



Community
of Democracies

Recommendations for the **Global Digital Compact**

Provided by the Community of Democracies Working Group
on Democracy & Technology

April 2023



Disclaimer

The recommendations below were compiled based on deliberations and inputs of members of the Community of Democracies' Working Group on Democracy & Technology (WGD&T) to be submitted as input for consideration for the Global Digital Compact. The process was facilitated by an expert consultant Mr. Christopher Jackson for the WGD&T.

Introduction

A thriving and democratic, digital ecosystem is rooted in the normative governing framework that protects and respects human rights and fundamental freedoms across the digital ecosystem. Human rights include the freedom of expression, freedom of peaceful assembly and association, freedom of religion or belief. While keeping this fundamental philosophy in mind and integrating it into the digital ecosystem, it is also imperative to develop core principles about the underlying infrastructure (i.e., people, processes, technology) that provide an accessible and reliable way for human rights to be exercised and protected.

The emerging Fifth Industrial Revolution, encompassing human and machine collaborations, must be intertwined and support changes in current policies, strategies, and multi-lateral agreements to ensure the well-being and continued protection of rights for all global stakeholders (e.g., international organizations, governments, businesses, civil society, academia, science & technology communities).

It is thus imperative the recommendations for the Global Digital Compact aim to protect human rights online and offline in a changing digital ecosystem, while ensuring they are iterative and accommodating of innovative emerging technologies and digital processes. Key tenets of this philosophy leverage the core democratic principles and practices outlined in the Warsaw Declaration¹.

Key Definitions

- **Security** – Protection of human rights – civil, cultural, economic, political, and social.
- **Privacy** – Right to not be subjected to arbitrary interference.
- **Cyber Hygiene** – Fundamental cybersecurity best practices that an organization’s users can put into use to protect themselves from cyber threats and threat actors (e.g., how to avoid phishing/scam emails, protecting passwords, securing personal devices).
- **Communities** – Consists of technology-related academia groups, corporations, and civil society organizations.

¹ The Warsaw Declaration is the founding document of the Community of Democracies. It consists of 19 principles of human rights, democracy, and the rule of law for the effective establishment and consolidation of democracy.

Recommendations

There are eight recommendations that could provide robust coverage of improving digital access, rights, and safety that align with many challenges of today's digital ecosystem, while also understanding that this ecosystem is constantly changing. These recommendations have been grouped into three categories:

1. **Accessibility** – Providing trustworthy, accountable, and affordable access to the Internet and other digital services to the unconnected. This includes physical infrastructure, and also requires expanding access to digital services by ensuring they are available to users across regions, devices, and price points.
2. **Safety** – Ensuring that people's privacy is protected; safeguarding and advancing in digital spaces the rights people have offline.
3. **Security and Reliability** – Securing the underlying infrastructure that comprises the digital ecosystem—software, hardware, and operational technology—in order to protect everything a user accesses, stores, or engages with in the digital ecosystem.

An overarching theme across the eight recommendations is that of **Bolstering the Multistakeholder System** that governs the digital world and looking beyond national-level action to include at every step the business, civil society, and other stakeholders involved in the operating of the ecosystem. It is important that work even at the national level be done in a multistakeholder and multi-sectoral way; meaning that even when focused on government approaches to technology governance, there is an accountability and stakeholder lens, inclusive of the business, civil society, and other stakeholders involved in the operating of the ecosystem. This is necessary to ensure that the three categories of recommendations are monitored, governed, updated, and advanced as the digital ecosystem and its components evolve.

These categories are not mutually exclusive, and the following recommendations overlap with each other. This demonstrates the intricate and integrated nature of the modern digital ecosystem. All categories need to be covered on an individual level, but with the knowledge that they are deeply connected. This ensures the protection of human rights in an ever-increasingly complicated and interconnected world.

These recommendations are approached through a **resilience lens**. The digital world is fast moving, interconnected, complex, and unpredictable. Trying to design programming to address what one assesses as key risks and needs today is likely to miss big pieces of the puzzle. A far more strategic approach is to focus on building resilient ecosystems capable of responding to threats and challenges as they arise. In addition, these recommendations seek to **leverage the UN's existing programming geared towards resilience as a key goal**, to ensure digital democracy programming is advanced through or supported by the work focused on health, agriculture, economic development and more. This comprehensive approach would also allow civil society organizations in existing ecosystems or fields to get support to improve their digital capacity. These recommendations attempt to encapsulate these two ideas through different, but overlapping, avenues.

The following recommendations are organized to meet the format requested by the Global Digital Compact, with each number representing a core principle and each underlying letter representing the key commitments that can help achieve the specific principle.

Increasing and Ensuring Digital Access and Understanding (Accessibility, Connectivity, and Security)

- 1. Shrink the digital divide by providing a means to connecting all to the Internet to provide a better quality of life, equal access to public services, and access to education & information, while avoiding digital fragmentation or isolation and preserving rights to freedom of opinion and expression.**
 - a. Encourage collaboration between key internet service providers (e.g., Amazon Web Services, Starlink, Verizon, Deutsche Telekom) and government leaders to develop initiatives for providing reliable Internet access to unconnected populations.
 - b. Encourage incentives (consisting of rewards and penalties) for Internet Service Providers (ISPs) to dedicate resources to creating infrastructure to support basic internet access to all populations.
 - c. Encourage relevant fora to consider more efficient ways to provide connectivity and the basic needs of Internet access. Utilize their sessions to learn more about next-generation technologies that can support Internet access.
 - d. Leverage outcome indicators from organizations involved in this work to help the UN track the overall health of human rights and democracy online at scale. These can include indicators of Internet shutdowns, connectivity restrictions, interoperability, regulatory and practical consistency on human rights standards and democratic norms.

- 2. Ensure universal access to education and provide global digital knowledge & literacy curricula to increase awareness and understanding of the digital ecosystem (e.g., development of e-skills and online safety).**
 - a. Call on UN fora to consider a set of resources that organizations can provide alongside community learning sessions to teach best practices and safety measures when using the internet and other digital services. This can be provided to organizations to understand how to utilize the internet and associated digital services. This can also be used by those already connected to the Internet but who lack additional understanding to maximize their use of services, or by those soon-to-be connected that will need to understand the basics of utilizing the internet while staying safe online.
 - b. These groups could hold periodic reviews to update these materials as the Internet and digital ecosystem fabric changes.

- c. These materials could be tailorable to meet the diverse needs of global populations while still maintaining a foundational primer to the digital ecosystem.
- d. These materials could also be used by governments to help improve digital services for their citizens to take advantage of more easily.
- e. These materials could be modified to help train cyber workforces, ensure the equality between men and women, and incubate new digital economies.

Combatting Digital Disinformation/Misinformation and Digital Human Rights Abuse (Safety, Security, and Trust)

3. Mitigate the proliferation of disinformation and misinformation while promoting an exchange of verified information by a multi-stakeholder group to provide transparency, participation, digital inclusion, resiliency, and to be fully accountable to the citizenry.

- a. Resource and partner with organizations and multistakeholder efforts that advance a resilient information environment, including academic, investigative, journalistic and research organizations that identify and track disinformation.
- b. Resource and support organizations and multistakeholder efforts that train communities to identify and counter disinformation/misinformation and increase digital literacy.
- c. Encourage multi-stakeholder groups consisting of representatives from governments, businesses, science & technology communities, and civil society organizations to discuss best practices for a consistent sharing of knowledge around identified disinformation/misinformation including tactics/methods for mitigating and countering them.
- d. Part of this work could have governments forming a consensus to not engage in or support disinformation/misinformation campaigns and/or actors.
- e. These multi-stakeholder efforts could develop and periodically release a portfolio of identified information (e.g., a summary report) on known disinformation/misinformation tactics and actors, supported by non-profit organizations that monitor these tactics.
- f. These multi-stakeholder efforts could disseminate these releases in a way that organizations can easily access them and provide them to peers and other relevant parties working on the ground.
- g. Additionally, these multistakeholder efforts can address misuse of technology agnostic of actors and threats, but rather focused on digital repression and technological misuse as a defining factor of how the information environment is used, abused, and misused. The UN could support capacity-building, investigative research, and trainings related to the environment that have proven to make individuals or organizations less susceptible to disinformation/misinformation. This could provide long-term support to invest resources meaningfully over time in regional institutions and systems.

4. **Drive transparency and increase knowledge about the information environment, which is an important component of the digital ecosystem for governments, citizens, and global community to understand its impact on democracy.**
 - a. Encourage better collaboration between industry, civil society groups, and governments to ensure meaningful transparency across the digital ecosystem, and then bolster accountability mechanisms to hold to account those limiting human rights or democracy on those platforms.
 - b. Resource and partner with open-source research and independent journalistic communities to ensure societies have insight into the impact of proposed laws, company actions, changes in ownership of key digital infrastructure, or other related actions.
 - c. Support and encourage multistakeholder efforts that contribute to a digital ecosystem that advances democratic values and human rights—including academic, investigative, journalistic, open-source research organizations, and communities of human rights and democracy defenders.
 - d. Support and encourage accountability mechanisms and the actors across sectors that play critical roles in holding industry and governments accountable for advancing a democracy- and rights-affirming digital ecosystem.

5. **Support expert bodies that independently monitor and report on actors and methods that contribute to the violation of human rights (e.g., civil, cultural, economic, political, and social). A recent example of this is the proliferation of Technology-Facilitated Gender-based Violence.**
 - a. Resource and support organizations and multistakeholder efforts that advance democracy- and rights-affirming approaches to governance of the digital information environment.
 - b. Encourage multi-stakeholder efforts to ensure a consistent sharing of knowledge around recognized/identified human rights abuses through the use of digital technologies.
 - c. These efforts could select regional rapporteurs led by civil society organizations representing each UN Regional group to support the provision of materials.
 - d. These efforts could provide a periodic release of collected information on recognized/identified actors and tactics that have been involved in human rights abuses, especially concerning privacy and human rights protections in the digital space.
 - e. These products could be released so that organizations can easily access them and provide them to peers and the citizenry. These releases could be provided in multiple languages and accessible formats.
 - f. Encourage better collaboration between social media corporations and human rights groups to share information and find cross-points where services may be facilitating abuses and potential mitigations.

Organizational Responsibility around Digital Assets and Infrastructure (Security and Reliability)

- 6. Governments, businesses, science & technology communities, and civil society organizations agree to promote cybersecurity protections into their missions and strategies. This comes with the acknowledgement that the protections are important for the integrity and privacy of data, services, and forums used by citizens.**
 - a. Support efforts to strengthen collaboration between governments, businesses, science & technology communities, and civil society organizations on developing a playbook for organizations to help integrate cybersecurity controls standards and privacy standards (e.g., ISO/IEC 27001, GDPR) into their current missions or investments and promote UN norms on responsible state behavior in cyberspace.
 - b. This playbook is meant to provide the standards and acknowledge the importance of integrating these standards for the protection of citizens.
 - c. Consult with major cybersecurity organizations to help develop these playbooks – or provide versions they already can access. A working group of other representatives from government, business, science & technology communities, and civil society organizations could make these easily accessible to organizations that are not familiar with these major cybersecurity organizations and their materials.
 - d. Consult with experts from global human rights, democracy, and political opposition communities to ensure the needs and concerns of these vulnerable communities are prioritized. Seek abundant input from multistakeholder communities in the Global South.
 - e. Encourage capacity-building and innovative sources of funding to help provide financial support to organizations lacking the means to integrate cybersecurity protections into their operations.
 - f. Encourage relevant multistakeholder groups and international organizations to provide free strategies, models, and playbooks to organizations lacking these resources that enable them to integrate cybersecurity protections into their operations. These advisory groups should partner with non-profit cybersecurity organizations to help develop these materials.

- 7. Cybersecurity should be seen as a social responsibility for both the protection of privacy as well as protecting the infrastructure that stores and transmits data, allows for forums to prevent censorship & a free exchange of ideas, while providing critical services to populations regardless of race, religion, belief, geography, sex, disability, or economic status.**
 - a. Encourage multi-stakeholder groups to further develop guidelines and best practices that help organizations understand the importance of cyber hygiene when performing services that are accessible to all sizes of organizations.

- b. These groups could periodically meet with key cybersecurity leaders across different industries and countries to socialize and support efforts to tailor guidelines.
 - c. These groups could also further bring together representatives from different industries and countries to discuss risks or challenges they have encountered to help improve guidelines. This may include making guidelines easier to understand, more generic to ensure all areas are covered, or determining if additional guidelines are required.
- 8. Every person has a right to equal access to public service and take part in public affairs through the digital ecosystem. Organizations should be responsible for adhering to relevant regulations when utilizing technologies, digital assets, and technical assets that ensure the continued provision of governmental, economic, or social services. This specifically concerns the digital supply chain that is often convoluted and easily exploited.**
- a. Consider a Global Digital Assurance group composed of representatives from technical bodies, government, business, academia, science & technology communities, and civil society organizations.
 - b. This group could consider establishing a Digital Assurance Framework that could be utilized by organizations to measure the effectiveness and safety of their use of digital assets.
 - c. This framework could initially pull from universal controls standards (ISO/IEC 27001) as a foundation for measuring digital security and privacy.
 - d. It could meet periodically to consider updates to its framework based on emerging risks and/or emerging technologies.
 - e. This group could develop a knowledge booklet for organizations to use to understand the digital supply chain, and what to look for when procuring new technologies or utilizing digital services (e.g., cloud services, dedicated platforms).