SPECIAL COMPETITIVE STUDIES PROJECT

FOREIGN POLICY

Interim Panel Report

December 2022

Contributors

SCSP LEADERSHIP

Dr. Eric Schmidt, Chair
Ylli Bajraktari, President & CEO

BOARD OF ADVISORS

Michèle Flournoy
Dr. Nadia Schadlow
William “Mac” Thornberry III
Robert O. Work

FOREIGN POLICY PANEL

Jafer Ahmad, Director
Hina Gir, Director
Isabelle Kern, Research Assistant
Channing Lee, Research Assistant
Lauren Naniche, Associate Director
Joe Wang, Senior Director

Special Thanks to Steve Feldstein, Zaid Zaid, Jaclyn Kerr, Chris Riley, Paul Lekas, Adam Deutsch, Alissa Starzack, Adrian Shahbaz, and Eli Sugarman.

The Foreign Policy Panel Interim Panel Report (IPR) is the fifth of six interim reports from the overall work that the Special Competitive Studies Project (SCSP) has conducted over the past year and that was summarized in our Mid-Decade Challenges to National Competitiveness report published on 12 September 2022. This report benefited greatly from insights and expertise by a number of individuals to whom we are deeply grateful. It aims to reflect many, though not all, of those insights. It was prepared by SCSP staff and, as such, it is not a consensus document of all the experts who assisted.

FOREIGN POLICY PANEL INTERIM PANEL REPORT

Defending Digital Freedom and the Competition for the Future of the Global Order

Framing

The United States could lose the digital future in two ways. The first would be to standby as the world's digital infrastructure and future technology platforms are built and dominated by authoritarian regimes led by the People's Republic of China (PRC). The second would be if the rest of the world, democratic and non-democratic alike, loses confidence in a digital future anchored in the principles of free speech, the protection of human rights, and the right to privacy, and instead drifts toward authoritarianism by a series of choices individual states make within their borders. In either case, the world becomes inhospitable to the interests of the United States and our allies and partners, bad for our businesses, and hostile to democratic values.

Against this backdrop, threats to digital freedom are growing around the world, and these alarming trends merit a concerted U.S.-led effort to reverse their course. Faith in the open Internet, and the potential for a globally connected world to empower individual liberty and promote economic prosperity, is wilting even in democracies. Authoritarian regimes are expanding their ability and willingness to harness new technologies and digital networks to exert control over their populations and interfere in the affairs of other nations.

Digital Freedom

The Declaration for the Future of the Internet (DFI)[1] and its more than 60 government signatories outline a vision of digital freedom comprised of a digital world that remains "open, free, global, interoperable, reliable, and secure" and includes the defense of core principles:

- the protection and advancement of human rights and fundamental freedoms of all people,
- a global Internet free from government-imposed shutdowns and censorship that allows for the free flow of data with trust,
- inclusive and affordable connectivity so that all people can benefit from the digital economy,
- trust in the global digital ecosystem, including through data privacy, and
- the multi-stakeholder approach to governance that keeps the Internet running for the benefit of all.

Nevertheless, opportunities exist to reverse the momentum. Recent protests in China and Iran are vivid reminders that citizens on the ground can still mobilize and communicate, even in closed information environments and in spite of powerful digital surveillance – often with assistance of circumvention technologies. In Ukraine, the government, civil society, and international partners provide a new model of how to defend against external attacks and affirm the power of an interconnected digital democracy. Around the world, advocates for digital freedom led by international and local civil society groups have made progress over the past year in pushing back on specific cases of politically motivated efforts to stifle digital freedom.[2] As the digital rights agenda intersects with wider strategic

[1] Declaration for the Future of the Internet, U.S. Department of State (2022).

[2] Civil society groups have succeeded in reversing the decline in some instances relying on a combination of litigation, research, and advocacy. See Adrian Shahbaz, et al., Countering an Authoritarian Overhaul of the Internet, Freedom House (2022).

considerations in all of these scenarios, more needs to be done to seize on and learn from these efforts.

This paper lays out the strategic stakes for digital freedom and offers initial recommendations for how the United States and like-minded partners can move from principles to action. It makes the case that digital freedom is a strategic technology priority for the United States, and highlights the need for the public sector and private sector to align their actions to advance shared interests on these issues. It recommends that the United States Government (USG) integrate digital freedom into a broader strategic framework to leverage a wider array of national tools to support digital freedom priorities, as well as reinforce the importance of a multi-stakeholder approach to coordinate action. To support these efforts, the paper also offers a notional "digital freedom playbook" for governments, information and communications technology (ICT)[3] companies, and civil society organizations (CSOs) that 1) lays out lessons learned from Russia's invasion of Ukraine, and how the effort to preserve Ukraine's sovereignty went hand-in-hand with the digital freedom agenda, and 2) provides recommended best practices for tackling increasingly frequent threats to digital freedom from governments within their national borders.

This paper does not address the full range of digital freedom issues and challenges.[4] It is an initial foray into a larger agenda to tackle a key element of the technology competition between open, democratic societies and closed, authoritarian systems – namely how the USG and like-minded partners can push back against digital repression and defend a digital world that remains to the largest extent possible "open, free, global, interoperable, reliable, and secure."[5]

The Strategic Stakes. Threats to digital freedom are a central arena in a larger strategic competition between the United States and the PRC. They underscore a hardening fault line in the contest between open societies and closed, autocratic systems. The global technology competition is a values competition, and ensuring that the United States and like-minded partners can refine a strategy, rooted in our values, to meet the escalating digital challenges the democratic world faces is a necessary and immediate first step.

The PRC represents a pole and catalyst for the most alarming trends. The PRC – and other closed systems – see the digital free flow of information and digital freedom as threats to their hold on power. An alternative vision to digital freedom,[6] predicated on control, is a core element of its

[3] For the purposes of this paper, we use "ICT" to encompass all technologies, from telecommunications equipment to software and digital platforms, that when combined allow for people to interact in the digital world.
[4] Including, for example, government surveillance; the PRC's, and other governments', export of digital infrastructure and tools of digital repression; and government-led physical and cyber attacks against digital activists.
[5] Declaration for the Future of the Internet, U.S. Department of State (2022).
[6] In a new white paper released on November 7, 2022, the PRC laid out its vision for a shared global future in cyberspace. It paints a world in which 1) nations possess "cyber sovereignty" rather than allowing a free and open Internet that transcends borders, 2) BRI countries cooperate with the PRC on cybersecurity through its Digital Silk

strategy to reshape and lead a new global order, alongside its plans to dominate the commanding heights of the techno-industrial economy.[7] It has created a parallel digital reality behind its Great Firewall that stands antithetical to nearly all aspects of digital freedom. It has a strategy to expand control over the world's digital infrastructure and export its tools of digital repression.[8] It promotes a vision of "cyber sovereignty"[9] that increasingly resonates with governments around the world. It provides the ideological justification for "splinternets" and more government intrusion in the digital sphere.[10]

Physical domination of the world's digital infrastructure is only one way that the PRC can reshape the global order.[11] If other governments embrace its tactics and espouse its ideological logic, they will drift into the PRC orbit. Governments across the political spectrum, including key swing states – those nations that do not seek to be locked-in to either U.S. or PRC technology or ideology – and some U.S. allies and democracies, are weighing how to similarly assert greater control over the digital sphere as they confront challenges in dealing with political polarization, data security, and the market power and role in their societies of ICT companies. They are drifting, however, from a balanced effort to address legitimate dilemmas to more draconian measures, resulting in an information dark age and the curtailing of basic freedoms.[12] They are resorting to a range of disruptions to connectivity, like Internet shutdowns and blocking access to websites, social media, and messaging platforms; censoring online content; surveilling their populations online; permitting, if not spreading, disinformation online; using legal threats and political pressure against ICT companies and their employees;[13] and/or compelling access to data without

Road, and 3) China participates actively in the UN process of cyberspace governance. Jointly Build a Community with a Shared Future in Cyberspace, The State Council Information Office of the People's Republic of China (2022).

[7] For further discussion, see Restoring the Sources of Techno-Economic Advantage, Special Competitive Studies Project (2022).

[8] Alina Polyakova & Chris Meserole, Exporting Digital Authoritarianism: The Russian and Chinese Models, Brookings (2019) ("Beijing's efforts to influence the global governance of cyberspace are organized around the concept of cyber (or internet) sovereignty.").

[9] Adam Segal, An Emerging China-Centric Order: China's Vision for a New World Order in Practice: China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace, National Bureau of Asian Research at 86 (2020).

[10] Each nation has a slightly different approach to establishing "cyber sovereignty," but co-option of Internet service providers or digital platforms is a common feature. Adam Segal & Gordon Goldstein, Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet, Council on Foreign Relations (2022).

[11] In addition to foundational digital infrastructure, the digital platforms and applications, or the rules by which they operate, matter in advancing or suppressing digital freedom. As one example, platforms and applications provide a proverbial second bite at the apple in terms of data collection that feeds surveillance. See Garrett O'Brien, BGI Shakes Up Sequencing, The Wire China (2022) (discussing these concerns around PRC-based genomic sequencing firm BGI).

[12] Freedom on the Net 2021: The Global Drive to Control Big Tech, Freedom House (2021).

[13] Steven Feldstein, Government Internet Shutdowns are Changing. How Should Citizens and Democracies Respond?, Carnegie Endowment for International Peace (2022); Adrian Shahbaz, et al., Countering an Authoritarian Overhaul of the Internet, Freedom House (2022); #KeepitOn: The Return of Digital Authoritarianism, Access Now (2022); Elissa Miller, Egypt Leads the Pack in Internet Censorship Across the Middle East, Atlantic Council (2018); Justin Sherman, Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior, Atlantic Council (2021); Eli Sugarman, The Russian and Chinese Governments' Threats to the Internet As We Know It, The Atlantic (2012); Wafa Ben-Hassine, #EgyptCensors: Evidence of Recent Censorship Events in Egypt, Access Now (2017).

reasonable due process[14] – often to suit political ends at odds with human rights and digital freedom.

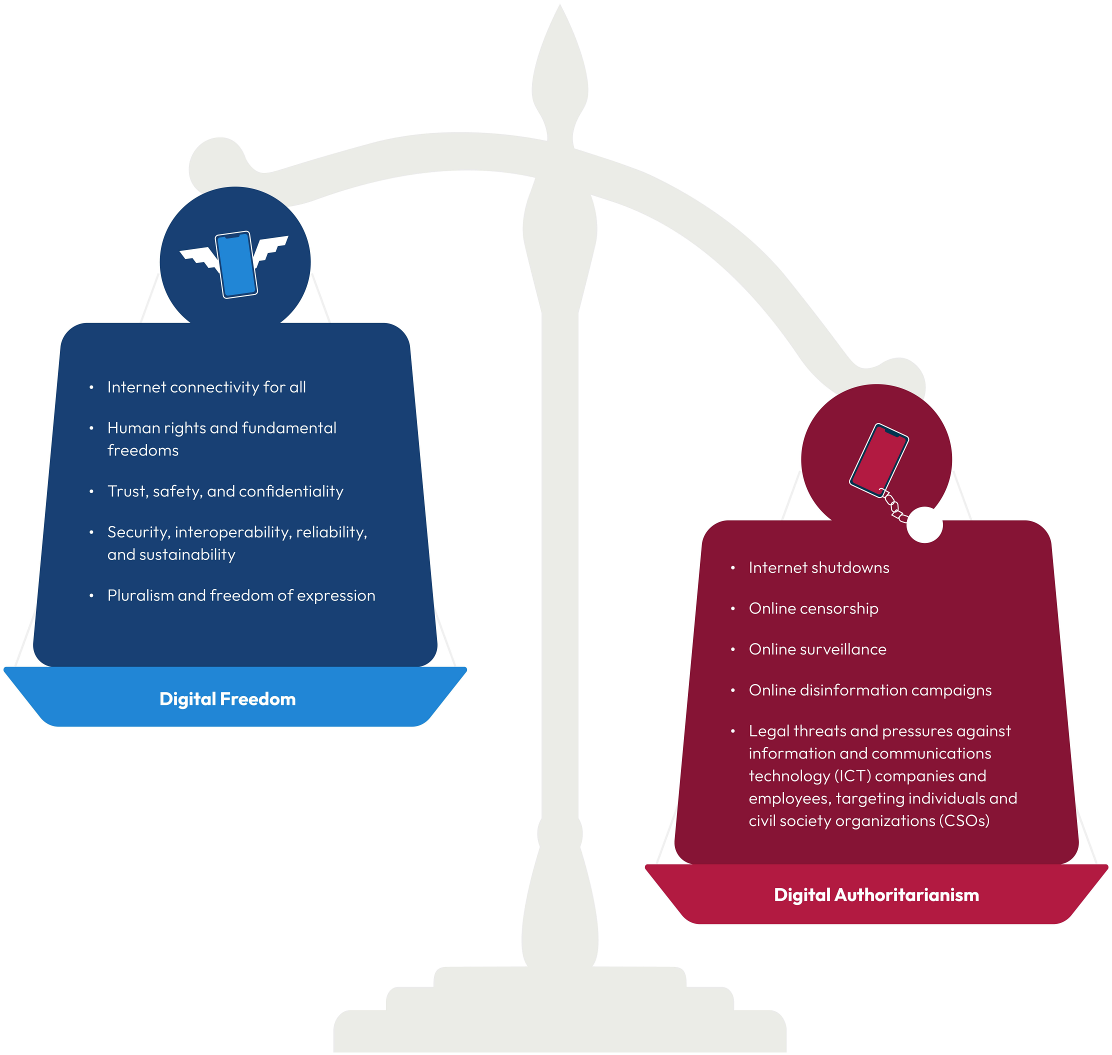
A future where these trends continue would threaten U.S. interests and those of people around the world. Instead of a free and open Internet connecting peoples, economies, and ideas around the world, the digital world would become splinternets with controls and firewalls that block flows of information and data deemed to be threatening to a government. At its extreme, a further fracturing of the digital world could reverse decades of U.S. and other like-minded partners' efforts to build a rules-based, open international order. Nations would retrench behind their firewalls with protectionist digital policies, curtail parts of the data-driven global economy, and "cleanse" their information environments of outside information. A future where every nation sets its own rules around narrow national interests evokes earlier eras of history when pure power governed global relations – we already see signs of this today with Russia's invasion of Ukraine. Such a world is in no one's interest, not even the PRC's.

The defense of digital freedom – and supporting those trying to uphold it – is a necessary element of a foreign policy for the United States, and like-minded partners, to meet the authoritarian challenge and prevent the return of pure power politics. As discussed in chapter four of SCSP's September 2022 report, Mid-Decade Challenges to National Competitiveness, on restoring U.S. global leadership in an age of technology competition, the United States must reaffirm what it stands for, realign its tools of statecraft to better meet the technology-driven opportunities and challenges it faces globally, and, ultimately, defend and promote a democratic, technology-enabled future where open societies are secure, prosperous, and free.[15] Governments resorting to repression – digital or physical – will only change their behavior if those committed to defending digital freedom can credibly link digital freedom concerns to incentives and penalties – economic, political, technological, and strategic.

[14] For instance, PRC law states that "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law." Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), DigiChina at art. 28 (2017). Article 7 of the National Intelligence Law of the People's Republic of China (2017) states that "Any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work." William Evanina, Keynote Remarks as Prepared for Delivery at International Legal Technology Association (ILTA) LegalSEC Summit 2019, U.S. Office of the Director of National Intelligence (2019). Companies based or operating in the PRC possess nominal rights and recourse under these laws. See Samm Sacks, Data Security and U.S.-China Tech Entanglement, Lawfare (2020). However, the robustness of those protections is suspect by the standards of liberal democracies. President Xi Jinping has expressly rejected "the path of Western 'constitutionalism,' 'separation of powers,' or 'judicial independence,'" hollowing essential judicial checks on state power to ensure due process. Charlotte Gao, Xi: China Must Never Adopt Constitutionalism, Separation of Powers, or Judicial Independence, Diplomat (2019) (quoting a 2019 article written by Xi in the CCP journal *Quishi*). Furthermore, despite the PRC's own constitution and commitments under ratified treaties, the PRC has continued "summarily and indefinitely detaining individuals without due process" in its campaign in Xinjiang. Giavanna O'Connell, How China is Violating Human Rights Treaties and its own Constitution in Xinjiang, Just Security (2020).

[15] Mid-Decade Challenges to National Competitiveness, Special Competitive Studies Project at 98 (2022).

Repressive Governments Are Tipping the Scale Toward Digital Authoritarianism



- Internet connectivity for all
- Human rights and fundamental freedoms
- Trust, safety, and confidentiality
- Security, interoperability, reliability, and sustainability
- Pluralism and freedom of expression

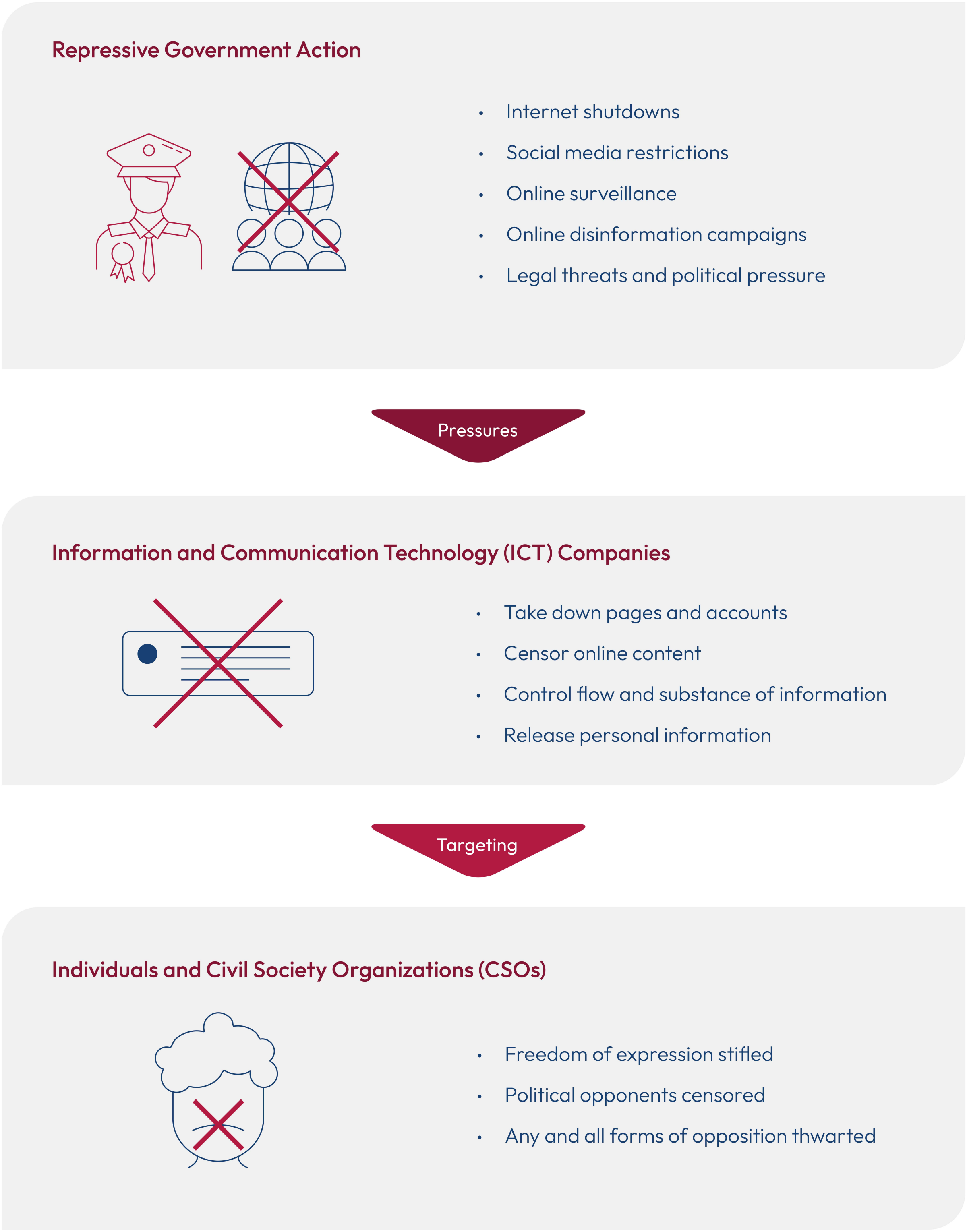
Digital Freedom

- Internet shutdowns
- Online censorship
- Online surveillance
- Online disinformation campaigns
- Legal threats and pressures against information and communications technology (ICT) companies and employees, targeting individuals and civil society organizations (CSOs)

Digital Authoritarianism

ICT Companies are Looking for Direction and Support in the Face of Asymmetric Government Pressure. Shifting roles between the public and private sectors lie at the center of global technology competition. The private sector has far outpaced the public sector – particularly in the United States – in technology innovation, adoption, and use. This has created an environment where responsibilities that were once generally considered to be the remit of government — such as defining the limits of free expression — are now shared with technology companies. While this was a democratizing feature of the Internet revolution that had inspired hope for a world with greater freedom, it has given way to the alarming trend of repressive governments seizing on ICT companies and the digital platforms they have created as conduits to channel repression.

How Repressive Government Action Targets Individuals and Civil Society Organizations



Repressive Government Action

- Internet shutdowns
- Social media restrictions
- Online surveillance
- Online disinformation campaigns
- Legal threats and political pressure

Pressures

Information and Communication Technology (ICT) Companies

- Take down pages and accounts
- Censor online content
- Control flow and substance of information
- Release personal information

Targeting

Individuals and Civil Society Organizations (CSOs)

- Freedom of expression stifled
- Political opponents censored
- Any and all forms of opposition thwarted

The power imbalance between ICT companies and repressive governments, which retain sovereign powers to regulate activities within their national borders, underpins a major difficulty of pushing back against repressive practices. While the ultimate targets for repression are individuals or groups in a country with repressive governments, ICT companies are frequently the ones that bear the brunt of government demands to censor content, block websites, handover data, and amplify pro-government messaging. Despite their global reach and wealth, even large multinational ICT companies are struggling to navigate between the dictates of governments and upholding digital freedom principles. Within the borders of any nation, that government's power will most often prevail.

The power asymmetry clarifies the chasm between championing larger digital freedom principles and trying to defend them in specific circumstances, and in so doing, illuminates the complex choices that companies face. ICT companies often face only unpalatable choices as they determine how to respond to demands from censorship to deplatforming, balancing commercial interests, company policies, employee safety, larger values-based commitments, and potentially conflicting regulatory regimes in places where they operate. Options for ICT companies to deal with repressive demands almost always require hard tradeoffs and rarely offer clear cut pathways. Even taking a seemingly clear moral stand by pulling out of a repressive environment creates its own greyzone, if doing so leaves the citizens with worse options for connectivity and creates an even more restrictive information environment.[16]

Many companies are looking for more consistent diplomatic support and guidance from democratic governments on how to respond to repressive dicates. Yet in such cases, the role of outside governments that espouse the democratic principles under attack can be limited, circumscribed by concerns about possible conflicts of interest in "defending" a private company or simply because digital freedom is not connected to a larger strategic agenda.[17] These dynamics need to change. Governments, ICT companies, CSOs, and others committed to digital freedom must act in closer coordination, guided by a larger strategic perspective and purpose.

[16] For example, consider the pushback telecommunications provider Telenor faced when it decided to sell off its operations in Myanmar, potentially ceding them to owners with ties to the country's military — a decision it made after weighing heavily the dilemma of complying with repressive local laws on one hand, and its values, international law, and human rights principles on the other. Jonathan Greig, Outrage over Telenor Myanmar Sale Grows as More Ties between Military and New Owner Revealed, ZDNet (2022).

[17] Part of the challenge is that while governments, ICT companies, and CSOs may be committed to defending digital freedom, each faces dilemmas in moving toward closer cooperation and aligning actions with each other. For the USG, rights-based arguments can be at odds with wider strategic priorities. Trying to intervene in support of a particular company may put the government in the position of being perceived to be giving that company preferential treatment. For ICT companies, aligning more closely with the USG (or any other government) risks undermining the independence of the private sector that is a hallmark of democracies and free markets, and inviting inaccurate narratives that they are instruments or extensions of the USG. For CSOs, dedicated to a non-governmental approach to advocating digital freedom, greater government involvement risks undermining that very model and creating a perception of CSOs being instruments of a foreign government. A further complicating issue for all three groups is the ongoing debate within the United States and like-minded governments on domestic technology governance issues like anticompetitive practices, the bounds of online speech, and data privacy.

Reaffirming Principles and Moving to Principled Action. The United States and many fellow democracies working with the multi-stakeholder community are trying to push back against digital repression by expanding the original Internet freedom agenda[18] into a wider vision of digital freedom. The *Declaration for the Future of the Internet* (DFI)[19] provides a valuable framework for an expanded set of digital freedom principles, helping inform the decisions that governments and ICT companies should make as they develop policies and respond to threats.

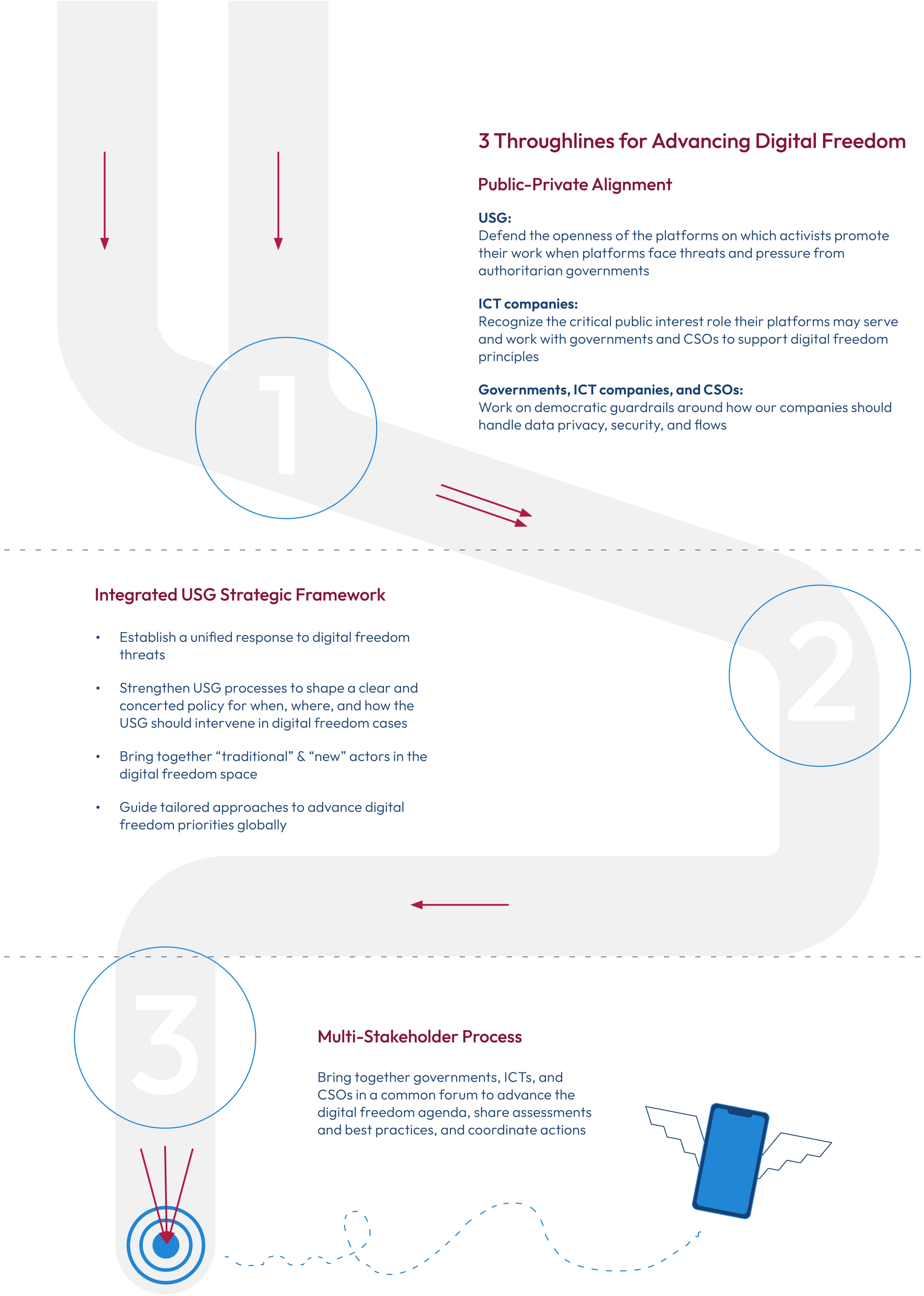
However, a statement of principles clarifies what is worth defending, not how it will be defended. Changing the calculations of governments that are considering taking repressive measures or have already done so will require more direct action by the USG and like-minded governments to support CSOs and ICT companies that promote digital freedom or serve as the platforms where threats to digital freedom occur.

Strategic Priorities

The United States and like-minded governments should properly frame digital freedom as a strategic priority within the global technology competition and align our national tools of statecraft to advance a vision of a world that protects individual rights, provides a level playing field for businesses, and defends nations against digital threats from foreign governments. Even as the United States continues an important domestic dialogue on technology governance and democratic guardrails, we cannot lose sight of the technology competition playing out internationally and the converging interests of like-minded governments, ICTs, and CSOs in defending a world anchored in basic principles of digital freedom.

To build on the success of ongoing government and civil society efforts and ensure commitments to principles translate into action, the key actors – the USG and like-minded governments, ICT companies, and CSOs – must find ways to work in concert. They must overcome their mutual weariness at cooperating too closely in order to overcome the power asymmetry between repressive governments and CSOs and ICT companies. In particular, the USG must take a stronger role in confronting foreign government-directed actions contrary to digital freedom — taken against ICT companies and CSOs — in order to counterbalance this asymmetry. In practice, that means situating digital freedom threats in a larger strategic context, adding more teeth to rhetorical support, and expanding coordination across like-minded governments, ICT companies, and CSOs to strengthen the response to authoritarian challenges. These begin with making three large organizational shifts.

[18] "[Across multiple presidential administrations], the United States has promoted what is broadly known as the "Internet freedom agenda." This mandate was both economic, calling for a relatively laissez faire approach to regulation, and political, promoting ideals of free speech on the Internet." Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet, Council on Foreign Relations at 19 (2022).
[19] Declaration for the Future of the Internet, U.S. Department of State (2022).



3 Throughlines for Advancing Digital Freedom

Public-Private Alignment

USG:
Defend the openness of the platforms on which activists promote their work when platforms face threats and pressure from authoritarian governments

ICT companies:
Recognize the critical public interest role their platforms may serve and work with governments and CSOs to support digital freedom principles

Governments, ICT companies, and CSOs:
Work on democratic guardrails around how our companies should handle data privacy, security, and flows

Integrated USG Strategic Framework

- Establish a unified response to digital freedom threats
- Strengthen USG processes to shape a clear and concerted policy for when, where, and how the USG should intervene in digital freedom cases
- Bring together “traditional” & “new” actors in the digital freedom space
- Guide tailored approaches to advance digital freedom priorities globally

Multi-Stakeholder Process

Bring together governments, ICTs, and CSOs in a common forum to advance the digital freedom agenda, share assessments and best practices, and coordinate actions

First, the global technology competition requires the United States to develop a new public-private alignment to advance its strategic technology priorities, including on digital freedom. The private sector is at the forefront of technological innovation, and this often puts it on the frontlines of the battle between digital freedom and digital repression. Just as the technology competition requires the USG to step up its role within a new geometry of innovation[20] and execute a techno-industrial strategy,[21] the USG cannot sit on the rhetorical sidelines when it comes to digital freedom.

- From a rights dimension, ICT companies are intertwined in digital freedom battles between repressive governments and civil society. They provide the platforms through which people around the world express themselves and connect to each other. Just as the USG endeavors to defend human rights activists facing threats around the world, the USG must also find a way to defend the openness of the platforms on which these activists rely. This is especially true when these platforms face threats and pressure from repressive governments.

- Conversely, as ICT companies recognize the critical public interest role their platforms serve, they must continue to work with receptive governments on how these platforms should support digital freedom principles. The USG and like-minded governments, ICT companies, and CSOs need to consider appropriate democratic guardrails for how companies handle data privacy, security, and flows without compromising their technological leadership.

- At the same time, digital freedom is about human rights *and* broader interests. Core digital freedom principles around inclusive connectivity and the free flow of information and data underpin the global digital economy. By expanding the aperture on digital freedom to also consider its intrinsic economic dimensions, we may unlock new tools of statecraft – such as leveraging trade policy – to advance the digital freedom agenda.

Second, the USG needs an integrated strategic framework to decide when, where, and how to respond to digital freedom threats as they happen and across the range of challenges from a Ukraine-like scenario to increasingly frequent repression like politically-motivated censorship. The purpose of the framework would be to nest digital freedom concerns within the wider strategic context and technology-related priorities, and to align USG-wide resources and capabilities to tackle specific threats in a consistent manner. USG responses to digital freedom

[20] See Harnessing the New Geometry of Innovation, Special Competitive Studies Project (2022).
[21] See Restoring the Sources of Techno-Economic Advantage, Special Competitive Studies Project (2022).

threats are often ad hoc or viewed narrowly through a human rights lens.[22] The USG needs to buttress rhetoric with consistent, balanced action.

- An institutionalized interagency process, led by the White House National Security Council, already exists to cover democracy and digital rights issues. Elevating this process to bring together "traditional" actors in the digital freedom space within democracy and human rights portfolios, with "new" interagency partners in trade, commercial promotion, sanctions, tech strategy, and regional portfolios, can better frame and integrate digital freedom into a larger strategic perspective, commensurate with the global technology competition. Appropriate senior points of contact should also be identified across the relevant departments and agencies to serve as focal points for coordinating intra- and interagency policy deliberation and action across this wider array of actors. This can then shape a clear and concerted policy for when, where, and how the USG should act in digital freedom cases.

- A strategic framework from such a White House-led process can then guide tailored approaches to advance digital freedom priorities bilaterally (and multilaterally if relevant), including down to country-level planning processes to prioritize funding and resource requests regarding digital freedom.

- A key aspect of a strategic framework must also be to build in alliance coordination across as many elements of the framework as possible, in order to bring in as many like-minded partners as possible to develop a shared perspective of the issues and build a greater toolkit for tackling shared challenges. Additionally, there must also be a process for engaging with allies and partners that may be trending against digital freedom principles, in order to persuade them to change course.

Third, digital freedom issues are inherently multi-stakeholder in nature, and thus need a multi-stakeholder approach to address challenges and opportunities as they arise. The multi-stakeholder digital freedom community should be a natural partner for the USG and like-minded governments to advance a digital freedom agenda, and vice versa. In addition to possessing technical and specialized expertise, ICTs and CSOs may also have deeper and wider roots in-country than the local U.S. diplomatic mission, which can be critical to informing effective policy action.

- Coordination across the multi-stakeholder community already occurs and should continue to inform and shape policy development. A sharper USG focus on digital freedom – guided by the aforementioned strategic framework – can strengthen the USG's engagement and

[22] Billy Perrigo, The Future of the Internet Is Under Greater Threat Than Ever Before—and Activists Say the U.S. Needs to Step In, Time (2021).

partnership with the multi-stakeholder community to undertake practical actions to advance digital freedom.

- A more robust multi-stakeholder approach could be achieved by building on existing fora – expanding their scope or membership – to bring together governments, ICT companies, and CSOs to cooperate on a comprehensive digital freedom agenda. For example, the Freedom Online Coalition (FOC) is an intergovernmental body that includes ICTs and CSOs in a non-member Advisory Network.[23] FOC task forces, such as the Task Force on Internet Shutdowns (TFIS), incorporate additional non-governmental partners as task force chairs,[24] but do not yet cover the full spectrum of threats to digital freedom. Additionally, the Global Network Initiative (GNI)[25] is an action-oriented convener for academics, civil society, ICT companies, and investors that engages with governments, but does not have governments as members.

A Digital Freedom Playbook

Connecting the three preceding throughlines, we offer an initial, notional "playbook" of best practices and practical actions the USG and like-minded governments, ICT companies, and CSOs can take individually and in coordination to counter threats to digital freedom. This playbook can serve as a point of departure for these stakeholder groups to discuss, refine, and use.

The playbook covers two categories of threats:

I. *Lessons learned from Ukraine for how nations should prepare to defend their digital ecosystems and preserve the core digital elements of democratic life when facing external aggression.* This section summarizes key steps the Ukrainian government, partner governments, ICT companies, and others took to safeguard digital freedom amidst conflict. While these steps can help prepare for major contingencies in the future, they are also applicable beyond the precipice of conflict and are valuable lessons-learned for digital freedom broadly.

II. *Recommended best practices for responding to a range of threats to digital freedom by governments seeking to assert control over ICTs and digital platforms, or otherwise leverage them to enable repression within their borders.* This section does not cover the

[23] Advisory Network, Freedom Online Coalition (last accessed 2022).
[24] Task Force on Internet Shutdowns (TFIS), Freedom Online Coalition (last accessed 2022).
[25] The Global Network Initiative is an alliance of Internet and telecom-munications companies, human rights and press freedom groups, investors, and academic institutions from around the world. GNI helps ICT companies respect freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content, or restrict communications. See Protecting And Advancing Freedom of Expression and Privacy in the ICT Sector, Global Network Initiative (last accessed 2022).

full scope of threats to digital freedom, but offers a series of possible responses that could apply to a wide range of scenarios.

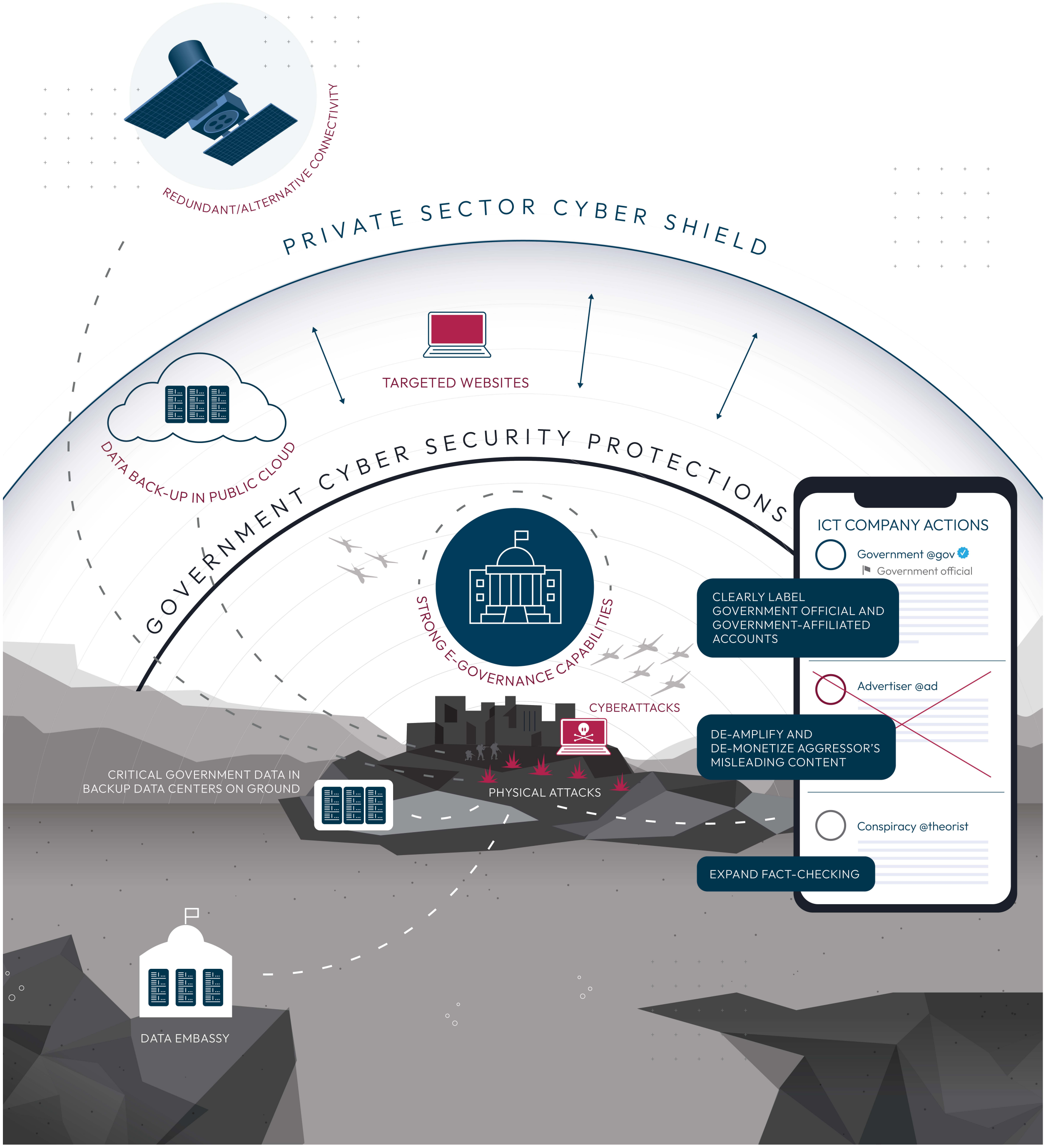
I. Lessons Learned from Ukraine: Protecting Nations' Digital Freedom from External Aggression

Russia's invasion of Ukraine has reframed the urgency and importance of many parts of the digital freedom agenda. As much as the invasion has reshaped the landscape of European security, this "first networked war"[26] has clarified the centrality of Internet connectivity to a nation's sovereignty; reminded the world of the potential of a tech-enabled democracy to provide basic government services; and demonstrated the central role of ICT companies in protecting against cyberthreats, providing platforms for digital services, and countering dangerous Russian-backed disinformation and cyber attacks. All of these are vital dimensions of how Ukraine is prevailing in a conflict against a vastly larger adversary and to sustain its democratic way of life. Conversely, the ability of ICT platforms to continue connecting people inside Russia and the outside world – with the support of digital freedom advocates – provides an essential two-way information lifeline that avoids an even worse case scenario of Russia becoming a nuclear superpower hermit state.

How the Ukrainian people and government, like-minded governments, ICT companies, and CSOs reacted and adapted to protect Ukraine's digital infrastructure and maintain digital connectivity, services, and ecosystems, consistent with digital freedom principles, offers important lessons for how other nations under threat can prepare and how the world can respond to another case of external aggression in the future. Equally importantly, the convergence of interests among democratic governments, digital freedom advocates, and private sector firms to support Ukraine against the Russian invasion offers an important model to reinforce the multi-stakeholder approach to address the spectrum of digital freedom threats that will define the immediate future.

[26] The First Networked War: Eric Schmidt's Ukraine Trip Report, Special Competitive Studies Project (2022).

Lessons Learned from Ukraine: Protecting Nations' Digital Freedom


REDUNDANT/ALTERNATIVE CONNECTIVITY
PRIVATE SECTOR CYBER SHIELD
TARGETED WEBSITES
DATA BACK-UP IN PUBLIC CLOUD
GOVERNMENT CYBER SECURITY PROTECTIONS
STRONG E-GOVERNANCE CAPABILITIES
CYBERATTACKS
PHYSICAL ATTACKS
CRITICAL GOVERNMENT DATA IN BACKUP DATA CENTERS ON GROUND
DATA EMBASSY
ICT COMPANY ACTIONS
Government @gov
Government official
CLEARLY LABEL GOVERNMENT OFFICIAL AND GOVERNMENT-AFFILIATED ACCOUNTS
Advertiser @ad
DE-AMPLIFY AND DE-MONETIZE AGGRESSOR'S MISLEADING CONTENT
Conspiracy @theorist
EXPAND FACT-CHECKING

1. *Ensure the digital continuity of states under threat, have an emergency plan to back up data in a crisis, and enable backup of government data outside of the area of conflict.* Up to a week prior to the Russian invasion, Ukrainian government services were running on servers located within government buildings. On February 17, Ukraine's Parliament amended its data protection law to permit government data to be transferred to the cloud, essentially allowing critical government data to be moved into data centers located outside of the nation.[27] This preserved the integrity of that data and the Ukrainian government's ability to operate and deliver basic services after the Russian invasion, even if Russia had destroyed the nerve centers of the government in Kyiv. As Ukrainian Deputy Prime Minister for Digital Transformation Mykhailo Fedorov said, "you can't destroy cloud with a missile."[28]

    ○ Nations and governments under threat, with the support of the USG, like-minded governments, and ICT companies, should ensure the digital continuity of the government under attack (or facing threat of attack) by enabling the secure backup of government and other critical data (e.g., financial data). This may require modifying existing national data protection and localization laws.

    ○ ICT companies should work with governments under threat to provide secure storage hardware to deliver data out of a threatened territory.[29]

    ○ Democratic governments should seriously weigh the downsides of data sovereignty requirements, especially when it comes to cooperation on cloud services. If a law similar to the currently debated proposals for digital sovereignty requirements[30] in the EU's Cybersecurity Certification Scheme for Cloud Services (EUCS)[31] had been in place in Ukraine prior to invasion, it would have prevented cloud service providers headquartered outside of Ukraine from being able to provide services that enabled the digital continuity of Ukraine's government. The USG should negotiate a way ahead with the EU to find a solution that enables U.S.-EU cooperation on cloud services, especially in times of crisis.

2. *Consider the practicality of establishing "data embassies."* A data embassy is a set of servers that store a nation's data in another nation's territory, while preserving sovereign

[27] Defending Ukraine – Early Lessons from the Cyber War, Microsoft (2022).
[28] Mykhailo Fedorov (@FedorovMykhailo), Twitter (Dec. 1, 2022, 6:23am).
[29] Amazon deployed teams with "Snowball" devices, ruggedized compute and storage hardware, to Ukraine to secure and transfer government data to the cloud. Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future, Amazon (2022).
[30] Vincent Voci, et al., The European Union's Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS): How "Sovereignty" Requirements Undermine Cybersecurity and Harm Transatlantic Ties, U.S. Chamber of Commerce (2022).
[31] EUCS – Cloud Services Scheme, European Union Agency for Cybersecurity (ENISA) (2020).

immunities and protections over that data — analogous to protections afforded to physical embassies.[32]

- Nations and governments under threat should consider establishing data embassies outside their territory as a precautionary measure. Such a mechanism would require establishing an international agreement and legal provisions, similar to those for the establishment of a physical embassy, to ensure appropriate access and security arrangements among involved government and private sector actors. Creating new alliance institutions – perhaps a "digital Vienna Convention" – can speed up the creation and management of data embassies across alliance members.

3. *Maintain connectivity with redundant and/or alternative connectivity, ideally in place before a conflict begins to help prevent or mitigate the effects of external attacks when they occur.*[33] After Russian forces destroyed Internet services in Ukraine, the United States, France, and Poland partially funded the deployment of thousands of SpaceX Starlink terminals to Ukraine to allow Ukrainians to access the Starlink network.[34]

   - The USG and like-minded governments, and ICT companies should continue to provide assistance around the world – prioritizing nations under threat – to support alternative means of maintaining Internet communications and connectivity. Such means can include: novel connection hardware[35] and "traditional" tools – like virtual private networks (VPNs), private servers, and mesh networks – that can enable connectivity, circumvent surveillance, and be incrementally deployed.

   - Funding should also be provided for training and education (via CSOs) around how to use those and other circumvention technologies for maintaining connectivity.

[32] Estonia set up the first ever data embassy in Luxembourg, in 2015. The data center is located in and protected by Luxembourg's technical capabilities and digital infrastructure, but remains under the control of the Estonian government. Estonia's agreement with Luxembourg could be a replicable model from a technical and legal standpoint. Data Embassy, e-Estonia (last accessed 2022).

[33] See e.g., Karina Tsui, Taiwan Has Publicly Announced It Is Considering Satellite-Based Alternatives, Washington Post (2022).

[34] Christiano Lima, U.S. Quietly Paying Millions to Send Starlink Terminals to Ukraine, Contrary to SpaceX Claims, Washington Post (2022).

[35] For example, novel connection hardware options could include high-speed internet via satellite constellation; hard-to-detect atmospheric laser communication terminals and a software platform for orchestrating networks across land, sea, air, and space; and/or a decentralized wireless telecom network with fifth-generation (5G) capabilities that enables users to share bandwidth from their personal Wi-Fi networks, at a range 200 times greater than standard Wi-Fi routers. Theresa Hitchens, Aalyria Envisions Communications Revolution for Earth, the Moon and Beyond, Breaking Defense (2022). The Future of Decentralized Wireless – Opportunities from 3G Shutdowns and 5G Alternatives, RCR Wireless News (2022). Cate Lawrence, Wow, There's an Actual Use for Blockchain? Helium Can Democratize Internet Connectivity, The Next Web (2021).

4. *Transfer public services online.* After the start of the invasion, Ukraine quickly transformed its digital public service platform, Diia,[36] into a comprehensive e-government platform. The platform uses government biometric authentication to access most public and banking services, including official identification (ID) documents such as passports, and taxes. It also facilitated centralized reporting of invading forces and casualties.[37]

   - The USG and like-minded governments should support the development and dissemination of e-government platforms, like that of Diia in Ukraine,[38] or the e-governance model implemented in Estonia,[39] to help transfer public services online for nations under threat.

   - ICT companies should also work with universities and academic institutions in nations under threat to support continuity of education services online.[40]

5. *Strengthen multi-stakeholder collaboration on cybersecurity capabilities of government, media, and other critical websites and services to protect the flow of essential information.* ICT companies hold the cybersecurity expertise and bandwidth to support foreign governments and local organizations in detecting, monitoring, and countering cyberattacks, sharing intelligence, and detecting malware signatures. In the case of Ukraine, for instance, ICT companies have provided free protection against distributed denial-of-service (DDoS) attacks for news sites and humanitarian organizations targeted by Russia.[41] A longer history of allied governments' cybersecurity support for the Ukrainian government was also crucial in preparing the Ukrainians to defend against cyberattacks.[42]

[36] Government Services Online, Diia (last accessed 2022).

[37] Lukasz Olejnik, Smartphones Blur the Line Between Civilian and Combatant, Wired (2022).

[38] Alexander Iosad & Oliver Large, State of Resilience: How Ukraine's Digital Government Is Supporting Its Citizens During the War, Tony Blair Institute for Global Change (2022).

[39] e-Estonia Guide, Enterprise Estonia (2020); Matt Reynolds, Welcome to E-stonia, the World's Most Digitally Advanced Society, Wired (2016).

[40] For example, in Ukraine, Amazon Web Services (AWS) helped expand remote learning opportunities and preserve students' research data. How Amazon is Assisting in Ukraine, Amazon (2022).

[41] Google's Project Shield provides free protection against DDoS attacks, and protects over 200 Ukrainian news and humanitarian organizations. Matt Brittin, Continuing to Support Ukrainians in Challenging Times, Google The Keyword (2022); Cloudflare's Project Galileo provides free protection against DDoS attacks, and protects Ukrainian news and humanitarian organizations. Since the onset of the Russian invasion of Ukraine, DDoS-mitigated traffic has reached as much as 10 percent of aggregate traffic, Project Galileo 8th Anniversary Report, Cloudflare Radar (2022).

[42] "It is likely that Ukraine, forewarned by Russian cyber actions that began as early as 2014, was better prepared as a result. It was also assisted in its cyber defense by friendly countries and private actors with whom it had developed cooperative relationships before the conflict. This preparation allowed it to deflect many Russian offensive cyber operations, suggesting that a well-prepared and energetic defense can have the advantage over offense in cyberspace." James A. Lewis, Cyber War and Ukraine, Center for Strategic and International Studies at 1 (2022).

- ○ ICT companies should continue to support and provide critical cybersecurity capabilities for nations and related groups and individuals under threat.

- ○ Reliance on pro bono services from the private sector cannot be expected in all circumstances, therefore the USG[43] and other like-minded governments[44] should continue to prioritize funding, training, and direct support to government partners in nations under threat to strengthen those nations' cybersecurity capabilities, including the physical security of cyber-critical infrastructure.

- ○ The USG should coordinate with ICT companies on appropriate cyberdefense implementation guidelines to ensure that the active defenses that ICT companies deploy do not present an unanticipated potential of escalation.

6. *Maintain the integrity of the information domain.* ICT companies put mechanisms in place to help fight the spread of Russian state-backed disinformation following Russia's invasion.[45] While capabilities and situational contexts vary across countries, steps ICT companies can take to help maintain the integrity of the information domain of nations under threat from hostile state-backed propaganda and disinformation include:[46]

- ○ Labeling government and government-affiliated accounts as such, particularly state-run media.

- ○ Establishing clear guidelines and policies for de-monetizing and de-amplifying potentially misleading content, such as pausing advertising in conflict areas to ensure critical public safety information is elevated, that ads do not detract from the dissemination of critical information, and that misleading content (under platform rules) cannot be monetized.

- ○ Expanding third-party fact-checking and content moderation capabilities in relevant local languages to support local fact-checking efforts.

[43] U.S. Support for Connectivity and Cybersecurity in Ukraine, U.S. Department of State (2022).
[44] For example, "the UK Foreign, Commonwealth and Development Office (FCDO), with technical advice from the National Cyber Security Centre, is sponsoring a program that enables Ukrainian agencies to access the services of commercial cybersecurity companies." Nick Beecroft, Evaluating the International Support to Ukrainian Cyber Defense, Carnegie Endowment for International Peace (2022). In addition, the €10.7 million "EU Support to Strengthen Cyber Security in Ukraine" project, led by the Estonian e-Governance Academy (eGA), has been running since March 2022 and will last until February 2023. Estonia Leading EU Project to Secure Ukraine's Cyber, Data Security, ERR News (2022).
[45] Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine, Meta (2022); Sinéad McSweeny, Our Ongoing Approach to the War in Ukraine, Twitter (2022).
[46] For a fuller discussion, see The 2022 Code of Practice on Disinformation, European Commission (2022).

- ○ Sharing information about prevalent tactics, techniques, and procedures used in state-backed disinformation campaigns when/if they occur.

- ○ Empowering researchers and users to understand how disinformation and state-backed propaganda operate in the information domain.

II. Responses to Government-Directed Digital Repression

The most pervasive threats to digital freedom come from various actions governments take within their borders,[47] such as a range of disruptions to connectivity, like Internet shutdowns and blocking access to websites, social media, and messaging platforms;[48] censorship and content moderation;[49] and legal threats and political pressure against ICT companies.[50] These do not represent the full scope of threats to digital freedom, but reflect common challenges the responses to which could also apply to a wider range of threat scenarios. Responses will necessarily depend on the circumstances, but to address the various gaps in advancing the digital freedom agenda discussed in this paper, the following are recommended best practices for how the USG can play a stronger role in supporting digital freedom, as well as how all stakeholders can protect targeted individuals and groups, shine light on repressive action, and confront repressive requests from governments.

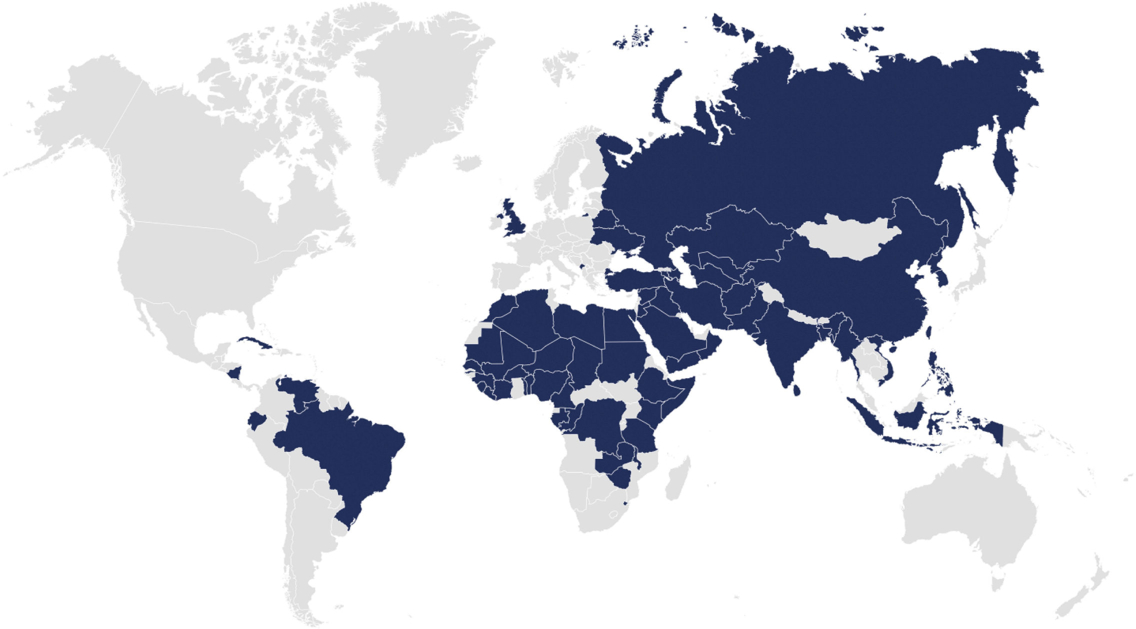
[47] State-based threats to digital freedom also are growing across borders. Digital tools are increasingly facilitating transnational repression where authoritarian governments suppress and coerce across borders. See Yana Gorokhovskaia & Isabel Linzer, Defending Democracy in Exile, Freedom House at 1 (2022). While not approaching the scale of authoritarian regimes' internal activities, these transnational tendrils are increasing, with the PRC as a primary actor. See Yaqui Wang, How China's Censorship Machine Crosses Borders — and into Western Politics, Human Rights Watch (2019).

[48] An Internet shutdown can be defined as an "intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." Deji Olukotun & Peter Micek, No More Internet Shutdowns! Let's #KeepItOn., Access Now (2016). Other disruptions to connectivity include targeted site-wide blocking of otherwise normally available and widely-used social media and messaging platforms.

[49] If disruptions to connectivity are blunt instruments to disrupt communication within a population and with the outside world, then censorship and content moderation are scalpels that cut out specific exercises of free speech and access to information. Governments already use these tools to target specific content at scale through required algorithmic filtering and blocking. Adrian Shahbaz, et al., Countering an Authoritarian Overhaul of the Internet, Freedom House (2022); Freedom on the Net 2022: China, Freedom House (2022); Meri Baghdasaryan, New Amendments to Intermediary Rules Threaten Free Speech in India, Electronic Frontier Foundation (2022).

[50] Governments are increasingly using legal threats and political pressure against ICT companies to suit domestic political purposes that are at odds with digital freedom. For example, India has pressured Meta to leave up government content on Facebook even though it violates the platform's hate-speech policies, and has pressured Twitter to remove content critical of the government's handling of COVID. Newley Purnell & Jeff Horwitz, Facebook's Hate-Speech Rules Collide with Indian Politics, Wall Street Journal (2020); Twitter Under Fire Over Deletion of Critical Covid Tweets in India, Guardian (2021).

Disruptions to Connectivity – Internet Shutdowns and Site-Wide Blocking, 2016-2022[51]



Internet shutdowns are intentional disruptions of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information. Other disruptions to connectivity include targeted site-wide blocking of otherwise normally available and widely-used social media and messaging platforms.

USG Actions

1. *Diplomatic Clarity and Advocacy. The USG should strengthen diplomatic advocacy against the spectrum of digital freedom threats, in coordination with the multi-stakeholder community.* ICT companies are seeking greater U.S. government advocacy and diplomatic support when they face threats from or are directed to comply with repressive actions by foreign governments. This can also be the first step in building out an action-focused complement to advance the principled positions outlined in the DFI.

    ○ A publicly-declared policy can help make clear how, where, when, and what the USG is ready to do regarding digital freedom and thus help organize public-private coordination to counter digital freedom threats. This can serve a deterrent effect by signaling the USG's willingness to respond to prescribed situations, but runs the risk of deeper failure if the USG does not respond to such situations.

    ○ For instance, there are anecdotal instances that U.S. diplomatic intervention – the USG engaging and raising an issue of concern with a foreign government – can be successful in shaping government behavior when foreign governments engage in

[51] SCSP analysis derived from Netblocks and Access Now.

repressive action. However, these instances of advocacy appear to be inconsistent and ad hoc. A clear policy, with coordination and intervention authority stemming from a White House-led process, can streamline and strengthen the impact of such interventions.

2. *Supporting Circumvention Technology. The USG should continue to prioritize and increase funding of on-the-ground circumvention capacity to nations at risk of digital repression.* This includes novel connection hardware as previously noted, and "traditional" tools (like virtual private networks (VPNs), personal VPN servers,[52] and mesh networks[53]).

    - Funding and programming for circumvention technologies should continue and increase to cover a range of work from supporting tech development and sustainment, to deployment and training on their use.

    - There have been anecdotal instances where the USG has been reluctant to work with or fund certain circumvention technologies because they were seen as tools for evading legitimate law enforcement and national security requirements.[54] A multi-stakeholder community should engage government officials to demystify the uses of such technologies, and discuss tradeoffs between privacy and security, as well as how such technologies can support digital freedom objectives.

    - In the case of Internet shutdowns, such technology and training ideally should be deployed before a shutdown takes effect. Insofar as shutdowns typically occur during times of unrest (e.g., elections, economic insecurity, popular discontent) and are thus predictable, building on-the-ground capacity ahead of time in risk-prone areas can prevent or mitigate the effects of shutdowns when they do occur.

3. *Sanctioning Violators. The USG should consider a sanctions program to implement targeted sanctions and visa restrictions against senior foreign government officials responsible for Internet shutdowns or other disruptions to connectivity.* The U.S. Department of the Treasury did this in the case of Iran's ongoing government-imposed

[52] For example, Outline, an open-source software project underlied by the open-source Shadowsocks encryption protocol, enables individuals to create their own personal VPN servers. It is currently being used to provide Internet access in Iran, Russia, and other parts of the world facing digital repression, directly and via CSOs such as nthLink. Yasmin Green, Iran's Internet Blackouts Are Part of a Global Menace, Wired (2022).

[53] For example, Mesh networks have also proven to be invaluable in Hong Kong and India to support communications during protests of the 2019 Hong Kong extradition bill, and the 2019 Indian Citizenship Amendment Act respectively. John Koetsier, Hong Kong Protestors Using Mesh Messaging App China Can't Block: Usage Up 3685%, Forbes (2019); Internet Shutdown in Delhi: Bridgefy is a Messaging App That Doesn't Need Internet, The Indian Express (2019).

[54] There is long standing tension between supporting privacy-promoting technologies and balancing the legitimate law enforcement concerns of rights affirming democracies. Shiva Maniam, Americans Feel the Tensions between Privacy and Security Concerns, Pew Research (2016).

Internet shutdown and censorship beginning in September 2022.[55] The Global Magnitsky human rights abuse sanctions also offers a model for how such a global sanctions program could function.[56] This would be an additional punitive measure beyond "naming and shaming" responsible officials that can potentially serve a deterrent effect and reinforce the importance the USG places on digital freedom.

- ○ The USG should also convene a multi-stakeholder process to weigh the benefits and costs of fully deplatforming sanctioned individuals and entities. There should be particular attention given to sanctioned foreign government officials and entities and whether the importance of permitting free expression may be outweighed by the harm that could come from their ability to disseminate disinformation.

- ○ The USG should also coordinate with ICT companies on appropriate sanctions implementation guidance to ensure sanctioned entities and individuals that are not deplatformed cannot monetize their platform presence (e.g., from ads on social media platforms).

4. *Effective Sanctions Implementation to Facilitate the Free Flow of Information. The USG should proactively engage the multi-stakeholder community on development of sanctions implementation guidance to ensure sanctions do not unintentionally hinder the activities of ICT companies supporting the free flow of information.* Following Russia's invasion of Ukraine in February 2022, confusion about the implementation of new sanctions and a public backlash against business activity in Russia led some ICT companies to withdraw (or contemplate withdrawing) from the Russian market.[57] In support of digital freedom principles, CSOs urged the USG not to disrupt Internet access and services for the Russian people,[58] leading to the U.S. Department of the Treasury clarifying exemptions to sanctions.[59] A similar situation played out in the wake of Iranian government crackdowns in September 2022, where sanctions unintentionally restricted rights-affirming Internet activity. The U.S. Department of the Treasury issued a general license to authorize ICT companies to "offer the Iranian people more options of secure, outside platforms and services,"[60] to ensure the Iranian people had access to platforms to communicate and bypass government censorship.

[55] Press Release, Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and Internet Censorship, U.S. Department of the Treasury (2022).
[56] Global Magnitsky Act, U.S. Department of State (2022).
[57] Craig Timberg, et al., Lumen, A Second Major American Internet Carrier, Pulling Out of Russia, Washington Post (2022).
[58] Joint Statement, Letter to U.S. Government: Do not disrupt internet access in Russia or Belarus, Access Now (2022).
[59] Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications, U.S. Department of the Treasury, Office of Foreign Assets Control (2022).
[60] Press Release, U.S. Treasury Issues Iran General License D-2 to Increase Support for Digital Freedom, U.S. Department of the Treasury (2022).

- In situations where sanctions programs may affect or target digital freedom activities, the USG (including the Departments of Treasury, State, and Commerce), in consultation with the multi-stakeholder community (especially including representatives familiar with the interests of civil society facing digital repression in a particular country) should issue clear guidance on whether digital freedom-related activities, like providing Internet connectivity services, are covered or exempted from sanctions. If exempted, the USG and the multi-stakeholder community should remain in close coordination to monitor the situation on the ground to ensure the exemption continues to be relevant for supporting digital freedom, and consistent with broader national security interests.

5. *Wielding Economic Tools. The USG should explore leveraging economic tools to dissuade states from taking repressive actions.* U.S. companies that refused to comply with censorship requirements have lost out on billions of dollars of revenue. A U.S. International Trade Commission (ITC) report on the economic impacts of censorship as a non-tariff barrier to trade by China, Russia, India, Vietnam, and other governments highlights that U.S. companies were often forced to censor political dissidents, LGBTQ content, and religious content or risk being blocked from operating in major foreign markets.[61]

    - In the same way that trade agreements have been used to raise labor standards in foreign markets,[62] the USG should explore whether they can also be used to lock-in values-based governance rules and technology design standards. At its most ambitious, this approach would seek to create a "digital trade zone" that creates economic incentives to adopt these rights-affirming rules and standards by linking them to greater access to and interoperability across digital markets.[63] U.S. efforts against data localization and other elements of the U.S.-Mexico-Canada Agreement[64] and the U.S.-Japan Digital Trade Agreement[65] could provide a basis for what certain rights-affirming digital trade and data flow provisions could look like.[66]

[61] Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses, U.S. International Trade Commission at 21-25 (2022).
[62] Jack Caporal, Work That Pays Off: The Strategic Dimensions of Labor Obligations in Trade Agreements, Center for Strategic and International Studies (2020).
[63] Robert Knacke, Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity, Council on Foreign Relations (2020).
[64] Agreement between the United States of America, the United Mexican States, and Canada 7/1/20 Text, Office of the U.S. Trade Representative (2022).
[65] U.S.-Japan Digital Trade Agreement Text, Office of the U.S. Trade Representative (2019).
[66] These two agreements also contrast with pacts like the Regional Comprehensive Economic Partnership (RCEP), in which the PRC insisted on terms allowing broad leeway for governments to conduct digital surveillance and censorship. See Regional Comprehensive Economic Partnership Agreement, RCEP (last accessed 2022).

- In addition, tracking countries' market access restrictions relating to digital freedom and their associated costs on U.S. companies, as the ITC report does, can provide a basis for the USG to consider or threaten the imposition of economic costs on those countries. Such punitive measures could deter or reverse the digital freedom threat.

- Outside of trade discussions, highlighting to governments the reputational costs and lost economic opportunities from foreign investment due to self-imposed Internet shutdowns could also discourage such behavior.[67]

6. *Coordination with Allies. The USG should proactively and regularly engage like-minded allies and partners on taking similar actions to support digital freedom, in order for joint actions to amplify the effect of these measures.*

    - Alliance action and coordination already occurs in intergovernmental bodies like the Freedom Online Coalition and through other bilateral and multilateral diplomatic engagements.

    - As noted throughout the above discussion on lessons learned from Ukraine, allied coordination and action-bolstered alliance efforts to help Ukraine defend its sovereignty against Russian invasion. Coordinating with allies on the development of the aforementioned measures and taking coordinated action in implementing them can strengthen their impact.

Protecting Targeted Individuals and Groups

7. *Enhancing Technical Security. ICT companies should continue to enhance technical security to protect at-risk individuals and groups, including:*

    - Working with developers of proxy servers and anonymous web-browsing protocols to ensure their platforms are technically accessible via those means.[68]

    - Providing technical guidance in local languages and channels to reach as broad an audience as possible in affected areas to allow users to better understand how to use their technology correctly (e.g., configuring VPNs).

    - Providing mechanisms for users to maintain personal safety and security, such as the ability to quickly lock their account profiles and/or remove sensitive account

[67] Steve Feldstein, Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?, Carnegie Endowment for International Peace (2022).
[68] For example, via The Onion Router (Tor), an open-source software enabling anonymous connection and communication. The Onion Router (Tor) (last accessed 2022).

information (e.g. address, contacts) when someone determines they may be at risk of politically-motivated detention or violence.[69]

Shining Light on Repressive Action

8. *Notifying Users and Promoting Transparency. ICT companies should continue to notify affected users and the broader public of repressive government requests made and acted upon, in real-time and via regular transparency reports, as appropriate.*

    ○ Many ICT companies publish regular transparency reports.[70] All ICT companies that receive government requests for private information and content censorship should follow best practices for transparency reporting.[71]

    ○ Transparency enables individuals, CSOs, and the broader public to get a better sense of what various governments are asking of ICT companies and to keep a pulse on the status of this particular aspect of digital freedom.

9. *Countering Bad Faith Take-Down Requests. ICT companies, in coordination with CSOs and government partners as appropriate, should develop public transparency procedures to counter bad faith take-down requests from pro-government trolls.*[72]

    ○ The fear of public exposure may deter some trolls. Transparency can also facilitate crowd-sourcing the task of finding and correcting bad take-down requests.[73]

[69] For example, Meta, Twitter, and LinkedIn deployed these measures for Afghan citizens amidst the Taliban's takeover of Afghanistan. Elizabeth Culliford, Facebook, Twitter and LinkedIn Secure Afghan Users' Accounts amid Taliban Takeover, Reuters (2021).

[70] Transparency Reporting Index, Access Now (last accessed 2022).

[71] For example, The Transparency Reporting Toolkit: General Best Practices for Content Takedown Reporting, New America (last accessed 2022).

[72] Bad-faith take down requests are those in which online safety or copyright policies are used disingenuously in order to take down content, and thereby silence views with which an individual or group disagrees. Such requests are often employed by pro-government trolls to silence human rights activists and political dissidents, as has been seen in a variety of cases, including the documenting of Uyghur oppression on YouTube, criticisms of President of Ecuador Rafeal Correa on Ecuadorian news outlets, and Vietnamese pro-democracy and environmental activists on Facebook. Eileen Guo, How YouTube's Rules Are Used to Silence Human Rights Activists, MIT Technology Review (2021); Alexandra Ellerbeck, How U.S. Copyright Law is Being Used to Take down Correa's Critics in Ecuador, Committee to Protect Journalists (2016); Sam Biddle, Facebook Lets Vietnam's Cyberarmy Target Dissidents, Rejecting a Celebrity's Plea, Intercept (2020).

[73] Daphne Keller, Using Transparency to Fight Takedown Trolls – A Model from the DMCA, Stanford Law School Center for Internet and Society (2017).

- Independent online resources[74] on worldwide requests to remove content from the Internet[75] can help expose and build awareness of bad-faith requests.[76]

10. *Exposing Internet Shutdowns. The USG, like-minded governments, ICT companies, and CSOs should continue exposing Internet shutdowns as they occur.*

    - The fear of public exposure and associated reputational costs may deter some governments from using Internet shutdowns as a tool of repression in certain circumstances, particularly if the financial costs of shutdowns can be articulated.[77]

    - CSOs, such as the Internet Society,[78] the #KeepItOn coalition,[79] the Open Observatory of Network Interference (OONI),[80] and Netblocks,[81] serve as major hubs for tracking shutdowns. In addition, a new multi-stakeholder effort, facilitated by the U.S.-EU Trade and Technology Council, coordinated by OONI and the Internet Society, and leveraging technical experts from ICT companies, recently published its first report on the Fall 2022 Internet shutdown in Iran,[82] and offers another venue for coalescing information.

Confronting Requests from Government

11. *Coordinating among Digital Platforms. ICT companies should coordinate consistent strategy and responses to repressive requests from governments.* Companies often

[74] For example, the Lumen database claims to grow by more than 40,000 notices per week, with voluntary submissions provided by companies such as Google, Twitter, YouTube, Wikipedia, Counterfeit Technology, Medium, Stack Exchange, Vimeo, DuckDuckGo, aspects of the University of California system, and Wordpress. As of the end of 2021, the project hosts over eighteen million notices, referencing close to four and a half billion URLs. In 2021, the project website was visited over nineteen million times by over one million unique users from virtually every country in the world. See About Us, Lumen (last accessed 2022).

[75] These requests for content removal include various complaints related to trademarks, defamation, privacy, and domestic and international court orders.

[76] Lumen Researcher Interview Series: Andrea Fuller, Wall Street Journal, Lumen Medium Blog (2021).

[77] Steve Feldstein argues that Internet shutdowns can bring significant financial and reputational damage to a country: "The more that countries' publics — not to mention large domestic businesses — become aware of these costs and generate backlash against these policies, the greater the likelihood that governments will reverse course on maintaining shutdowns." Steven Feldstein, Government Internet Shutdowns are Changing. How Should Citizens and Democracies Respond?, Carnegie Endowment for International Peace (2022).

[78] The Internet Society is a non-profit working to promote secure and global access to the Internet. Our Mission, Internet Society (last accessed 2022).

[79] Access Now launched the #KeepItOn coalition in 2016 to help unite and organize the efforts of activists and organizations across the world to end Internet shutdowns. It represents 280 civil society organizations internationally. #KeepItOn, Access Now (last accessed 2022).

[80] The Open Observatory of Network Interference is a non-profit software monitoring Internet censorship around the world, set up in 2012. About, Open Observatory of Network Interference (last accessed 2022).

[81] Founded in 2017, Netblocks is a nonprofit monitoring cybersecurity and governance of the Internet. They have a dedicated Internet Observatory, tracking and reporting on Internet disruptions and online censorship. The Internet Observatory, Netblocks (last accessed 2022).

[82] Technical Multi-Stakeholder Report on Internet Shutdowns: The Case of Iran amid Autumn 2022 Protests, Open Observatory of Network Interface (2022).

respond to government requests in isolation, even when such requests cover content or issues that affect multiple ICT companies or platforms.

- It is possible that strategy and response coordination across ICT companies may have helped them resist pressure from and/or maintain some leverage in dealing with the Russian government, when faced with Russia's censorship and take down requests surrounding Russian civil society's *Smart Vote* initiative.[83]

12. *Tailoring Responses. ICT companies should continue to leverage credible country-level human rights reports and assessments*[84] *to inform their response plans to governments' content moderation or censorship requests, while taking into account local cultural norms that do not violate human rights concerns.*[85] For example:

    - For governments rated positively (e.g., "free"): Comply in the narrowest manner possible.

    - For governments rated moderately (e.g., "partly free"): Challenge the request, using all available tools of law and policy, and if need be, comply in the narrowest manner possible.

    - For governments rated poorly (e.g., "not free"): Challenge or decline the request, using all available tools of law and policy, including possible deferral via a letters rogatory[86] process.

13. *Exhausting Legal Alternatives. ICT companies and CSOs should continue to make use of any and all legal alternatives*[87] *to fight government-imposed disruptions to connectivity and threats against ICT companies.*

    - This could include: 1) due process claims focused on the details of how a government order was issued, 2) freedom of expression claims based on

[83] Alexander Kazakov, Under Pressure: How the Russian Authorities Have Expanded Their Fight against Alexey Navalny's 'Smart Vote' Initiative ahead of September's Parliamentary Elections, Meduza (2021).

[84] Such as Freedom's House Internet Freedom Scores or the U.S. Department of State's Country Reports on Human Rights Practices. See Internet Freedom Scores, Freedom House (last accessed 2022); Country Reports on Human Rights Practices, U.S. Department of State (last accessed 2022).

[85] Newley Purnell & Jeff Horwitz, Facebook's Hate-Speech Rules Collide with Indian Politics, Wall Street Journal (2020).

[86] Letters rogatory are "the customary means of obtaining judicial assistance from overseas in the absence of a treaty or other agreement." See Preparation of Letters Rogatory, U.S. Department of State (last accessed 2022).

[87] Peter Micek & Madeline Libbey, Judges Raise the Gavel to #KeepItOn around the World: As Governments Continue to Shut Down the Internet, Courts Are Becoming a Viable Way To Fight Back, Access Now (2019).

constitutional protections or international legal obligations,[88] and 3) economic impact claims.[89]

- In some cases, litigation against ongoing or past Internet shutdowns can not only end current shutdowns, but can help prevent future ones.[90] ICT companies and CSOs should pull on each others' expertise and experience, as relevant, to leverage litigation as a tool to push back against repressive government requests. CSO coalitions like the Access Now's #KeepItOn coalition offer a network of global institutional knowledge when it comes to litigation.

[88] Such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).

[89] Aayush Rathi & Arindrajit Basu, Dialing in the Law: A Comparative Assessment of Jurisprudence on Internet Shutdowns, Association for Progressive Communications, CYRILLA Initiative at 9-11 (2020).

[90] For example, the Economic Community of West African States (ECOWAS) Community Court of Justice ruled that a 2017 Internet shutdown in Togo was illegal, and ordered the Togolese government to pay restitution and maintain Internet connectivity in the future. Amnesty International Togo, et al., v. The Togolese Republic, ECOWAS (2020).

SCSP.AI