CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

AUGUST 2019

New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?

Camino Kavanagh

New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?

Camino Kavanagh

For your convenience, this document contains hyperlinked source notes indicated by teal-colored text.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Introduction

Significant technological advances are being made across a range of fields, including information communications technology (ICT); artificial intelligence (AI), particularly in terms of machine learning and robotics; nanotechnology; space technology; biotechnology; and quantum computing to name but a few. These breakthroughs are expected to be highly disruptive and bring about major transformative shifts in how societies function.

The technological advances in question are driven by a digital revolution that commenced more than four decades ago. These innovations are centered on the gathering, processing, and analyzing of enormous reams of data emerging from the information sciences with implications for countless areas of research and development. These advances promise significant social and economic benefits, increased efficiency, and enhanced productivity across a host of sectors.

Technology's Disruptive Potential

But there are mounting concerns that these technologies and how they are used will pose serious challenges, including labor force dislocations and other market disruptions, exacerbated inequalities, and new risks to public safety and national security. The technologies are mostly dual use, in that they can be used as much to serve malicious or lethal purposes as they can be harnessed to enhance social and economic development, rendering efforts to manage them much more complex.[1] Relatively easy to access and use, most of them are inherently vulnerable to exploitation and disruption from both near and far.

In parallel, geopolitical tensions around the world are growing, and most countries increasingly view these technologies as central to national security. The potential for misuse is significant. And greater economic integration and connectivity mean that the effects and consequences of technological advances are far less localized than before and are liable to spread to countries and industries worldwide.

Technological innovation is largely taking place beyond the purview of governments. In many cases, the rate of innovation is outpacing states' ability to keep abreast of the latest developments and their potential societal impacts. And even if one or a handful of national governments devise policies for managing these effects, the global reach of many emerging technologies and their impacts requires new approaches to multilateral governance that are much more difficult to agree on. A greater number and variety of actors must be involved to initiate, shape, and implement both technical and normative solutions.

Yet, like governments, many of these other actors do not have (or simply do not invest in) the means to consider the broader, cross-border societal implications of their investments, research, and

innovations. When they do so, identifying the most relevant or effective policy-oriented or normative-focused platforms to discuss these implications can be challenging, not least because existing platforms sometimes do not consider the variety of actors implicated, the cross-border reach of the technologies in question, and the different value and political systems at play. This is particularly the case when technologies are designed for profit-making alone and their trajectories are entirely dependent on market forces.

Today's technological advances are deemed disruptive not only in market terms but also in the sense that they are "provok[ing] disruptions of legal and regulatory orders" and have the potential to "disturb the deep values upon which the legitimacy of existing social orders rests and on which accepted legal and regulatory frameworks draw."[2]

Complex, dynamic frameworks already govern some fields of technology. For instance, cyberspace is governed by an amalgamation of existing international law; as well as an ever-growing, complicated array of political agreements; technical standards and protocols; trade, business, and human rights standards; research principles; national regulations; and self-regulation in the private sector. These legal and normative touchstones are underpinned by existing norms, values, and principles. They span different policy areas and issues, enlist a dizzying host of actors, and straddle numerous international regimes. What is more, they are complemented by a growing body of confidence- and capacity-building measures and efforts aimed at enhancing security and resilience.[3] Yet important elements of this regime remain contested, even as new risks and vulnerabilities—such as those related to the Internet of Things, AI, and other technologies—emerge and need to be managed.

Looming Governance Dilemmas

The World Economic Forum's (WEF) founder, Klaus Schwab, has described technological advances (for better or worse) as a "revolution" due to their "velocity, scope, and systems impact."[4] In discussing what he has dubbed a "Fourth Industrial Revolution," Schwab emphasized a number of emerging policy and normative issues. Similarly, a 2019 paper prepared for the WEF stressed the need to "transform traditional governance structures and policy-making models" and adapt more "agile" methods of governance.[5]

But responding to the attendant risks and challenges will not require just exploring new governance structures, tools, and processes. This task calls for a deeper understanding of the social, cultural, economic, and geopolitical contexts in which policy, norms, and regulations are crafted as well as a firmer grasp of the overarching questions of power and conflict that shape humanity's relationships with technology. Moreover, significant public engagement is sorely needed, since governments and companies cannot—and should not—expect to resolve these dilemmas alone.

Some of the key challenges include:

Identifying key principles and values: Relevant actors must articulate a vision of the principles and values—such as equity, equality, inclusivity, responsibility, transparency, and accountability—that might be negatively impacted by certain technological advances and how those values might best be protected. This task will require new thinking on how to ensure certain technologies (like predictive algorithms, biotechnology, or technologies allowing space resource exploitation) do not exacerbate existing socioeconomic inequalities, or how best to respond to new encroachments on personal privacy involving the body and the brain. Certain forms of research (like some aspects of biological engineering) may need to be restricted.

Determining appropriate principles and values requires more than a shared understanding of how technological innovations are evolving, how they have been designed, and how they might be used. Such normative reflection also calls for a clear sense of the different values and principles held by various communities worldwide as well as the means and actors by which such values and principles should be protected. It also necessitates going beyond the mere articulation and proliferation of principles to the practical application and acknowledgment of associated challenges and limitations.

Engaging stakeholders effectively: Legislators, regulators, private business leaders, researchers, and civic actors need to be ready to respond more responsibly and effectively to the effects and consequences of technological advances and the potential societal risks they pose. Ongoing experiments with new rules, principles, and protocols to deal with concrete relevant policy issues are certainly noteworthy, one example being the WEF's "agile" governance initiative.[6] Yet implementing these responses at scale and applying them to a host of cross-border socioeconomic and security challenges will be a complex challenge. This task likely will require a blend of approaches, increased spending in independent public research, and the involvement of many actors other than just states. To this end, it is vital that relevant actors delineate domestic and international responsibilities to determine which technology-related challenges should be addressed at home and which problems require cross-border coordination and cooperation.

Broadening existing platforms of multilateral engagement: Clarifying how various actors (and not just states) can responsibly contribute to the work of multilateral mechanisms focused on how existing international law or political norms apply to state uses of certain technologies is imperative. These platforms include the various United Nations (UN) Groups of Governmental Experts (GGEs), as well as other specialized working groups concerned with matters of technology (including ICT, machine learning, autonomous weapons, biotech, and space technology) and international security. Such efforts can also advance ongoing discussions about how to ensure that multilateral mechanisms are agile enough to determine when new global norms or rules (binding and/or nonbinding ones) are

required to manage technology-driven challenges and risks and constrain certain applications of these technologies or specific behaviors by states and other actors.

Craft suitable regulations: Fresh approaches to policy and regulation are also needed. For instance, advances in ICT, machine learning, biotechnology, and the convergence of these technologies are already driving multifaceted discussions on the focus and rationale of relevant policies and the most suitable type of regulation (precautionary, preventive, reactive, or a combination of all three). Questions also abound around whether to opt for hard regulation, soft policy initiatives (such as guidelines, certification procedures, and labeling schemes) that stop short of binding regulations, or the current trend of self-governance measures by private entities. As noted above, a key question is how to ensure these regulatory solutions are fit for purpose, and whether they should be coordinated nationally or internationally. Given the cross-border effects of the technologies at play as well as the growing convergences between them, uncoordinated national rules and policies will likely be ineffective.

Enhance transparency, oversight, and accountability: Finally, new policy and regulatory approaches will require greater investment in transparency, oversight, and accountability mechanisms. This will necessitate agreeing on the nature of national regulatory oversight bodies and determining whether they should be public, private, or of a mixed composition. This task should also entail ensuring that technology companies and organizations accept greater scrutiny. For example, tech companies should heighten internal monitoring and external reporting of their self-regulatory initiatives, provide appropriately insulated, publicly funded researchers with safe access to their data, and, above all, ensure that accountability covers all aspects of the supply chain and that both the direct and indirect costs (such as labor and environmental costs) of the technologies in question are clearly understood.[7] Agreeing on what is ethically acceptable in terms of industry's role in funding and participating in oversight mechanisms (such as ethics councils and advisory boards) is an equally important lever for injecting legitimacy into some of these processes. Such scrutiny would also help identify remaining gaps and engage more actors to help gauge if and how a certain technology or its application should be regulated.

Challenges to Effective Governance and Coordination

The international environment is hardly conducive to discussions of how best to coordinate responses to the complex, cross-border dilemmas emerging around new technologies. In some corners, existing multilateral platforms are increasingly perceived as unsuitable for resolving these challenges. The international community is notoriously slow at adopting new rules and institutions to deal with new challenges, and the quandaries posed by questions of national sovereignty and democratic legitimacy are persisting. In contrast, corporate actors appear to be racing ahead, intent on shaping the "science, morality and laws" of new technologies such as AI, with limited public debate underpinning or guiding their efforts.[8] Many of these same companies and the technologies

they produce or exploit are increasingly viewed as instruments of state power, a fact that only adds to these sovereignty and legitimacy-related questions.

Meanwhile, growing strategic competition between the world's leading powers, especially in high-tech sectors, does not bode well for multilateral efforts to respond cooperatively and effectively. Such a competitive landscape is contributing to regulatory fragmentation and will likely delay much needed normative and regulatory action. This potential impasse places strains on existing efforts and could further delay the attainment of pressing social and economic objectives such as the 2030 UN Sustainable Development Goals, which are already under stress. Moreover, the resulting trust deficit between countries poses a significant threat to international peace and security, one that existing political institutions are not necessarily prepared to handle.

Throughout history, new challenges (including those relating to technology and governance) have generally opened new opportunities and channels for cooperation. Today is no different, although the challenges at hand are highly complex and are emerging at a time of systemic political change and a rising sense of conflict and crisis. More meaningful dialogue and cooperation—however difficult—on how technological developments are affecting societies and the uses and applications of technology generating the most disruption and contestation are urgently required. Such an approach would likely afford greater legitimacy to emergent governance efforts, while also tethering them to the common good. As one expert noted in the context of the WEF's Fourth Industrial Revolution initiative:

> The moment you start saying that technology is the most powerful force today, then what you have done is argue that people have a right to shape how technologies are developed and used. In practice, this means consciously trying to shape technological trajectories, it means setting research agendas, it is to direct foreseeable technologies, to articulate uses that might benefit the majority and not the few; placing technology inside of democratic politics.[9]

Developed on the basis of interviews with experts and extensive research, this analysis assesses four areas of technology around which governance dilemmas are evident and discusses the emergent responses. These four areas include ICT, AI, biotechnology, and space technology. The decision to focus on these fields was informed by their disruptive character, the potential national and international security risks associated with their dual-use character, and the growing degree of state competition emerging around them. Importantly, this focus is also informed by the fact that these same issues are underscoring the urgent need for greater cooperation and strengthened governance frameworks to manage the associated risks. Greater understanding of these efforts can help inform how relevant actors approach current—and prepare for new—technology-related governance challenges.

Information and Communications Technology

While it is not a new area of technology, there is no doubt today that continuous advances in networked computing and other aspects of ICT are converging with advances in other technological fields, greatly increasing human dependence on these digital tools.[10] Governments around the world are establishing new institutions, identifying the policy implications of this growing digital dependence, and developing integrated frameworks for whole-of-government approaches to manage the resulting economic and societal transformations. Despite the associated benefits, humanity's growing dependency on ICT continues to present significant risks. Cybersecurity and the stability of ICT systems more generally have become top policy priorities.

The Current Normative Landscape

The "regime complex" governing ICT stems from multiple sources: the existing body of international law, political agreements, and voluntary norms; an ever-growing body of technical protocols and standards on internet governance managed by technical groups and research communities; national regulations; self-regulation by the private sector; and other forms of nonbinding soft law.[11] These norms span different topical areas, straddle numerous international regimes, and require the engagement of multiple actors.

These norms and governance mechanisms aim to strengthen cybersecurity in national and global terms; enhance international security and stability more broadly as well as general human well-being; and promote responsible behavior by drawing on existing rules, values, and principles. For instance, human rights, privacy norms, and the freedom of opinion and expression have been bolstered by a norm upholding the right to privacy in the digital age and the confirmation by the UN Human Rights Council that human rights apply online as they do offline.[12]

Many states, however, do not appear to be upholding these norms, and beyond basic privacy and human rights questions, there are increasing concerns surrounding the human costs of cyber operations, notably operations that affect healthcare and industrial systems or those that can generate systemic effects.[13] Where cyber crime is concerned, progress is equally slow. States have not managed to agree on an international framework to counter cyber crime, although many states are leaning on the existing Council of Europe (Budapest) Convention and bilateral treaties as they adopt national cyber crime legislation and cooperate on this issue.

As for international peace and security, the work of a series of UN GGEs (five to date) has reaffirmed the applicability of international law, including the UN Charter, to cyberspace and has recommended a number of voluntary, nonbinding political norms aimed at encouraging states to use ICT responsibly.[14] The norms seek to promote restraint, best practices, and other forms of positive behavior.

Specifically, many of the norms draw from existing principles of international law and address several facets of responsible use of ICT by states, including the importance of recognizing the challenges of attribution, preventing the use of a state's territory for the commission of internationally wrongful acts, not conducting or knowingly allowing activity that damages critical infrastructure and essential services to the public, safeguarding national computer emergency response teams (CERTs) and their systems from malicious cyber activities, responding to requests for assistance by other states, and reporting and sharing information on vulnerabilities. The norms also include ensuring the integrity of supply chains, upholding human rights online and privacy rights in the digital age, and enhancing cooperation and information sharing with regard to terrorist and other criminal cases that involved cyber operations.[15] Subsequently, the UN General Assembly recommended that states "be guided in their use of ICT" by the 2015 GGE report.[16]

Several international, regional, and other specialized bodies have since endorsed the GGE recommendations. Nonetheless, efforts to advance this work stalled when a new GGE (established in 2016) failed to produce a consensus report mainly due to disagreements on international law and the future work of the group. As the topic has become more politicized, in December 2018, the UN General Assembly's First Committee agreed to establish two new parallel processes: an Open-Ended Working Group involving the entire General Assembly and a new twenty-five-member GGE.[17]

Other intergovernmental organizations complement these UN-led efforts. For example, regional organizations such as the Association of Southeast Asian Nations (ASEAN), the European Union (EU), and the Organization of American States (OAS) all have endorsed the GGE norms. So, too, have the Group of 20 (G20) and international financial institutions. Additionally, the G20 has developed guidance on strengthening the cyber resilience of the financial system and has sought to foster a norm aimed at protecting the integrity of financial data.[18] Some specialized organizations, such as the International Atomic Energy Agency, have been actively developing capacity-building tools, guidance, and standards including, for instance, resources for protecting the computer and information systems of nuclear infrastructure.[19]

In national terms, states are under increasing pressure to ensure that government agencies, cybersecurity firms, and researchers discover and disclose cyber vulnerabilities in a more timely fashion and prevent these vulnerabilities from being illicitly traded or otherwise misused. In some states, these efforts are evolving into vulnerability equities processes (VEPs) or coordinated vulnerability disclosure mechanisms. While a principal aim is to strengthen transparency and oversight of government use of discovered zero-day vulnerabilities, there are concerns that such processes are bureaucratically complex and expensive and that they might remove pressure on companies to produce more secure products and services. Moreover, explicit processes for managing vulnerabilities might be seen as legitimizing government hacking.[20] Yet, realistically, governments

will unlikely eschew all use of vulnerabilities, so imposing greater due diligence, transparency, and oversight in this domain would be more beneficial than not doing so.

On a related note, another important factor is designing more secure ICT products and systems so states do not use vulnerabilities in the technology products and services that underpin people's daily lives against citizens and other states. The costs to the global economy are certainly significant, and there are growing concerns about the potential human costs.[21] The principle of security by design (see below) has been gaining currency among many engineers and entrepreneurs.

In light of persisting cybersecurity risks, governments also are moving toward more regulatory-focused solutions, many of which stop short of formal regulation. For instance, in 2018, the EU adopted a broad instrument called the Cybersecurity Act, which includes a voluntary certification framework to help ensure the trustworthiness of the billions of devices connected to the Internet of Things underpinning critical infrastructure, such as energy and transportation networks, and new consumer devices like driverless cars.[22] The framework aims to "incorporate security features in the early stages of their technical design and development (security by design)," ensuring that such security measures are independently verified and enabling users to determine a given product's "level of security assurance."[23] The effectiveness of such initiatives has yet to be gauged, although skeptics often point to challenges around voluntary certification schemes in other sectors. For instance, a scandal involving the automobile manufacturer Volkswagen (an incident commonly referred to as Dieselgate) showed the limitations of one such voluntary scheme. In such cases, the objectives may be good, but inherent conflicts of interest in process design, monitoring, and oversight tend to undermine these goals in the longer term.[24]

The Cybersecurity Act follows on the heels of the EU's General Data Protection Regulation (GDPR), which seeks to bolster EU citizens' data privacy and harmonize data privacy laws across Europe. The 2016 EU Directive on Security of Network and Information Systems is the first piece of legislation on cybersecurity that the EU has adopted.[25] In the United States, there is increasing pressure on companies to prioritize consumer protection and citizen safety, as well as to introduce "proactive responsibility and accountability into the marketplace," including through product liability. Such an approach might be particularly useful when security flaws are easily prevented "by commonly accepted good engineering principles."[26]

Meanwhile, technical issues related to internet infrastructure remain largely within the purview of the so-called I* organizations, which include the Regional Internet Registries, the Internet Corporation for Assigned Names and Numbers, the Internet Engineering Task Force, the Internet Architecture Board, the Internet Society, and the World Wide Web Consortium, as well as the regional associations of country code domain name registries.[27] Initiatives such as the Internet Governance Forum promote multi-stakeholder policy dialogue on internet-related issues, while

intergovernmental bodies (including the World Summit on the Information Society, the International Telecommunication Union, and the European Telecommunications Standards Institute) deal with some policy aspects of internet governance. And a number of UN departments and agencies provide governments with capacity building as well as technical, legislative, and other forms of support, as do national technical bodies such as CERTs and computer security incident response teams (CSIRTs), in line with a provision (Action Line 5) of the World Summit on the Information Society's Tunis Agenda.[28]

Initiatives promoted by or otherwise involving other societal actors are also proliferating. For instance, in 2018, former UN secretary general Kofi Annan established the Annan Commission on Elections and Democracy in the Digital Age, which aims at "reconcil[ing] the disruptive tensions between technological advances and democracy."[29] Another body known as the Global Commission on the Stability of Cyberspace, established in 2017, is studying how norms can enhance stability in cyberspace. Following consultations, it produced a 2018 "norm package" intended to shape the behavior of both state and nonstate actors on issues ranging from preventing supply chain tampering to combating offensive cyber operations by nonstate actors.[30] An earlier initiative, the Global Commission on Internet Governance, has advocated for an internet that is "open, secure, trustworthy and accessible to all," stressing the need for a "new social compact" designed to protect the rights of users, establish norms for responsible public and private use, and ensure the kind of flexibility that encourages innovation and growth.[31]

Industry actors are also active in multiple ways. While some of these efforts may be seen as an attempt to forestall regulation, many aim to pressure industry actors or states to commit to behaving more responsibly. For instance, in 2018, Siemens launched a Charter of Trust for a Secure Digital World at the Munich Security Conference, a document that outlined principles that the initial signatories (eight companies and the Munich Security Conference) believe to be essential for establishing trust between political actors, business partners, and customers as the world becomes more dependent on digital technology.[32] The number of charter signatories has since grown to sixteen.[33]

Microsoft, too, has promoted norms of responsible behavior for both state and industry actors, and the company has reportedly responded more positively than other corporate peers in terms of complying with new regulations such as the EU's GDPR.[34] The firm has also raised the idea of a "Digital Geneva Convention," a binding instrument that would protect users from malicious state activity.[35] Along with several other industry leaders, Microsoft has also announced the Cybersecurity Tech Accord, which advocates for increased investment in (and heightened responsibility for) cybersecurity by leading industry actors.

In 2018, the company launched a new initiative entitled Defending Democracy Globally.[36] This initiative aims to work with democracies worldwide to (1) "protect campaigns from hacking"; (2) "increase political advertising transparency online"; (3) "explore technological solutions" to protect electoral processes; and (4) "defend against disinformation campaigns."[37] The initiative emerged in tandem with the company's launch of a Digital Peace Now campaign, which calls for greater government action as well as improved cyber hygiene on the part of users. Interestingly, this campaign is silent on private sector action.[38]

In November 2018, the French government incorporated many of these initiatives under the umbrella of an initiative called the Paris Call for Trust and Security in Cyberspace, which scores of governments, industry players, and civil society actors joined.[39] Yet the announcement that has produced the most headlines is Facebook founder Mark Zuckerberg's call for greater government and regulatory action, notably in the areas of "harmful content, election integrity, privacy, and data portability" following the March 2019 attacks in Christchurch, New Zealand.[40] Importantly, he stressed the need for more effective privacy and data protection in the form of a "globally harmonized framework" urging, somewhat ironically, that more countries adopt rules such as the EU's GDPR as a common framework. Zuckerberg's opinion piece received a lukewarm reception, and many experts remain skeptical of his intentions.[41]

What Lies Ahead?

Despite this progress, significant governance challenges remain for cyberspace. Efforts to not only protect data, privacy, and human rights online but also attend to national and international security concerns are improving in some cases. For instance, according to one assessment, the EU's GDPR provides much stricter guidelines and "strict security standards for collecting, managing, and processing personal data." But the instrument does provide exemptions for data controllers or processors when it comes to "national defense, criminal investigations, and safeguarding the general public)."[42] Progress remains much more limited or has even regressed in other countries and regions.

On cyber crime, despite concerns about the growing scale, economic and societal costs, and other risks of online criminal activity, states have not been able to (and likely will not) agree on a common framework for dealing with cyber crime or other malicious online activity that imperils users and hampers economic growth and development. This state of affairs is unlikely to change, given that some states continue to insist on the need for a common framework, while others remain wedded to the expansion of the existing Budapest Convention.

There are other challenges too. Progress remains slow in terms of achieving public and private sector commitments to bridge existing technological divides and move the digital transformation agenda forward. Inequalities within and between states (and cities) are growing even as technological

advances continue to be made. This situation may make it even more challenging to meet the UN Sustainable Development Goals.[43]

Some countries will further challenge modalities of internet governance, particularly states that view greater state involvement in internet governance as crucial to national security. These divergences over how the internet should be governed continue to foment tensions among states and other stakeholders.[44] Meanwhile, several countries have announced they will seek to build their own national alternatives to the global internet, possibly further fracturing an (already fractured) world wide web, though some observers have questioned the feasibility of such alternatives.[45]

As for international security, while tensions between countries continue to fester around normative restraints on state behavior, two new multilateral processes will commence this year through an Open-Ended Working Group (September 2019–July 2020) and a new GGE (December 2019–May 2021).[46] Many observers view the two processes as conflicting and competing initiatives (given that the former was proposed by Russia and the latter by the United States). Some parties also view them as outdated (since the main actors in both mechanisms are states, although, importantly, both have included consultative mechanisms to engage with other actors such as regional organizations, private companies, academia, and civil society). But there is a signaled interest in ensuring the processes are both complementary and constructive.

That said, there are concerns, for instance, that GGE discussions on *how* international law applies to cyberspace might once again hit a wall. As noted, disagreements on international law–related issues were partly what impeded the last GGE from producing a consensus report. Since then, some states have decided to publicly share their views on how international law applies, although, to date, only a few states—Australia, France, the United Kingdom (UK), and the United States—have done so.[47] Nonetheless, it is hoped that the two new processes will make further contributions to the discussion, as per their mandates.[48] Importantly, the resolution establishing the GGE also suggests that the report include an annex in which participating governmental experts can include national views on how international law applies to the use of ICT by states.[49]

Meanwhile, some countries—and some nonstate actors—appear to remain committed to a binding international treaty. Yet the likelihood of such a treaty is perhaps slim, not least because the key actors crucial to any agreement view cyberspace and cybersecurity in very different strategic terms; at present, there appear to be limited incentives to agree on a new regime.

Beyond binding international law, the coming twenty-four months will serve as an important window into progress that has been made toward socializing and institutionalizing the political, nonbinding norms and confidence-building measures that past GGEs recommended. The two new UN processes and their associated consultative mechanisms will serve as important platforms for

sharing national experiences and lessons on how states are implementing the norms and confidence-building measures nationally and through regional organizations, and how other actors actively contribute to this end.[50]

Other groupings will likely be proactive. For example, the Group of Seven (G7) members recently committed via the Dinard Declaration to sharing lessons and experiences on said norms, and it is likely they will channel those lessons and experiences into the multilateral process.[51] Similarly, multi-stakeholder groups such as the Global Commission on the Stability of Cyberspace or industry initiatives such as the Tech Accord will surely present lessons and experiences from the norms they too have been advocating.

How countries hold each other accountable for violating norms is just as important. Indeed, some states' persistent misuse (and potentially lethal use) of ICT is driving a dangerous security dilemma involving tit-for-tat activities that have significant escalatory potential. Beyond the fact that such activities raise serious questions about the rule of law, most related crisis-management or confidence-building mechanisms would likely prove ineffective in the event of escalation if there are no real channels of diplomatic dialogue between key states. Such channels are largely nonexistent at present. In this respect, more political and financial investment in operationalizing existing commitments to confidence building, track 1 or 1.5 dialogues, and other cooperative measures is imperative.

The growing number of initiatives aimed at fostering greater cybersecurity and stability do not (and perhaps cannot) deal with some of the structural issues driving insecurity and instability. This is particularly the case with respect to ICT products and services, which remain highly vulnerable to exploitation by actors with malicious intent.[52] Greater, and more participatory, dialogue on the nature of global ICT market trends and the structural levers for making ICT products and services more safe and secure is urgently required and should not be inhibited by the growing (and valuable) focus on VEPs and other similar measures.

Finally, existing threats and vulnerabilities will surely be compounded by new problems. This means that conceptions of security will need to be reconsidered over time and that existing normative and governance frameworks will likely need to be adapted. For instance, new threats and vulnerabilities related to the Internet of Things are emerging: as the lines between human agency and "smart agent-like devices" become increasingly blurred, the safety and security of related services and devices remain serious problems.[53] Likewise, new threats are also developing in relation to critical systems dependent on AI (such as the growing number of sectors and industries reliant on cloud computing), critical satellite systems, and information and decisionmaking processes, which are increasingly susceptible to manipulation for political and strategic effect. Heightened strategic competition and deteriorating trust between states further compounds these challenges. More than ever, countries

need to invest in diplomacy to foster greater dialogue, cooperation, and coordination on the ICT-related issues that pose the greatest risks to society.

Artificial Intelligence

Although AI research has existed for more than five decades, interest in the topic has intensified over the past few years. This highly complex field emerged from the discipline of computer science. The classic definition of AI dates back to 1955, when John McCarthy and his fellow researchers characterized artificial intelligence as "making a machine behave in ways that would be called intelligent if a human were so behaving."[54] Noting that a similar counterfactual understanding of AI underpins the earlier Turing test, Florini and Cowls conceptualize AI as "a growing resource of interactive, autonomous, and often self-learning agency (in the machine learning sense . . .), that can deal with tasks that would otherwise require human intelligence and intervention to be performed successfully." Succinctly put, AI can be viewed as a "reservoir of smart agency on tap."[55]

AI encompasses numerous subdisciplines including natural language processing, machine inference, statistical machine learning, and robotics.[56] Certain subdisciplines such as deep machine learning and machine inference are often seen as points along a continuum on which progressively fewer human beings are required in complex decisionmaking.[57] Some observers believe this will eventually lead to artificial general intelligence or superintelligence that either achieves or surpasses human intelligence.[58] Yet it is fiercely debated whether AI will ever actually achieve or exceed such cognition and abstract decisionmaking capabilities.[59]

Nonetheless, advances in the various AI subfields are expected to bring about great economic and social benefits. Communications, healthcare, disease control, education, agriculture, transportation (autonomous vehicles), space exploration, science, and entertainment are just a few of the areas already benefiting from breakthroughs in AI. Yet the risks inherent in the ways these technologies are researched, designed, and developed and how they might be used can just as easily undermine these benefits.

The immediate risks and challenges include the expansion of existing cybersecurity threats and vulnerabilities into increasingly critical AI-dependent systems (like cloud computing); unintended or intended consequences as AI converges with other technologies including in the biotech and nuclear domains; algorithmic discrimination and biases; weak transparency and accountability in AI decisionmaking processes; overly narrow ways of conceptualizing ethical problems; and limited investment in safety research and protocols. Meanwhile, policymakers are fixated on predictions about how automation will transform industries, the labor force, and existing forms of social and economic organization. Predictions that automation and advanced machine learning may exacerbate

economic inequalities in particular have stoked anxiety. Several studies on subjects like the future of work, the future of food, and even the future of humanity seek to allay these concerns, while also highlighting and forecasting risk.[60]

Different AI applications and models derive (or will derive) much of their power from large quantities of collected, stored, and processed online data. Concerns over data protection, privacy, and other principles and values such as equity and equality, autonomy, transparency, accountability, and due process are growing. The dual-use nature of AI applications also makes it difficult to constrain their development and regulate their use. Moreover, recently world leaders including Chinese President Xi Jinping, Russian President Vladimir Putin, and U.S. President Donald Trump have made public declarations painting AI in terms of national power projection, a trend that suggests the development and use of such technologies will be complicated by growing strategic competition (in geopolitical, military, economic, and normative terms).[61] Moreover, some countries' desire to use AI as a "critical enabler and force multiplier for capabilities across all aspects of military power" is becoming increasingly evident.[62]

In short, further advances in AI likely will significantly alter the contours of economics, sociopolitical life, geopolitical competition, and conflict. According to some observers, the technology may even pose existential risks. Yet there is still time to think seriously about AI and develop stronger responses to the challenges ahead.

The Current Policy and Normative Landscape

Several classes of actors are playing important roles in advancing discussions about some of these issues, including nongovernmental organizations (NGOs) and nonprofits, commercial actors, governments, and multilateral forums. These efforts are resulting in the proliferation of new rules, values, principles, tenets, standards, and declarations, making it increasingly difficult to make sense of where these various standards overlap, create unnecessary duplications, or cause confusion and ambiguity.[63]

Nonprofits and multi-stakeholder initiatives: A number of initiatives involving leading scientists, technologists, researchers, civil society organizations, and investors in the fields of AI and robotics are promoting important principles to help mitigate risks and spread the benefits of AI.

Examples include the Asilomar Principles, developed in 2017 to "underpin the future development of AI and ensure shared opportunities and benefits of AI for all."[64] The twenty-three principles cover research goals, funding for safety-related research, questions of human control and responsibility, privacy, shared benefits and prosperity, efforts to ensure that AI is not used to fuel an arms race or develop lethal autonomous weapons and other military capabilities, and other values and risks. This principle on military applications and the central question of human control are integral to a

campaign spearheaded by an international coalition of NGOs—the Campaign to Stop Killer Robots.[65] The principles and the question of meaningful human control are also central to the recent Lethal Autonomous Weapons Pledge signed by key companies, organizations, and individuals,[66] and the 2015 Open Letter on AI and Autonomous Weapons signed by a host of AI and robotics researchers.[67]

Meanwhile, AI Now, a research institute working out of New York University, has produced a number of in-depth reports on various governance challenges relating to AI. This work includes promotion of principles such as fairness, accountability, and transparency across all aspects of the production and life cycles of AI systems and an assessment of (accountability for) both the direct and indirect effects of these systems. On a related note, the institute has also published what it calls the "Algorithmic Accountability Policy Toolkit."[68] More recently, it examined the principle proliferation trend and proposed that existing efforts should be unified under a common framework (discussed below).

For its part, the Institute of Electrical and Electronics Engineers (IEEE) continues to update its 2016 "global treatise" on principles and recommendations for designing AI systems in ethical ways that promote human well-being; this document was developed from more than 1,000 crowd-sourced contributions from across business, academic, and policy circles.[69] In 2019, the IEEE launched an effort to move beyond the articulation of principles. The Principles Into Practice initiative, also founded on crowd-sourced contributions, is centered on validating the existing principles.[70] The results of this effort will likely be monitored closely.

Meanwhile, the Partnership on AI to Benefit People and Society brings together a growing number of research and civil society groups as well as major AI companies to promote similar principles. The group's aim is to "study and formulate best practices on AI technologies, advance the public's understanding of AI, and serve as an open platform for discussion and engagement about AI and its influences."[71]

Commercial actors: Some companies are gradually realizing the need to create new governance structures and "clearly define how AI progress and implementation are managed" before they are compelled to do so by governments.[72] For instance, Open AI, a firm that participates in the Partnership on AI, has developed its own charter outlining the principles underpinning its work and overall strategy, a document crafted in consultation with other actors.[73] Anchored in a pledge to act in "the best interests of humanity throughout [artificial general intelligence] development," the principles commit the company to ensuring: broadly distributed benefits; long-term safety; technical leadership (to effectively address AI's impact on society), and cooperation with other research and policy institutions worldwide to tackle the global challenges associated with artificial general intelligence and provide related public goods.[74]

Technology companies are increasingly propelled by the growing threat of regulation and are seeking to ensure that whatever regulation comes about is favorable to their interests and does not stifle innovation. At the same time, their actions are also driven by a deep understanding of the potential risks of how AI technologies might be used. For instance, in response to the company's ethics being called into question by its own staff over a military contract, Google adopted seven principles to guide its AI work.[75] These include developing AI that is socially beneficial, avoids creating or reinforcing unfair bias, is built and tested for safety, is accountable to people, incorporates privacy design principles, upholds high standards of scientific excellence, and is made available for uses that accord with these principles. Other companies have made similar announcements, like Microsoft's "AI Principles,"[76] or Accenture's broader "Ethical Framework for Responsible AI and Robotics."[77] Others such as Salesforce have established dedicated research streams on AI ethics and values, specific personnel positions such as "chief ethical and humane use officer," and other entities like ethics advisory councils.[78]

Governments: Political actors increasingly view AI as a strategic technology with immense promise in the areas of economics, politics, and national defense. According to a recent report, at least twenty-seven national governments have articulated an interest in "encouraging and managing the development of AI technologies" and are organizing their efforts through national policies, strategies, and doctrine.[79] They are also working to mitigate the societal risks posed by increased automation and digitization. Certainly, there are mounting concerns about robots taking over a broad range of blue- and white-collar jobs and the associated impact these job losses would have on societies around the world. Yet some experts suggest that the speed of such automation could be blunted. They have stated that although the uptake of robotics will certainly influence service sectors such as construction, healthcare, and business, in other sectors it will more likely lead to job transformation rather than replacement.[80] Consequently, governments are increasingly urged to invest in social safety nets and human capital, so that workers can build the skills required for a transforming labor market.[81]

AI subfields such as machine learning, deep learning, and robotics have important competitive advantages for national security and defense. Over the past few years, China, Russia, the UK, and the United States, in particular, have been engaged in an intense competition to dominate the field. Each of these countries are spending huge amounts of resources on innovation; in many instances, they have developed or are developing close ties with global technology leaders in AI for social policy as well as defense R&D, not least because private sector investment in AI continues to significantly outpace that of governments.[82] Growing interest in the military applications of AI is already evident in discussions on topics like how machine learning can enable "high degrees of automation in labour-intensive activities such as satellite imagery analysis and cyber defense."[83]

But the military aspects are broader. Take, for example, the United States, where Congress is grappling with issues ranging from balancing public and commercial funding for AI development, articulating congressional and executive oversight roles and responsibilities for AI development, reconciling AI-related R&D and autonomous systems with ethical considerations, identifying the legislative or regulatory changes needed for the integration of military AI applications, and figuring out how it can help manage the AI competition globally.

The national security risks AI is expected to pose include AI-related strategic competition and related security dilemmas; cybersecurity risks to critical AI-dependent systems; consequential convergences with dual-use technologies in biotech, the nuclear domain, and other fields; and the overall unpredictability surrounding AI algorithms and their vulnerability to bias, theft, and manipulation. One particularly vexing potential tool of manipulation is deepfakes, which are "realistic photo, audio, and video forgeries" that could be weaponized for "information operations."[84]

Some researchers are helping deepen humanity's understanding of these AI-related security risks. A recent comparative study of national AI security policies and strategies across ten countries by the Center on Long-Term Cybersecurity points to highly diverging approaches to AI security.[85] Unless reconciled, these differences could, over the long term, present serious risks to both national and international security.

Multilateral Forums: AI is increasingly appearing on the agendas of various UN norm-shaping bodies and other specialized agencies (including the UN Conference on Disarmament; the UN Educational, Scientific, and Cultural Organization [UNESCO]; the International Labor Organization; and the World Bank) as well as other international and regional organizations (such as the EU, the Organization for Economic Cooperation and Development [OECD], and the Council of Europe).

These various bodies are focusing on matters like the economic consequences of labor displacement as well as safety, ethical, and security risks, including those associated with AI-augmented surveillance and data privacy. In addition, a number of these organizations—including some UN entities—are engaging with academics and industry actors to determine how AI solutions might best be marshalled to help address global humanitarian and development challenges and meet the UN Sustainable Development Goals and the Paris Agreement for Climate Change. In some instances, notably in the field of ethics, individual governments or regional groups have established new institutions, such as working groups or centers on AI and ethics, as well as ministerial or ambassadorial positions.

In regional terms, the EU has ratcheted up its engagement on AI. For instance, the European Group on Ethics in Science and New Technologies has intensified its calls for an "internationally recognized

ethical framework for the design, production, use and governance of AI, robots and autonomous systems," requiring "a collective, wide-ranging and inclusive process."[86] In April 2018, the EU published a Declaration on AI Cooperation,[87] which was soon followed by the EU Communication on Artificial Intelligence.[88] The communication establishes a European Initiative on AI, which aims to boost Europe's technological and industrial capacity in AI and its uptake, tackle its socioeconomic effects, and ensure suitable legal and ethical standards are in place. This framework is based on EU values and aligned with the Charter of Fundamental Rights of the EU, including "forthcoming guidance on existing product liability rules, a detailed analysis of emerging challenges and cooperation with stakeholders, through a European AI Alliance, for the development of AI ethics guidelines."[89] Such guidelines, in turn, would build on the work of the European Group on Ethics in Science and New Technologies.

Soon thereafter, the EU established a High-Level Expert Group on Artificial Intelligence (AI HLEG). Composed of members of industry, academia, and civil society, it will support the implementation of the European Initiative on Artificial Intelligence. The AI HLEG will make recommendations on future AI policy developments; offer guidance on related ethical, legal, and societal issues; and serve as the steering group for the European AI Alliance's work. It will interact with other initiatives, help stimulate a multi-stakeholder dialogue, gather participants' views, and reflect those views in its analysis and reports. How the EU intends to scale these initiatives and guidelines internationally remains unclear.

Both the OECD and the Council of Europe are also heightening their engagement on AI. For instance, drawing on the OECD Council Recommendations on AI, in May 2019, the OECD adopted a set of principles aimed at promoting "artificial intelligence (AI) that is innovative and trustworthy and that respects human rights and democratic values," and ensuring greater accountability of those involved in developing, deploying or operating AI systems. The principles were developed to complement existing OECD standards in critical areas such as privacy, digital security risk management, and responsible business conduct.[90] A month after these principles were adopted, the G20 Ministerial Meeting on Trade and Digital Economy adopted its own "human-centered AI principles," which also draw on the OECD principles. The G20 principles are accompanied by guidance for policymakers. This guidance is anchored in concepts such as "maximizing and sharing the benefits from AI," "minimizing risks and concerns," "international cooperation," and "inclusion of developing countries and underrepresented populations."[91] Meanwhile, the Council of Europe's Committee of Ministers, Parliamentary Assembly, and commissioner for human rights have launched a series of normative discussions and initiatives.[92]

There is a growing perception that military applications of AI require normative action and that the responsible and ethical use of AI systems in the military should be prioritized.[93] One of the most prominent examples is lethal autonomous weapon systems. Using sensor suites and advanced

machine learning algorithms, these weapons can identify a target, make an engagement decision, and guide a weapon to destroy the target, independent of human intervention or control.[94] These weapons systems have received significant attention since 2016, when parties to the UN Convention on Certain Conventional Weapons (CCW) established a GGE to study the legal, normative, ethical, technological, and military dimensions of emerging technologies and how they apply to lethal autonomous weapons systems. Unlike GGEs established by the UN General Assembly's First Committee on Disarmament and International Security, the CCW GGE allows for the participation of the research community, civil society, and the private sector. Many of these nongovernmental actors participate in the Campaign to Stop Killer Robots.

In 2017, the CCW GGE agreed on several issues for study, including how best to characterize the systems under consideration so as to promote a common understanding of concepts and characteristics relevant to the objectives and purposes of the CCW.[95] The GGE also agreed to consider the human element in the use of lethal force; contemplate aspects of human-machine interaction in the development, deployment, and use of emerging technologies related to lethal autonomous weapons systems; and review potential military applications of related technologies. Importantly, the group was asked to submit options for addressing the humanitarian and international security challenges posed by technologies related to lethal autonomous weapons in the spirit of the convention.[96]

Since 2017, twenty-eight countries have joined the call for a ban on fully autonomous weapons.[97] At the meeting of the first session of the CCW GGE in 2018, eighty-five states "publicly elaborated their views on lethal autonomous weapons systems in a multilateral forum," with some pushing for the development of a legally binding instrument on fully autonomous weapons.[98] The UN secretary general has also voiced support for some form of normative restraint on the use of such technologies,[99] although he recognizes that states have differing positions on the issue. For instance, in his Agenda for Disarmament, he stated that while "a growing number of States, including some with advanced military capabilities, have called for a preventative prohibition on lethal autonomous weapon systems," other states believe that "existing international humanitarian law is sufficient to address the risks."[100] Importantly, however, he notes that regardless of which position individual countries take, there is agreement between all parties that, "at minimum, human oversight over the use of force is necessary."[101]

Agreeing on an overall ban will likely be complicated, given countries' conflicting positions on the issues at hand as well as competing interests and agendas.[102] Yet the conversation continues. The CCW GGE's October 2018 report outlined several issues for further study by a new GGE that commenced its work in March 2019. In addition to the issues listed above, the new GGE's agenda also includes "possible guiding principles," such as the application of "international humanitarian law" as well as "aspects of human-machine interaction in the development, deployment, and use of

emerging technologies related to lethal autonomous weapons systems."[103] The new GGE's first session was held from March 25 to March 29, 2019, with a much stronger emphasis on "inter-State dialogue," although the group also involved other actors, as per past practice.[104] This session laid a foundation for the second session of the GGE slated for August 2019.

What Lies Ahead?

Unknowns about how the potential benefits and risks of AI will play out in the coming decades will force policymakers to confront a series of interconnected governance problems. Significant coordination and cooperation between public and private actors will be necessary. And internationally speaking, it is imperative to establish participatory or cooperative mechanisms to understand the evolving implications of AI and how best to manage them, while navigating the uncertainties and risks of future developments.

These mechanisms will need to be informed by broader public discussion and engagement on a range of issues. First, much wider public dialogue is required on the ethical values and principles put at risk by the development of complex AI models and systems as well as the nature and direction of change they are engendering. This dialogue should involve exchanges and dialogue on the emerging body of principles and values that public and private entities are (sometimes jointly) promoting and conversations about more transparently managing the associated cross-border risks.

The current trend, true of governmental and nongovernmental bodies alike, toward developing principles and guidance for AI (the principle proliferation discussed above) suggests there may be much duplication where the principles overlap and significant potential for "confusion or ambiguity where they differ."[105] Moreover, the majority of these principle-driven initiatives tend to be emerging in advanced Western economies, in turn suggesting a degree of fragmentation that may be difficult to reconcile in the medium to long term if alternative voices are not brought into the discussion. This trend has profound implications for ongoing efforts to achieve a more equitable distribution of AI-related benefits. So-called fairness norms advocate for making coordinated AI development paths in specific fields or sectors provide reasonable compensation or benefit sharing to those exposed to risk.

Yet there is hope. For instance, based on comparative analysis it conducted of current, high-profile efforts to promote ethical AI, the AI Now Institute has recommended an overarching framework consisting of five central tenets to overcome such duplication, confusion, and ambiguity. Drawn largely from the field of bioethics, these framing principles include beneficence, nonmaleficence, autonomy, and justice as well as one new principle—explicability, which incorporates both the sense of intelligibility (how a specific AI system works) and the ethical sense of accountability (how to track who ultimately holds responsibility for the effects of an AI system).[106] This overarching

framework could be an important foundation for cross-regional dialogue aimed at ensuring more ethical AI that benefits societies across the globe.

Second, the question of transparency and accountability requires a specific mention, not least where corporations are concerned. According to one expert, most corporate statements on AI-related policy and principles appear to "leav[e] more wiggle room than a pair of clown pants."[107] Until recently, most corporate initiatives promoting ethical AI were detached from fundamental questions such as the nature and scope of accountability and related monitoring and oversight mechanisms. Yet more troubling is "the conflict[s] of interest in commercial AI giant[s] researching the ethics of [their] own technology's societal impacts."[108] Given the broad societal effects of AI, some form of public-private engagement or compact on this issue needs be sought. But it has become increasingly challenging to find academics not already entangled, "in some consulting form or other, to one tech giant or another."[109]

The nature and composition of oversight bodies is equally problematic. For instance, while some companies have established ethics boards, they are not always open or transparent about their membership or operations. For instance, DeepMind, a company purchased by the Alphabet Group in 2014, has created DeepMind Ethics and Society, a research unit focused on exploring "the key ethical challenges facing the field of AI."[110] The group pledges that its work should be "governed by a set of principles that seek to guarantee the rigor, transparency and social accountability of this work," including by helping technologists put ethics into practice and by helping society anticipate and manage the impacts of AI in a manner that benefits all.[111] At the same time, however, the company has been criticized for the lack of transparency around its AI Ethics Board.[112] This board was written into a contract called the Ethics and Safety Review Agreement when the Alphabet Group acquired the company. The agreement essentially puts control of DeepMind's "most valuable and potentially most dangerous technology"—its core artificial general intelligence technology—under the governance of the ethics board, whose actual composition has never been made public.[113]

Policymakers and other actors, nonetheless, can draw important lessons from the emerging practices of some companies. For instance, Axon (formerly Taser)—a U.S. company that develops body cameras and weapons for law enforcement—recently announced the establishment of an AI and Policing Technology Ethics Board to help guide the development of its products and services.[114] This decision was likely influenced by the heavy criticism that followed the company's offer to provide police officers across the United States with free body cameras in what critics saw as a normative and ethical vacuum.[115] Axon has since established an independent board with a mission to "provide expert guidance to the company on the development of its AI products and services, paying particular attention to its impact on communities."[116] It has listed the board's members and committed to publishing annual reports describing the body's work, including AI product development guidelines established at its first meeting.

This is undoubtedly an important move. However, the board's operating principles will likely raise additional questions as to how boards like these—diverse and professional as they are—can provide legitimate guidance and oversight for products and services that have profound implications for a diverse range of communities if the public itself is not engaged in the process. In the case of Axon, the connection with broader policing policy and democratic oversight appears to be lacking. That being said, the establishment of the independent board and the additional questions it has raised is still an interesting step that companies championing AI ethics might learn from as this complex and competitive field moves forward.

Third, it is necessary to have a deeper discussion on how best to balance investment in the research and design of safety protocols, equity, transparency, and accountable decisionmaking with investment in technological advances. To date, most investment has gone toward the latter. Distilling and sharing lessons from sector-specific AI and automation piloting, sandboxing efforts, and initial regulatory steps (like those under way in the EU) can advance this discourse. In addition, such an approach can help engender more informed conversation on the nature and scope of the regulatory, legal, and oversight frameworks that might be required for particular AI systems in the future.

Fourth, while all states have the right to shape their own AI national security policies and strategies as they deem fit, greater convergence around ultimate goals is required to safeguard against broader systemic risk. As research into AI-related national security policy and strategy development deepens, further thought might be afforded to the recommendations put forward in the recent report by the Center on Long-Term Cybersecurity. Particularly notable are those recommendations related to promoting early coordination around identified common interests; encouraging public investment in identifying and sharing best practices; understanding the risks of prioritizing one subset of issues over another and the opportunities and challenges that may be ignored; ensuring greater accountability of the technology sector; and pressing for greater inclusivity in the shaping of government policy and strategy.[117]

Fifth, public discourse on AI must tackle the issue of how international norms, rules, and principles can mitigate (or even prevent) novel ways of misusing AI and maintain peace and stability as the global balance of power shifts. In the short term, legal and ethical questions related to whether weapons systems should be permitted to make life and death decisions (that is, the question of meaningful human control, or explicability) will likely remain central and differentiated from questions pertaining to the application of international humanitarian law or other rules for other national security uses of AI systems and capabilities. Yet efforts should be made to ensure that these important discussions on lethal autonomous weapons systems do not drown out consideration of pressing normative issues relating to AI and national security.[118]

To this end, it may be necessary to establish more concrete and integrated mechanisms for navigating the uncertainties of future developments in AI and autonomous systems and for managing related risks, including those resulting from the growing relevance of AI to strategic competition. Other issues related to the growing militarization of AI will likely appear on the multilateral security agenda in the coming years.[119] Initiatives such as the UN Institute for Disarmament Research's Trust But Verif AI Project can bring fresh thinking to debates surrounding AI and international peace and security.[120] This specific project aims to bring together AI technologists, arms control practitioners, and other experts in regulatory and technology control policy to consider how AI arms control might be feasible.

Biotechnology

Significant advances are also being made in the field of biotechnology, which the UN defines as "any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use."[121] In recent years, the field's principal breakthroughs have occurred in genome editing, gene drives, and synthetic biology. Current trends suggest there will be a profusion of biotechnology products that are significantly different in type, scope, and complexity than previous ones. Lower barriers to access have opened the field to more and more actors.

Technological advances are spurring rapid growth in the bioeconomy. According to the Nuclear Threat Initiative's (NTI) biosecurity program, the global bioeconomy in 2014 accounted for a significant portion of world trade and offered societal benefits in the areas of energy, food production, healthcare, and other sectors vital to sustainable development. For instance, India's bioeconomy was already valued at more than $4.3 billion in 2012.[122] Meanwhile, the EU's bioeconomy was reported to already be generating a turnover of more than 2.3 trillion euros (or about $2.6 trillion) as well as some 18 million jobs in 2015.[123]

Given this economic potential, many countries are investing in the field. In 2013, the Chinese government allotted $11.8 billion for "biotech innovation from 2015 to 2020."[124] And many countries—including China, Denmark, Singapore, the UK, and the United States—are creating biofoundries to develop new technologies and spur product development in living systems.[125] Meanwhile, new global academic consortia are discussing solutions to the ethical and regulatory challenges emerging around synthetic biology and its potential to modify existing living organisms or create "hitherto unknown [ones]."[126]

Public awareness about biotechnology-related risks and challenges is growing in many countries. The debacle involving Chinese researcher He Jiankui's claim to have altered the genes of twin girls to prevent them from contracting human immunodeficiency virus (HIV) is a case in point, not just because of the skepticism surrounding his claims but also because of the ethical questions his research raises, including about what it means to be human.[127] Meanwhile, national regulatory agencies are struggling to keep pace with the rate and scope of change, and it is becoming increasingly challenging to balance the competing interests of industry, academia, the rest of society, and the state. Internationally, rapid advances in biotechnology and persisting divides between states have heightened the potential consequences of a biological attack, placing new pressures on existing regimes such as the Biological Weapons Convention (BWC). As the world becomes more dependent on biological systems, there is a greater need to strengthen existing governance systems, including norms and oversight mechanisms, and to identify new ones where appropriate.

The Current Normative Landscape

Biotechnology offers humans a vastly improved understanding of the basic building blocks of life. The Human Genome Project finished mapping the human genome in early 2000, identifying every one of the roughly 20,000–25,000 genes in human deoxyribonucleic acid (DNA).[128] Since then, researchers have made significant advances in gene editing and gene drive research. Genome editing involves the precise cutting and pasting of DNA segments by specialized proteins. The method that has captured the most attention is called clustered regularly interspaced short palindromic repeats (or CRISPR) and CRISPR associated protein 9 (Cas9). This simple, versatile, and cheap technology was initially discovered in the late 1980s, and more recently researchers have learned how to use CRISPR and Cas9 for gene editing.[129]

CRISPR is now being tested for various uses such as treating some genetic diseases, growing climate-resilient crops, combating vector-borne diseases like malaria, designing food and drugs, and even saving endangered species from extinction. The technology also carries significant potential for what are termed autologous treatments, which involve teaching cells to "fight disease in one's own body, delete hereditary diseases for one's self and one's own offspring, and shape new generations of organisms as genetic modifications are passed to future generations."[130] Few other new technologies offer more hope for alleviating disease. At the same time, gene editing could bring about unpredictable permanent genetic changes, some of which could harm humankind and the biosphere.

Several advances in the field raise new ethical and normative questions and risks that require new solutions, particularly in four key areas, some of which overlap:

Ecological risk: Gene alterations can generate unpredictable and undesirable consequences in the modified species, as well as in other species, and can even give rise to new and unknown animal and

human diseases. Researchers are investigating how gene drive systems can be used to eradicate diseases; the most advanced of these projects seeks to wipe out malaria-carrying mosquitoes. And some scientists had hoped to use a CRISPR gene drive to prevent the extinction of wildlife species threatened by invasive organisms. The thinking went that modifying an invasive organism's DNA to reduce its ability to reproduce and then releasing that organism back into the wild would cause the fertility-reducing gene to spread through the invasive population, eradicating the pests. But a recent study by some of the same scientists found that altered genes might actually spread to places where that same organism is not invasive at all, but a well-established part of the local ecosystem.[131] Such unintended consequences would pose unacceptable risks.

Such projects demonstrate the need to first develop safer versions of this powerful technology and raise important issues related to standards and regulation. The consequences of using such technologies are not contained within national borders, and these effects will likely require some form of transnational mechanism that considers the views of all stakeholders. This calls for a more harmonized approach to biotech policy, especially since rules and practices of gene editing vary significantly from country to country. Meanwhile, all stakeholders, including those funding and supporting research, need to ensure adherence to existing guidance such as the World Health Organization's (WHO) 2014 set of guidelines for testing genetically modified mosquitoes.[132] According to some experts, this push to shore up standards might require the establishment of some form of accountability mechanism that can, at a minimum, oversee adherence to this guidance and identify possible obstacles to implementation.[133]

Another ecological risk is the potential for biological attacks against food and water resources, which, as discussed further below, would cause economic damage as well as a "loss of confidence in the food supply, and possible loss of life."[134] For example, a recent study determined that scientists' deepening understanding of the genomes of plants and animals will make it theoretically possible to target vulnerabilities with greater precision or to create new varieties of organisms with potentially harmful properties. The authors posit that "if plant or animal pathogens [a]re engineered to spread widely in the world in crops or herds, respectively, the result could be widespread and lasting food shortages."[135]

Other health and safety risks: Incidents like laboratory accidents or research aimed at rendering deadly viruses more contagious or pathogenic pose dangers as well. Relatedly, the publication of such techniques and research outcomes could educate and empower malevolent actors. Concerns of this kind arose from research published by two scientists in 2012 in prominent journals (*Nature* and *Science*). Both had succeeded in genetically engineering strains of the avian flu virus (H5N1).[136] The controversial decision to publish their research findings stemmed from intense public concerns that the virus could leak out of a laboratory in the event of an accident. More seriously, the research could be leveraged by terrorists to create a biological weapon and unleash a devastating pandemic.

National guidance, regulations, and codes of conduct by the research community are helping address some of these challenges.[137] Globally, the International Standards Organization is developing new standards to harmonize attempts to help laboratories manage biological risk, drawing from EU and WHO efforts to establish and implement effective biorisk management systems.[138] But there are still important gaps. As biotechnology becomes cheaper and more readily available, these softer forms of regulation will likely be insufficient for managing the associated risks.

Questions of consent and human-induced permanent genetic changes also raise new quandaries. For example, fears about modifying fetuses or otherwise enhancing subjects' aesthetic performance or other attributes drive concerns about genetic discrimination, human cloning, and eugenics. National regulations and practices on this aspect of biotechnology greatly vary from state to state. For example, many countries cite ethical considerations to either prohibit or otherwise circumscribe certain human CRISPR trials to treat or prevent disease or disability in germline cells (as opposed to somatic cells).[139]

In other contexts, such research is banned. For instance, the Chinese authorities have since investigated the case involving He Jiankui and concluded that he "organised a project team that included foreign staff, which intentionally avoided surveillance and used technology of uncertain safety and effectiveness to perform human embryo gene-editing activity with the purpose of reproduction, which is officially banned in the country."[140] Stanford University, too, has launched an investigation into the links between Stanford academic staff and the Chinese scientist.[141] Yet the fact that He did actually manage to successfully test gene editing on the twin embryos has raised new questions about how to manage risks and unintended consequences as well as how to ensure better research oversight.[142]

Rule of law risks: Law enforcement agencies' growing use of data-sensitive biotechnologies—such as fingerprinting, systematic collection of human DNA samples, and the introduction of biometric identifiers and intelligent implants—all pose important societal risks, including to core principles of the rule of law and human rights. For instance, in the United States, law enforcement agencies have shown a mounting interest in accessing privately run genetic genealogy banks after using DNA information from a genealogy website to identify a suspect in the infamous Golden State Killer case.[143] The fact that the owners of some of these websites have provided full access to law enforcement, unbeknownst to their users, has raised serious questions about privacy, consent, and due process.[144]

International security risks: Concerns are also mounting about the dual-use nature of technological advances in the life sciences and their potential for malicious use. The diversity of possible applications of genome engineering and gene drive technology (including the production of

bioweapons) and the potential impacts are unpredictable. While such biotech applications would likely still require the resources of a state or large enterprise, the technological barriers to acquire, develop, and use biological agents as weapons have lowered significantly in recent years. The risk of biological warfare, biocrimes, and bioterrorism are particularly grave.

Apropos of biological warfare, the BWC is a legally binding treaty that outlaws the use of biological weapons and codifies a strong, age-old, and cross-cultural norm against the use of disease as a weapon. But the BWC is institutionally weak and lacks verification, monitoring, and enforcement provisions. Furthermore, the convention may be unable to keep pace with rapid scientific and technological developments.

Notably, because biological science is inherently dual use—the same tools and technologies that can be used to benefit society can also be used to cause deliberate harm—the key difference is user intent. While there are no concrete examples of novel developments inconsistent with the aims of the BWC, advances in biotechnology do have security-related implications. Such advances make the development and production of biological weapons easier and more accessible, even if such research endeavors are largely pursued for entirely legitimate purposes (such as general scientific discovery, public health, and food production) and therefore cannot, in and of themselves, be prohibited.

It is unclear whether or not the erosion of technical and access barriers might lead to the more widespread acquisition and use of biological weapons. While scientific and technical advances may continue to put pressure on the norm against using disease as a weapon, they also can serve as a deterrent. For example, the creation of versatile diagnostic and therapeutic platforms could enable a rapid response to any engineered threat, deterring nefarious actors from considering biology as a potential tool of large-scale terror, as discussed above.[145] Yet, without accompanying advances to monitor compliance and differentiate between offensive and defensive (or peaceful) intent, advances in biotechnology could make it harder to identify violations of the BWC.

The convention's eighth review conference was held in November 2016 and ended without an agreement on any significant steps to enhance the treaty's effectiveness, including the creation of a regular advising mechanism to assist in monitoring and assessing relevant scientific developments. At the same time, several regional workshops, funded by the EU and the United States, are under way, as are workshops aimed at making the BWC's post-review conference discussions on science and technology more global and diverse. These workshops hopefully will help provide a baseline for future review and assessment.

Beyond the risks of full-on biological warfare, there are other international security risks. One such risk is the growing convergence of biotech and AI, notably in the area of synthetic biology. While AI-powered bioengineering is mostly used for benign and beneficial purposes at present, a U.S.

National Academy of Sciences report cautions that these technologies "expand the risks of bioweapons because new or more virulent pathogens could be created from scratch."[146]

Despite a certain degree of hype, the use of biotechnology to commit terrorist attacks or other criminal acts remains limited. Recent research points out that there has only been one documented death attributable to biocrimes (although that is debatable),[147] a number of bioterrorism incidents with no directly associated deaths,[148] and five deaths from a documented lone-wolf terrorist incident in the United States.[149] Nonetheless, as the technological barriers to harnessing biological agents as weapons have fallen, such risks increase. The growing availability of new biotech tools could make it possible for terrorist groups to create and modify pathogens or otherwise misuse biological materials and expertise.[150] Groups such as al-Qaeda and the self-proclaimed Islamic State have reportedly called on "scientists, doctors, and engineers to join their cause, which includes the use of specialized skills to inflict harm."[151]

What Lies Ahead?

The current framework for governing biotech-related ethical and normative challenges and for managing biological risk is fragmented. Responsibilities are dispersed across different intergovernmental agencies and national regulatory and oversight bodies.[152] For decades, the WHO has helped shape norms relating to biotechnology, healthcare, and bioethics. The UN and other international and regional bodies have long played a role in shaping principles, standards, and norms in some of these areas with mixed results. For its part, UNESCO has also been involved in bioethics since the 1970s. Its work revolves around the sociocultural, legal, and ethical implications of advances in the life sciences (including biotechnology), and it has established bodies such as the International Bioethics Committee to study such matters.

The UN is also responsible for enforcing the ban enshrined in the BWC (which entered into force in 1975), the first multilateral disarmament treaty banning the development, production, and stockpiling of a specific category of weapons of mass destruction. Through a number of resolutions, the UN Security Council, too, has engaged on certain biotech-related issues, notably in relation to strengthening member states' capacities to prevent biocrime and bioterrorism. These include UN Security Council Resolution 2325 (2016), which calls on all states to strengthen national antiproliferation regimes in the course of implementing UN Security Council Resolution 1540 (2004), which in turn seeks to keep nonstate actors from acquiring nuclear, biological, and chemical weapons of mass destruction and to submit timely reports on their efforts to do so.

Through its Group on Ethics and Science in New Technologies (EGE), the EU, too, is increasing its attention to biotechnology and its normative implications. After an earlier statement on gene editing, the EGE is preparing an opinion on gene editing, due to be completed in the summer of 2019. The opinion will focus on the "bigger picture of this issue," which crosses existing ethical

divides, as well as "specific aspects of concern" such as "gene editing applied to animals" and "gene editing in the context of biodiversity and ecosystems."[153] International forums like the WEF are also seeking to shape new related governance solutions. For instance, in addition to its work on the Fourth Industrial Revolution, the forum has established a Global Future Council on Biotechnology to consider ethical and safety issues emerging from biotechnology-related discoveries, applications, and policy issues.[154]

In national terms, rules and practices relating to certain biotech applications (like gene editing) continue to differ widely from country to country. Policymakers around the world are struggling to keep pace with the latest developments and adapt domestic institutions to manage the risks associated with the emergence of future advances and products. Countries have not yet aligned their respective efforts, although some are advocating for more global responses, including consensus on guiding ethical principles, through bodies such as the WHO.[155] In this respect, the WHO's decision to establish an Expert Advisory Committee to "examine the scientific, ethical, social and legal challenges associated with human gene editing" with the aim of advising and producing recommendations on "appropriate governance mechanisms for human gene editing" may be a step in the right direction.[156]

Beyond these formal multilateral institutions, scientific associations, research communities, and publishers all play an important role in developing principles, standards, and norms to guide biotechnology research and innovation. For instance, the U.S. National Academy of Sciences has proposed a set of principles to manage the challenges associated with human gene editing. The principles include promoting well-being, transparency, due care, responsible science, respect for persons, fairness, and transnational cooperation.[157] Relevant industry actors do not appear to be engaging significantly on ethical and normative issues, although efforts are under way to strengthen such engagement and encourage self-regulation on the basis of existing ethical values and principles.[158] Meanwhile, there are renewed calls for public and private funders of biotechnology research to do more to ensure that the research they are supporting is conducted "in compliance with standards such as those advanced by the WHO" and related bodies, regardless of where the research takes place.[159]

In recent discussions at the UN General Assembly, the WEF, and the Munich Security Council, key stakeholders have been urged to find creative ways to reduce biological risks. In response, the NTI program on biosecurity, the Wellcome Trust, and the WEF are pushing for the establishment of new global norms by leaders in the virology and synthetic biology communities, as well as models for adopting such norms.[160] To this end, in 2018, these three organizations launched a joint initiative aimed at bringing together leaders and experts in genomics, virology, synthetic biology, bioethics, security, insurance, and scientific publishing. Following an initial roundtable, the NTI aims to

convene a multi-stakeholder council to spur the adoption of new global norms and technical approaches that enhance biosecurity innovation and reduce risk.[161]

Undoubtedly, given the sheer number of ethical and normative issues at hand, governments and other key actors will need to ensure a more aligned, cooperative, and participatory policy environment. Countries need to make progress and identify cases in which international cooperation and coordination could help resolve persisting or emerging challenges. Doing so would engage more stakeholders, increase efficiency, raise overall safety and standards, and reduce risk. This approach would also promote greater transparency and accountability, conferring much-needed legitimacy on policymaking, norm-shaping, and regulatory processes. And it will be necessary to identify whether current platforms adequately serve this purpose or whether new ones are needed.

Space Technology

Historically, outer space has been shaped by strategic and resource competition between major powers.[162] Today, overlapping advances in technology are enabling new forms of commercial and military activity in space. With more tangible threats, lower access barriers, and a growing number of stakeholders, there is an urgent need for states and other actors to engage in more dialogue and cooperation to determine how relevant governance frameworks can best be strengthened.

Developments in Space Technology

Although outer space was originally dominated by states, it has become a theater for economic growth, innovation, and private commercial activity. Over the past decade alone, the international commercial space sector has diversified significantly. According to the OECD, in 2013 outer space generated some $250 billion in revenue, including such sectors as the space manufacturing supply chain, satellite services, and consumer services such as satellite television and global positioning system (GPS) devices.[163]

Innovation has continued to transform a variety of space-related economic sectors, including the satellite industry. Large and small companies alike as well as universities are increasingly using powerful miniature satellites originally developed for costly scientific research purposes in low Earth orbit. These small satellites are often developed with off-the-shelf commercial components. Amateurs, sometimes funded through crowd-sourcing campaigns, also use them. Beyond that, technological innovation is also poised to open and/or expand new sectors such as commercial space launches and space tourism, space manufacturing, and resource recovery (asteroid mining). In some countries, privately backed investments in rocket launches, rocket recovery, and the delivery of payloads to space stations, for instance, are already producing breakthroughs and delivering noteworthy efficiency compared to government-funded competitors.

In some cases, actors are innovating on the back of existing space technology. For instance, the use of space-based remote sensors is transforming how a diverse range of fields operates, including humanitarian assistance, crisis management, and agriculture. Social media and technology companies are assessing how to use satellites in low Earth orbit to expand access to the internet (and their own products and services) in remote areas. These technological advances are expected to provide new opportunities for economic growth, development, and the involvement of new actors. In 2014, the OECD inferred that "countries with long-established space programmes face growing challenges as lower costs and technological advances draw more countries and companies into the sector and give rise to a burgeoning commercial space industry."[164] By 2017, the total value of space-related industries was estimated at $350 billion and forecast to grow to about $2.7 trillion by 2040, according to Bank of America, a trend rendered possible by "new drivers," such as "reusable launch by SpaceX, the growth of both private ownership in the market, investment and financing by more than 80 countries and the falling launch costs from vehicles by the likes of Rocket Lab and Vector."[165]

At the same time, increased activity in outer space presents new risks, such as the possibility of collisions and the hazardous debris that could result from such collisions. And the fact that states increasingly view the space economy as a new source of power is driving strategic competition at a time of heightened geopolitical tensions. This will likely influence related normative discussions. Furthermore, despite the growing number of actors engaging in commercial space activity, these talks tend to take place in a handful of wealthy nations, meaning that the number of potential participants and beneficiaries of the space-based economy remains low. This reality exacerbates concerns about technology-related divides and questions of equitable access to the benefits of economic activity in space.

Beyond commercial activities, over the past few decades, there has been growing interest in the use of space as a medium to support tactical military operations and other existing uses related to strategic defense. Both existing and emerging space powers are investing more in military space systems for communications, navigation, and reconnaissance purposes, so as to ensure the operability of a range of capabilities, including drones and precision weapons. Such systems can be used to detect potential targets, attack adversaries, and otherwise harm the interests of others. Many states are also investing in technologies that can disrupt or destroy these same space-based capabilities.

The fact that modern militaries rely heavily on satellite systems means that these space assets have become potential targets. This is a particularly pertinent point for modern navigation systems and the growing possibility that the GPS or global navigation satellite system may be susceptible to being disrupted or destroyed. The United States—being heavily reliant on satellite technologies—has acknowledged these vulnerabilities. Washington views Russia's and China's pursuit of anti-satellite

weapons (ASAT), including laser-armed, satellite-hunting aircraft, as an attempt "to reduce U.S. and allied military effectiveness" and "to offset any perceived US military advantage derived from military, civil, or commercial space systems."[166] These troubling trends are driving defense-spending increases in resiliency and redundancy, including considerations of how best to achieve GPS-dependent position, navigation, and timing (PNT) assurance, which is "a core and defining ingredient of a modern, networked military that can operate with precision across all domains: air, land, sea, space and information."[167] Trump's recent directive to create a Space Force as a sixth branch of the U.S. military under the Air Force reflects this calculus.[168]

In some cases, PNT assurance is being discussed in conjunction with possible terrestrial ASAT components—such as the development of new space-based shields with the added protection of new ground-based military hardware—and other capabilities for disrupting satellites such as communications and GPS jamming. According to the UN Institute of Disarmament Research, the Chinese, Russian, and U.S. militaries are "developing capabilities that can target space assets, including missile defense interceptors and maneuvering satellites."[169] These leading militaries are also investing in technologies and techniques designed to counter their rivals' space-enabled intelligence, surveillance and reconnaissance, and precision strike activities.

Undoubtedly, using these capabilities against an adversary's space assets in a conflict or even preemptively could have disastrous consequences for the Earth's orbit and the planet itself. In addition, the development and testing of ASAT capabilities is also worsening the risks posed by hazardous space debris. For instance, debris from China's 2007 direct ascent ASAT test is still in orbit (and will likely remain there for decades).[170] Although India's more recent March 2019 test was conducted in low orbit (reportedly allowing the debris to disperse over time), this test still posed safety risks, including to the International Space Station.[171]

Beyond the aforementioned security concerns, vulnerabilities in satellite and spacecraft computer systems could be potential targets for cyber attacks by states, their proxies, or terrorist groups. And there is mounting concern that state actors could wield offensive cyber capabilities or operations as part of their anti-satellite toolboxes. For instance, an attack on GPS satellites would be felt across a wide range of economic and social sectors, potentially affecting the delivery of essential public services such as power supplies, banking services, and credit card services, all of which rely on GPS.[172]

The Current Normative Landscape

Technological developments enabling increased commercial and military space activities are reanimating old questions about the nature of human activity in outer space. A set of new questions is also coming to the forefront, answers to which may require adapting the international normative framework governing outer space activities and revising relevant national policies and regulations.

These worries are not new. The Sputnik satellite launch in 1957 and the ensuing space race between the United States and the Soviet Union drove initial concerns that outer space would be used for nonpeaceful purposes, namely for the placement and deployment of nuclear weapons and the deployment of military satellites that could enable or warn of nuclear attacks. Policymakers also worried about commercial satellite applications, particularly those for monitoring, remote sensing, and broadcasting. These technologies could directly capture information from inside a state or beam information into a state. At this time, only the world's two major powers possessed the financial and technological wherewithal necessary to explore and exploit outer space.

As decolonization occurred, a debate unfolded over the growing military uses of outer space. The debate involved sovereignty-related principles such as prior consent and jurisdiction as well as newer principles such as equitable access to the benefits derived from commercial satellite use. The latter resulted in the establishment of the UN Committee on the Peaceful Uses of Outer Space (COPUOS) in 1959, as well as the current body of international space law and related nonbinding measures and guidance. These various instruments have shaped national space policies and regulations ever since.

The 1967 Outer Space Treaty is the central instrument in this body of law and remains the principal framework governing activities in outer space today. The treaty's principles were negotiated to advance international peace and security. It was not intended to regulate human spaceflight and exploration. Rather, it granted rights for the exploration and use of outer space, provided those activities are "carried out for the benefit and in the interests of all countries."[173] The principles were designed to ensure that "Outer Space, the Moon and other celestial bodies" remained an arena for peaceful activity and that no single entity or nation could claim sovereignty over outer space.[174] Throughout the Cold War, adherence to the treaty as well as the major powers' doctrines of deterrence helped ensure that military activity in outer space did not lead to escalated tensions.

Yet concerns about military activity in outer space have persisted. Since the early 1980s, several attempts have been made to restrict certain activities. Numerous proposals have been made at the UN General Assembly or the Conference on Disarmament for the "prevention of an arms race in outer space."[175] These proposals include a nonbinding UN General Assembly resolution called the Prevention of an Arms Race in Outer Space (PAROS), which has been passed every year since 1982. The resolution "reaffirms the fundamental principles of the 1967 Outer Space Treaty" and "advocates for a ban on the weaponization of space."[176] It also advocates for "further measures to prevent an arms race in outer space" and "calls on the Conference on Disarmament to establish an ad-hoc committee on issues relating to PAROS."

Other proposals include Chinese- and Russian-backed draft instruments aimed at preventing the placement of weapons in outer space and prohibiting the use of anti-satellite weapons and a related 2008 treaty proposal. In 2014, Moscow and Beijing submitted a new version of a draft proposal called the Treaty on the Prevention of the Placement of Weapons in Outer Space, and Russia proposed a new UN General Assembly resolution containing a pledge against the placement of weapons in outer space. For various legal, technical, and political reasons—including concerns about verifiability or a lack of equitability—these proposals have not advanced. The EU's alternative efforts to promote a nonbinding International Code of Conduct for Outer Space Activities outside the purview of the UN and the Conference on Disarmament have not gained traction either. While there was likely limited disagreement on the substance of the proposed code of conduct, the process of institutionalizing it was mired in problems from the outset.

In 2011, the UN General Assembly established a GGE to study transparency and confidence-building measures related to outer space activities. The group was tasked with developing recommendations on rules of conduct and measures aimed at expanding the transparency of outer space activities and space programs. It produced a consensus report in 2013, welcomed by the UN General Assembly in Resolution 68/50 and subsequent resolutions that encouraged member states to review and implement the proposed measures. The UN General Assembly also referred the report for consideration to the Committee on the Peaceful Uses of Outer Space, the Disarmament Commission, and the Conference on Disarmament. But progress on implementing the GGE recommendations has been slow, and distrust has continued to prevail. To date, only one UN member, the United States, has submitted a report to the General Assembly outlining how it is implementing the recommendations of the 2013 GGE report.[177]

There was some hope that progress could be achieved. For instance, the Conference on Disarmament (finally) established four subsidiary bodies in February 2018 to advance its work. One of these subsidiary bodies was to focus on the "prevention of an arms race in outer space."[178] Yet, in 2019, the Conference on Disarmament failed to reestablish the four bodies. For its part, the Disarmament Commission has held informal discussions over the past two years on the practical implementation of transparency and confidence-building measures. Member states have agreed to take up the issue in the commission's 2018–2020 three-year cycle, although it is unclear what this will mean in practical terms.

On a slightly more positive note, COPUOS has continued its complementary work on substantive and legal issues relating to peaceful uses of outer space. Building on the 2007 Space Debris Mitigation Guidelines, it is working to develop guidelines aimed at increasing the odds that outer space activities are sustainable over the long term. These more recent efforts play an important confidence-building role as well.

In addition, it appears as if public pressure is effectively generating some good practices regarding ASAT testing and the imperative not to create debris. For instance, the public outcry that followed China's 2007 ASAT test appears to have convinced Beijing that this capability must test in a controlled manner, without blowing up objects and scattering debris in space. But this does not mean that the country will not use alternative ASAT capabilities. According to a recent report, China has conducted numerous tests of technologies "for close approach and rendezvous in both low-earth orbit (LEO) and geosynchronous orbit (GEO) that could lead to a co-orbital ASAT capability."[179] There is not enough evidence to conclude whether Beijing will gain this operational capability in the near future. The same report notes that Russia, the United States, and numerous other countries also have developed—or are developing—novel ASAT and other counterspace capabilities in five categories: direct ascent, co-orbital, electronic warfare, directed energy, and cyber.

What Lies Ahead?

Looking to the future, a number of technology-related issues will likely remain or appear on the international space agenda. The space environment is radically different now than it was when the existing normative framework was adopted. Space law will likely need to be revisited to account for new forms of commercial exploration, resolve issues relating to states' obligations in terms of international cooperation and coordination, and ensure equitable future economic access in accordance with the Outer Space Treaty.

When the treaty was being negotiated, there were already attempts to restrict space exploration to government enterprises, largely in reaction to the U.S. private sector's dominance of the commercial satellite industry. The resulting compromise laid out in Article VI of the treaty permits private activities in outer space, making national governments legally responsible for the actions of their nationals. Yet today new commercial activities are raising new questions. The first missions to probe the moon for resources are already scheduled to launch in 2020. In accordance with their obligations under international law to "authorise and continually supervise" such activity conducted by their nationals, several countries—including Luxemburg, the United Arab Emirates, and the United States—have already adopted new legislation concerning resource extraction rights in space, while also loosening regulations to enable commercial activity.[180] Other states—including France, Germany, Japan, and the UK—will soon follow suit.

But it is likely that this dash to exploit space resources will foment new tensions. Resource recovery in space will likely be scrutinized on the basis of sovereignty. Article I of the treaty states that "outer space, including the moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies." But the treaty's subsequent article states clearly that space resources are "not subject to national appropriation." Some experts interpret this latter provision as a prohibition on the extraction of space resources

and have criticized recent U.S. legislation for entitling U.S. companies engaging in commercial recovery of space resources "to possess, own, transport, use and sell the space resources obtained."[181] Furthermore, countries with limited capabilities will likely decry unequal and inequitable access to space resources. It may well be that the emerging body of national rules and regulations will eventually need to align with international views on the activities in question in the form of an international agreement on managing commercial space exploration and utilization.

An important step forward was the creation in 2017 of the Hague International Space Resources Governance Working Group. In the absence of a clear framework to govern the extraction of space resources, this multi-stakeholder group has been studying existing concepts "to ensure that they meet existing treaty obligations regarding on-orbit operations and space resource rights."[182] The group's overall aim is to complement other global, regional, and national efforts and prepare a foundation for a new international regulatory framework for space resource–related activities. Reaching consensus on what is and is not permitted under the terms of the treaty will undoubtedly be challenging. At the same time, the number of actors intent on leveraging space—to foster commercial activity and spur economic growth, for instance—may actually incentivize dialogue and agreement on common principles. So, too, should other more global objectives such as the UN Sustainable Development Goals.

On questions relating to military uses of outer space, it is likely that the debate over a space-based arms race will continue and remain divisive. In 2017, the UN General Assembly established a new GGE under the Conference on Disarmament with the specific mandate to "consider and make recommendations on substantial elements of an international legally binding instrument on the prevention of an arms race in outer space, including, inter alia, on the prevention of the placement of weapons in outer space."[183] There had been serious doubts that a new GGE could achieve much in the current environment, as all major powers and a growing number of smaller states are developing counterspace capabilities. Two sessions of the GGE were held, one in 2018 and another in 2019. However, the group failed to produce a consensus report.

Still, the group reportedly held fruitful discussions on a range of issues relating to "a safe, secure and sustainable use of outer space" and the importance of transparency and confidence-building measures became evident in the group's deliberations.[184] The work of this GGE might be complemented by more practical efforts, such as an agreement on and the implementation of ASAT test guidelines.[185] The latter would be based on widely accepted best practices; linked to the recommended transparency and confidence-building measures in outer space activities; grounded in work under way within COPUOS, the Conference on Disarmament, and the Disarmament Commission; and related to ongoing work on debris mitigation and the long-term sustainability of outer space activities. Such guidelines, the UN Institute for Disarmament Research explains, would respect states' rights "to possess or develop anti-ballistic missile (ABM) or ASAT capabilities,

provided they do so in a manner that is recognized as being responsible," while enhancing stability in outer space and limiting the potential hazards of weaponization.[186]

Again, the potential for economic growth and development derived from commercial space activity could serve as an important incentive for such efforts. Nonetheless, in each of these areas, maintaining dialogue on the core principles and norms that should guide activity in outer space—particularly those that restrain destabilizing behaviors and ensure equitable access to potential benefits—will be imperative as will ensuring that the private sector, industry associations, and other relevant actors in these government-led processes and mechanisms are given greater opportunities to voice their views.

Conclusion

The array of new technologies emerging on the world stage, the new threats they can pose, and the associated governance dilemmas highlight a set of common themes. First, an explosive growth of technological innovation is outstripping the capacity (or willingness) of technology creators, private investors, national governments, and the existing multilateral system to understand, monitor, and effectively govern the attendant effects and consequences.

Second, these technologies offer great benefits to society while, at the same time, imposing grave risks ranging from malicious use to exacerbating socioeconomic inequalities. Despite the range of initiatives under way and broad acknowledgment of the governance challenges at hand, it is alarming to see how lackluster the responses have been to date. Without the necessary political will and concerted cooperation across actors and regions, it will be impossible to ensure that technologies are used responsibly; their benefits are shared equitably; and the serious ethical, social, economic, personal safety, environmental, and national security risks are managed deftly.

Third, this absence of political will and cooperation is driven, increasingly, by structural dynamics that undermine efforts to reach consensus. Technology is a deeply embedded facet of geopolitical competition, particularly among the great powers, and such innovation is central to both spurring economic growth and gaining a military edge. As a result, few powerful states have been willing to restrict their pursuit of perceived technological advantages. The effects of this security dilemma are growing more acute as economic, political, and military competition among China, Russia, the United States, and a growing number of middle powers increases. This competitive dynamic is already evident in the areas of ICT and outer space, and similar trends are emerging in relation to AI, biotechnology, and other areas not discussed in this paper such as quantum computing and

nanotechnology. States (including the great powers) have overcome heated competition and heightened tensions in the past. They should commit to doing the same now.

Fourth, the economic model undergirding global technology markets, driven by the need for companies to reach economies of scale in terms of how many users they have, has led many companies to focus on offering products and services first and fixing resulting problems later. This mentality has left software, hardware, and supply chains vulnerable to disruption, manipulation, and capture by governments, criminal groups, and other malicious actors around the world. Again, this state of affairs is evident in the field of ICT, and similar behavior will likely surface in other technological areas as well. Notably, these fields call on a wide array of (sometimes antagonistic) actors to coordinate and reach agreement, including individual states, the companies driving innovation, technologists, civil society, international organizations, and academic institutions.

While these dynamics offer an unfavorable outlook for cooperation, there is, in parallel, a wide range of efforts already under way to deal with emerging challenges and risks. Some of these actions are being spearheaded by governments, while others are the product of a host of actors from across an equally wide array of disciplines and sectors. These efforts—complex, fragmented, and wide-ranging (and often nonproductive) as they may be—need to be acknowledged, strengthened, and scaled. Lessons—both positive and negative—must be shared across regions, as these experiences might inform more efficacious approaches or models for effective governance and multiactor cooperative arrangements.

The UN, too, should be able to support its member states and all other stakeholders by facilitating dialogue and cooperation on the policy and normative challenges stemming from technological advances. Through a number of initiatives, including his Agenda for Disarmament, his Strategy on New Technologies, and the establishment of a High-Level Panel on Digital Cooperation, the UN secretary general has acknowledged this.[187] The initiatives signal a recognition that these advances are emerging at a critical moment in international relations, a time when consensus is becoming increasingly difficult to achieve and during which efforts to manage and govern new risks and challenges are becoming increasingly complicated. Like other leaders, he understands that supporting ongoing efforts and facilitating dialogue and cooperation will be difficult, yet he also grasps that the UN has a responsibility to safeguard its principles and purposes. The body's member states (and their national governments) should do the same, as the world's dependence on cutting-edge technology continues to deepen.

About the Author

Camino Kavanagh is a visiting fellow in the Department of War Studies at King's College London. She also works as an independent consultant, with current contracts including a senior advisory role with the UN Department of Political Affairs' Policy and Mediation Division on a project relating to conflict prevention and emerging technologies. Kavanagh served as rapporteur/consultant of the 2016–2017 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. She is involved in a number of policy and research initiatives on ICT and emerging technologies as they relate to conflict and international security. Kavanagh received her PhD from the Department of War Studies at King's College London in 2016.

Acknowledgments

This publication could not have been produced without the valuable contributions of many individuals. First, the author would like to thank the Carnegie Endowment for International Peace for agreeing to publish it, particularly George Perkovich, Kate Charlet, Tim Maurer, Charlotte Stanton, and Ryan DeVries for reviewing and providing such valuable feedback. The author also offers thanks to the United Nations Foundation for funding the initial research that led to this publication and especially to Kaysie Brown and Megan Roberts for their constructive feedback. She also wishes to express her gratitude to Marc Jacquand and Fabrizio Hochschild of the Executive Office of the UN Secretary General for the opportunity to work on the Secretary-General's Strategy on New Technologies in 2018 and develop some of that work further through this publication.

Finally, the author is grateful to a number of experts who shared their insights on the governance and normative dilemmas emerging in their respective fields. This list includes Kerstin Vignard and Daniel Porras at the UN Institute for Disarmament Research, Gillian Goh at the UN Office of Disarmament Affairs, Piers Millet and Carrick Flynn at the Future of Humanity Institute, Beth Cameron and Jacob Jordan at the Nuclear Threat Initiative, Michael Page at OpenAI, Madeline Carr at University College London, Paul Cornish at LSE IDEAS, and Nigel Inkster at the International Institute for Strategic Studies.

Notes

1 Camino Kavanagh and Paul Cornish, "Preventive Diplomacy, ICT and Inter-State Conflict: A Review of Current Practice with Observations," *Swiss Federal Department of Foreign Affairs*, (forthcoming 2019).

2 Roger Brownsword, Eloise Scotford, and Karen Yeung, (eds.), *Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford Handbooks Online, 2017).

3 Harvard professor Joseph S. Nye Jr. refers to this framework as "the global regime complex governing global cyber activities." See Joseph S. Nye, Jr., "The Regime Complex for Governing Global Cyber Activities," Global Commission on Internet Governance, May 2014, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

4 World Economic Forum, "The Fourth Industrial Revolution: What It Means, How to Respond," January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

5 World Economic Forum, "Agile Governance: Reimagining Policy Making in the Fourth Industrial Revolution," January 2018, http://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf.

6 World Economic Forum, "The Fourth Industrial Revolution: What It Means, How to Respond."

7 Yochai Benkler, "Don't Let Industry Write the Rules for AI," *Nature*, May 2019; Vol. 569 (7755):161, https://www.nature.com/magazine-assets/d41586-019-01413-1/d41586-019-01413-1.pdf; and Luciano Floridi and Josh Cowls, "A Unified Framework of Five Principles for AI in Society," *Harvard Data Science Review,* June 23, 2019, https://doi.org/10.1162/99608f92.8cd550d1.

8 Benkler, "Don't Let Industry Write the Rules for AI."

9 Anne Marie Engtoft Larsen, "Regulation for the Fourth Industrial Revolution," WEF Podcast Episode 5, [interview portion with Rob Sparrow of Monash University], January 30 2018, https://www.weforum.org/agenda/2018/01/podcast-regulation-for-the-fourth-industrial-revolution/.

10 Joseph S. Nye Jr., "The Regime Complex for Governing Global Cyber Activities."

11 Ibid.

12 UN Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet," Resolution 20/8, July 16, 2012, https://www.right-docs.org/doc/a-hrc-res-20-8/; and UN Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet," Resolution 26/13, July 14, 2014, http://hrlibrary.umn.edu/hrcouncil_res26-13.pdf.

13 Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations: Starting the Conversation," November 14, 2018, International Committee of the Red Cross Humanitarian Law and Policy (blog), https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/.

14 UN Office of Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security," https://www.un.org/disarmament/ict-security/; UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Document A/65/201, July 30, 2010, https://undocs.org/A/65/201; UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Document A/68/98*, June 24, 2013, http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf; and UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Document A/70/174, July 22, 2015, https://undocs.org/A/70/174. On the applicability of international law, see the international law sections in UN General Assembly Document A/68/98* and UN General Assembly Document A/70/174. For an analysis of the outcome of these reports, see Camino Kavanagh,

"The United Nations, Cybersecurity and International Peace and Security: Responding to Complexity in the 21st Century," United Nations Institute for Disarmament Research (UNIDIR), 2017, http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

[15] See Section III of UN General Assembly Document A/70/174, 7.

[16] UN General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," Resolution 70/237, December 2015, 3, https://undocs.org/en/A/RES/70/237.

[17] UN member states can propose the establishment of GGEs via the General Assembly (or, in this case, its First Committee on Disarmament and International Security). The proposal is then put to a vote and adopted via a resolution if endorsed. See UN General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security, Document A/C.1/73/L.37, October 18, 2018, https://undocs.org/A/C.1/73/L.37; and UN General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," Document A/C.1/73/L.27/Rev.1, October 29, 2018, https://undocs.org/A/C.1/73/L.27/Rev.1.

[18] G20 Information Center, "Communiqué [G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany]," March 17–18, 2017, http://www.g20.utoronto.ca/2017/170318-finance-en.html; and Tim Maurer, Ariel Levite, and George Perkovich, "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, June 29, 2016, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

[19] See, for instance, International Atomic Energy Agency (IAEA), "IAEA Launches International Training Course on Protecting Nuclear Facilities from Cyber-Attacks," October 24, 2018, https://www.iaea.org/newscenter/pressreleases/iaea-launches-international-training-course-on-protecting-nuclear-facilities-from-cyber-attacks; and IAEA, "IAEA Computer and Network Security," https://www.iaea.org/topics/computer-and-information-security.

[20] On VEPs, their genesis, and their character, see Katherine Charlet, Sasha Romanosky, and Bert Thompson, "It's Time for the International Community to Get Serious about Vulnerability Equities," *Lawfare*, November 15, 2017, https://www.lawfareblog.com/its-time-international-community-get-serious-about-vulnerability-equities; and Sven Herpig and Ari Schwartz, "The Future of Vulnerability Equities Processes Around the World," *Lawfare*, January 4, 2019, https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

[21] Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations: ICRC Expert Meeting 14–16 November 2018 - Geneva," International Commitee of the Red Cross, https://www.icrc.org/en/document/potential-human-cost-cyber-operations. and the UN Department of Political and Peacebuilding Affairs and Humanitarian Dialogue Center, "Digital Technologies and Mediation in Armed Conflict," March 2019, https://peacemaker.un.org/sites/peacemaker.un.org/files/DigitalToolkitReport.pdf. The digital version of the toolkit is available here: https://peacemaker.un.org/digitaltoolkit.

[22] Digital Europe, "DIGITALEUROPE's Position Paper on the European Commission's Proposal for a European Framework for Cybersecurity Certification Scheme for ICT Products and Services," December 15, 2017, https://www.digitaleurope.org/resources/digitaleuropes-position-paper-on-the-european-commissions-proposal-for-a-european-framework-for-cybersecurity-certification-scheme-for-ict-products-and-services/.

[23] Eileen Donahue, Melissa Hathaway, James A. Lewis, Joseph S. Nye Jr., Eneken Tikk, and Paul Twomey, "Getting Beyond Norms: New Approaches to International Cyber Security Challenge," Center for

International Governance Innovation, September 7, 2017, 9, https://www.cigionline.org/sites/default/files/documents/Getting%20Beyond%20Norms.pdf.

[24] Karen Yeung, "Regulation for the Fourth Industrial Revolution," WEF Podcast Episode 5, [interview portion with Karen Yeung, formerly of King's College London], January 30 2018, https://www.weforum.org/agenda/2018/01/podcast-regulation-for-the-fourth-industrial-revolution/.

[25] European Commission, "2018 Reform of EU Data Protection Rules," European Commission, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules; and European Commission, "The Directive on Security of Network and Information Systems (NIS Directive)," https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[26] Ibid.

[27] See the following explanation of the I* organizations: "I* Organizations," Asia-Pacific Network Information Center, https://www.apnic.net/community/ecosystem/iorgs/.

[28] "Call to Protect the Public Core of the Internet," Global Commission on the Stability of Cyberspace, November 2017, https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf.

[29] Kofi Annan Commission on Elections and Democracy in the Digital Age, "About the Commission," https://www.kofiannanfoundation.org/our-work/kofi-annan-commission/.

[30] "Norm Package Singapore," Global Commission on the Stability of Cyberspace, November 2018, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

[31] "One Internet," Center for International Governance Innovation and Chatham House, 2016, Available at: https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf.

[32] See Siemens, "The Charter of Trust Takes a Major Step Forward to Advance Cybersecurity," February 15, 2019, https://www.siemens.com/press/en/feature/2018/corporate/2018-02-cybersecurity.php.

[33] Siemens, "Presentation on the Siemens Charter of Trust," March 2019, https://assets.new.siemens.com/siemens/assets/public.1552654550.55badda4-4340-46d3-b359-f570e7d1f4c2.charter-of-trust-presentation-en.pdf.

[34] Romain Dillet, "50 Tech CEOs Come to Paris to Talk About Tech for Good," *TechCrunch*, May 23, 2018, https://techcrunch.com/2018/05/23/50-tech-ceos-come-to-paris-to-talk-about-tech-for-good/.

[35] Microsoft, "A Digital Convention to Protect Cyberspace," Microsoft Policy Papers, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

[36] Tom Burt, "Announcing the Defending Democracy Program," Microsoft, April 13, 2018, https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program/.

[37] Ibid.

[38] Microsoft, "Digital Peace Now," https://digitalpeace.microsoft.com.

[39] "Cybersecurity: Paris Call for Trust and Security in Cyberspace," France Diplomatie, November 12, 2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[40] Mark Zuckerberg, "The Internet Needs New Rules. Let's Start in These Four Areas," *Washington Post*, March 30, 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.993b6d276366

[41] For instance, author Roger McNamee described it as "a monument to insincerity and misdirection." Roger McNamee, "Mark Zuckerberg Says He Wants to Fix the Internet. Don't Take Him Seriously," *Guardian.* April 2, 2019, https://www.theguardian.com/commentisfree/2019/apr/02/mark-zuckerberg-fix-the-internet.

[42] "Balancing Security and Public Interest: The GDPR and the Public Sector," Trend Micro, April 9, 2018, https://www.trendmicro.com/vinfo/au/security/news/online-privacy/balancing-security-and-public-interest-gdpr-and-public-sector. For an explanation of the roles of data controllers and processors, see "Controllers and Processors," GDPR EU.org, https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/.

[43] Kaysie Brown, "What Happens After the High-Level Political Forum? Here Are 4 Areas to Watch," UN Foundation (blog), July 20, 2018, http://unfoundationblog.org/what-happens-after-the-high-level-political-forum-here-are-4-areas-to-watch/.

[44] Deborah Brown, "What to Expect at the 2018 ITU Plenipotentiary Conference and What It Means for the Internet," Council on Foreign Relations, March 12, 2018, https://www.cfr.org/blog/what-expect-2018-itu-plenipotentiary-conference-and-what-it-means-internet.

[45] See, for example, "Russia Must Build Own Internet in Case of Foreign Disruption, Putin Says," *Moscow Times,* February 21, 2019, https://www.themoscowtimes.com/2019/02/21/russia-must-build-own-internet-in-case-of-foreign-disruption-a64578.

[46] UN Office for Disarmament Affairs, "Submission of the Report of the Secretary-General on Resolution 73/27 on Developments in the Field of Information and Telecommunications in the Context of International Security and Resolution 73/266 on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security," UN Document ODA/2019-00116/ICTS, February 6, 2019, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/19-074nve.pdf.

[47] Brian Egan [former legal adviser to the U.S. Department of State], "Remarks on Stability and International Law in Cyberspace," U.S. Department of State, November 10 2016, https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

[48] UN General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," Document A/C.1/73/L.27/Rev.1, paragraph 5, October 29, 2018, https://undocs.org/A/C.1/73/L.27/Rev.1; and UN General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," Document A/C.1/73/L.37, paragraph 3, October 18, 2018, https://undocs.org/A/C.1/73/L.37.

[49] Ibid.

[50] UN Office for Disarmament Affairs, "Submission of the Report of the Secretary-General on Resolution 73/27 on Developments in the Field of Information and Telecommunications in the Context of International Security and Resolution 73/266 on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security."

[51] G7, "Dinard Declaration on the Cyber Norm Initiative," G7 Foreign Ministers Meeting, Dinard – Saint-Malo, April 6–7, 2019, https://www.elysee.fr/admin/upload/default/0001/04/d37b5326306c7513b58c79d26938f678d95cb2ff.pdf.

[52] Camino Kavanagh, "Stemming the Exploitation of ICT Threats and Vulnerabilities: An Overview of Current Trends, Enabling Dynamics and Private Sector Responses," UNIDIR, June 25 2019, http://www.unidir.org/files/publications/pdfs/stemming-the-exploitation-of-ict-threats-and-vulnerabilities-en-805.pdf.

[53] Ibid.

[54] John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude E. Shannon, "Proposal for the Dartmouth Summer Research Project on Artificial Intelligence," *AI Magazine* 27, no. 4 (2006): 12, https://aaai.org/ojs/index.php/aimagazine/issue/view/165. (This piece was originally written in August 1955 but was published in this journal issue.

[55] Floridi and Cowls, "A Unified Framework of Five Principles for AI in Society."

[56] Rodney Brooks, "The Origins of Artificial Intelligence," FoR&AI, April 27, 2018, https://rodneybrooks.com/forai-the-origins-of-artificial-intelligence/; John Mallery, "Intelligent Computation in National Defense Applications: Artificial Intelligence or Magic?," the 2018 Roundtable on Military Cyber Stability, Framing presentation in the session entitled "Applications of New Technologies in National Defense," Washington, DC, July 17, 2018; and Rodney Brooks, "The Seven Deadly Sins of AI Predictions," *MIT Technology Review*, October 6, 2017, https://www.technologyreview.com/s/609048/the-seven-deadly-sins-of-ai-predictions/.

[57] International Institute for Strategic Studies (IISS), *The Military Balance 2018*, Chapter 1, Part 2, "Big Data, Artificial Intelligence and Defence" (London: IISS, 2018), https://www.iiss.org/publications/the-military-balance/the-military-balance-2018.

[58] See, for instance, Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, (New York: Knopf, 2017); and Nick Bockstrom, *Superintelligence: Paths, Dangers, Strategies*, (Oxford: Oxford University Press, 2014).

[59] "The Weaponization of Increasingly Autonomous Technologies: no. 8 Artificial Intelligence (A Primer for CCW Delegates)," UNIDIR, 2018, http://www.unidir.ch/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-artificial-intelligence-en-700.pdf.

[60] See the International Labor Organization's Future of Work research series and its Global Commission on the Future of Work, the OECD's Future of Work Initiative, and the WEF's Preparing for the Future of Work Initiative. On the future of food, see Lassonde School of Engineering, "Can AI Help Feed the World? The Future of Food is Here," *Medium*, April 16, 2018, https://medium.com/lassondeschool/can-ai-help-feed-the-world-the-future-of-food-is-here-429e7c10290b; and Emiko Terazono, "Future of Food: Inside Agritech's Silicon Valley," *Financial Times*, October 15, 2018, https://www.ft.com/content/199cae4c-cbc6-11e8-b276-b9069bde0956. On the future of humanity, see research by the Future of Humanity Institute and the Future of Life Institute as well as Michio Kako, *The Future of Humanity: Our Destiny in the Universe*, (New York: Penguin Books, 2019).

[61] James Vincent, "Putin Says the Nation That Leads in AI 'Will be the Ruler of the World,'" *Verge,* September 4, 2017, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world; Zhou Xin and Choi Chi-yuk, "Develop and Control: Xi Jinping Urges China to Use Artificial Intelligence in Race for Tech Future," *South China Morning Post,* October 31, 2018, https://www.scmp.com/economy/china-economy/article/2171102/develop-and-control-xi-jinping-urges-china-use-artificial; and White House Office of Science and Technology Policy, "Accelerating America's Leadership in Artificial Intelligence," February 11, 2019, https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/.

[62] Elsa Kania, "Great Power Competition and the AI Revolution: A Range of Risks to Military and Strategic Stability," *Lawfare*, September 19, 2017, https://www.lawfareblog.com/great-power-competition-and-ai-revolution-range-risks-military-and-strategic-stability.

[63] Floridi and Cowls, "A Unified Framework of Five Principles for AI in Society."

[64] Future of Life Institute, "Asimolar AI Principles,"https://futureoflife.org/ai-principles/.

[65] Campaign to Stop Killer Robots, "About Us," https://www.stopkillerrobots.org/about/.

[66] Future of Life Institute, "Lethal Autonomous Weapons Pledge," https://futureoflife.org/lethal-autonomous-weapons-pledge/?cn-reloaded=1.

[67] Future of Life Institute, "Autonomous Weapons: an Open Letter From AI and Robotics Researchers," https://futureoflife.org/open-letter-autonomous-weapons/.

[68] Meredith Whittaker et al., "AI Now Report 2018," New York University AI Now Institute, December 2018, https://ainowinstitute.org/AI_Now_2018_Report.pdf; and AI Now Institute, "Algorithmic Accountability Policy Toolkit", October 2018, https://ainowinstitute.org/aap-toolkit.pdf.

[69] Institute of Electrical and Electronics Engineers (IEEE), "Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems," first edition, 2016, https://ethicsinaction.ieee.org/#read; and IEEE, "The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems," https://standards.ieee.org/industry-connections/ec/autonomous-systems.html.

[70] Ibid.

[71] Partnership on AI, "Tenets," https://www.partnershiponai.org/tenets/.

[72] Salil Sethi, "7 Predictions for Artificial Intelligence in 2019," OpenSource.com, February 5, 2019, https://opensource.com/article/19/2/predictions-artificial-intelligence.

[73] Open AI, "Open AI Charter," https://blog.openai.com/openai-charter/.

[74] Ibid.

[75] Google, "AI at Google: Our Principles," https://blog.google/technology/ai/ai-principles/.

[76] Microsoft, "Microsoft AI Principles," https://www.microsoft.com/en-us/ai/our-approach-to-ai.

[77] Accenture, "Responsible AI and Robotics: An Ethical Framework," https://www.accenture.com/gb-en/company-responsible-ai-robotics.

[78] Salesforce, "AI Ethics and Values," https://einstein.ai/ethics; and Salesforce, "Paula Goldman Joins Salesforce as Chief Ethical and Humane Use Officer, Salesforce," https://www.salesforce.com/company/ethical-and-humane-use/.

[79] Jessica Cussins Newman, "Toward AI Security: Global Aspirations for a More Resilient Future," University of California, Berkeley, Center for Long-Term Cybersecurity, February 2019, https://cltc.berkeley.edu/wp-content/uploads/2019/02/Toward_AI_Security.pdf.

[80] World Bank, "The Changing Nature of Work: World Development Report 2019," 2019, http://documents.worldbank.org/curated/en/816281518818814423/pdf/2019-WDR-Report.pdf; and Simone D. McCourtie, "With AI, Jobs Are Changing But No Mass Unemployment Expected—UN Labour Experts," United Nations, September 4, 2018, https://news.un.org/en/story/2018/09/1018292.

[81] World Bank, "The Changing Nature of Work."

[82] Daniel Araya, "Artificial Intelligence and the End of Government," *Forbes,* January 4, 2019, https://www.forbes.com/sites/danielaraya/2019/01/04/artificial-intelligence-and-the-end-of-government/#27e90bc3719b; and UK Department for Business, Energy, and Industrial Strategy and Department for Digital, Culture, Media and Sport, "AI Sector Deal," updated May 2019, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal.

[83] Greg Allen and Taniel Chan, "Artificial Intelligence and National Security," Harvard Kennedy School Belfer Center for Science and International Affairs, July 2017, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

[84] Kelley M. Sayler, "Artificial Intelligence and National Security," Congressional Research Service, Updated January 2019, 11, https://fas.org/sgp/crs/natsec/R45178.pdf.

[85] Cussins Newman, "Toward AI Security."

[86] European Group on Ethics in Science and New Technologies, "Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems," European Commission Directorate-General for Research and Innovation, March 9, 2018, https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.

[87] "EU Declaration of Cooperation on Artificial Intelligence," European Commission, April 10, 2018, https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence.

[88] European Commission, "Communication on Cooperation on Artificial Intelligence for Europe," (COM(2018) 237 final), April 25, 2018, https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

[89] Ibid, 4.

[90] Organization for Economic Co-operation and Development (OECD), "OECD Principles on AI," May 2019, https://www.oecd.org/going-digital/ai/principles/. The OECD boasts that these "are the first such principles signed up to by governments" and that, in addition to OECD members, a number of other countries—including Argentina, Brazil, Colombia, Costa Rica, Peru, and Romania—have signed up.

[91] G20, "G20 Ministerial Statement on Trade and Digital Economy," June 2019, https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[92] Council of Europe Committee of Ministers, "Technological Convergence, Artificial Intelligence and Human Rights: Recommendation 2102," 2017; Council of Europe Committee of Ministers, "Technological Convergence, Artificial Intelligence and Human Rights: Reply to Recommendation," October 19, 2017; Council of Europe Commissioner for Human Rights "Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights," May 2019; and Council of Europe Committee of Ministers, "Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes" February 13, 2019. All three of these documents available on the Council of Europe's webpage on artificial Intelligence. See Council of Europe, "Council of Europe and Artificial Intelligence," https://www.coe.int/en/web/artificial-intelligence/home.

[93] Cussins Newman, "Toward AI Security."

[94] Kelley M. Sayler, "Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems," Congressional Research Service, March 27, 2019, https://fas.org/sgp/crs/natsec/IF11150.pdf; and Daniel S. Hoadley and Kelley M. Sayler, "Artificial Intelligence and National Security," Congressional Research Service, updated January 30, 2019, 14, https://fas.org/sgp/crs/natsec/R45178.pdf.

[95] For more details, see Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, " Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)," (UN Document CCW/GGE.1/2017/3), December 22, 2017, https://undocs.org/CCW/GGE.1/2017/3.

[96] Ibid.

[97] The twenty-eight countries are: Algeria, Argentina, Austria, Bolivia, Brazil, Chile, China, Colombia, Costa Rica, Cuba, Djibouti, Ecuador, Egypt, El Salvador, Ghana, Guatemala, the Holy See, Iraq, Mexico, Morocco, Nicaragua, Pakistan, Panama, Peru, the State of Palestine, Uganda, Venezuela, and Zimbabwe. See Future of Life Institute, "Lethal Autonomous Weapons Pledge," https://futureoflife.org/lethal-autonomous-weapons-pledge/.

[98] Campaign to Stop Killer Robots, "Country Views on Killer Robots," April 13 2018, https://www.stopkillerrobots.org/wp-content/uploads/2018/04/KRC_CountryViews_13Apr2018.pdf.

[99] Campaign to Stop Killer Robots, "UN Head Calls for a Ban," November 12, 2018, https://www.stopkillerrobots.org/2018/11/unban/.

[100] UN Office of Disarmament Affairs, *Securing Our Common Future: An Agenda for Disarmament,* (New York: United Nations, May 2018), 55, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit.

[101] Ibid.

[102] For differing reasons, four of the five permanent members of the UN Security Council have reportedly rejected moving to negotiate new international law on autonomous weapons.

[103] Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, "Report of the 2018 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems."

[104] For a detailed overview of these issues, see Permanent Mission of the Republic of North Macedonia to the UN, WTO and Other International Organizations in Geneva, "Chairperson's Letter on the Provisional Agenda," Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous

Weapons Systems, March 19, 2019, https://www.unog.ch/80256EDD006B8954/(httpAssets)/E2B8A8216FE382FBC125839B00608672/$file/190208+LAWS+-+Chair's+first+letter+to+accompany+Provisional+Agenda+(%D1%84).pdf; and 2019 Group of Governmental Experts on Lethal Autonomous Weapons Systems, "Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects," UN Office of Disarmament Affairs, March 19, 2019, https://www.unog.ch/80256EE600585943/(httpPages)/5C00FF8E35B6466DC125839B003B62A1?OpenDocument.

105 Floridi and Cowls, "A Unified Framework of Five Principles for AI in Society."

106 Ibid, 4-8.

107 Tristan Greene, "Google's Principles for Developing AI Aren't Good Enough," Next Web, June 8, 2018, https://thenextweb.com/artificial-intelligence/2018/06/08/googles-ai-principles-7-shades-of-gray-area/.

108 Natasha Lomas, "A Discussion About AI's Conflicts and Challenges," *TechCrunch*, June 17, 2018, https://beta.techcrunch.com/2017/06/17/a-discussion-about-ais-conflicts-and-challenges/?_ga=2.250353861.219450613.1532680997-423792798.1532680997.

109 Natasha Lomas, "DeepMind Now Has an AI Ethics Research Unit. We Have a Few Questions for It . . . ," *TechCrunch,* October 4, 2017, https://techcrunch.com/2017/10/04/deepmind-now-has-an-ai-ethics-research-unit-we-have-a-few-questions-for-it/?guccounter=1.

110 DeepMind, "DeepMind Ethics and Society: About Us," https://deepmind.com/applied/deepmind-ethics-society/.

111 DeepMind, "Principles," https://deepmind.com/applied/deepmind-ethics-society/principles/.

112 Lomas, "DeepMind Now Has an AI Ethics Research Unit. We Have a Few Questions for It . . . "; and Alex Hern, "Whatever Happened to the DeepMind AI Ethics Board Google Promised?" *Guardian,* January 26, 2017, https://www.theguardian.com/technology/2017/jan/26/google-deepmind-ai-ethics-board.

113 Hal Hodson, "DeepMind and Google: The Battle to Control Artificial Intelligence," *Economist 1843 Magazine*, April–May 2019, https://www.1843magazine.com/features/deepmind-and-google-the-battle-to-control-artificial-intelligence; Lomas, "DeepMind Now Has an AI Ethics Research Unit. We Have a Few Questions for It . . . "; and Hern, "Whatever Happened to the DeepMind AI Ethics Board Google Promised?"

114 Axon, "Axon AI and Policing Technology Ethics Board," https://es.axon.com/info/ai-ethics.

115 Jake Laperruque, "Taser's Free Body Cameras Are Good for Cops, Not the People," *Wired*, April 15, 2018, https://www.wired.com/2017/04/tasers-free-body-cameras-good-cops-not-people/.

116 Axon, "Axon AI and Policing Technology Ethics Board."

117 Cussins Newman, "Toward AI Security," 4.

118 See, for example, UNIDIR, "The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values," 2015, http://www.unidir.org/files/publications/pdfs/considering-ethics-and-social-values-en-624.pdf; UNIDIR, "The Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward," 2014, https://www.files.ethz.ch/isn/185834/considering-how-meaningful-human-control-might-move-the-discussion-forward-en-615.pdf; and IISS, *The Military Balance 2018*, Chapter 1, Part Two "Big Data, Artificial Intelligence and Defence."

119 Jayshree Pandya, "The Weaponization of Artificial Intelligence," *Forbes,* January 14, 2019, https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial-intelligence/#7c6f03bb3686.

120 See UNIDIR, "Trust but Verif AI: Options for Regulating Defence and Security AI Technologies," http://www.unidir.org/programmes/security-and-technology/trust-but-verif-ai-options-for-regulating-defence-and-security-ai-technologies.

[121] United Nations, "Convention on Biological Diversity," Article 2: Use of Terms, https://www.cbd.int/convention/articles/default.shtml?a=cbd-02.

[122] Author interview with NTI, July 2018. For the India figure, see Burrill Media, Biotechnology Industry Organization, and the Association of Biotechnology Led Enterprises, "Accelerating Growth: Forging India's Bioeconomy," 2014, https://www.bio.org/sites/default/files/files/Burrill_AcceleratingGrowth_India-6-9-final.pdf.

[123] European Commission's Knowledge Centre for Bioeconomy, "EU Bioeconomy," September 1, 2018, https://ec.europa.eu/knowledge4policy/sites/know4pol/files/2018_09_01_bioeconomi_infographic_update_en.pdf. The infographic is based on the following peer-reviewed publication: Tévécia Ronzon and Robert M'Barek, "Socioeconomic Indicators to Monitor the EU's Bioeconomy in Transition," *Sustainability* 10 no. 6, (May 26, 2018), https://www.mdpi.com/2071-1050/10/6/1745.

[124] James C. Greenwood, "Biotech in China," Biotechnology Innovation Organization, January 2013, https://www.bio.org/sites/default/files/files/Biotechnology-Industry-Pg62-64.pdf.

[125] Author interview with NTI, July 2018; European Commission, "What Is the Bioeconomy?," May 9, 2018, https://ec.europa.eu/research/bioeconomy/index.cfm; [Obama] White House, "National Bioeconomy Blueprint," April 2012, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf; Beate El-Chichakli et al., "Policy: Five Cornerstones of a Global Bioeconomy," *Nature* 535, no. 7611 (2016): 221–222, https://www.nature.com/news/policy-five-cornerstones-of-a-global-bioeconomy-1.20228; and Beth Baker, "Synthetic Biology and the Marketplace: Building the New Bioeconomy," *BioScience* 67, no. 10 (2017): 877–883, https://doi.org/10.1093/biosci/bix101.

[126] Arjun Bhutkar, "Synthetic Biology: Navigating the Challenges Ahead," *Journal of Biolaw and Business* 8 no. 2, (2005):19–29.

[127] Ed Yong, "The CRISPR Baby Scandal Gets Worse by the Day," *Atlantic*, December 3, 2018, https://www.theatlantic.com/science/archive/2018/12/15-worrying-things-about-crispr-babies-scandal/577234/.

[128] U.S. National Library of Medicine, "Genetics Home Reference: Your Guide to Understanding Genetic Conditions," June 25, 2019, https://ghr.nlm.nih.gov/primer/basics/gene.

[129] See Martin Jinek et al., "A Programmable Dual-RNA–Guided DNA Endonuclease in Adaptive Bacterial Immunity," *Science*, 337, no. 6096, (August 17, 2012): 816–821, https://science.sciencemag.org/content/337/6096/816; and Le Cong et al., "Multiplex Genome Engineering Using CRISPR/Cas Systems," *Science*, 339, no. 6121 (February 15, 2013), 819–823, https://science.sciencemag.org/content/339/6121/819.

[130] Maria Patrão Neves and Christiane Druml, "Ethical Implications of Fighting Malaria With CRISPR/Cas9," *BMJ Glob Health* 2 no. 3, (2017): 1–2, https://gh.bmj.com/content/2/3/e000396.

[131] Charleston Noble et al., "Current CRISPR Gene Drive Systems Are Likely to Be Highly Invasive in Wild Populations," *eLife*, June 19, 2018, https://elifesciences.org/articles/33423.

[132] World Health Organization, "The Guidance Framework for Testing Genetically Modified Mosquitoes," 2014, http://www.who.int/tdr/publications/year/2014/guide-fmrk-gm-mosquit/en/.

[133] Author interview with NTI, June 2018.

[134] U.S. National Academies and the Department of Homeland Security, "Biological Attack, Human Pathogens, Biotoxins and Agricultural Threats: A Fact Sheet," 2004, https://www.dhs.gov/sites/default/files/publications/prep_biological_fact_sheet.pdf

[135] Monica Schoch-Spana et al., "Global Catastrophic Biological Risks: Towards a Working Definition," *Health Security*, 15 no. 4, (August 1, 2017), 327, https://www.liebertpub.com/doi/10.1089/hs.2017.0038.

[136] Maski Imai et al., "Experimental Adaptation of an Influenza H5 HA Confers Respiratory Droplet Transmission to a Reassortant H5 HA/H1N1 Virus in Ferrets," *Nature*, 486, (June 21, 2012), 420–428, https://www.nature.com/articles/nature10831; and Colin A. Russell et al., "The Potential for Respiratory Droplet-Transmissible A/H5N1 Influenza Virus to Evolve in a Mammalian Host," *Science*, 336 (June 22, 2012): 1541–1547, https://science.sciencemag.org/content/336/6088/1541.

[137] See, for instance, the following two documents, the latter of which was revised in 2013 to include dual-use technologies. U.S. Department of Health and Human Services, "Framework for Guiding Funding Decisions About Proposed Research Involving Enhanced Potential Pandemic Pathogens," December 2017, https://www.phe.gov/s3/dualuse/Documents/p3co.pdf; or Science Council of Japan, "Code of Conduct for Scientists: Revised Version," 2013, http://www.scj.go.jp/ja/scj/kihan/kihan.pamflet_en.pdf.

[138] Ibid. Also see: European Committee for Standardization, "Laboratory Risk Management," September 2011, http://www.uab.cat/doc/CWA15793_2011.

[139] National Academy of Sciences and National Academy of Medicine, "Human Genome Editing: Science, Ethics and Governance," 2017, https://www.nap.edu/catalog/24623/human-genome-editing-science-ethics-and-governance. On the highly controversial practice of germline editing, see Joel Achenbach, "Ethicists Advise Caution in Applying CRISPR Gene Editing to Humans," *Washington Post,* February 14, 2017, https://www.washingtonpost.com/news/speaking-of-science/wp/2017/02/14/ethicists-advise-caution-in-applying-crispr-gene-editing-to-humans/?utm_term=.dfd0a40218a2.

[140] Phoebe Zhang, "China Confirms Birth of Gene-Edited Babies, Blames Scientist He Jiankiu for Breaking Rules," *South China Morning Post*, January 21, 2019, https://www.scmp.com/news/china/science/article/2182964/china-confirms-gene-edited-babies-blames-scientist-he-jiankui.

[141] "Stanford Investigates Links to Scientist in Baby Gene-Editing Scandal," *Guardian,* February 8, 2019, https://www.theguardian.com/science/2019/feb/08/stanford-investigates-links-to-scientist-in-baby-gene-editing-scandal.

[142] Chinese officials formally recognized He Juankui's research and the potential sanctions he could face as a result for the first time in January 2019. Austin Ramzy and Sui-Lee Wee, "Scientist Who Edited Babies' Genes Is Likely to Face Charges," *New York Times,* January 21, 2019, https://www.nytimes.com/2019/01/21/world/asia/china-gene-editing-babies-he-jiankui.html.

[143] According to the *New York Times*, Joseph DeAngelo was identified and later charged with twenty-six counts of murder and kidnapping "after a genealogist helped investigators in California identify a third cousin of Mr. DeAngelo's through GED match and other genealogical records." See Elizabeth Joh, "Want to See My Genes? Get a Warrant," *New York Times,* June 11, 2019, https://www.nytimes.com/2019/06/11/opinion/police-dna-warrant.html.

[144] Ibid.

[145] Author interviews with Beth Cameron and Jacob Jordan, NTI, July 2018. Also see Piers Millet and Andrew Synder-Beattie, "Existential Risk and Cost-Effective Biosecurity," *Health Security,* 15 no. 4, (2017): https://www.liebertpub.com/doi/10.1089/hs.2017.0028.

[146] National Academies of Sciences, Engineering, and Medicine, "If Misused, Synthetic Biology Could Expand the Possibility of Creating New Weapons; DOD Should Continue to Monitor Advances in the Field, New Report Says," June 19, 2018, http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=24890. This piece was cited in Cussins Newman, "Toward AI Security," 19. Also see Eleonore Pauwels, "The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI," United Nations University, May 2, 2019, https://cpr.unu.edu/the-new-geopolitics-of-converging-risks-the-un-and-prevention-in-the-era-of-ai.html.

[147] According to an article in *Clinical Microbiology and Infection*, the murder of Hungarian dissident Georgi Markov in London in 1978 with a ricin pellet that was injected into the victim with an umbrella "could be considered an act of biocrime." See Hugo Jan Jansen et al., "Biological Warfare, Terrorism and

Biocrime," *Clinical Microbiology and Infection,* 20 no. 6, (June 2014): 488–496, https://reader.elsevier.com/reader/sd/pii/S1198743X14641732?token=AFE37540897C1FA821BF43B528E3FE75A1DCEB1FDE9FE237962B44A475988F1FC8433AA1E092F2437BD416B51AC884A9.

148 V. Barras and G. Greub, "History of Biological Warfare and Bioterrorism," *Clinical Microbiology and Infection,* 20 no. 6, (June 2014), 497–502, https://www.sciencedirect.com/science/article/pii/S1198743X14641744.

149 Federal Bureau of Investigation, "Amerithrax or Anthrax Investigation," https://www.fbi.gov/history/famous-cases/amerithrax-or-anthrax-investigation.

150 Interviews with Beth Cameron and Jacob Jordan, NTI, July 2018.

151 Gryphon Scientific, "Risk and Benefit Analysis for Gain of Function Research: Final Report," 2016, 177–179, http://gryphonsci.wpengine.com/wp-content/uploads/2018/12/Risk-and-Benefit-Analysis-of-Gain-of-Function-Research-Final-Report-1.pdf.

152 Author interview with Richard Lennane, Geneva Disarmament Platform, January 2018.

153 The request for the opinion was made in a letter from European Commissioner for Research, Innovation and Science Carlos Moedas in July 2018. See Carlos Moedas, "Untitled Letter," European Commission, July 10, 2018, https://ec.europa.eu/info/sites/info/files/research_and_innovation/ege/letter_chair_of_the_ege_group.pdf .

154 World Economic Forum, "How Biotechnology is Evolving in the Fourth Industrial Revolution," May 2018, https://www.weforum.org/agenda/2018/05/biotechnology-evolve-fourth-industrial-revolution/; and World Economic Forum "Global Future Council on Biotechnology," https://www.weforum.org/communities/the-future-of-biotechnology.

155 "China, Unhampered by Rules, Races Ahead in Gene-Editing Trials," *Wall Street Journal*, January 21, 2018, https://www.wsj.com/articles/china-unhampered-by-rules-races-ahead-in-gene-editing-trials-1516562360.

156 See World Health Organization Advisory Committee on Human Genome Editing, "Global Health Ethics: Human Genome Editing," December 14, 2018, https://www.who.int/ethics/topics/human-genome-editing/en/.

157 Ibid.

158 Author interviews with Beth Cameron and Jacob Jordan, NTI, May 2018.

159 Bill Gates, "Gene Editing for Good: How CRISPR Could Transform Global Development," *Foreign Affairs*, May/June 2018, https://www.foreignaffairs.com/articles/2018-04-10/gene-editing-good.

160 Author interview with Beth Cameron, NTI, May 2018.

161 Ibid.

162 Benjamin Bahney and Joshua Pearl, "Why Creating a Space Force Changes Nothing: Space Has Been Militarised From the Start," *Foreign Affairs*, March 26, 2019, https://www.foreignaffairs.com/articles/space/2019-03-26/why-creating-space-force-changes-nothing; and Camino Kavanagh, "Information Technology and the State: The Long View," PhD Thesis, King's College London Department of War Studies, unpublished, 2016.

163 OECD, "The Space Economy at a Glance," 2014, 3, https://www.oecd.org/sti/futures/space-economy-at-a-glance-2014-highlights.pdf.

164 Ibid.

165 Michael Sheetz, "The Space Industry Will Be Worth Nearly $3 Trillion in 30 Years, Bank of America Predicts," CNBC, October 31 2017, https://www.cnbc.com/2017/10/31/the-space-industry-will-be-worth-nearly-3-trillion-in-30-years-bank-of-america-predicts.html.

166 Victoria Samson, "U.S. Assessments and Evolving Perceptions of Space Threats and Capabilities," Secure World Foundation, December 12, 2018, https://swfound.org/media/206305/us-assessments-and-evolving-perceptions-of-space-threats-and-capabilities.pdf.

[167] Scott Welles and William Nichols, "Resilient Position, Timing and Navigation (PNT) Requires New Thinking About Systems Navigation," *Defense One*, 2017, https://www.defenseone.com/media/resilient_positioning_navigation_and_timing_thought_piece_presented_by_booz_allen.pdf.

[168] Bahney and Pearl, "Why Creating a Space Force Changes Nothing: Space Has Been Militarised From the Start."

[169] Daniel Porras, "Towards ASAT Test Guidelines," UNIDIR, 2018, 2, http://www.unidir.org/files/publications/pdfs/-en-703.pdf.

[170] Brian Weeden, "2007 Chinese Anti-Satellite Test Fact Sheet," Secure World Foundation, updated November 23, 2010, https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf.

[171] Amitabh Sinha, "India's ASAT Test Created Debris, Raised Risk for International Space Station: NASA," *Indian Express*, April 3, 2019, https://indianexpress.com/article/india/nasa-says-400-pieces-of-debris-in-orbit-indias-asat-test-increased-risk-to-iss-by-44-5653898/.

[172] For instance, the *Atlantic* describes how, in 2015, a barely noticeable error disrupted "GPS-dependent timing equipment around the world for around 12 hours." Although there were redundancies built into the systems, in different parts of the United States and Canada "police, fire, and EMS radio equipment stopped functioning." In several locations, BBC digital radio could not be accessed. Moreover, the article reports that the glitch was also detected in electrical power grids. Dan Glass, "What Happens If GPS Fails," *Atlantic,* June 13, 2016, https://www.theatlantic.com/technology/archive/2016/06/what-happens-if-gps-fails/486824/.

[173] UN Office for Outer Space Affairs, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies," December 19, 1966, http://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf.

[174] Ibid.

[175] See the UN Office of Disarmament Affairs (UNODA) and the UN Conference on Disarmament's documents related to the Proposed Prevention of an Arms Race in Space (PAROS).
UNODA and the UN Conference on Disarmament, "CD Documents Related to Prevention of an Arms Race in Outer Space, October 12, 2017, https://www.unog.ch/80256EE600585943/(httpPages)/D4C4FE00A7302FB2C12575E4002DED85?OpenDocument; and UNODA, "Group of Governmental Exerts on Further Effective Measures for the Prevention of an Arms Race in Outer Space," https://www.un.org/disarmament/topics/outerspace/paros-gge/.

[176] Federation of American Scientists, "Prevention of an Arms Race in Outer Space: General Provisions," 2013, https://fas.org/programs/ssp/nukes/ArmsControl_NEW/nonproliferation/NFZ/NP-NFZ-PAROS.html.

[177] UN Conference on Disarmament, "Note Verbale Dated 29 August 2016 From the Delegation of the United States of America Addressed to the Secretary-General of the Conference on Disarmament Transmitting the Submission of the United States to the Conference on Disarmament: "Implementing the Recommendations of the Report (A/68/189*) of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities to Enhance Stability in Outer Space," September 16, 2016, https://undocs.org/pdf?symbol=en/CD/2078.

[178] International Panel on Fissile Materials (IPFM), "Conference on Disarmament Fails to Re-establish Subsidiary Bodies," IPFM blog, March 14, 2019, http://fissilematerials.org/blog/2019/03/conference_on_disarmament.html.

[179] Brian Weeden and Victoria Samson (eds.), "Global Counterspace Capabilities: An Open Source Assessment," Secure World Foundation, April 2018, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

[180] See Article VI of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.

[181] In 2015, former president Barack Obama signed the Space Resource Exploration and Utilization Act, which is part of the Commercial Space Launch Competitiveness Act (H.R. 2262). See U.S. Congress, "U.S. Commercial Space Launch Competitiveness Act [H.R. 2262]," November 25, 2015, https://www.congress.gov/bill/114th-congress/house-bill/2262.

[182] University of Leiden, "The Hague International Space Resources Governance Working Group," https://www.universiteitleiden.nl/en/law/institute-of-public-law/institute-for-air-space-law/the-hague-space-resources-governance-working-group.

[183] United Nations, "Further Practical Measures for the Prevention of an Arms Race in Outer Space," UN Document A/RES/72/250, January 12, 2018, https://undocs.org/en/A/RES/72/250.

[184] United Nations, "Report by the Chair of the Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space," January 31 2019, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/oral-report-chair-gge-paros-2019-01-31.pdf. The report was prepared by the chair in accordance with paragraph 5 of Resolution A/RES/72/250, which requested the chair to "organize a two-day open-ended intersessional informal consultative meeting, in 2019, so that all Member States can engage in interactive discussions and share their views on the basis of a report on the work of the Group to be provided by the Chair in his own capacity." Also see United Nations, "Further Practical Measures for the Prevention of an Arms Race in Outer Space," UN Document A/RES/72/250, January 12, 2018, https://undocs.org/A/RES/72/250.

[185] Porras, "Towards ASAT Test Guidelines."

[186] Ibid.

[187] UN Office of Disarmament Affairs, *Securing Our Common Future: An Agenda for Disarmament*; United Nations, "UN Secretary-General's Strategy on New Technologies," September 2018, https://www.un.org/en/newtechnologies/; and United Nations, "Secretary-General Launches High-Level Panel on Digital Cooperation," July 12, 2018, https://www.un.org/en/digital-cooperation-panel/. Please also see the panel's final report: United Nations, "The Age of Digital Interdependence," June 2019, https://www.un.org/en/pdfs/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ENG.pdf.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org