Policy Brief **October 2024**

A digital world worth living for

A Green compass for a human-centric international digital policy

By Sabine Muscat

Paper Summary

The securitization of digital technologies in the face of geostrategic competition presents a challenge to the European vision of a human-centric digital transformation. This paper makes suggestions for how an approach centered in human security and feminist foreign policy along with an updated vision of the network society can balance these hard power dynamics and contribute to a free, inclusive, sustainable and just global digital society.

The author describes how Green-minded actors and their allies in Germany and the EU can shape such a world by defending fundamental rights and principles and by protecting and empowering citizens and communities – through active engagement in global governance debates, through safeguarding rights and principles at home and abroad, and through co-creating infrastructure, systems and mechanisms that reflect Green values.

Methodology and special thanks

The methodology used was a review of official documents and expert analysis as well as interviews with Green advisors in the Bundestag and European Parliament, German government officials, experts and civil society representatives. A special thanks for their input and feedback goes to Nina Locher and Eva Mattes (Office of German MP Tobias Bacherle), Louisa Well and Michael Kolain (Advisors to the Greens in the Bundestag), Ralf Bendrath (Greens/EFA advisor at the European Parliament), Jan Philipp Albrecht (Heinrich Böll Foundation), Geraldine de Bastion (Konnektiv/ Global Innovation Gathering), Friederike von Franqué (Wikimedia Deutschland), Henriette Litta (Open Knowledge Foundation Deutschland), Léa Auffret (BEUC), Kristina Irion (University of Amsterdam), Philipp Schulte and David Hagebölling (BMDV), Daniel Voelsen (SWP).

Many thanks also to Giorgio Francescini (German Ministry for Foreign Affairs) and Vérane Meyer (German Ministry of the Environment) for initiating and overseeing this project when they were working at the Heinrich Boell Foundation – as well as to all the others who have inspired it through their research, public talks or private conversations on the sidelines of tech policy gatherings in 2024, from the Mercator Forum Digitale (Ohn-) Macht in Essen to the CPDP conference in Brussels and re:publica in Berlin.

About the author

Sabine Muscat is an independent policy analyst and strategic communications consultant based in Brussels with a focus on international digital policy and digital development cooperation. She previously built and led the Digital Policy /& Technology Program at the Heinrich Boell Foundation Washington, DC between 2019 and 2023. A journalist by training, Sabine worked as a Washington correspondent and Asia desk editor for German media (Financial Times Deutschland, Welt/N24, F.A.Z.). Building on her MA in Chinese Studies, she reported from China and Asia as a journalist and later worked as a freelance communications advisor for the Mercator Institute for China Studies.

Content and main points

Introduction: Global digital society in times of geostrategic competition

A Green compass for a human-centric international digital policy

SHAPE & DEFEND: **Stand up for democratic digital norms and governance**

- Stand up for human rights/ democracy/ sustainability
- Support civil society in multi-stakeholder internet governance
- Prevent authoritarian capture of UN processes (e.g. Cybercrime Convention)
- Advocate for inclusion of Global Majority in global digital governance

DEFEND & PROTECT: **Apply a feminist lens to achieve cybersecurity for all**

- Advocate for human security approach to international law in cyberspace
- Push for German/EU re-engagement on AI arms control
- Fight cybercrime and digital violence applying an intersectional gender lens
- Focus on protecting vulnerable groups from dis- and misinformation

PROTECT & EMPOWER**: Ensure digital rights for citizens and communities**

- Stand up for freedom of speech at home and abroad
- Prevent erosion of digital rights in the EU (e.g. Chat Control)
- Counter erosion of data protection standards in trade agreements
- Expose and combat EU hypocrisy (e.g. biometric surveillance at EU borders)

EMPOWER & SHAPE**: Promote a digital transformation for the common good**

- Put citizens and communities in control of data
- Promote equitable access to digital infrastructure, knowledge and innovation
- Advocate for digital commons with open-source code and open standards
- Double down on engagement for a digital and green transition

Outlook: A Green window of opportunity

Introduction: A global digital society in times of geostrategic competition

Hard power has become the theme of our decade. Around the world, nation-states and nationalist movements are reinforcing borders and pushing back against the forces of globalization. The internet and digital technologies are at the center of this shift. They are shaping military conflicts from Ukraine to Gaza. Access to the means of their production is at the core of the geostrategic rivalry between China and the United States. The stakes are high for Germany and the EU: We are in a race to secure critical infrastructures, ensure access to tech supply chains and bolster our "digital sovereignty" by incentivizing domestic innovation and reducing our dependence on foreign technology.

Reconciling this hard reality with the vision of a human-centric globalized digital society is a sticky problem for Green policymaking. The problem is similar to the test that a security-oriented foreign policy presents to the German Green-led Foreign Ministry's commitment to a progressive feminist foreign policy, which also applies to the digital space.

Nevertheless, the stickiness does not mean that the goals are irreconcilable. A mix of hard power (from cyberdefense to sanctions and investment or export controls), cyberdiplomacy and global digital investments will be necessary to create the spaces in which the vision can survive and grow. **Green civil society actors can fill these spaces with support for progressive members of the digital community as well as with fresh ideas.**

In order to define the vision, it is helpful to refer back to two concepts that emerged in the post-Cold War optimism of the 1990s: the ideal of the network society promoted by the early Internet pioneers and the human security paradigm that emerged within the UN.

The promoters of the "**network society"** explored the liberalizing potential of a disruptive invention: the World Wide Web. The early days of the internet were fueled by this utopian vision of borderless communication between autonomous individuals – with the undeniable flaw that it mostly applied to an elite of white men in highly developed parts of the world.

The vision still survived the 2000s mostly intact, but we all know where things went from there. The 2010s marked the moment when publics and policymakers worldwide realized that powerful tech monopolies had undermined the internet's promise of self-determination by commercializing every mouse click in return for "free" services. It was also the decade when authoritarian governments – with China in the lead – stepped in to wrest power back from their outspoken and internationally connected "netizens". The Chinese Great Firewall put an end to the 1990s vision of a borderless digital world.

The 2020s are shaping up to be the decade when democratic governments and societies have started fighting back against the economic monopolization as well as the political fragmentation of the digital space – with the goal to save what's left of the global network society and to use both hard and soft power to defend the open internet and digital rights against abuse by big tech companies and techno-authoritarian governments. **For Green-minded actors, it is important to lead in that fight.**

At the same time, Greens need to continue to be motivated by another concept from the post-Cold War era with the aim to serve the less privileged part of humanity. In 1994, UNDP's Human Development Report first coined the concept "human security" to overcome the traditional focus on the nation-state, which often failed individuals and communities within their borders. The report defined human security along seven pillars of human well-being that had to be in place to guarantee "freedom from fear" and "freedom from want": economic security, food security, health security environmental security, personal security, community security, and political security. The impact of digital technologies on all these areas did not yet feature at the time, but they became firmly anchored in the UN's 2030 Sustainable Development Goals.

A 2022 UNDP report titled "Threats to Human Security in the Anthropocene" devotes an entire chapter to "Digital technology's threats to human security" – from cyberwarfare and malicious cyberattacks, from disinformation on social media to algorithmic discrimination, from labor conditions in the digital economy to uneven access to technological innovation.

Human security was controversial from the beginning – partly because governments were uncomfortable with the challenge it allegedly posed to state sovereignty. It was later replaced by the term "people-centered security" in many UN documents, signaling a shift that envisions the role of donors as facilitators between states and civil society. These nuances also play a role in discussions on whether the EU's concept of a "human-centric" digital transformation (centered in the European Declaration on Digital Rights and Principles) is the same as a "people-centered" digital transformation. The terms are often used interchangeably, but the latter appears to be preferred by countries that are eager to prioritize collective over individual rights. Clear definitions are needed when using one or the other. However, at a time when national security dominates the policy discourse even in liberal democracies and when authoritarian countries lobby for state-centric approaches to global governance, either term provides a framework for describing a policy approach that places the focus on people and communities rather than nation-states.

Human-centric geopolitics? A Green compass for international digital policy

Guided by the concept of human security and an inclusive vision of the network society, Green-minded civil society actors can set out to fill Germany's and the EU's international digital policy with life.

Germany and the EU view it in their geostrategic interest to defend their values in the digital age. In its 2023 Conclusions on Digital Diplomacy, the European Council refers to "threats to the human rights-based and human-centric model for digital transformation" in a "challenging geopolitical context" and states that "the importance of the leadership of the EU and its Member States on international digital governance is growing."

In a similar vein, the German coalition government pledged to defend freedom and democracy in the digital age in its Strategy for International Digital Policy of February 2024, stating that the EU's "strategic sovereignty" depends on a "multilateral and rules-based digital order." Building on the 2022 national Digital Strategy, the document spells out Germany's digital security and foreign policy goals in the areas Democracy, Prosperity and Resilience. The section dealing with resilience complements the country's first National Security Strategy in 2023, which focused on technological sovereignty and cybersecurity. Germany's first China Strategy also addresses the geostrategic competition over technology.

The international digital policy strategy goes beyond the geostrategic competition by highlighting the role of digital technologies as tools for solving global challenges that are also addressed in the UN SDGs such as climate change, public health risks and inequality. The fact that the final document is infused by a global justice perspective and calls to empower civil society can be traced back in no small part to the joint efforts of two progressive MPS, the Green Tobias Bacherle and the Social Democrat Armand Zorn.

Greens enjoy international credibility for shaping the EU's values- and right-based concept of a human-centric digital transformation. The European Declaration on Digital Rights and Principles bases this concept on fundamental human rights and dignity, freedom, democracy, equality, the rule of law as well as in the principles of solidarity, inclusion and sustainability. European Greens were the driving forces behind the General Data Protection Regulation (GDPR), which became a global template for establishing data protection as a fundamental right. Greens also played a visible role in shaping the Digital Services and Digital Markets Act, which were aimed at protecting democratic society and its citizens from manipulation and disinformation and marked concentration in the tech sector. The new AI Regulation takes a risk-based approach to the technology, banning uses that are considered to bear unacceptable risks (such as social scoring for citizens) and regulating high-risk applications in sectors such as education, employment and health care.

As this triad of EU comprehensive digital policy legislation is now in the enforcement stage, critical oversight by Green-minded actors and civil society will remain crucial. At the

same time, these actors need to develop keen sensors and a moral compass for the complex challenges of global digital governance, some of which this paper will lay out.

1. Green actors need to be part of a multistakeholder coalition that **SHAPES** international norms and standards for everything from data transfers to AI and other digital technologies. At the same time, this coalition needs to **DEFEND** existing norms and governance models against authoritarian efforts to undermine them.

2. Green actors should be part of solutions to **DEFEND** German and European digital infrastructure with the goal to **PROTECT** individuals – and particularly gender minorities and other vulnerable groups – from cyberattacks or disinformation campaigns as well as to counter global setbacks for freedom of speech and independent media.

3. Green actors should renew the fight to **PROTECT** personal information at a time when data protection is undermined by surveillance technology and digital trade agreements. They should advocate to **EMPOWER** individuals and communities to be stewards of their own data through fair and secure sharing architectures.

4. Green actors should work towards putting the vision of digital commons into practice to **EMPOWER** individuals and communities. They have to push Germany and the EU to provide strategies and funding to **BUILD** inclusive and sustainable digital public infrastructures for the common good – at home and globally.

Across all international digital governance conversations, Greens have a responsibility to work towards the goal that German and EU positions and actions reflect core values such as human rights, democracy, inclusion, shared prosperity, sustainability, human security and global justice.

SHAPE & DEFEND: Stand up for democratic digital norms and internet governance

The international process that resulted in the Global Digital Compact (GDC) illustrated the sticky problem of preserving a global network society in a nation-state dominated arena. The GDC was published as an annex to the Pact for the Future at the UN Summit of the Future in September 2024. The global framework for digital cooperation sets out shared principles for an "inclusive, open, sustainable, fair, safe and secure digital future for all." The document firmly links the goal to close "all digital divides between and within countries" with the UN's Sustainable Development Goals. It also does justice to the human security concept with commitments to human rights (including information integrity and data privacy and to the inclusion of a long list of vulnerable groups – from women and children to indigenous peoples and refugees.

Yet, the discussions about consecutive drafts ahead of the Summit had highlighted many of the fault lines – between democracies and authoritarian countries as well as between states and non-state actors. The GDC's achievement is to expand digital governance beyond the circle of leading technology nations. At the same time, democracies and civil society worry about a centralization of governance – especially of AI (see text box below) – at the UN headquarters. After all, sidelining non-state actors would fit the agendas of authoritarian countries.

Classic internet governance – as it used to be called – started from a different place. In the early years, its main task was to set technical norms for the new technology. However, even those norms have become politicized, with power struggles between China and Russia on the one hand and the United States and its Western allies on the other playing out in standardization bodies, notably at the UN's International Telecommunications Union (ITU).

The political dimension of internet governance has evolved since 2003, when all 193 UN states agreed at the first World Summit on the Information Society (WSIS) in Geneva that the global information society had to be "people-centered, inclusive and development-oriented." From this consensus emerged the multistakeholder model, which was institutionalized in the Internet Governance Forum (IGF) at the second summit in Tunis in 2005. The IGF mandate is up for renewal at the WSIS+20 Review in 2025 – and while the final document expresses prominent support to the forum in principle, it lacks a strong funding commitment to a future IGF.

The only game in town? Making sense of the global cacophony on AI

Artificial Intelligence is the hottest topic in the current digital governance debates – and many players are competing to establish their own approach as the global model. There is no doubt that AI will lead to profound changes in our economies and societies, in matters of national security and warfare, in our environment and even in our bodies. AI intersects with most other major issues that shape our digital future, namely cyberwarfare and cybersecurity, disinformation and discrimination, surveillance technologies, data storage

and data governance, extended reality and solving global challenges such as managing the digital and green twin transition.

The EU AI Act was passed into law in early 2024, a few months after President Biden's 2023 Executive Order instructed US government agencies on the "safe, secure and trustworthy development and use of Artificial Intelligence." Both the U.S. and the EU have converged around a risk-based approach, which regulates technologies and applications based on the level of risk they present to the public and bans those that are considered as unacceptable (such as citizen scoring in the EU AI Act). However, the EU's horizontal approach competes with the US approach, which differentiates by sector. China was ahead of the curve in regulating recommendation algorithms and Generative AI – from synthetic content to chat bots like Chat GPT – and is currently working on a national AI law. And there is hardly a country – including in Africa, Asia or Latin America – without a national AI strategy.

There has been movement at the international level as well. In May 2024, the Council of Europe adopted the first international AI treaty, which includes several non-European countries such as the United States, Japan and Israel. The legally binding convention is a step towards forging compromise among democracies, but it was also criticized by digital rights organizations for its broad carve-outs for the private sector and national security. The "AI Safety Summit" organized by the United Kingdom in 2023, which resulted in the "Bletchley Declaration", brought 27 governments and leading tech companies on board, but stopped at a vague commitment to identify AI risks, without solutions for addressing them.

The UN, which has also taken on AI as part of the Global Digital Compact process –is arguably the best forum to ensure representation of the Global Majority. The UN tasked a "High-Level Advisory Body on AI" with proposals for future regulation.[1] In its final report that was published ahead of the UN Summit of the Future in September 2024, the expert panel points to out "global AI governance gaps." The report contains the recommendation to create of an international scientific panel on AI, modelled on the Intergovernmental Panel on Climate Change (IPCC), as well as a public-private global fund for AI "to put a floor under the AI divide."

Amid the fast-paced development of AI and the governance cacophony surrounding it, it is important for Greens to stay engaged but to not lose track of all the intersecting policy issues in their own right. "Digitalization is far more than Artificial Intelligence," a group of German civil society organizations wrote in their comments on the first policy brief for the Global Digital Compact, which was – like the final version – very AI-heavy.

The Global Digital Compact is not the only process that reflects the tensions between state-led and human rights-based forces at the UN. The negotiations over a UN Cybercrime Convention have been a wake-up call for everyone standing up for human rights and

[1] Its members include German Green MP Anna Christmann, who currently serves as the Federal Government Coordinator of German Aerospace Policy.

democracy. Russia initiated the negotiations in 2019 with the goal to establish a competing legal framework to the Budapest Convention on Cybercrime. The treaty was voted out of the ad-hoc committee on 8 August 2024 and is now scheduled for a vote by the UN General Assembly before the end of 2024.

EU countries and the U.S. face the difficult decision to sign a treaty that falls short of the Budapest standards or to leave the global lead on cyber issues to their adversaries if they stay out. Human rights organizations and private sector stakeholders warn that the treaty could be misused for surveillance and repression of political dissent. They are highly critical of the document's expansive definition of cybercrimes, which leaves room to go beyond attacks on computer systems and include, for example, online content. At the same time, critics worry that human rights safeguards may not be strong enough, and an analysis by the Global Initiative Against Transnational Organized Crime points out that technical assistance measures in evidence collecting do not include measures for judicial support or oversight. In an open letter urging governments not to adopt the treaty, a group of civil society and industry stakeholder warns that a lack of protections would put cybersecurity experts and researchers at risk of criminal prosecution.

Should the document pass the UNGA vote, it will gain the force of an international treaty whose members will be able to access UN resources for cooperating on a repressive cyber agenda.

Green policymakers and their civil-society partners will have to do everything in their power to expose and oppose current and future efforts at authoritarian capture of UN processes. They will have to anticipate new challenges to the rights-based global order by Russia, China and its allies, and to build advocacy strategies for countering such efforts before they garner broader support.

DEFEND & PROTECT: Apply a feminist lens to achieve cybersecurity for all

The authoritarian attempt to undermine human rights norms in the name of cybersecurity at the UN should not detract attention from the fact that cyberthreats – committed by state actors, terrorist groups, criminals or hackers – are real and that they disproportionately affect the most vulnerable citizens and communities.

Cyberwarfare presents the most extreme digital threat to human security, through lethal autonomous weapons or through digitally enabled attacks on critical infrastructure such as water and electricity grids. There is general agreement among most states, international organizations and legal experts that international law applies in cyberspace.[2] However, some countries – including Russia – have questioned the applicability of international humanitarian law during an armed conflict to cyberoperations. It is difficult for civil society actors to exert influence in this area, but strong multistakeholder coalitions can produce results. In October 2023, guidelines published by the International Committee of the Red Cross for the application of humanitarian law to protecting civilians from cyber threats during armed conflicts gained unequivocal support from two of the largest hacktivist groups active in the war in Ukraine, the Russian-affiliated Killnet and the Ukrainian IT Army.

Uphill battle against killer robots: Autonomous weapons and algorithmic targeting

Technology has come a long way since the Obama era's use of unmanned drones in the counterterrorism fight in non-battlefield setting such as Yemen, Pakistan, and Somalia. In today's armed conflicts, automated weapons are supercharged with algorithms that identify patterns and help with targeting decisions – ushering in a new era of the "killer robots" debate, which had faded away after failed efforts to ban such systems.

The U.S., China and Russia use AI and advanced robotics for the development of a next-generation of military systems. Israel has made headlines with the use of algorithmic target identification systems, which have made decisions on striking what Israel claimed to be Hamas targets with limited human oversight and a wide range of tolerance for civilian casualties.

Lethal autonomous weapons are back on the international agenda with a major international conference on the topic in Vienna in April 2024 and an August 2024 report for the UN General Assembly. In the latter, UN Secretary General Antonio Gutierrez calls for

[2] How it applies is an issue of debate since international law regulates the behavior of states, but cyberspace is a domain of many actors. This complicates the attribution of attacks, e.g. of private hackers under state control, or of defining the threshold for when a malicious cyber activity constitutes a breach of sovereignty and/or amounts to wrongful intervention or even use of force. Many countries, including Germany, have published legal positions, guided by the Tallinn manuals, a process led by NATO's Cooperative Cyber Defence Center of Excellence. A team of experts is currently working on the third update, the Tallinn Manual 3.0.

"the conclusion, by 2026, of a legally binding instrument to prohibit lethal autonomous weapons systems that function without human control or oversight and that cannot be used in compliance with international humanitarian law, and to regulate all other types of autonomous weapons systems." A ban on the use of such technologies appears out of reach, as military powers like the United States, China, Russia and Israel are not willing to accept limitations in the technological arms race. However, the majority of contributions to the UN report by states and civil society groups expressed support for some form of prohibitions or regulation.

It complicates matters that, as a general-purpose technology, AI is inherently a dual-use technology with civilian and military applications. On the one hand, this helps conflict parties with lower budgets such as Ukraine, which according the New York Times has turned into a "Drone Silicon Valley". One the other hand, it also raises risks of uncontrolled proliferation that are more diffuse than the risks posed by nuclear weapons. Emerging international initiatives such as the process on Responsible AI in the Military Domain (REAIM), set up by the Netherlands, acknowledge this.

The new EU AI Act excludes military applications from its scope but brings them in through the risk-based approach that puts dual-use applications in the highest risk category, which requires human oversight. At the same time, the EU aims to develop synergies between civilian and defense research, through the European Defence Fund, but also in its next EU framework program for research and innovation (FP10) after 2028. A European Commission White Paper proposing different options for shifting away from the civilian focus under Horizon Europe has sparked controversy in the academic community.

Green-minded actors should engage in discussions about EU-wide and global governance of dual-use and military AI applications, for example by building on the AI Act's tiered approach to risk assessment as Raluca Csernatoni of the Carnegie Endowment proposes.

More common types of cyberattacks, from data breaches to hate speech and digital violence to disinformation campaigns, can also cause considerable personal and financial harm. National cyberdefense as well as private-sector cybersecurity offers tend to focus on protecting public or private sector systems (information security). A broader feminist approach includes private citizens and civil society organizations, and investigates which groups are disproportionately harmed since they lack adequate support (such as gender or racial/ethnic minorities, migrant/refugee populations or persons with disabilities, as well as the actors working with these groups). Many of these actors cannot afford private cybersecurity software or emergency services. Cyberattacks can be especially damaging for low-income countries and regions, which lack sufficiently secure infrastructure and rely on foreign software and digital services.

Incidents of cybercrime such as identity theft, breaching of bank accounts or money extortion scams have risen sharply since the Covid-19 pandemic. The global costs of cybercrime are estimated to almost triple from $8.44 trillion in 2022 to $23.84 trillion by 2027, according to data from Statista, the FBI and IMF. The theft of personal information can be more damaging to vulnerable groups such as women, homosexual or trans people.

Gender-based digital violence has also been on the rise in the same period. Online threats against women have multiplied in countries ranging from Australia to Sri Lanka. Green advocacy and coalition-building can highlight this concerning trend, which is often treated as a consumer rights issue while disregarding the underlying structural inequality.

Disinformation is the other big category of cyberthreats. Underneath the threshold of warfare, disinformation campaigns that are directly or indirectly under the control of a foreign state are at the center of what NATO, the European Commission and the German Ministry of the Interior classify as hybrid threats. In the 2024 super election year, Russian interference – by amplifying conspiracy theories, posting polarizing content from social media accounts or creating AI-generated deepfakes – was detected ahead of elections in the UK, in France as well as for the European Parliament. In the Global Majority, pro-Russian accounts fueled polarization ahead of polls from Senegal to South Africa. The U.S. fears interference from Russia, China and Iran in its presidential elections in November 2024.

Not all disinformation is foreign-directed; in most countries, the bulk of it is homemade. It shows up in the form of intentional disinformation on election candidates or politically controversial issues such as climate change. It often takes the form of personal attacks against political opponents or hate speech against certain groups. Women, gender minorities or immigrants are targeted in more aggressive ways, leading to risks for their mental and physical safety. False information can also take the form of unintentional yet harmful misinformation such as false medical information during the Covid-19 pandemic. Here again, marginalized groups (lower income or immigrant communities or women in the Global Majority) tend to be more vulnerable as they have less access to trustworthy sources or to basic digital literacy education.

Green-minded actors should monitor cyberattacks from a feminist security perspective and engage in international efforts to prevent or mitigate them by providing secure infrastructure and addressing harms caused. They should focus on protecting vulnerable groups, enabling safe democratic participation, and providing access to resources ranging from cybersecurity to digital literacy trainings to reliable information on issues affecting human security such as climate change.

PROTECT & EMPOWER: Digital rights for citizens and communities

Digital rights – from freedom of expression and information to data protection to freedom from algorithmic discrimination and surveillance – are under threat worldwide. Participation in the network society relies on citizens who feel that it is safe to speak up without running risks of censorship, data breaches, discrimination or surveillance.

European citizens enjoy a comparatively high level of protection due to comprehensive rights-based digital legislation and the EU has firmly anchored digital rights in the principles of human dignity, freedom, democracy, equality, the rule of law and human rights. **Given the political instability in many EU member states and the diminished Green influence after the 2024 elections to the European Parliament, it will be important for Green actors and their allies to keep fighting for a strong EU as a means of protecting digital rights.**

German and European Greens are highly visible in international conversation on digital rights based on their contribution to the EU's rights- and values-based approach to digital policy (official EU documents use the more neutral term "human-centric"). This reputation can be directly linked to the General Data Protection Regulation (GDPR).[3] The legislation has changed the business practices of big tech companies and served as a model for similar laws around the world. It remains to be seen whether the EU's legislation on platforms (Digital Services and Digital Markets Act) and artificial intelligence (EU AI Act) can unleash a similar "Brussels effect" worldwide. Maintaining this credibility is the prerequisite for co-shaping a global digital society of empowered individuals. There is no reason for complacency, even in the EU. If the EU cannot uphold its values internally, it stands to be accused of hypocrisy by those it aims to convince abroad.

Freedom of expression and information. Germany and the EU are strong advocates for freedom of expression and information as well as independence of the media. In its International Digital Policy Strategy, Germany vows to uphold a global, open, free and secure internet based on the principles of the Declaration for the Future of the Internet, which were proposed by the United States and was endorsed by more than 70 democracies.

Green-minded actors should stand up against censorship and internet shutdowns, which have become a vehicle for quelling dissent and democratic discourse in many parts of the world. Activist are monitoring this concerning trend closely in the global super election year 2024. They should lend support to prosecuted journalists and digital human rights defenders whenever and wherever possible.

The European Media Freedom Act, which the European Parliament passed in March 2024, strengthens protections for journalists and whistle-blowers. It also introduces transparency standards for media ownership and funding sources. While greeting the law as an improvement, Green negotiators did not succeed with their aim to include a complete ban

[3] As a member of the European Parliament, the current co-president of the Heinrich Böll Foundation Jan-Philipp Albrecht served as the EP's lead negotiator with the other European institutions for the GDPR.

on the use of spyware against journalists – an issue that Green-minded actors should keep pursuing in light of continuing revelations about governments around the world using the NSO Group's Pegasus spyware against dissidents and journalists.

Data access by law enforcement. Digital rights activists are continuously fighting back attempts by law enforcement to get broad data access authorities. The EU Child Sexual Abuse Regulation has become a symbol of a law that pits the cybersecurity needs of a vulnerable group (children) against the right to private communication. The proposal would allow unwarranted scanning of private messages for files and images of child abuse. **Green actors view this as a disproportionate interference into the fundamental right to privacy.** They were driving forces behind the European Parliament's rejection of the proposal in early 2024. A pan-European civil society campaign called Stop Scanning Me shaped public opinion on the draft legislation, making it known as "Chat Control". However, another failed attempt by the Belgian presidency to reintroduce the proposal in the summer of 2024 shows that the digital rights community should not let down their guard.

Cross-border data transfers. The fact that GDPR has become a model for data protection laws around the world does not mean that the global battle over data protection is decided. International efforts to harmonize cross-border data transfers, also called "data flows", represent a crucial test for the rights-based EU approach to protecting personal information and its policy of basing data transfers to non-EU countries on adequacy determinations.[4]

In the arena of global data governance, the aim to protect personal information interacts with both the economic incentive to facilitate data-sharing for innovation and the geopolitical goal of prioritizing data-sharing with like-minded liberal democracies in the competition with systemic rivals. It will be important not to let these (at times) conflicting policy priorities undermine the security and privacy of EU citizens.

Digital rights as a commodity: The role of data flows in trade agreements

In November 2023, U.S. Trade Representative Katharine Tai announced to put on hold and review the U.S. negotiating position on digital trade in multilateral talks (known as the Joint Statement Initiative) at the WTO. Through this announcement, the U.S. dropped previous demands to prohibit national restrictions on cross-border data flows as well as requirements to review source code of software. Authoritarian countries such as China often use data

[4] The EU allows unconditional data transfers to countries who offer a level of data protection that it determines as adequate with that of GDPR. There is no solid solution for data flows to many countries, including the United States and China. The EU-U.S. Data Privacy Framework of 2023 allows self-certified U.S. companies to receive personal data of EU citizens without additional safeguards. The agreement replaced the former EU-U.S. Privacy Shield agreement, which had been struck down by the Court of Justice of the European Union. The new agreement still stands on uncertain legal ground, given that the U.S. foreign surveillance law and practice has not changed beyond introducing new redress mechanisms for EU citizens.

localization requirements to limit the free flow of information, which is why the policy reversal caused an outcry among the U.S. human rights community critical of China.

Nevertheless, there are legitimate reasons to restrict data flows. The EU allows data transfers only to countries that offer adequate protection of its citizen's personal data. Katharine Tai recognized that for the U.S., which currently does not have federal legislation on data protection or AI, it is important not to let trade agreements limit its room for future domestic tech legislation.

The shift in the U.S. negotiating position was awkward for the European Commission (EC), since the latter had supported the former in its previous stance, prohibiting national requirements for data localization and forcing reviews of software source code. At the same time, the European Consumer Organisation (BEUC) have applauded the U.S. move and warned that by upholding the anti-localization position, the EU might undermine the EU's General Data Protection Regulation. They also worry that data transfer provisions in the EU's bilateral trade agreements might open windows for legal challenges against GDPR. In their view, the Commission has watered down its 2018 position on including strong protections for personal data in trade agreements with the UK and Japan. They warn of similar language creeping into negotiations with South Korea and Singapore.

For those eager to protect the EU's digital rights achievements, it remains crucial to counter the narrative motivated by the geostrategic competition with China, which suggests that legitimate data protection[5] can be equated with authoritarian data control. In their 2023 Hiroshima Leadership Communiqué, the G7 countries acknowledged this difference stating that, "unjustified obstacles to the free flow of data" should be distinguished from "legitimate public policy interests." Based on this distinction, G7 countries are eager to establish international standards within the initiative "Data Free Flow with Trust" (DFFT), first introduced by Japan in 2019. The OECD is tasked with formulating these standards.

The G7 process deserves close attention by German and European Greens. Experts have praised the OECD declaration on government access to personal data. Nevertheless, they worry about a compromise between GDPR and the weaker cross-border privacy rules agreed by APEC members, among them the U.S. and China. The outcome of the G7/OECD process will be non-binding, but it could become a template for future trade agreements.

The more relevant question is to ask why data (and source code) should be a part of trade agreements in the first place. From a rights-based perspective, data transfers are best dealt with in agreements such as the Council of Europe's Convention 108+, an internationally

[5] There are three major motivations for imposing data flow restrictions ("data localization"): 1. Individual rights: Preventing personal data from flowing to jurisdictions where their protection cannot be guaranteed. 2. National security: These carve-outs can be legitimate but are often used to justify authoritarian control. 3. Economic development: The goal is to keep the value-add of data processing in the country of origin.

binding treaty whose signatories commit to protecting personal data as a human right. Digital rights experts worry that the G7/OECD process might sideline such agreements.

Biometric surveillance. The EU AI Act in principle bans practices such as real-time biometric identification (e.g. facial recognition) by the police in public spaces and emotion recognition in sensitive environments such as schools and the workplace. **What worries Green lawmakers and digital rights activists is the long list of exceptions for law enforcement, national security and migration control,** which allow for widespread surveillance at the EU's external borders, creating additional risks for a vulnerable group: people on the move. The EU's hypocrisy on the issue of surveillance is also obvious in the continued trading of surveillance technology with countries with spotty human rights records. These injustices will have to be addressed if the EU wants to be seen as a rights-based digital policy actor.

Workers' rights in the digital economy. The digital economy has produced unfair and exploitative labor conditions. With strong Green support, the EU Platform Workers Directive emerged from the European legislative process in April 2024. The measure, which will have to be implemented by EU member states through national legislation, aims to strengthen the rights of workers in the gig economy (from Uber drivers to Amazon warehouse workers), who are often misclassified as self-employed, allowing platforms to evade labor, tax and social security legislation. More efforts are needed to address the conditions of platform content moderators and workers who train AI algorithms for image or language recognition. In an open letter to U.S. President Biden, 97 African content moderators accused U.S. tech companies of "systemically abusing and exploiting African workers," highlighting the plight of these workers – from low pay to emotional distress. A lot of this work happens under similar conditions in the EU where contractors for those tech companies hire workers – often of foreign origin – to perform these tasks, as highlighted by a Spanish court ruling that a Meta content moderator suffered work-related mental trauma. The "Data Workers' Inquiry" project captures reports from people in this industry from Syria to Germany[6] – illustrating that this is an issue that needs to be addressed at a global level.

Green-minded actors need to be at the forefront of preventing the erosion of digital rights within the EU, from the right to encryption of private communication to secure cross-border data flows to protection from censorship and surveillance.

[6] This project, which adapts the adapt Karl Marx's 1880 Workers' Inquiry to the digital economy, is a joint initiative by the Weizenbaum Institute, the Technical University of Berlin, and the Distributed AI Research Lab.

EMPOWER & SHAPE: Promote a digital transformation for the common good

The road to a free and networked global digital society leads through empowering citizens and communities by giving them control over their data and by providing them with access to the infrastructure, resources and knowledge they need to shape their own digital future.

In its International Digital Policy Strategy, Germany pledges increased engagement within the EU's Global Gateway Initiative and the G7 Partnership on Global Infrastructure and Investment with the goal of "scaling" digital infrastructure in line with "our interests and values." The document mentions increased cooperation within EU, G7 and NATO on building out subsea and terrestrial cables, satellite constellations and "green" data centers.

Two issues that are mentioned at the very end of the strategy ("We use digitalization to solve global challenges" – with reference to the UN's Sustainable Development Goals) provide room for broader engagement by Green policymakers and Green-minded stakeholders. One is the promotion of open-source and open standards to create Digital Public Goods and the other is Germany's international commitment to a sustainable digital transformation in line with our climate and environmental goals.

Data sharing. There is a growing need for global data sharing to further knowledge access/exchange and innovation. Medical data can lead to the development of new cures. Transportation data can support sustainable traffic planning. However, citizens should be in charge of deciding when and how to share their data and with whom – and they should be able to trust that their information is handled and stored in the safest possible way. Apart from pushing back against clauses in trade agreements that risk lowering data protection, Green actors should support rights- and sovereignty-respecting alternatives to global "data flows".

Novel data governance approaches provide the ability to query data without moving it. Examples include federated cloud solutions used in the business sector, and the EU's approach to building public shared data spaces in sectors such as health, agriculture or mobility as a counterweight to tech monopolies. These approaches also have benefits for the climate and the environment since they reduce duplication of data by sending copies across borders. Successful European models could be the best argument for a new international approach to data-sharing outside of the trade logic.

Access to digital infrastructure. A geopolitical view of digital policy cannot exclude the dimension of development cooperation with the so-called Global South. Global Majority is the more useful term because it signals that Germany, the EU and their democratic allies in the Global North cannot expect to set global rules without entering into broader coalitions with an open mind, fresh ideas and adequate financing. The G20 summit in India and the BRICS summits in South Africa in 2023 made it clear that leading countries in Africa, Asia and Latin America – internally divided as they may be, especially between India and China – collectively aim for a stronger role in shaping the future direction of the global order.

For much of the Global Majority, universal and meaningful connectivity to the internet and digital devices remains a major unresolved challenge. The EU has set out to address this gap through Global Gateway, the initiative that was launched in 2021 to counter China's Belt and Road. With this initiative, the EU and its member states combine development priorities (addressing the global connectivity divide, working towards reaching the SDGs) with strategic interests to bolster digital sovereignty in an age of geopolitical and systemic competition. Digital infrastructure was identified as a core pillar. Yet, investments in this area have lagged behind other sectors like transportation and clean energy.

Even in light of shrinking development cooperation budgets, Green-minded actors in Germany and the EU should push for mobilizing public-private co-financing for digital infrastructure – ensuring that European offers result in secure and sustainable infrastructure and are complemented by "soft elements" that increase human security and empower citizens and communities, such as regulatory support and digital literacy training.

Access to knowledge and innovation. Apart from the infrastructure, equitable access to software, tools and knowledge is another key prerequisite for ensuring an inclusive digital transformation. This requires new approaches to international patent and copyright regimes as well as public support for open-source software solutions (e.g. Github and Apache) and knowledge commons (e.g. Wikipedia or open educational resources). Green-minded actors are advocating for a Digital Knowledge Act to break down barriers to knowledge access for researchers and for the public good in the EU.

From Digital Public Infrastructure to Digital Commons: Open-source and open standards

The development of a Digital Public Infrastructure and a Digital Public Space aligns with Green values of gender equity, sustainability and digital rights, as well as with German and European visions of digital sovereignty.

The Indian G20 presidency's focus on Digital Public Infrastructure (DPI) in 2023 gave a clear indication for where emerging economies see the greatest potential for digital cooperation. In the G20 definition, DPI enables secure and interoperable access to services such as health care, financial services, and education. DPI – such as the India Stack – typically consists of three core building blocks: identity verification, payment systems and data exchange.

There is however no universally agreed definition of DPI. A G7 ministerial meeting proposed a narrower version that views DPI as providing access to only government services, not private services such as banking. Other questions are: What role should the private sector play in building and operating those systems? Should DPIs rein in market concentration (and strengthen national digital sovereignty) by setting standards such as interoperability? Lastly, should DPI come with the requirement of open rather than proprietary technology?

"States have lost their monopoly on public infrastructures," stated Henri Verdier, France's Ambassador for Digital Affairs, at a conference at the European Parliament in November 2023. Bringing the state back is the first step in pushing back on the commercialization of our public life. Yet citizens and communities should be empowered at the same time, in order to safeguard against state-led centralization. The Open Future Foundation, therefore,

deliberately uses the term Public Digital Infrastructure (with the word public in front), which it defines as "an infrastructure in the public interest but also with public participation."

The concept of "digital commons" reflects this participatory aspect, where collectively created and managed resources are open to the public. "The only projects that stopped Big Tech were Linux, Wikipedia [and] Open Street Maps," said Verdier. In the list of digital services, which the EU has identified as "very large online platforms" under the DSA, Wikipedia – with its global network of more than 280,000 volunteers who write and edit content for the free online encyclopedia in hundreds of languages – is the only non-commercial offer.

What these models have in common is that they rely on open-source solutions such as open software, open data or open AI models. These solutions reduce technological lock-ins through proprietary software (by U.S. or Chinese big tech companies). They promote inclusion by facilitating access to social services and the economy and by allowing a global community to maintain and adapt them and to innovate based on them. The UN Secretary General's Roadmap for Digital Cooperation defines open-source products that advance the sustainable development goals as Digital Public Goods.

Germany's Ministry for Economic Cooperation and Development (BMZ) is a member of the Digital Public Goods Alliance, which is a multistakeholder initiative endorsed by the UN. Germany and the EU should ensure that solutions are developed with high standards for data protection and data security and with safeguards against biased or discriminatory use.[7]

Apart from all this, global engagement can help Germany's domestic digitalization by creating a two-way street for innovation. Germany and the EU lag behind countries like India in global registries listing Digital Public Infrastructures and Digital Public Goods.[8] Germany is addressing such gap domestically through its Sovereign Tech Fund under the Federal Agency for Disruptive Innovation (SPRIN-D), which supports the maintenance of open-source software. There are growing calls to replicate such national initiatives at the EU level. The President of the Italian National Innovation Fund Francesca Bria has called on the EU to set up a €10 billion Digital Sovereignty Fund with the goal to establish digital public infrastructures and digital commons as alternatives to the monopolistic platform models: "Europe can establish itself as a leader in a technology landscape where innovation serves the public good."

Digital and Green twin transition. The European Green movement has a particular responsibility to advocate for a digital transition that addresses climate change and environmental degradation rather than adding to these problems with the excessive carbon

[7] In India, the Aadhaar biometric identification system – which provides a unique identification number to citizens and residents – has helped to connect hundreds of millions of citizens to digital public and financial services. Human rights organizations claim that it has also led to the exclusion of marginalized groups. In Kenya, similar concerns have delayed the rollout of its Maisha Namba digital ID program.

[8] The EU made the global DPI database hosted by the G20 with its cross-border Covid warning app.

footprint of digital technologies. Greens in the German Bundestag acknowledged this responsibility in their position on digitalization and climate protection in November 2023.

For many years, the focus of these debates has been on the use of digital technologies such as AI for averting negative consequences of extreme weather events or for optimizing energy and transportation systems as well as agricultural production. These innovations deserve public support, but the focus on "AI for Good" has often distracted the policy conversation from the energy and resource use of digital technologies. The electricity use of these technologies has risen exponentially due to the computing power needed for training and using large-language and image recognition models. Other critical issues are the immense water use for cooling data centers as well as the rising demand for rare minerals to build computing hardware, from data centers to electronic consumer devices.

At the international level, Germany is engaged in the Coalition for Digital Environmental Sustainability (CODES), which was set up in 2021 in response to the UN General Secretary's roadmap for global digital cooperation, Our Common Agenda. The initiative aims to accelerate innovation of digital tools and just solutions for national climate mitigation and adaptation goals and other environmental commitments. Addressing the negative impact of the digital sector on our climate goals, the coalition has also set out to develop harmonized greenhouse gas reporting standards for the digital industry as well as sustainable procurement rules and digital product passports for the circular economy.

Green policymakers in the EU can be proud of recent progress on the circular digital economy. In April 2024, the European Parliament approved the Ecodesign Regulation, which introduces digital product passports with information on a product's origin, composition, and possibilities for repair and disassembly. At the same time, the new Right to Repair Directive aims to reduce electronic waste by making it easier and cheaper to repair household goods such as digital devices rather than replacing them.

A lot of work remains to be done when it comes to the climate and environmental impact of AI. Greens successfully negotiated a requirement for environmental impact assessments, in addition to human rights assessments for high-risk AI systems, into the European Parliament's draft. However, there was not much left of those provisions in the final version agreed with the Commission and the Council.

For a truly Green international digital policy, it is important to address the role of AI and other digital technologies at national levels and as part of the European Green Deal. At the same time, Green actors should promote German and European participation in international initiatives such as CODES as well as financial, technical and regulatory support to cooperation partners representing the Global Majority.

Outlook: A Green window of opportunity

The Green window of opportunity to shape the next phase of Germany's and the EU's digital foreign and security policy is now. The EU has established itself as global leader in tech governance, in no small part due to Green efforts. Yet in light of shrinking global space for human rights and democracy and of fierce geotechnological competition between the US and China, there is no time for complacency. As Europe struggles to catch up on innovation, the United States and others work on catching up with regulation. Europe will have to work hard to maintain its rights-based approach to digital policy while also establishing itself as a responsible tech innovator with global market power.

As part of the government coalition in Germany, which also includes the Social Democrats and the Liberals, Greens have the opportunity to shape the final phase of discussions about the Global Digital Compact, global AI principles, and the future of multistakeholder Internet governance at the UN. This room for action may shrink given the coalition's uncertain future past 2025, and Greens will also have to adjust to their weaker status in the European Parliament after the shift to the right in the 2024 elections.

Nevertheless, even below those highest levels of power, **Green-minded stakeholders** can balance the dominant hard power paradigm by lending support to broader coalitions and amplifying the voice of civil society and stakeholders from the Global Majority. **By doing so they can work towards a global tech ecosystem that protects human rights and democracy, and anchors all solutions to global challenges in feminist, human-centric and environmental values and principles.**

The fight for a better digital future ultimately goes hand in hand with the goal of creating safe spaces for economic and social development and for empowering individuals and communities vis-à-vis companies and states. It has to be guided by a better version of the network society vision: a vision that is anchored in human security, strives for gender equity and inclusion, and aims to reduce harms to the climate and the environment caused by the digital transformation.