Coordinating committee for the governance of artificial intelligence

Thorsten Jelinek (Taihe Institute),
Danil Kerimi (World Economic Forum (WEF)),
Wendell Wallach (Yale University Interdisciplinary Center for Bioethics)

November 24, 2020 | Last updated: December 10, 2020  Tags: Digital society, Multilateralism

This policy brief proposes a Group of 20 (G20) Coordinating Committee for the Governance of Artificial Intelligence (CCGAI) to coordinate the mitigation of cyber-physical threats and long-term structural imbalances on a global level. The G20 is the correct institution for this role given its influence on international policy. The CCGAI requires further institutionalization of the G20 to increase trust and legitimize such a global umbrella role. It must also counter the fragmentation of today's digital regime complex. The challenges of Artificial Intelligence (AI) governance, the institutional features of the CCGAI, and an initial agenda are highlighted, including the proposal of a Coordinating Forum as an informal forerunner of the CCGAI.

Challenge

There is an urgent need for a global coordination of AI governance (Wallach and Marchant 2019). Intelligent automation, coupled with the reuse of mass data and ubiquitous digitalization, has become a global driver for economic and geopolitical competitiveness. However, no single country or stakeholder can effectively mitigate the changing landscape of direct cyber-physical threats and longer-term structural imbalances that will impact entire societies, economies, and governments, as well as international relations (Brundage et al. 2018). AI applications span a broad array of domains and pose unique risks in each. Such technology determinism ultimately raises fundamental questions concerning human dignity and existence and therefore needs to be addressed on a global level (Scharff and Dus 2014).

The proliferation of normative frameworks, which advocate for a responsible use of AI, reveal the widespread perception of a fundamental ethical and governance gap (Jobin, lenca and Vayena 2018; Zeng, Lu and Huangfu 2018). While those frameworks have been defined rapidly, respective governance approaches, which designate possibilities for collaboration and should be guided by those normative commitments, are still lacking and will be much more difficult to realize. There are at least three fundamental dynamics that undermine the governance of AI and, conversely, make a global coordinating mechanism an urgent necessity (Jelinek 2020):

First, AI is based on disparate technologies that have different threat and risk scenarios across different applications, sectors, and geographies. Those technologies that are advancing and being deployed rapidly will eventually permeate all aspects of human life. Existing regulations and traditional regulatory approaches do not match this complexity, nor can they keep up with the speed of AI advancement and adaptation (Wallach and Marchant). Second, AI governance, which includes coordinated actions concerning ethics, norms, policies, industry standards, laboratory practices, and engineering solutions, is exposed to fierce competition over global AI leadership. Competition fosters innovation, but also compromises responsibility and leads to a concentration of AI resources and power imbalances. Third, cultural differences and competing political interests and systems, especially the current state of competition, lead to conflicting normative frameworks and regulations. They increase tension between state actors and further undermine much-needed international cooperation. Those differences and tensions are perpetuated through rising nationalism and populism as well as a heightened distrust in multilateralism (Jelinek 2020; Morse and Keohane 2014).
AI increasingly amplifies the broader discourse on digitalization and cyberspace, which already manifests as a highly fragmented “regime complex” (Nye 2014). Without global coordination and joint interventions, the increasing demand for digital sovereignty could turn into technological nationalism and reinforce a low-trust environment. AI bears its own technological risks, but it is human behavior and the use of AI that primarily risk reinforcing the current trajectory of humankind. Furthermore, as history has entered the downward spiral of “contested multilateralism” and “great power competition,” the risk of experiencing more of the downside of AI and technology determinism is likely (Jelinek 2020; Morse and Keohane 2014; Scharff and Dus 2014). A globally disruptive trend within an already fragmented environment requires a globally coordinated response. The G20 is the obvious institution to implement a CCGAI due to the group’s considerable influence on international policy coordination and framework design (Hilbrich and Schwab 2018).

Proposal

Balancing the need for competition, innovation, and cooperation while mitigating the risks and undesirable consequences attributed to AI poses a daunting challenge for governments. This challenge arises from the dual-use, uncertain, and all-embracing character of AI, as well as from an already fragmented cyber regime complex and the increasing lack of international cooperation and trust (Morse and Keohane 2014; Nye 2014). Therefore, this policy brief proposes the implementation of a G20 CCGAI (cf. Wallach and Marchant 2019). In 2019, the G20 agreed on a set of norms for “human-centered AI that promotes innovation and investment” (G20 Japan 2019). The G20 should build on those recommendations, which were derived from the OECD Principles on AI (2019), and implement the proposed mechanism. For the G20, this would be an opportunity to actively reduce and mitigate AI threats and risks while countering today’s fragmentation through integration, coherence, and respect for differences.

Demand for an international coordinating mechanism

The informal organization of a deliberative, international forum by a rotating secretariat that facilitates loose linkages and groupings between the most powerful state and non-state actors is considered to be the force that has guaranteed the continuation of the G20 since its inception. However, such informality and flexibility has also been scrutinized as the G20’s weakness and limitation (Benson and Zürn 2019; Slaughter 2020). The establishment of a G20 CCGAI would demand further institutionalization of the G20, but only concerning the issue of AI governance (cf. Cihon, Maas and Kemp 2020). In this policy brief, such centralization is deemed necessary to improve the effectiveness, not only of the G20, but also of the entire cyber regime complex in reducing and mitigating AI cyber-physical threats and longer-term structural imbalances. The G20 is one among various actors within the cyber regime complex but has the capacity for such global stewardship and can improve the overall functionality of today’s cyber regime complex.

A proliferation of non or partially integrated organizational, national, and regional normative and pre-regulatory approaches has been the initial response to this globally emerging technology. There are clear advantages of decentralized, network-driven, and polycentric governance arrangements (Cihon, Maas and Kemp 2020; Shackelford 2019). They are efficient in identifying the wide range of uncertainties, policy issues, and innovative solutions adjusted to local or regional requirements (European Commission 2020a, 2020b). However, those approaches occur within a cyber regime complex that is already determined by a sentiment that encourages a “return to the nation state” (Nye 2014, 3). Today’s demand for digital sovereignty, which seeks balance between protection and collaboration, risks both undermining multilateralism and leading to “digital nationalism” (Jessop 2011; Morse and Keohane 2014; Scharff and Dus 2014). The result is a dysfunctional regime complex that will weaken local and regional approaches and render them ineffective (cf. Keohane and Victor 2010; Nye 2014). Thus, only a comprehensive approach coordinated on a global level is effective to prepare against, mitigate, and recover from future threats and structural imbalances, and eventually address still distant scenarios of a transhumanist era (Wallach and Marchant 2019).

A CCGAI does not imply a single legal structure with direct enforcement authority and a fully integrated international cyber regime complex. Such levels of centralization would be neither feasible nor desirable. However, the CCGAI must strive to counter fragmentation by striking a balance between the G20 as an informal and crisis response-driven institution and a G20 that takes on a formal global umbrella role for ongoing cooperation and coordination. Such an umbrella role would build upon and align with established procedures, shared long-term orientations and action plans, and joint presentations and appearances (cf. Hilbrich and Schwab 2018). The implementation of a CCGAI would require further institutionalization of the G20 based on, but not limited to, the following four institutional features that would mandate the CCGAI as a “metagovernor” (cf. Benson and Zürn 2019; Cihon, Maas and Kemp 2020; Hilbrich and Schwab 2018; Schedler 1999; Schoite 2011):
1. **Comprehensive coordination** is a metagovernance (Jessop 2011) task designed to institutionalize linkages between the CCGAI and relevant actors within the G20 complex, including committees, boards, task forces, and engagement groups such as the Business 20 (B20), Civil Society 20 (C20), and Think 20 (T20). The overall task is to synchronize, integrate, and delegate responsibilities and decision-making between the competencies. Such an empowering coordinating function must also formally build and maintain linkages between the G20 and the main actors and hierarchies within the broader AI and cyber regime complex. In this process, the CCGAI does not seek to compete against other institutions and regimes but to facilitate collaboration with the aim of achieving integration and supporting the implementation of a global agenda for responsible AI governance. The coordination function could serve to prepare and negotiate international agreements and treaties and help the G20 develop from a discrete into an active agent.

2. **Accountable procedures** are paramount to gaining legitimacy and trust (Buchanan and Keohane 2006; Schedler 1999; Scholte 2011; Shackelford 2019). Coordinating between member states, competencies, hierarchies, and governance networks and reaching decisions require transparent, rule-based, justifiable, and sanctionable procedures. Such formalization is crucial, but it is not transparency alone that contributes to the effectiveness of the CCGAI. Coordination must also remain flexible and leave space for informality, both of which have contributed to the continuation of the G20. As consensus will not always be feasible within the current fragmented context and with uncertain technology, the CCGAI must also follow a normative procedure for tolerating ambiguity and conflict. The CCGAI should look for common views, respect differences, and facilitate debate over differences in hopes of forging common views over time (Cihon, Maas, and Kemp 2020).

3. **Strategic foresight** allows for improving the effectiveness of coordination and decision-making (Cihon, Maas, and Kemp 2020). It requires monitoring the development and application of AI and related policies, incubating and accelerating policy responses, and proposing early warnings and global mitigation strategies in relation to a continuously updated spectrum of AI threats and risks. The CCGAI would not promulgate new governance instruments; rather, it would share oversight outcomes and catalyze the instruments that have already been promulgated or proposed. The CCGAI could analyze how existing governance and regulatory instruments fit together, where they agree, and where gaps and policy conflicts still need to be addressed. Foresight should also be utilized to measure the CCGAI’s own capability to lead and improve the functionality of the AI and cyber regime complex based on the following six criteria: coherence, accountability, effectiveness, determinacy, sustainability, and epistemic quality (cf. Keohane and Victor 2010). Foresight information should be stored in the already existing G20 Repository of Digital Policies (G20 Argentina 2018).

4. **Public consultation** improves the transparency and effectiveness of the governance coordination process and creates legitimacy and trust (Benson and Zürn 2019; Buchanan and Keohane; Cihon, Maas, and Kemp 2020). A consultation mechanism needs to be formalized where stakeholders, especially civil society groups and non-G20 countries, are integrated into a separate secretariat and contribute at the level of official policy discussions. Public consultation is a platform for providing feedback, raising concerns, and addressing asymmetric power relations and domination, including the needs of small nations and underserved communities. It should be an instrument that enables an inclusive coordination process, empowers self-organization and governance networks, and helps to accommodate a multilayered, multidisciplinary, and polycentric environment. Fair access instead of preferential treatment must be provided. Public consultation is a mechanism for true multi-stakeholder input, and allows the G20 to remain open, flexible, and reflexive. The CCGAI should collaborate with other organizations, specifically the United Nations, that have already established strong links with civil society and run programs for digital cooperation.

**Coordinating forum as intermediate step**

The implementation of such institutional features requires a consensus among the G20 member states as well as the acquisition of additional resources to plan, implement, and operate a CCGAI. Asking for such commitment might prevent the establishment of a CCGAI. Hence, this policy brief also proposes a **Coordinating Forum for the Governance of AI (CFGAI)** that could function as an intermediate step toward the establishment of a CCGAI. Such a light version of a CCGAI would not require any reform, but would invite major stakeholders to discuss the goals, principles, and institutions of a future coordinating committee as well as the risk and themes outlined within this policy brief. Participation would be on a voluntary, but recurring, basis to ensure a continuation of the debate and follow up with joint declarations and tasks. The CFGAI should be understood as a precursor that tests and implements new institutions and, ultimately, leads to the establishment of a coordinating committee.

**Prevention and mitigation of direct threats and structural imbalances**

For effective coordination, it is necessary to specify the object of coordination itself, which includes the different dimensions, sectors, and specific aspects of AI norms, governance, and engineering. The joint target of coordination and policy discussions involves at least a
specific aspects of AI norms, governance, and engineering. The joint target of coordination and policy discussions involves at least a common definition of AI (cf. Corea 2018), the broader AI ecosystem (cf. Lorenz and Saslow 2019), and the risk profile (cf. Brundage et al. 2018). There are various definitions of each of those domains, which need to be revisited, and a common understanding needs to be reached and frequently updated by the CCGAI. This policy brief draws the focus to the latter—a comprehensive AI risk profile (Brundage et al. 2018; Jelinek 2020). This should be at the center of prioritizing international coordination and realizing the G20’s commitment to human-centered AI. The use of AI has been cautioned against as a source of unprecedented risks. Those risks can be clustered into two groups (Jelinek 2020, 2): (a) threats that are experienced directly in a specific domain and (b) risks that are structural and unfold over a longer period of time.

A. Direct threats: The advancement and diffusion of AI technologies impact the landscape of cybersecurity threats. Cyber threats will change and intensify tremendously due to the adversarial use of AI. There will be an expansion of existing threats, more effective and targeted threats, and the emergence of entirely new types of cyber-physical threats. In addition to such intentional attacks, there will be unintended and unpredictable accidents, which will also be the target of intentional exploitation. Against such an intensifying scenario of cyber-physical threats, the question of AI security has already become a matter of national security and protection of critical national infrastructure. Without stronger commitment for global coordination and responsibility, AI security questions might further divide and fragment the cyber regime complex.

B. Structural imbalances: The structural imbalances have longer-term consequences. They are more difficult to anticipate, but their impact is expected to be much more widespread and pervasive. As AI risks reinforce technology determinism, the structural imbalances will impact all dimensions of human affairs, including the economy, social, political, and international relations. Economically, mass labor displacement, underemployment, and de-skilling are likely outcomes, which especially threaten low- and middle-income countries. For societies, increasing lack of dignity, privacy, and meaning will threaten physical and psychological well-being and social cohesion. Politically, AI increases the structural risk of shifting the power balance between the state, the economy, and society by limiting the space for autonomy. While authoritarian states could slide into totalitarian regimes, democracies could witness the erosion of their institutions. A fierce global competition over AI leadership risks disrupting existing international relations. Ultimately, proliferation and ease of access to offensive, AI-enabled cyber capabilities, notably lethal autonomous weapons, increases the risk of ongoing asymmetric conflicts.

A CCGAI would need to monitor and map the full spectrum of direct threats and structural risks and understand the emerging interdependencies between AI and the broader dimensions of human affairs. Although security is generally not a domain of the G20, AI security should be included given its risk of reinforcing the fragmentation of the cyber regime complex. The purpose of such comprehensive monitoring is both to direct policy discussions and develop international mitigation strategies, early warning systems, and crisis response plans. Derived from this risk spectrum, the following themes for a global coordination agenda are proposed:

1. Digital sovereignty: policies balancing digital and technology sovereignty, multilateralism, and a global level playing field.
2. Inclusive digital economy: ensuring a just transformation of work and society, while promoting AI and data as drivers for a digital global economy, innovation, and competitiveness.
3. Market power imbalances: addressing the needs of developing nations and underserved communities through capacity building and adaptation of development models.
4. International security: possible conventions, roles, and responsibilities in cyberspace concerning the proliferation of offensive cyber technologies.
5. System failures: minimizing and mitigating the risks of unintended system failures and exploitations of engineering loopholes.
6. AI for common good: utilizing technology for the common good, including areas such as decarbonization, health and pandemics, energy, food, and inequality.
7. Coordination architecture: as governance failure is a primary risk itself, coordination and governance mechanisms must remain part of ongoing discussions and reform.

Organization and cooperation
The CCGAI should have a coordinating committee, advisory group, working group, cooperation accelerator, policy incubator, and observatory with foresight and help desk capacity. As the highest-level body, the coordinating committee should be a permanent, chartered committee, led by annually rotating co-chairs, and convene the heads of state and government and key non-state representatives. Its members must agree on common objectives and norms, designing and implementing the coordinating mechanism, defining and adhering to the criteria for the functionality of the CCGAI, including coherence, accountability, effectiveness, determinacy, sustainability, and epistemic quality. The committee will follow the institutional features of the CCGAI, like the four features proposed above. The members should seek consensus, make recommendations, and agree upon plans and actions, but need to remain respectful of differences. The CCGAI must maintain itself as an agile, cooperative, and comprehensive international coordinating mechanism (cf. Wallach and Marchant 2019). Initially, the CCGAI should agree upon a common charter that captures the commitment of the member states as well as the overall goals and procedures of the CCGAI.

The G20 needs to build its own coordination capacity to carry out the function of a CCGAI, should incorporate related work that has been done within the G20 complex, and establish linkages to existing procedures, declarations, principles, and tools. Notably, it should revisit the Digital Economy Development and Cooperation Initiative (G20 China 2016), Digital Economy Ministerial Declaration (G20 Germany 2017), and Ministerial Statement on Trade and Digital Economy and AI Principles (G20 Japan 2019). It should also utilize the G20 Repository of Digital Policies (G20 Argentina 2018). However, the CCGAI cannot and must not own and carry out all proposed functions and topics. Some of them should be carried out by other multilateral organizations, but the CCGAI should remain the primary coordinating body.

Obstacles to the coordinating committee

Competition between the bigger powers, rising nationalism and populism, as well as the disruption of the post-war liberal order likely undermine the establishment of a G20 CCGAI due to the fear of compromising influence and power (Cihon, Maas and Kemp). There is an ongoing resistance within the G20 to reforming itself. However, the group was established due to the rise of the multipolar world and middle-power countries. It is those countries that have a strong interest in multilateralism and a CCGAI. A G20 CCGAI would also complement the newly established G7 Global Partnership on Artificial Intelligence (U.S. Department of State 2020). Additionally, the B20 might resist as large businesses seek to maintain their privileged and informal access to the G20 (Martens 2017). To balance private sector interests and help to increase trust in businesses and institutions, the G20 should forge public-private partnerships that provide a vision for a caring digital economy (cf. Chierchia et al 2017) and help to ensure that essential digital resources are managed as common resources (Ostrom 1990).

Disclaimer

This policy brief was developed and written by the authors and has undergone a peer review process. The views and opinions expressed in this policy brief are those of the authors and do not necessarily reflect the official policy or position of the authors' organizations or the T20 Secretariat.

References


Existing Initiatives & Analysis