Digital Rights At The U.N. HRC 49 And Beyond

Just four days before the U.N. held the 49th session of the Human Rights Council (HRC49), the agency's most powerful body, the U.N. Security Council, held an emergency meeting to try to stop Russia from invading Ukraine. Russia went ahead anyway. Russia had also initiated an Ad-Hoc Committee on Cybercrime. It was perhaps an all-time low for the public's faith in the U.N.'s power to ease geopolitical tensions and enable international cooperation.

Today, the situation has changed. Russia has been removed from the Human Rights Council and Committee on NGOs, and their initiatives have lost legitimacy across the U.N. And as the 49th session unfolded, we saw many reasons to keep the faith in the U.N.'s capacity to tackle key issues for the future of human rights. As we explain in this briefing, the U.N. is recognizing the importance of digital rights in shaping that future.

Digital rights violations enable and escalate offline violence, deepening humanitarian crises. The calculated attacks targeting digital systems – essential to people's safety and wellbeing – are unacceptable. At this critical juncture in history, when human rights violations are rampant from Ukraine to Myanmar we remain committed to defend and extend the digital rights of users at risk, including through our strategic advocacy efforts at the U.N. and other multilateral bodies.

The U.N. Secretary General kicked off HRC49 decrying the internet for being what he called the "Wild West for human rights," characterized by digital divides, disinformation campaigns, internet shutdowns, censorship, and the proliferation of spyware. These themes featured heavily at HRC49 – from resolutions to interactive dialogues and side events. We saw progress in advancing international norms and standards that will be valuable for future digital rights advocacy. We have prepared this briefing to help delegates make further progress on these vital and important issues for human rights, including developing recommendations for moving forward at the Council's upcoming 50th session and beyond.

In this brief, while non-exhaustive, we cover:

I. Internet shutdowns, disinformation, and civic space;
II. Surveillance of human rights defenders, particularly women human rights defenders;
III. Biometrics and digital identity; and
IV. Cybercrime and cybersecurity

Building on our initial U.N. advocacy, as captured in our HRC49 Digital Rights Brief, and in our ongoing advocacy efforts including oral interventions, we analyze the outcomes of human rights and digital-focused processes, namely HRC49 and the Ad Hoc Committee to Elaborate an International Convention on Cybercrime (AHC on Cybercrime), to equip delegates with the background necessary for future digital rights advocacy at the U.N.

I. INTERNET SHUTDOWNS, DISINFORMATION, AND CIVIC SPACE

Internet shutdowns interfere with a range of human rights. Such disruptions not only attack fundamental rights, but also have a severe negative impact on the economy, health care, and education. Governments often cite "preventing the spread of misinformation/disinformation" as a means to justify shutdowns. Yet data collected from the #KeepItOn coalition — a global campaign composed of more than 280 organizations from 105 countries fighting internet shutdowns — confirms that such governments typically order shutdowns under circumstances that are in fact aimed at quelling protests, or gagging citizens during important national events like elections. The overall effect ultimately shrinks civic space both online and off. In this section we cover advocacy initiatives at HRC49 on internet shutdowns, disinformation, and the continued issue of meaningful civil society access to the U.N., as evidenced in the AHC on Cybercrime process.

On March 4, the Human Rights Council (the Council) held an Urgent Debate on the **situation of human rights in Ukraine stemming from the Russian aggression**. In a rapid resolution (A/HRC/RES/49/1) the Council voted to establish an independent commission of inquiry as a result of Russia's aggression against Ukraine – 32 in favour, 13 abstentions, and 2 votes against adoption of the resolution (from Russia and Eritrea). Establishment of such a body is crucial for further accountability for human rights violations, in parallel with ongoing efforts at the U.N's International Court of Justice. We delivered an oral statement during the Urgent Debate (38:50), drawing attention to cyberattacks that compound suffering in Ukraine and threaten human rights online and offline. The resolution reiterated digital rights concerns, stressing the "importance of maintaining free, open, interoperable, reliable, and secure access to the internet," while also condemning internet shutdowns (OP7). Indeed, U.N. experts, civil society, and governments are all uniting to bring the human rights implications of internet shutdowns to the forefront of urgent country-specific situations, including at the recent 32nd Special Session of the Council on the human rights implications of the ongoing situation in Sudan (A/HRC/S-32/2), in which we also intervened.

On March 21, the U.N. Special Rapporteur on the situation of human rights in Myanmar, Thomas Andrews, presented his report (A/HRC/49/76) to the Council. The extensive report featured a section on freedom of expression, assembly and association, narrowing in on the issues of (1) media freedom (2) internet restrictions and (3) surveillance. We welcomed the Rapporteurs' report and delivered an oral statement during the Rapporteur's Interactive Dialogue (54:37), where we drew attention to the military's cemented chokehold on the internet and its actions to expand its digital toolkit to undermine human rights in Myanmar. Our statement underscores the need for a comprehensive arms embargo on surveillance and censorship equipment or related intelligence assistance to Myanmar's military. We also urge tech companies to invest and cooperate more to protect against and remedy rights violations, and call on Myanmar to stop throttling and shutting down the internet.

At HRC49, the European Union (EU) led the resolution to renew the mandate on the "Situation of human rights in Myanmar," (A/HRC/49/L.12), which was adopted by consensus. The resolution now contains important *operational* language calling for the "lifting of Internet shutdowns and all other Internet

restrictions, which hinder the flow of information essential for accountability" (OP19). Building on agreed-upon internet shutdowns language in existing country-specific U.N. resolutions, such as the recent General Assembly Third Committee resolution on the Situation of human rights in Iran (A/RES/76/178), we advocated to advance digital rights language in other Council country-specific resolutions at HRC49 including Belarus (A/HRC/49/L.13), South Sudan (A/HRC/49/L.15), Nicaragua (A/HRC/49/L.20), and Iran (A/HRC/49/L.7), to name a few. The Belarus resolution maintained language on internet shutdowns, while the Nicaragua resolution merely sprinkled "online and offline" throughout the text, the South Sudan resolution made no reference to digital rights, and the Iran resolution fell short of its General Assembly counterpart, with no reference to internet shutdowns. This is notable given the human rights situation in these countries. In Nicaragua, civic space has been shrinking, online and offline, since the November 2021 election. South Sudan previously shut down the internet. In Iran, the government continues to intentionally shut down the internet, particularly during protests, to limit access to information and hide evidence of serious human rights violations. We are disappointed that such digital rights violations were not captured in the renewed country-specific texts.

At HRC49, the Council adopted Universal Periodic Review (UPR) country reports from the Council's 40th UPR session (UPR40). Access Now, with the support of our civil society partners, submitted five digital rights-focused stakeholder submissions on South Sudan, Syria (including our participation in the UPR Info Pre-Session on Syria), Uganda, Venezuela, and Zimbabwe, ahead of UPR40. We also submitted a stakeholder report on Sudan whose UPR was postponed from the 39th session to UPR40. We welcome more State recommendations addressing the impact of human rights online as well offline. In light of our recommendations, we particularly appreciated **Lithuania's** recommendation to Sudan to *"investigate the physical and digital attacks against, and the harassment of journalists, media workers and human rights defenders, and ensure freedom of expression*" and **Canada's** recommendation to Uganda to *"respect freedom of expression online, including by ending the practice of enforcing internet shutdowns and taxing the use of social media*."

Overall, we anticipate that the Council will advance more international norms and laws regarding internet shutdowns at the upcoming 50th session. The U.N. High Commissioner for Human Rights will issue her highly anticipated report on internet shutdowns pursuant to the Council's 2021 resolution on "The promotion and protection of human rights and the internet" (A/HRC/RES/47/16). The advancements on internet shutdowns at HRC49, particularly in urgent discussions regarding human rights, clearly signify the intrinsic link between on and offline human rights violations in humanitarian crises and beyond.

At HRC49, Ukraine and others presented a new resolution on the "Role of states in countering the negative **impact of disinformation on the enjoyment and realization of human rights**" (A/HRC/49/L.31/Rev.1) which was adopted by consensus. The resolution included strong *preambular* language on internet shutdowns and censorship as well as more references to disinformation in the digital age. We support this resolution's human rights-based approach to addressing disinformation. This is the first HRC-led resolution on state actions to counter disinformation and is situated in broader U.N. efforts to address the issue, including the Pakistan-led disinformation resolution (A/RES/76/227)

first presented at the General Assembly's Third Committee in September 2021, as well as reports from U.N. experts (see e.g. A/HRC/47/25). Indeed, the issue of disinformation is gaining increased government action, particularly regarding the Ukraine crisis. On March 2, Canada, as 2022 chair of the Freedom Online Coalition (FOC), issued a call to action on the state-sponsored disinformation in Ukraine. Endorsed by 19 other FOC Members, the statement calls for the cessation of conducting and sponsoring disinformation campaigns, the end of internet shutdowns, and for states to refrain from content restrictions that violate international human rights law.

Two years amid the COVID-19 pandemic and meaningful **civil society access to U.N. processes** remains a systemic hurdle, particularly at the New York headquarters. The AHC on Cybercrime's 1st session in New York was no exception. Ahead of the 1st session, Access Now – along with over 125 civil society organizations and academics – sent a letter to Members of the U.N. AHC on Cybercrime to ensure that its work includes meaningful civil society participation, and that any proposed convention on cybercrime incorporates clear and robust human rights safeguards. While civil society organizations, Access Now included, had the opportunity to participate –- solely through virtual means – and present and defend their positions, U.N. Member States and the U.N. must do more to ensure that in adapting work to social distancing measures during the pandemic, they do not limit the meaningful inclusion of civil society voices in U.N. discussions. Strictly virtual participation for civil society cannot be the default. This is why Access Now strongly supports State-led initiatives, such as **Denmark** and **Costa Rica's** #UNMute campaign, which has reiterated calls for meaningful civil society access at the General Assembly, Human Rights Council, and important U.N. events, such as the U.N. Climate Change Conference in Glasgow (COP26) and the 66th session of the Commission on the Status of Women (CSW66).

Recommendations to U.N. Member States:

- ➔ Continue to condemn internet shutdowns particularly through country specific statements, issued during multilateral sessions;
- ➔ Bring awareness and attention to the impact of internet shutdowns on civil and political rights, and increase awareness and attention of such human rights violations on economic, social and cultural rights, particularly linking to the broader achievement of U.N. Sustainable Development Goals and the 2030 Agenda through the Broadband Commission and High-level Political Forum on Sustainable Development (HLPF) studies;
- ➔ Raise internet shutdowns in overseas development aid screening processes. Specifically, incorporate internet shutdowns into development aid monitoring indicators;
- ➔ The UPR is an important U.N. process aimed to address human rights issues worldwide. Yet the impact of human rights in the digital age – particularly the right to privacy – is largely lagging in this U.N. process. Since it is clear that human rights violations online enable and escalate offline violence, we therefore recommend that more States prioritize and make explicit recommendations regarding the impact of human rights in the digital age to States under review during the UPR process;
- ➔ Civil society has important technological and human rights expertise to meaningfully contribute to U.N. discussions. U.N. Member States should strongly advocate for meaningful civil society access

and participation by focusing on principles of transparency, timeliness, equity, diversity, and ensuring secure accommodation for virtual, hybrid, and in-person participation.

II. SURVEILLANCE OF HUMAN RIGHTS DEFENDERS, PARTICULARLY WOMEN HUMAN RIGHTS DEFENDERS

The arbitrary or unlawful use of surveillance technologies violates human rights and causes real-world harm. The rampant abuse and culture of impunity surrounding this technology also contravenes well-established international norms. We welcome the more dominant focus on surveillance of human rights defenders (HRDs) – particularly women human rights defenders (WHRDs), as the Council session overlaps with the annual March 8 International Women's Day. In this section we cover the side events and resolutions at HRC49 that yielded important developments on surveillance of human rights defenders, acknowledging the long-needed and important gender dimensions that rightfully took the spotlight this session.

The impact of targeted surveillance on women can be particularly grievous, given that cultural, political, societal, economic, and gender power asymmetries often grant authorities opportunities to weaponize the information they extract through defamation, blackmail, and doxxing. This can include the publishing of private and intimate photos and conversations online. The U.N. General Assembly has defined violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life." This includes "physical, sexual and psychological violence perpetrated or condoned by the State, wherever it occurs"-- including online.

Overall, hacking stifles the exercise of a range of fundamental rights by creating a chilling effect on speech and democratic participation. For women targets, digital surveillance is a ticking bomb. They live in fear of how their personal information, including private photos, videos, and conversations, could be used against them at any given point, opening the door for harassment and abuse. This is especially worrying in regions, such as MENA, where governments have routinely used doxxing of women and LGBTQ+ activists in order to smear and intimidate them into silence.

On 15 March, Access Now's Marwa Fatafta spoke on a panel for the virtual side event *Digital Security Threats Facing HRDs/WHRDs in the MENA Region.* The event was organized in partnership with the Gulf Center for Human Rights, Front Line Defenders, and the U.N. Special Rapporteur on human rights defenders. The speakers highlighted the myriad threats HRDs face online, especially the impact of unlawful surveillance of women activists and HRDs. Civil society organizations urged U.N. Member States to initiate immediate and impartial investigations into the use of surveillance technologies to target and monitor activists.

On 29 March, Access Now, together with the United States (U.S.) and the European Union Trade and Technology Council (U.S.-E.U. TTC) Partnership, held *Protecting Defenders Online*, a virtual side event at HRC49. The event highlighted threats faced by WHRDs online, best practices for governments to counter these threats, and civil society recommendations for the U.N., the U.S., and the E.U. to consider. The U.S. Acting Assistant Secretary Lisa Peterson and the E.U. Special Representative for Human Rights Eamon Gilmore sent a united message "to HRDs and those who threaten them that the U.S. and the E.U. prioritize this issue within the TTC and will work together to bring this to the forefront of [their] foreign policy and advocate for proper accountability." Remarkably, Ambassador Catalina Devandas, Permanent Representative of Costa Rica to the United Nations in Geneva, became **the first State representative to publicly call for the "immediate moratorium on the use of spyware technology until a regulatory framework that protects human rights is implemented."** The call from Ambassador Devandas comes at a moment when most of the momentum demanding accountability for the use of Pegasus spyware is driven by civil society and international organizations, while governments remain largely silent, despite regularly reported new confirmed cases of infection. Costa Rica's pressing call for a moratorium on spyware should be seen as an **invitation for other States to publicly reject** the dangerous technology, and place a hold on buying and using tools that have proved to facilitate human rights violations.

Norway continued to lead its resolution on HRDs at HRC49. This year, the resolution (A/HRC/49/L.9) focused on "Recognizing the contribution of human rights defenders, including women human rights defenders, in conflict and post-conflict situations, to the enjoyment and realization of human rights." Given the timely focus of the resolution, civil society organizations, Access Now included, sent an Open Letter calling on U.N. Member States to ensure that the resolution adopted by the Council incorporates strong language on important issues. We particularly advocated to regulate surveillance tools to ensure that such tools are not used to violate human rights, and to refrain from shutting down the internet. The resolution, which was adopted by a vote on the account of Russia – 39 in favour, 0 against, 8 abstentions – nonetheless contains important *operational* paragraphs calling on States to refrain from internet shutdowns, "including interference with the use of technologies, such as encryptions [*sic*] and anonymity tools" (OP 8(h)) and to refrain from "the use of surveillance technologies against human rights defenders, including through hacking" (OP 8(g)).

Recommendations to U.N. Member States:

- ➔ Join existing State-led initiatives, including the multilateral "Export Controls and Human Rights Initiative"" to take spyware threats seriously;
- ➔ Join efforts led by States, such as Costa Rica, to place an immediate moratorium on the use, sale, and transfer of surveillance technologies produced by private firms until adequate human rights safeguards and regulation is in place. To support this transition, Access Now and other civil society organizations have developed 13 Principles to guide law enforcement and policymakers in ensuring respect for human rights in surveillance activities;
- ➔ Advance international norms to recognize unlawful or arbitrary surveillance as a form of violence against women;

- ➔ Establish an independent mechanism with oversight of companies selling spyware to monitor and investigate their use and ensure that use is consistent with human rights;
- ➔ Adopt legislation and implement regulations that mandate transparency and strict human rights due diligence on the sale, transfer, and use of surveillance technologies, including on outcomes. Such studies should be conducted before the sale or transfer and throughout any partnerships with other companies and/or governments, include liability for harms which are not properly prevented; Ensure that any legislation that is adopted to regulate surveillance technology companies is developed in consultation with human rights defenders who have been impacted by surveillance technologies.

III. BIOMETRIC DATA AND DIGITAL IDENTITY

Biometric identifiers, including fingerprints, iris scans, and facial geometry, have become increasingly popular as a means of enrolling individuals into systems, including digital identity systems, and then authenticating users. Biometric data is vulnerable to hacking just like other authentication methods. However, unlike a password, biometric indicators cannot simply be reset or changed as needed. This poses a higher security risk, since it becomes increasingly difficult to repair the damage done by leaks or hacks of biometric data, and thus restore sanctity to biometric-based systems. This section highlights some developments at HRC49 regarding two forms of interference with the right to privacy in the digital age (1) the use of biometric technologies and (2) digital identity programs.

The previously mentioned E.U.-led Myanmar resolution (A/HRC/49/L.12) contains notably important language on the right to privacy while drawing on issues such as hacking, surveillance, collecting personal data, and the use of biometric technologies. The resolution specifically calls for the protection of human rights, including the right to privacy and "*halting all measures to implement online surveillance systems, including unlawful or arbitrary interception of communications, unlawful or arbitrary collection of personal data, unlawful or arbitrary hacking and the unlawful or arbitrary use of biometric technologies*," and repealing or reforming numerous laws in accordance with international human rights standards (OP25). Such language aligns nicely with the Council's thematic resolution on the "Right to privacy in the digital age" presented during the Council's 48th session (A/HRC/RES/48/4).

On March 10, the U.N. Special Rapporteur on the right to privacy, Dr. Ana Brian Nougrères, presented her report (A/HRC/49/55) to the Council. The report, titled *Privacy and personal data protection in Ibero-America: A step towards globalization*, focused on privacy and data protection in Ibero-America as a framework towards *global* principles of privacy and data protection. Given the Rapporteur's lack of meaningful engagement with civil society thus far, we prioritized delivering an oral statement (1:07:53) during the Rapporteur's interactive dialogue. We specifically drew attention to the two forms of interference with the right to privacy in the digital age: (1) surveillance technology, including biometric surveillance technologies and (2) ill-considered, badly designed, and poorly implemented digital identity programs. Such calls are echoed in our broader #WhyID campaign, where we urge leaders of international development banks, the U.N., international aid organisations, funding agencies, and

national governments to question the need for digital identity initiatives before pursuing such programs.

Recommendations to U.N. Member States:

- ➔ Clearly articulate the objectives, needs, and benefits of any digital ID programs and put sufficient safeguards in place to minimize the risks of human rights violations;
- ➔ The potential impact on human rights of all existing and potential digital identity programs must be independently evaluated. They must be checked for necessary safeguards and detailed audit reports must be made public, for scrutiny. If the necessary safeguards are not in place, the digital identity programs must be halted;
- ➔ Digital identity programs should not collect or use biometrics for the authentication of users, until it can be proven that such biometric authentication is completely safe, inclusive, not liable to error, and is the only method of authentication available for the purpose of the program.

IV. CYBERCRIME AND CYBERSECURITY

Access Now maintains that approaches to cybersecurity policy should be user-centric, systemic, and anchored in open and pluralistic processes. Cyberwarfare adversely impacts a range of human rights and cyber operations targeting journalists, civil society organizations, and HRDs are particularly alarming and should be prohibited in all circumstances. Individuals who work in defense of civil liberties, rights, and democracy are themselves a form of "critical infrastructure" that must be safeguarded as we enhance legal structures on cybercrime and cybersecurity; these defenders are often providing direct, essential services and advocating for the needs of the most vulnerable.

From February 28 through till March 11, the U.N. held its 1st session on the Ad Hoc Committee on Cybercrime in New York. The AHC commenced at a time where political tensions could not be higher; or trust in the international community to tackle such issues lower. Russia initiated this AHC process, but many States took to the mic to condemn its illegal invasion of Ukraine, and reject Russian proposals.

On March 1, we made an oral intervention (1:34:25) in the session on general debate in the AHC calling on delegates to advance a human-centric approach to cybersecurity, and combat cybercrime without harming human rights. The next day, on the margins of the AHC in New York, we moderated an active and engaged hybrid panel discussion titled: "What Future for International Cybercrime Cooperation?" organized by the #LetsTalkCyber initiative and EU Cyber Direct. The event"aimed to address critical issues that will shape the outcome of the process, facilitate dialogue between different stakeholders, and identify opportunities for them to provide input and support governments during the negotiations." Discussion centered on a human rights-based approach to cybercrime, capacity building – including on the EU commitment to African partners – and the role of sovereignty amidst the US-UK CLOUD Act and similar proposals that give states direct access to data held by private sector actors in foreign countries.

On March 24 and 25, the AHC flipped to the other side of the pond to Vienna where the U.N. hosted the 1st intersessional consultation on the AHC. Access Now addressed the AHC during the agenda Item 2: "Criminalization." Our message was three-fold. First, decisions around the approach and scope of criminalization in cybercrime legal frameworks have a direct bearing on human rights, particularly around potential criminalization of protected speech and legitimate online behavior. Second, international harmonization efforts must absorb the lessons around national practices, including on focusing on cyber-dependent crime versus cyber-enabled crime. Third, that criminalization efforts on cybercrime also need to help ensure that the cybersecurity community is enabled and not harmed, requiring a sharper focus on "intent" and other related standards when addressing unauthorized access to ICT systems and networks. We followed this with a submission to the AHC in April to aid with the second substantive session, on the issues of criminalisation, procedural safeguards and law enforcement.

On March 24, we addressed the virtual dialogue meeting convened by Ambassador Gaffoor, the Chair of the U.N. Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies. We stressed that the OEWG would benefit from hearing from humanitarian actors, human rights defenders, and the digital security community that assists civil society around the new threat actors and cyber disruptive activity they have faced as 2022 has advanced, illustrated by the cyber attack targeting the ICRC. We suggested that the OEWG should hold a focused discussion on the topic of the current status of cyber threats to humanitarian actors and human rights defenders. We also brought the OEWG's attention to the uptake in cyber mercenary and cyber attack for hire operators, and recommended that the OEWG act upon the specific recommendations made by OHCHR expert group on Mercenaries in its October 2021 report (A/76/151), which had asked the OEWG to further address human rights concerns arising from the involvement of mercenaries and related actors in cyberoperations.

Recommendations to U.N. Member States:

- ➔ Act to embed human rights at the core of any international legal framework on cybercrime;
- ➔ Encryption and secure communications tools play a key role in deterring unauthorized access to communications and data, and preventing crime. Any new initiative should be guided by the May 2015 report of the former U.N. Special Rapporteur on Freedom of Opinion and Expression (A/HRC/29/32);
- ➔ Authorities must not create hostile environments for those who speak up with concerns about information security; specifically, they must seek to not persecute, discredit, or defame individuals who express their concerns about computer systems, security mechanisms, databases, and other related tools. We must ensure that we create clear requirements around "intent" when criminalizing unauthorized access, and that national laws across all agreeing states require a heightened intent requirement that is beyond mere knowledge in cases of unauthorized access to computer systems or databases;
- ➔ Data sharing initiatives must adhere to principles of dual-criminality, proceed in writing under standard protocols, and raise, not lower, protections against arbitrary or unlawful interference;

- ➔ International efforts to harmonize approaches to cybercrime must therefore seek to avoid including content or speech related provisions, and focus on a global consensus approach to cyber-dependent crimes. International cooperation measures are crucial, but can also have the danger of impacting privacy and other fundamental human rights.
- ➔ International discussions around cybersecurity and responsible state behaviour must hear from humanitarian actors, human rights defenders, and the digital security community that assists civil society around the new threat actors and heightened cyber disruptive activity they have faced in 2022;
- ➔ The U.N. Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies must address human rights concerns arising from the involvement of mercenaries and related actors in cyberoperations.

Whether in Ukraine or Myanmar, the openness and security of digital spaces matters for human rights. Access Now engages in bilateral discussions and advocacy campaigns regarding the impact of state sanctions on digital rights (see also our recent submission to the U.N. Special Rapporteur on Freedom of Association and of Assembly). **Sanctions** have become a primary measure taken in response to Russia's war on Ukraine. While the U.N. has not yet issued binding sanctions in this conflict, its forums and committees have served as flash points in diplomatic arguments. More quietly, research continues into the impact of sanctions on human rights, and the specific harms caused by "overcompliance." Access Now submitted to an upcoming report on "secondary sanctions, civil and criminal penalties for circumvention of sanctions regimes, and over-compliance with sanctions" while states answered a survey on "Unilateral sanctions in the cyber world." We look forward to using the findings to advance digital rights and reduce corporate overcompliance with state sanctions in ways that leave users unconnected and vulnerable online.

As we look ahead to the next session of the HRC, we hope to help bring more civil society voices to the U.N. Now, more than ever, world leaders must hear directly from those impacted by the weaponization of the internet against people targeted for persecution, discrimination, human rights abuses, ethnic cleansing, and other atrocities. We hope you join us in advocating for this openness, and help us build a more powerful platform for civil society worldwide.

April 2022

Access Now 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 contact:

Peter Micek | General Counsel and U.N. Advocacy Manager | peter@accessnow.org |

Laura O'Brien | Senior U.N. Advocacy Officer | laura@accessnow.org |