/news/telenor-will-transfer-call-data-records-for-18m-subscribers-to-junta-linked-company> [↑](#footnote-ref-49)
50. Access Now (2022, March). It’s not over until it’s over: sanctions must stop Telenor’s sale to the Myanmar military. Available at <https://www.accessnow.org/sanctions-telenor-sale-to-myanmar-military/> [↑](#footnote-ref-50)
51. Myanmar Now (2021, July). Telenor will transfer call data records for 18m subscribers to junta-linked company. Retrieved on July 18, 2022 from <https://www.myanmar-now.org/en/news/telenor-will-transfer-call-data-records-for-18m-subscribers-to-junta-linked-company> . [↑](#footnote-ref-51)
52. Reuters (2022, July). Exclusive-Myanmar's junta rolls out Chinese camera surveillance systems in more cities -sources. Available at

<https://www.reuters.com/article/us-myanmar-surveillance-exclusive-idAFKBN2OL0J6> [↑](#footnote-ref-52)
53. Access Now (2022, July). Twitter thread on military roll-out of surveillance systems. Available at <https://twitter.com/accessnow/status/1547479721394315264> [↑](#footnote-ref-53)
54. Access Now (2021, August). Online safety resources for Afghanistan’s human rights defenders. Available at <https://www.accessnow.org/online-safety-resources-afghanistan/> [↑](#footnote-ref-54)
55. Access Now (2022, March). Digital safety tips against cyber attacks in Ukraine. Available at <https://infogram.com/ukraine-safety-tips-for-civil-society-en-1h8n6m3kmkp1z4x?live> [↑](#footnote-ref-55)
56. Access Now (2021, October). Access Now addresses the U.N. Security Council on countering hate speech online. Available at <https://www.accessnow.org/un-security-council-address-online-hate-speech/> [↑](#footnote-ref-56)
57. TikTok (2022, March). Bringing more context to content on TikTok. Available at <https://newsroom.tiktok.com/en-us/bringing-more-context-to-content-on-tiktok> cited in <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/> [↑](#footnote-ref-57)
58. The Washington Post (2022, April). TikTok created an alternate universe just for Russia. Available at <https://www.washingtonpost.com/technology/2022/04/13/tiktok-russia-censorship-propaganda-tracking-exposed/> cited in Access Now (2022, July). Updates: Digital rights in the Russia-Ukraine conflict. Available at <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/> [↑](#footnote-ref-58)
59. The Guardian (2022, March). TikTok algorithm directs users to fake news about Ukraine war, study says. Available at <https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to-fake-news-about-ukraine-war-study-says> cited in Access Now (2022, July). Updates: Digital rights in the Russia-Ukraine conflict. Available at <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/> [↑](#footnote-ref-59)
60. The Moscow Times (2021, January). Social Media Platforms Delete Russian Posts Promoting Navalny Protests - State Censor. Available at <https://www.themoscowtimes.com/2021/01/22/social-media-platforms-delete-russian-posts-promoting-navalny-protests-state-censor-a72701> [↑](#footnote-ref-60)
61. .Coda (2022, May). A Russian user looks inside TikTok’s propaganda-filled digital bubble. Available at <https://www.codastory.com/newsletters/russia-tiktok-propaganda/> cited in Access Now (2022, July). Updates: Digital rights in the Russia-Ukraine conflict. Available at <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/> [↑](#footnote-ref-61)
62. Frontier Myanmar (2022, March). ‘Watermelon suppression’: doxing campaign targets pro-democracy soldiers and police. Available at

<https://www.frontiermyanmar.net/en/watermelon-suppression-doxing-campaign-targets-pro-democracy-soldiers-and-police/>; Frontier Myanmar (2022, January). ‘Online mob’ assists silent strike crackdown. Available at <https://www.frontiermyanmar.net/en/online-mob-assists-silent-strike-crackdown/> [↑](#footnote-ref-62)
63. Reuters (2020, December) YouTube faces complaints of lax approach on overseas election misinformation. Available at

<https://www.reuters.com/article/us-youtube-myanmar-misinformation-idUSKBN28S0QE> [↑](#footnote-ref-63)
64. Htaike Htaike Aung (2022, January). Twitter thread on Telegram doxxing in Myanmar. Available at <https://twitter.com/barnyar/status/1488105742532071425?lang=en> [↑](#footnote-ref-64)
65. Freedom Online Coalition (2022, March). Statement on behalf of Canada, Chair of the Freedom Online Coalition: A call to action on state-sponsored disinformation in Ukraine. Available at <https://freedomonlinecoalition.com/statement-on-behalf-of-canada-chair-of-the-freedom-online-coalition-a-call-to-action-on-state-sponsored-disinformation-in-ukraine/> [↑](#footnote-ref-65)
66. Access Now (2021, October). Access Now addresses the U.N. Security Council on countering hate speech online. Available at <https://www.accessnow.org/un-security-council-address-online-hate-speech/> [↑](#footnote-ref-66)
67. Bloomberg (2022, April). Internet Shutdowns Surge From India to Russia After Covid Dip. Available at

 <https://www.bloomberg.com/news/articles/2022-04-28/internet-shutdowns-surge-from-india-to-russia-after-covid-dip> [↑](#footnote-ref-67)
68. Access Now (2021). Russia throttled Twitter to censor content — Here’s what happens next. Retrieved February 18, 2022, from <https://www.accessnow.org/russia-throttled-twitter/>. [↑](#footnote-ref-68)
69. WIRED (2021, March). Russia's Failure to Throttle Twitter Isn't a Sign of Weakness. Retrieved March 21, 2022, from <https://www.wired.com/story/opinion-russias-failure-to-throttle-twitter-isnt-a-sign-of-weakness/> . [↑](#footnote-ref-69)
70. The Moscow Times (2020, December). Russia Fines Google for Failing To Remove Banned Content. Retrieved March 21, 2022, from <https://www.themoscowtimes.com/2020/12/17/russia-fines-google-for-failing-to-remove-banned-content-a72400>. [↑](#footnote-ref-70)
71. The New York Times (2021). Google and Apple, Under Pressure From Russia, Remove Voting App. Retrieved March 22, 2022, from <https://www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html>. [↑](#footnote-ref-71)
72. Roskomnadzor (2021). Federal Service for Supervision of Communications, Information Technology and Mass Communications. Retrieved March 22, 2022, from <https://rkn.gov.ru/news/rsoc/news73836.htm>. [↑](#footnote-ref-72)
73. POLITICO (2022, March). Russia expands laws criminalizing 'fake news'. Retrieved April 6, 2022, from <https://www.politico.eu/article/russia-expand-laws-criminalize-fake-news/> [↑](#footnote-ref-73)
74. Access Now (2022, July). Updates: Digital rights in the Russia-Ukraine conflict. Available at <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/> [↑](#footnote-ref-74)
75. Twitter thread (2022, April). Available at <https://twitter.com/gil_iryna/status/1510604876992106505> cited in Access Now (2022, July). Updates: Digital rights in the Russia-Ukraine conflict. Available at <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/> [↑](#footnote-ref-75)
76. The Washington Post (2021, May). Facebook’s AI treats Palestinian activists like it treats American Black activists. It blocks them. Available at <https://www.washingtonpost.com/technology/2021/05/28/facebook-palestinian-censorship/> [↑](#footnote-ref-76)
77. Access Now (2021-2022). Update: internet access, censorship, and the Myanmar coup. Retrieved on July 18, 2022 from <https://www.accessnow.org/update-internet-access-censorship-myanmar/> [↑](#footnote-ref-77)
78. Myanmar Now (2021, March). Myanmar becomes a nation without newspapers. Available at <https://www.myanmar-now.org/en/news/myanmar-becomes-a-nation-without-newspapers> [↑](#footnote-ref-78)
79. Access Now (2022, January). Analysis: the Myanmar junta’s Cybersecurity Law would be a disaster for human rights. Retrieved on July 18, 2022 from <https://www.accessnow.org/analysis-myanmar-cybersecurity-law/> [↑](#footnote-ref-79)
80. Id. [↑](#footnote-ref-80)
81. See, e.g. OHCHR, Call for contributions – Toward a universal system of monitoring to assess the human rights impact of unilateral sanctions, available at <https://www.ohchr.org/en/calls-for-input/2022/call-contributions-toward-universal-system-monitoring-assess-human-rights> [↑](#footnote-ref-81)
82. The Economist, Western sanctions on Russia are like none the world has seen, 5 March 2022, available at <https://www.economist.com/briefing/2022/03/05/western-sanctions-on-russia-are-like-none-the-world-has-seen> [↑](#footnote-ref-82)
83. See, e.g. EU sanctions on Myanmar Minister of Transport and Communication Admiral Tin Aung San. “Since he took over the ministry, there have been numerous shutdowns and deliberate slowing-downs of the internet, as well as orders for providers to prevent Facebook, Twitter and Instagram on-line.” Official Journal of the European Union, COUNCIL IMPLEMENTING REGULATION (EU) 2021/998

of 21 June 2021, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2021.219.01.0045.01.ENG&toc=OJ%3AL%3A2021%3A219I%3ATOC>. [↑](#footnote-ref-83)
84. The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities, 3 Nov. 2021, available at <https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities>. See also, Reuters, U.S. lawmakers call for sanctions against Israel's NSO, other spyware firms, 15 Dec. 2021, available at <https://www.reuters.com/world/us/exclusive-us-lawmakers-call-sanctions-against-israels-nso-other-spyware-firms-2021-12-15>. [↑](#footnote-ref-84)
85. See, e.g. discussion of Magnitsky Sanctions at Human Rights First, available at, <https://www.humanrightsfirst.org/topics/global-magnitsky>, and Redress, available at <https://redress.org/magnitsky-sanctions> [↑](#footnote-ref-85)
86. Justice for Myanmar, (2022, March). Telenor Group violtaing sanctions through installation and imminent transfer of german Lawful Intercept Gateway, available at: <https://www.justiceformyanmar.org/press-releases/telenor-group-violating-sanctions-through-installation-and-imminent-transfer-of-german-lawful-intercept-gateway> [↑](#footnote-ref-86)
87. Access Now, (2022, March) It’s not over until it’s over: sanctions must stop Telenor’s sale to the myanmar military, available at <https://www.accessnow.org/sanctions-telenor-sale-to-myanmar-military/> [↑](#footnote-ref-87)
88. Access Now, (April, 2022), Facing the consequences: Access Now welcomes legal action against NSO Group, available at: <https://www.accessnow.org/legal-action-nso-group/> [↑](#footnote-ref-88)
89. Foreign Policy (2021, May). Outdated US policies Are Helping Iran Censor Its Citizens, available at <https://foreignpolicy.com/2021/05/06/iran-internet-censorship-us-sanctions/> [↑](#footnote-ref-89)
90. Slate (2014, January). Time to Rethink Tech Sanctions Against Sudan. Available at <https://slate.com/technology/2014/01/sudan-sanctions-are-keeping-secure-communications-tools-from-activists.html> [↑](#footnote-ref-90)
91. Aljazeera (2011, November). When sanctions make things worse. Available at <https://www.aljazeera.com/opinions/2011/11/23/when-sanctions-make-things-worse> [↑](#footnote-ref-91)
92. See a list of inaccessible applications and services at “Iran Tech Sanctions Overcompliance”, available at <https://docs.google.com/spreadsheets/d/1RnILSWZXGgK_bRGTyBxZzXf0YvesHnMfDj9LD-KpMG8> [↑](#footnote-ref-92)
93. Business Insider, (October, 2021), If Biden actually wants to help Iranians, there’s an easy way to do it, available at: <https://www.businessinsider.com/biden-wants-to-help-iranians-heres-how-to-do-it-2021-10> [↑](#footnote-ref-93)
94. Aljazeera, Locked out: Did US tech company over comply with Iran sanctions? Available at: <https://www.aljazeera.com/economy/2019/7/31/locked-out-did-us-tech-company-overcomply-with-iran-sanctions> [↑](#footnote-ref-94)
95. Github Blog, Advancing developer freedom: GitHub is fully available in Iran, (January, 2021) available at: <https://github.blog/2021-01-05-advancing-developer-freedom-github-is-fully-available-in-iran> / [↑](#footnote-ref-95)
96. See, ARTICLE19, Iran: Tightening the Net 2020 After Blood and Shutdowns, Sept. 2020, available at <https://www.article19.org/ttn-iran-november-shutdown>. [↑](#footnote-ref-96)
97. The Washington Post (2022, March). The Ukrainian leader who is pushing Silicon Valley to stand up to Russia. Available at <https://www.washingtonpost.com/technology/2022/03/02/mykhailo-fedorov-ukraine-tech/> [↑](#footnote-ref-97)
98. Access Now (2022, March). Letter to U.S. government: Do not disrupt internet access in Russia or Belarus. Available at <https://www.accessnow.org/letter-us-government-internet-access-russia-belarus-ukraine/> [↑](#footnote-ref-98)
99. Department of the Treasury Washington D.C. Office of Foreign Assets Control (2022, April). Russian Harmful Foreign Activities Sanctions Regulations 31 CFR part 587. Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications. Available at <https://home.treasury.gov/system/files/126/russia_gl25.pdf> [↑](#footnote-ref-99)
100. The White House (2022, April). FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia. Available at <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/> [↑](#footnote-ref-100)
101. Department of the Treasury Washington D.C. Office of Foreign Assets Control (2022, April). GENERAL LICENSE NO. 27. Certain Transactions in Support of Nongovernmental Organizations’ Activities. Available at <https://home.treasury.gov/system/files/126/russia_gl27.pdf> [↑](#footnote-ref-101)
102. Department of the Treasury Washington D.C. (2022, April). Fact Sheet: Preserving Agricultural Trade, Access to Communication, and Other Support to Those Impacted by Russia’s War Against Ukraine. Available at <https://home.treasury.gov/system/files/126/russia_fact_sheet_20220419.pdf> [↑](#footnote-ref-102)
103. Access Now (2022, June). UK protects free flow of information amidst Russian sanctions. Available at <https://www.accessnow.org/uk-information-russia-sanctions/> [↑](#footnote-ref-103)
104. Twitter thread (2022, April). @navalny. Truth and free information hit Putin's insane regime just as hard as Javelins. This is a thread about opening the second front against the war criminal from the Kremlin — the informational front. Available at <https://twitter.com/navalny/status/1514589869204508675?s=20&t=jtf9k2bfp42cZ9MlU4OpLA> [↑](#footnote-ref-104)
105. Twitter thread (2022, May). @natynettle. Cautionary tale: [@Namecheap](https://twitter.com/Namecheap) [@SlackHQ](https://twitter.com/SlackHQ) & [@Mailchimp](https://twitter.com/Mailchimp) have pulled their service to civil society voices in [#Russia](https://twitter.com/hashtag/Russia?src=hashtag_click) & [#Belarus](https://twitter.com/hashtag/Belarus?src=hashtag_click). In no-doubt-well-meaning haste they're trying to impose costs on [#Putin](https://twitter.com/hashtag/Putin?src=hashtag_click). But they skipped due diligence & are now silencing some of his fiercest critics. Available at <https://twitter.com/natynettle/status/1504205743251206147?s=20&t=nQaqlzJbo4xIjjouGUBH7A> [↑](#footnote-ref-105)
106. Twitter thread (2022, May). @natynettle. Here's the bad news: civil society org [@Tep\_st](https://twitter.com/Tep_st)'s certificate won’t be renewed this year because upstream provider [@SectigoHQ](https://twitter.com/SectigoHQ) won't issue certs to any .ru domains, citing “US Export restriction laws.” Available at <https://twitter.com/natynettle/status/1504993206601142275?s=20&t=nQaqlzJbo4xIjjouGUBH7A> [↑](#footnote-ref-106)
107. CNN Politics (2022, April). A Russian opposition leader wants to fight Vladimir Putin with ads on YouTube. Available at <https://edition.cnn.com/2022/04/28/politics/youtube-google-ads-russia-what-matters/index.html> [↑](#footnote-ref-107)