ICM
INDEPENDENT
COMMISSION ON
MULTILATERALISM

POLICY PAPER
MAY 2017

The Impact of New Technologies on Peace, Security, and Development

INDEPENDENT COMMISSION
ON MULTILATERALISM

ABOUT THE INDEPENDENT COMMISSION ON MULTILATERALISM

The Independent Commission on Multilateralism (ICM) is a project of the International Peace Institute (IPI). It asks: How can the UN-based multilateral system be made more "fit for purpose"?

In answering that question, the ICM has analyzed fifteen topics. These include armed conflict, humanitarian engagements, sustainable development, and global public health, among others (see complete list in Annex 2). The goal of the ICM is to make specific recommendations on how the UN and its member states can improve responses to current challenges and opportunities.

The ICM undertook simultaneous tracks of research and consultation for each issue area on its agenda. The Commission initially launched in New York in September 2014, followed by subsequent launches in Vienna, Geneva, and Ottawa. In February 2015, the ICM briefed delegates from the five UN Regional Groups in New York. The Commission also convened meetings with Ambassadorial and Ministerial Boards in New York, Vienna, and Geneva. Global outreach included briefings to officials in Addis Ababa, Berlin, Brasilia, Copenhagen, New Delhi, London, Madrid, Montevideo, and Rome. Civil society and private sector outreach and engagement also constituted an important component of the ICM's consultative process, including a briefing specifically for civil society in June 2015.

The research process began with a short "issue paper" highlighting core debates and questions on each of the fifteen topics. Each issue paper was discussed at a retreat bringing together thirty to thirty-five member state representatives, UN officials, experts, academics, and representatives from civil society and the private sector. Based on the inputs gathered at the retreats, each issue paper was then revised and expanded into a "discussion paper." Each of these was uploaded to the ICM website for comment and feedback, revised accordingly, and presented at a public consultation. The public consultations were webcast live on the ICM's website to allow a broader audience to take part in the discussions.

This paper is one of the fifteen final "policy papers" that emerged from this consultative process. A complete list of events taking place as part of consultations on this specific issue area and of those involved is included in Annex 1. The recommendations from all the policy papers are summarized in the ICM's September 2016 report *Pulling Together: The Multilateral System and Its Future*.

Contents

Executive Summary

A new wave of technology is driving rapid global change. This technological change has created new opportunities for multilateral cooperation, but the UN has at times struggled to keep up with the pace of change. This struggle results in part because private sector and civil society actors are often in the lead when it comes to technological innovation. Another challenge is that new technologies present not only opportunities but also new threats to humans and their freedoms. To effectively keep up and adapt, the UN must determine where it can play a useful role and where existing mechanisms and other actors are better placed.

New technologies present opportunities for multilateral cooperation across a wide range of areas. The potential of new technologies to support sustainable development is widely recognized, and this is the area where the UN has come the farthest in integrating them into its discussions and work. The ten-year review of the World Summit on the Information Society (WSIS+10) drew a strong link between new technologies and sustainable development, including in the 2030 Agenda. Though far from a panacea, these technologies also provide opportunities for preventing conflict and for responding to humanitarian needs. The UN recognized the potential for new technologies to enhance peace operations in the 2015 reports of the Expert Panel on Technology and Innovation in UN Peacekeeping and the High-Level Independent Panel on Peace Operations. Technology can also transform the relationship between governments and their people, though not always for the better.

While new technologies offer wide-ranging opportunities to improve people's lives, they also present challenges, many of which require multilateral, multistakeholder solutions. One such challenge is the enduring "digital divide" both between and within countries, which has led to several multilateral mechanisms for transferring technology to the developing world. Internet governance also faces a challenge in its democratic deficit. While many believe multilateral actors should stay out of Internet governance, selective multilateralism in this area could help address this deficit, as long as what is already working well is preserved. In addition, cyber threats and new technologies such as armed drones require the multilateral system to develop new laws and norms and to adapt existing international human rights and humanitarian laws to meet these challenges.

Based on these opportunities, challenges, and existing multilateral responses, the paper provides a number of recommendations for the UN and member states:

1. **Identify a UN focal point on cyber issues:** The appointment of a clear UN focal point on cyber issues would consolidate the UN's currently disjointed approach and make it a more credible player on an issue that demands greater international engagement.

2. **Map UN venues dealing with new technologies:** Mapping the venues where new technologies are being used could identify good practices and needs, thereby helping streamline and consolidate efforts to more effectively use technology to achieve the UN's objectives.

3. **Ensure coherence among new mechanisms:** New technology transfer mechanisms need to be connected to one another to accelerate progress toward achieving the 2030 Agenda and the Paris Agreement without duplicating efforts and competing for resources.

4. **Create a "cyber and innovation compact" with the private sector and civil society:** Inputs and expertise from these actors should be accorded far greater pride of place across the multilateral system.

5. **Recognize cyberspace as a global public good:** This could be done through a General Assembly resolution declaring that cyberspace should be used for “peaceful purposes” in the interests of humanity.

6. **Establish a UN-guaranteed depository as a safe-keeper of big data:** Member states could mandate this body to help collect, structure, and store data, especially from regions where the infrastructure is not safe or sufficient.

7. **Consolidate and build analytical capacity:** The UN could help provide greater analytical and statistical capacity when member states lack it.

8. **Support and integrate confidence-building measures:** The UN Secretariat and member states should develop a strategic approach to implement these measures at the regional and subregional levels to ensure the security and sustainability of cyberspace.

Introduction[1]

A new wave of technology is driving rapid global change. This is the latest of several "waves" of technological change that have taken place throughout modern history, driven by inventions ranging from steam power to electricity to the automobile. The current technological wave is remarkable for its speed and its level of impact on economic development and social transformation.[2] Sometimes called the "fourth technological revolution," it "is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres."[3]

This technological change has created new opportunities for multilateral cooperation. The need for a multilateral response to technological change is nothing new; it was recognized as early as 1865 with the creation of the International Telegraph Union (ITU, renamed the International Telecommunication Union in 1934), the oldest existing international organization. Since then, the UN has been seeking not only to find its role in addressing new technologies but also to integrate these technologies into its other areas of work—from sustainable development to humanitarian engagement to peacebuilding and conflict resolution.

Nonetheless, the UN and other multilateral institutions have struggled to keep up with the pace of technological change. This struggle results in part because private sector and civil society actors are often in the lead when it comes to technological innovation. International governance of the Internet, for example, has largely taken place outside of multilateral and state institutions—and many argue it should stay that way. Another challenge is that new technologies not only present opportunities for increasing the greater good but also can pose a threat to humans and their freedoms. In adapting to new technologies and addressing these threats, the UN must determine where it can play a useful role and where existing mechanisms and other actors are better placed.

Based on extensive consultations with representatives of states, various UN entities, and civil society, as well as subject-matter experts, this paper explores the impact of new technologies on peace, security, and development and identifies areas where the multilateral system could play a positive role. It does not aim to give a comprehensive overview of the landscape of new technologies; it aims to analyze opportunities these technologies present across a number of areas and how the multilateral system anchored in the UN is addressing them. The paper also explores how the multilateral system is addressing several crosscutting challenges posed by new technologies. Finally, it offers the multilateral system concrete recommendations on how to benefit from new technologies and develop frameworks and norms to govern and regulate their use.

[1] The ICM is grateful to Anja Kovacs for her expert contributions to this paper.

[2] Jeffrey D. Sachs, *The Age of Sustainable Development* (New York: Columbia University Press, 2015), p. 82.

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

Harnessing the Potential of New Technologies

Multilateral cooperation on information and communications technologies (ICTs) dates back to the creation of the ITU in 1865. Since then, and particularly with the advent of the Internet and mobile phones, opportunities for ICTs to support sustainable development, prevent conflict, improve humanitarian action, and transform state-society relations have greatly expanded. These new technologies have also led to an exponential increase in the amount of data being produced, which can be used to measure the impact and improve the effectiveness of work in a range of spheres. UN peace operations in particular can benefit from new technologies, from unmanned aerial vehicles to global positioning system (GPS) tracking devices.

Supporting Sustainable Development

The potential of ICTs to support economic development is widely recognized. For example, there is an estimated 1.38 percent increase in gross domestic product (GDP) for every 10 percent increase in broadband penetration in low- and middle-income countries.[4] As such, economic development is the area where the UN has come the farthest in integrating new technologies into its discussions and work. The 2000 UN Millennium Declaration, which laid out goals for a more peaceful, prosperous, and just world, contained a commitment to "ensure that the benefits of new technologies, especially information and communication technologies,... are available to all."[5] The following year, when the UN General Assembly endorsed holding the World Summit on the Information Society (WSIS), it put this process explicitly in the service of reaching the Millennium Development Goals (MDGs).[6]

The link between new technologies and sustainable development was again highlighted in the outcomes of several major UN conferences in 2015: the Sendai Framework for Disaster Risk Reduction, the Addis Ababa Action Agenda on financing for development, the 2030 Agenda for Sustainable Development, the Paris Agreement on climate change, and the World Summit on the Information Society +10 (WSIS+10) outcome document.

The WSIS+10 reviewed the previous ten years of implementation of the WSIS, including its commitment to sustainable development. Its outcome document, which the General Assembly adopted in December 2015, committed member states to build a "people-centric, inclusive, open and development-oriented information society where everyone can create, access, utilize and share information and knowledge."[7]

The outcome document called for close alignment between the follow-up of the WSIS+10 and the 2030 Agenda, which was adopted just three months before. Due to the cross-cutting nature of ICTs, they contribute to all seventeen of the Sustainable Development Goals (SDGs) laid out in the 2030 Agenda. Target 9.c specifically calls on member states to "significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least-developed countries by 2020." The

[4] International Telecommunication Union, "Impact of Broadband on the Economy," April 2012, p. 4.

[5] United Nations, *Millennium Declaration*, UN Doc. A/RES/55/2, September 8, 2000, para. 20.

[6] UN General Assembly Resolution 56/183 (January 31, 2001), UN Doc. A/RES/56/183.

[7] UN General Assembly Resolution 70/L.22 (December 13, 2015), UN Doc. A/70/L.33, para. 5.

2030 Agenda also contains a commitment to "fully operationalize the technology bank and science, technology and innovation capacity-building mechanism for least-developed countries."[8] These targets have the potential to accelerate progress in the countries that need it most. Nonetheless, it has been argued that ICTs should feature more prominently in the 2030 Agenda.[9]

The WSIS+10 outcome document also officially endorses another global plan linking ICTs and sustainable development, which the ITU adopted in 2014: the Connect 2020 Agenda for Global Telecommunication/ICT Development.[10] The 2020 Agenda commits member states to "an information society… where telecommunication/ICT enables and accelerates socially, economically and environmentally sustainable growth and development for everyone." Its four goals and seventeen targets include increasing global access to ICTs, bridging the digital divide between developed and developing countries, and reducing waste and emissions resulting from ICTs.[11] Implementation of the 2020 Agenda will complement and reinforce the SDGs.

While new technologies have driven economic growth, they have also contributed to environmental pollution. Storing data in the "cloud" requires massive digital warehouses that use enormous amounts of energy—roughly equivalent to the output of thirty nuclear plants worldwide.[12] The metals needed to build the components of ICT devices are often extracted in developing countries using environmentally destructive methods. Moreover, the amount of electronic waste (or e-waste) is rapidly increasing; it exceeded 40 million tons in 2014 and is growing by 4 to 5 percent per year.[13] Much of this waste is toxic and is illegally dumped in developing countries.[14]

Multilateral action on e-waste has taken place through the Global Partnership on Waste Management, whose work on e-waste management is led by the ITU. The work plan developed under this partnership aims "to mainstream and disseminate environmentally sound management of e-waste in developing countries" through development of sustainable business plans.[15]

Like ICT, data, both "big" and "small," can play a crucial role in efforts to promote sustainable development, particularly in measuring progress toward the SDGs. Data provides benchmarks to assess and enhance the effectiveness of development efforts. According to the Independent Expert Advisory Group on a Data Revolution for Sustainable Development, "Without high-quality data providing the right information on the right things at the right time, designing, monitoring and evaluating effective policies becomes almost impossible."[16] While the lack of high-quality data hurts developing countries most, challenges in data collection, standardization, disaggregation, and timeliness compromise sustainable development in all countries.

"Big data" presents a largely untapped opportunity

[8] UN General Assembly Resolution 70/1 (September 25, 2015), UN Doc. A/RES/70/1, paras. 9.b, 17.8.

[9] David Kirkpatrick, "The Impact of New Technologies on Peace, Security, and Development," keynote address to the Independent Commission on Multilateralism, October 23, 2015, available at www.icm2016.org/IMG/pdf/kirkpatrick_-_icm_keynote.pdf .

[10] UN General Assembly Resolution 70/L.22, para. 25.

[11] International Telecommunication Union Resolution 200, *Connect 2020 Agenda for Global Telecommunication/Information and Communication Technology Development*, 2014.

[12] James Glanz, "Power, Pollution and the Internet," *New York Times*, September 22, 2012, available at www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html .

[13] C. P. Baldé, F. Wang, R. Kuehr, and J. Huisman, "The Global E-Waste Monitor 2014," United Nations University Institute for the Advanced Study of Sustainability, 2014, available at https://i.unu.edu/media/unu.edu/news/52624/UNU-1stGlobal-E-Waste-Monitor-2014-small.pdf .

[14] John Vidal, "Toxic 'E-Waste' Dumped in Poor Nations, Says United Nations," *The Guardian*, December 14, 2013, available at www.theguardian.com/global-development/2013/dec/14/toxic-ewaste-illegal-dumping-developing-countries .

[15] See http://web.unep.org/ietc/what-we-do/global-partnership-waste-management-gpwm .

[16] Independent Expert Advisory Group on a Data Revolution for Sustainable Development, *A World that Counts: Mobilising the Data Revolution for Sustainable Development*, United Nations, November 2014, p. 2, available at www.undatarevolution.org/wp-content/uploads/2014/11/A-World-That-Counts.pdf .

for sustainable development. "Big data for development" involves "turning imperfect, complex, often unstructured data into actionable information."[17] While big data is not a panacea, according to a report by UN Global Pulse it could "allow decision makers to track development progress, improve social protection, and understand where existing policies and programmes require adjustment."[18] The success of big data in supporting development depends on support from governments and collaboration among governments, the private sector, and academics. It also depends on the development and implementation of new norms and institutional frameworks for responsibly using and sharing big data.[19]

In terms of "small data," collection of statistics at the national, district, and municipal levels requires more investment in data-literacy training, as well as development and increased availability of software. Basic spreadsheet programs, such as Excel or Google Sheets, can cost little or nothing, and professional-grade statistical packages, such as R and Python's Pandas library, are open-source. Commitment to the principles of open data, open standards, open source, and open innovation could broaden the community of analysts and policymakers integrating and scaling out solutions toward the delivery of the SDGs. A number of UN agencies, including the UN Children's Fund (UNICEF), UN Development Programme (UNDP), and UN Office for the Coordination of Humanitarian Affairs (OCHA), have joined dozens of other development actors in endorsing these and other "Principles for Digital Development."[20]

A number of UN initiatives have begun recognizing the potential of data for development. The UN Global Pulse initiative was created in 2009 "to accelerate discovery, development and scaled adoption of big data innovation for sustainable development and humanitarian action."[21] In 2013 the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda called for a "data revolution for sustainable development, with a new international initiative to improve the quality of statistics and information available to people and governments."[22] The following year, the Independent Expert Advisory Group on a Data Revolution for Sustainable Development published a report calling for a UN-led effort to foster and promote innovation to fill data gaps, mobilize resources to overcome inequalities in data access, and improve leadership and coordination.[23]

Following the adoption of the 2030 Agenda for Sustainable Development in 2015, the Global Partnership for Sustainable Development Data, a global network of governments, NGOs, and businesses, was created to ensure governments have the data tools they need to meet the SDGs. The Digital Impact Alliance, housed in the United Nations Foundation, was also launched in 2015 to bring together the public and private sectors in using data to help the most vulnerable people.[24]

Preventing and Responding to Violence and Conflict

New technologies can also help bolster conflict prevention, which is at the very foundation of the UN Charter but continues to suffer from a lack of political and financial investment. ICTs provide opportunities to collect data about crime and conflict and reduce the gap between warning and response. For example, crisis mapping, social media mapping, and crowdsourcing tools can help

[17] Emmanuel Letouzé, "Big Data for Development: Challenges and Opportunities," UN Global Pulse, May 2012, p. 6, available at www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf .

[18] Ibid., p. 4.

[19] Ibid, p. 42.

[20] See http://digitalprinciples.org/ .

[21] See www.unglobalpulse.org/about-new .

[22] High-Level Panel of Eminent Persons on the Post-2015 Development Agenda, *A New Global Partnership: Eradicate Poverty and Transform Economies through Sustainable Development*, United Nations, 2013, available at www.post2015hlp.org/wp-content/uploads/2013/05/UN-Report.pdf .

[23] Independent Expert Advisory Group on a Data Revolution for Sustainable Development, *A World That Counts*.

[24] See http://digitalimpactalliance.org/what-we-do/ .

generate data on conflict indicators. The data generated from these tools can help identify patterns associated with conflict and peace in order to better inform efforts to prevent conflict or to monitor violations of cease-fires or human rights.[25] It is dangerous, however, to assume that technologies provide an easy solution to preventing conflicts. They represent just one conflict prevention tool among many, need to be adapted to specific contexts, and should reflect local input.[26]

It is also important to consider the potential negative impact of ICTs. The same technologies that can be used to spread messages of peace can also be used to propagate radical ideologies, as demonstrated by the Islamic State's use of social media to promote violent extremism. UN Secretary-General Ban Ki-moon acknowledged this risk in his 2015 Plan of Action to Prevent Violent Extremism, which notes that "the rapid expansion of violent extremist ideologies…is being facilitated by the technological revolution." Among other things, this plan of action recommends that UN member states work with social media companies and the private sector to develop national communications strategies, research the relationship between social media and violent extremism, and provide online forums for victims to tell their stories.[27]

The multilateral system has increasingly recognized the potential of ICTs to prevent violence and conflict. The 2005 Tunis Commitment, a consensus statement of the WSIS, recognized the important role ICTs can play in preventing and resolving conflict, supporting humanitarian action, facilitating peacekeeping, and assisting post-conflict peacebuilding and reconstruction.[28] The UN Development Programme (UNDP) has implemented programs using new technologies to prevent conflict and is further exploring ways in which ICTs can contribute to peace, security, and sustainable development.[29] At the regional level, the Intergovernmental Authority on Development (IGAD), which includes eight countries in East Africa, launched an ICT4Peace project as part of its Conflict Early Warning and Response Mechanism (CEWARN). However, such mechanisms have not always used the data they retrieve to take meaningful early action.[30]

Bolstering Humanitarian Responses

There have been increasing multilateral efforts to use ICTs and data to bolster humanitarian responses, both in situations of violent conflict and in the wake of natural disasters. OCHA led development of guidelines for incorporating big data into humanitarian operations in 2015.[31] OCHA has also spearheaded efforts to increase sharing of and access to humanitarian data, including through a Centre for Humanitarian Data it established in 2017.[32]

Other technologies, such as unarmed unmanned aerial vehicles (UAVs), or drones, can facilitate data collection for humanitarian responses. UAVs are increasingly part of the immediate response to large-scale natural disasters, as demonstrated by the 2015 earthquake in Nepal. Beyond disaster response, UAVs have been used to conduct mapping exercises to reduce the risk of disasters. UAVs are also contributing to search-and-rescue operations in the Mediterranean by helping to identify boats of migrants and refugees in need of assistance. Though not yet broadly practical, in the future UAVs could

[25] International Federation of the Red Cross and Red Crescent Societies, *The Red Cross and Red Crescent's Principled Approach to Innovation*, June 2015, available at http://blogs.icrc.org/gphi2/2015/07/08/1173/ .

[26] Francesco Mancini, ed., "New Technology and the Prevention of Violence and Conflict," International Peace Institute, April 2013, available at www.ipinst.org/2013/04/new-technology-and-the-prevention-of-violence-and-conflict .

[27] UN Secretary-General, *Plan of Action to Prevent Violent Extremism*, UN Doc. A/70/674, December 24, 2015.

[28] World Summit on the Information Society, *Tunis Commitment*, UN Doc. WSIS-05/TUNIS/DOC/7-E, November 18, 2005, para. 36.

[29] UN Development Programme, "Issue Brief: Using Technologies for Conflict Prevention," March 2012.

[30] Sheldon Himelfarb, "Can Big Data Stop Wars before They Happen?" *Foreign Policy*, April 25, 2014, available at http://foreignpolicy.com/2014/04/25/can-big-data-stop-wars-before-they-happen/ .

[31] Katie Whipkey and Andrej Verity, *Guidance for Incorporating Big Data into Humanitarian Operations*, UN OCHA, September 2015, available at http://digitalhumanitarians.com/sites/default/files/resource-field_media/IncorporatingBigDataintoHumanitarianOps-2015.pdf .

[32] See www.agendaforhumanity.org/initiatives/3848 .

help deliver humanitarian relief to hard-to-reach areas.[33]

Two other initiatives addressing the role ICTs can play in improving humanitarian action were launched at the 2016 World Humanitarian Summit. The Global Humanitarian Lab aims to serve as a partnership between humanitarian organizations, the private sector, governments, and affected populations to facilitate bottom-up innovation, including in learning and digital fabrication technologies.[34] The Global Alliance for Humanitarian Innovation focuses on developing consistent and more effective policies and standards for enhancing humanitarian action, including by systematically innovating humanitarian technologies.[35] The hope is that these two initiatives will be mutually reinforcing.

Moving toward Tech-Enabled Peace Operations

UN peace operations can benefit immensely from integrating new technologies into their work. Particularly useful for peace operations are technologies that facilitate monitoring and observation, including unmanned aerial vehicles (UAVs), video monitoring systems, motion detectors, and satellite imagery.[36] These technologies can particularly help peace operations in the asymmetric threat environments in which they increasingly operate.

As the use of new technologies in peace operations expands, their benefits and drawbacks have attracted increasing attention from researchers and policymakers. For example, while UAVs can improve data collection, transportation, and communication in peace operations, they also become part of the conflict dynamic, with all the attendant risks.[37] The ways these new technologies are used can also be controversial. In particular, intelligence gathering remains a sensitive subject for the UN and its membership, even if it has lost some of its negative connotations.[38] Nonetheless, new technologies can benefit peace operations in many less controversial areas of their mandates, including monitoring and protection of civilians. ICTs can also facilitate “participatory peacekeeping,” whereby peace operations give locals a place to send their observations, alerts, and insights, which can build confidence between peacekeepers and local populations.[39]

The UN is starting to make significant progress in incorporating new technologies into its peace operations. In 2014 the UN secretary-general mandated a panel of experts to look into the use of technology and innovation in UN peacekeeping. In its final report, the panel stated that “the availability and effective use of [modern] technology represents the essential foundation—the very least that is required today—to help peacekeeping missions deploy to and manage complex crises that pose a threat to international peace and security.” The report recommends integrating new technologies into many aspects of peacekeeping operations, including to sustain the basic needs underpinning the ability of missions to function, help missions execute their mandates more effectively, and streamline mission support operations. It also recommends institutionalizing innovation and continuous technological adaptation.[40]

The UN secretary-general’s High-Level Independent Panel on Peace Operations (HIPPO) endorsed these

[33] Faine Greenwood, “Above and Beyond: Humanitarian Uses of Drones,” *World Politics Review*, September 22, 2015.

[34] See www.globalhumanitarianlab.org/ .

[35] See www.thegahi.org/ .

[36] A. Walter Dorn, *Keeping Watch: Monitoring Technology and Innovation in UN Peace Operations* (Tokyo: United Nations University Press, 2011).

[37] Helena Puig Larrauri and Patrick Meier, “Peacekeepers in the Sky: The Use of Unmanned Unarmed Aerial Vehicles for Peacekeeping,” ICT4Peace Foundation, September 2015, available at https://ict4peace.wordpress.com/2015/09/01/peacekeepers-in-the-sky-the-use-of-unmanned-unarmed-aerial-vehicles-for-peacekeeping/ .

[38] See Olga Abilova and Alexandra Novosseloff, “Demystifying Intelligence in UN Peace Operations: Toward an Organizational Doctrine,” International Peace Institute, July 2016, available at www.ipinst.org/2016/07/demystifying-intelligence-in-un-peace-ops .

[39] A. Walter Dorn, “Smart Peacekeeping: Toward Tech-Enabled UN Operations,” International Peace Institute, July 2016, available at www.ipinst.org/2016/07/smart-peacekeeping-tech-enabled .

[40] Expert Panel on Technology and Innovation in UN Peacekeeping, *Performance Peacekeeping*, December 22, 2014, available at www.performancepeacekeeping.org/offline/download.pdf .

recommendations, suggesting that priority be placed on "enabling" technologies to improve safety and security, capacity for early warning and civilian protection, health and well-being, and shelter and camp management.[41] The extent to which these recommendations are implemented remains to be seen.

Transforming State-Society Relations

ICTs also present opportunities to empower citizens and transform their relationship with the state. Social media and mobile phones have revolutionized people's ability to organize and coordinate protest movements, from the Arab uprisings to protests in Ukraine to the Occupy Movement. Real-time photos and videos uploaded to social media can also expose government corruption or abuse and increase government responsiveness to citizen concerns.

Crowdsourcing, in particular, presents an opportunity to empower citizens and transform their relationship with the state.[42] Crowdsourcing can augment more traditional routes for participation, such as elections and referenda. It can make government decision-making processes more inclusive and transparent and allow citizens to better assess their outcomes, indirectly increasing their legitimacy.[43] One recent example is Iceland's attempt to crowdsource a new constitution, which included extensive use of social media to gather feedback.[44] Many countries have experimented with online participatory governance, from websites where citizens can provide the government feedback to virtual "town hall" meetings. These participatory and deliberative approaches can promote a move from vertical toward horizontal power structures.

The UN incorporated elements of crowdsourcing to increase the transparency and participatory nature of the process for selecting the secretary-general in 2016. This process included the use of social media and an online platform for people to ask questions to secretary-general candidates.[45] The secretary-general's envoy on youth also launched a crowdsourcing initiative as part of the Global Partnership for Youth in the Post-2015 Development Agenda.[46] These and other such processes provide opportunities for multilateral institutions to engage and partner with civil society.

However, ICTs do not always transform state-society relations for the better. Access to new technologies is often uneven and can be manipulated by governments. Users face privacy and security risks, particularly as some governments crack down on social media users or use new technologies in ways that break down citizen trust, such as by conducting mass surveillance.[47] Moreover, the easy manipulation of information and sources and the risk of viral dissemination without verification can propagate misinformation and fake news. Social media users also risk finding themselves in "information cocoons" where they are not exposed to differing opinions, potentially increasing political polarization.

[41] United Nations, *Uniting Our Strengths for Peace—Politics, Partnership and People: Report of the High-Level Independent Panel on Peace Operations*, UN Doc. A/70/95-S/2015/446, June 17, 2015, para. 313.

[42] The term "crowdsourcing" was originally defined as the use of new technologies and social media to solicit contributions or share real-time information, generally in a business context. It has since come to be applied to a wide variety of situations where ideas, opinions, labor, or something else is "sourced" from a potentially large group of people. It has also increasingly been applied in government and policy contexts; as one commentator put it, "If elections were invented today, they would probably be referred to as 'crowdsourcing the government.'" Jeff Howe, "The Rise of Crowdsourcing," *Wired*, June 1, 2006; Daren C. Brabham, *Crowdsourcing* (Cambridge, MA: MIT Press, 2013); Vili Lehdonvirta and Jonathan Bright, "Crowdsourcing for Public Policy and Government," Policy and Internet Blog, University of Oxford, August 27, 2015, available at http://blogs.oii.ox.ac.uk/policy/crowdsourcing-for-public-policy-and-government/ .

[43] Lehdonvirta and Bright, "Crowdsourcing for Public Policy and Government."

[44] Hélène Landemore, "We, All of the People: Five Lessons from Iceland's Failed Experiment in Creating a Crowdsourced Constitution," *Slate*, July 31, 2014, available at www.slate.com/articles/technology/future_tense/2014/07/five_lessons_from_iceland_s_failed_crowdsourced_constitution_experiment.html .

[45] See www.un.org/apps/news/story.asp?NewsID=53641#.WNQYWGe1uUk .

[46] See www.un.org/youthenvoy/2014/02/crowdsourcing-initiative-on-youth-in-the-post-2015-development-agenda-launched-today/ .

[47] Helena Puig Larrauri and Anne Kahl, "Technology for Peacebuilding," *Stability: International Journal of Security & Development* 2, no. 3 (2013).

Compared to its work in other areas, the multilateral system has been slow to recognize the potential for new technologies to improve—or worsen—state-society relations. But in 2011 eight governments and nine civil society organizations launched the Open Government Partnership, which has expanded to seventy-five countries. In endorsing the Open Government Declaration, countries have pledged to "increase access to new technologies for openness and accountability," including making more information public and creating secure online spaces for public engagement.[48] While still in its early stages, this partnership demonstrates the possibility of increased multilateral engagement on governance and technology.[49]

[48] Open Government Partnership, "Open Government Declaration," available at www.opengovpartnership.org/about/open-government-declaration.

[49] Jeremy M. Weinstein, "Transforming Multilateralism: Innovation on a Global Stage," *Stanford Social Innovation Review* (Spring 2013).

Multilateral Approaches to Cross-Cutting Challenges

While new technologies offer wide-ranging opportunities to improve people's lives, they also can exacerbate inequality between and within countries or open dangerous new frontiers for conflict. Many of the challenges presented by new technologies will require multilateral, multi-stakeholder solutions.

Overcoming the Digital Divide

Access to ICTs remains highly unequal between developed and developing countries, as well as between rich and poor and between men and women within countries. This is not new: landline phones and electricity have also not spread equally around the world. Moreover, mobile phones may have helped developing countries leapfrog their communications infrastructure past landlines directly to cell towers.

Nonetheless, although there are 97 mobile-phone subscriptions per 100 people globally, residents of the least-developed countries still lag behind, particularly in rural areas that lack a mobile signal. The divide is even more striking in terms of access to the Internet; while 82 percent of people in developed countries use the Internet, the proportion is just 35 percent in developing countries, 21 percent in Africa, and 9 percent in the least-developed countries.[50] According to the MDGs Gap Task Force, "As long as more people are offline than online, it is not possible to talk about a global information society."[51] While some of this divide is due to lack of mobile broadband infrastructure (particularly in Africa), other barriers include unaffordability of mobile services, citizens' lack of digital awareness and skills, and unavailability of locally relevant content.[52] In some areas, moreover, a striking gender gap in access to and use of ICTs has emerged.[53]

Bridging the digital divide requires increasing investment, transferring technology from the developed to the developing world, and building the capacity of developing countries to research and develop new technologies. But because these technologies are generally developed in the private sector rather than by member states, multilateral efforts in this area have been limited. Research and development of new technologies are driven more by the market than by lofty global goals, and multilateral negotiations to improve global access to technology are often difficult and slow.

Nonetheless, several new multilateral mechanisms aim to increase transfer of technology to developing countries. The Technology Facilitation Mechanism for sustainable development was launched at the UN Sustainable Development Summit in September 2015. This mechanism comprises: (1) a UN interagency task team on science, technology, and innovation for the SDGs; (2) an annual multi-stakeholder forum on science, technology, and innovation for the SDGs; (3) and an online platform

[50] International Telecommunications Union, "ICT Facts and Figures," 2015, available at www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf .

[51] MDG Gap Task Force, "Taking Stock of the Global Partnership for Development," United Nations, 2015, pp. 68–69, available at www.un.org/development/desa/dpad/document_gem/mdg-gap-task-force-report/ .

[52] GSMA, "Connected Society: Mobile Connectivity Index Launch Report," 2016, available at www.mobileconnectivityindex.com/widgets/connectivityIndex/pdf/ConnectivityIndex_V01.pdf .

[53] GSMA, "Bridging the Gender Gap: Mobile Access and Usage in Low- and Middle-Income Countries," 2015, available at www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/02/GSM0001_03232015_GSMAReport_NEWGRAYS-Web.pdf .

for information on existing initiatives, mechanisms, and programs.[54] This mechanism has the potential to facilitate access to technologies that will enhance the implementation of the 2030 Agenda in developing countries. As called for in SDG 17, the General Assembly also established a Technology Bank for Least Developed Countries in 2016, which aims to build national and regional technological capacities and facilitate the transfer of technologies to the least-developed countries.[55]

In addition, in 2010 the Conference of the Parties to the UN Framework Convention on Climate Change established a Technology Mechanism to facilitate development and transfer of technology to support action on mitigating and adapting to climate change. The Paris Agreement on climate change subsequently established a Technology Framework to accelerate the innovation of technologies to facilitate adaptation and mitigation and "provide overarching guidance to the work of the Technology Mechanism." When it comes to peace operations, the emergence of "technology-contributing countries" could help narrow the technological gap between developed and developing countries participating in peacekeeping.[56]

Governing the Internet

Another divide faces the Internet itself: while the Internet is regularly labeled a "global public good," there is growing recognition of the democratic deficit in Internet governance. Questions around governance of the Internet have been controversial, in part due to its multi-stakeholder nature. Public authorities have not played a major role in regulating the Internet, leaving it largely to private regulation by engineers and experts who have made major decisions through unstructured procedures.[57] Despite this lack of regulation, the existing system has been remarkably successful; any changes to governance of the Internet will need to preserve and extend what is working well and avoid unintended damage to stability, security, and accessibility.[58]

Ever since the WSIS process, a coalition of some states and a wide range of nongovernmental organizations has vocally opposed greater involvement by governments in governing the Internet, whether by individual states or multilateral organizations. Criticisms focus especially on the lack of required technical expertise among government officials, the slow pace of discussions at the UN, and the potential politicization of Internet governance.[59]

Nonetheless, a growing number of actors recognizes that, depending on the issue and the stage of discussions, there is space for multilateralism and involvement of more stakeholders in Internet governance. In addition, all stakeholder groups seem to be increasingly realizing and recognizing that voices from developing countries are underrepresented in global Internet governance forums.[60] As states increasingly assert their sovereignty over the Internet, it is important to disentangle what can be decided locally and what needs to be decided globally.

With the completion of the WSIS+10 in December 2015, questions regarding the role of the multilateral system in governing cyberspace have gained a particular salience. The WSIS+10 outcome document

[54] See https://sustainabledevelopment.un.org/TFM .5

[55] See http://unohrlls.org/custom-content/uploads/2016/12/FINAL-Press-Release-23-December-2016-Technology-Bank-for-Least-Developed-Countries-established-by-UN-General-Assembly.pdf .

[56] Dorn, "Smart Peacekeeping."

[57] Andrea Renda, "Cybersecurity and Internet Governance," Council on Foreign Relations, May 3, 2013, available at www.cfr.org/councilofcouncils/global_memos/p32414 .

[58] Mark Cooper, "Why Growing Up Is Hard to Do: Institutional Challenges for Internet Governance in the 'Quarter-Life Crisis' of the Digital Revolution," *Journal on Telecommunications and High Technology Law* 11, no. 1 (2013); Centre for International Governance Innovation, "Finding Common Ground: Challenges and Opportunities in Internet Governance and Internet-Related Policy," November 2014, available at www.cigionline.org/publications/finding-common-ground-challenges-and-opportunities-internet-governance-and-internet-0 .

[59] Cooper, "Why Growing Up Is Hard to Do."

[60] See, for example, many of the submissions made, across stakeholder groups, as inputs into the non-paper for the WSIS+10 review in July 2015. The 2030 Agenda for Sustainable Development recognizes that underrepresentation of the voices of developing countries affects a wide range of sectors.

reaffirmed the provisions of the WSIS agreed in Geneva and Tunis, including that governance of the Internet should be "multilateral, transparent and democratic" and should ensure "an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism."[61] The WSIS had also agreed that all stakeholders should be involved: states in assuming their "sovereign right" of policy authority; the private sector in developing the Internet; civil society, particularly at the community level; intergovernmental organizations in coordinating public policy issues; and international organizations in developing standards and relevant policies.[62] The WSIS+10 outcome document also reaffirmed that "the same rights that people have offline must also be protected online."[63]

Establishing Laws and Norms for Cyberspace

While the potential use of ICTs for development, governance, and peace has posed questions about how to govern the Internet, issues related to security—and to cybersecurity in particular—have made these questions more urgent.[64] As the barriers to entry in the cyber domain are low, cyberspace includes many and varied actors—from criminal hackers to terrorist networks to governments engaged in cyber espionage. Cybercrime and cyberattacks can undermine the safety of Internet users, disrupt economic and commercial activity, and threaten military effectiveness.[65] Moreover, more widely available technologies such as mobile phones and the Internet are increasingly used to support war efforts by facilitating communication, influencing public opinion, creating and teaching new warfare techniques, gathering intelligence, and engaging in cyberattacks.[66]

Though initiatives to create normative frameworks for cyberspace have broken important ground, considerable work is needed to develop norms on offensive cyber action by states, including on cyberespionage and responsibility of states for actions emanating from their territory. The question thus continues to be raised whether existing international laws, even if applicable, are sufficient to deal with cyber threats.

Both states and scholars have identified the need for a new treaty to address cybersecurity.[67] In 1998 Russia proposed a treaty governing cyber weapons similar to those governing nuclear, chemical, and biological weapons, but the proposal did not gain significant support. Others have argued for a more comprehensive treaty addressing cybersecurity. This approach reflects existing regional efforts to address cybercrime, including the 2001 Convention on Cybercrime (also known as the Budapest Convention) among Western states. This convention requires parties to harmonize domestic criminal legislation and promote international collaboration in addressing transnational cybercrime.[68]

Any attempt to create new cybersecurity laws will require policymakers to address several major underlying issues. The first thing to consider is which actors the laws will address. Most existing laws focus on private actors without distinguishing between their motives, but it may be best for a different set of rules to apply when cyberattacks originate from a state. There is also a question of whether to distin-

[61] World Summit on the Information Society, *Declaration of Principles*, UN Doc. WSIS-03/GENEVA/DOC/4-E, December 12, 2003, paras. 48–49.

[62] World Summit on the Information Society, *Tunis Agenda for the Information Society*, UN Doc. WSIS-05/TUNIS/DOC/6(Rev. 1)-E, November 18, 2005, para. 35.

[63] UN General Assembly Resolution 70/L.22.

[64] The term "cyber" denotes not only the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (winter 2011).

[65] Jigsaw, "Digital Attack Map," available at https://jigsaw.google.com/products/digital-attack-map/ .

[66] Tim Maurer and Scott Janz, "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context," International Relations and Security Network, October 17, 2014, available at www.css.ethz.ch/en/services/digital-library/publications/publication.html/187945 ; NATO StratCom Centre of Excellence, "Analysis of Russia's Information Campaign against Ukraine," 2015, available at www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine .

[67] Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," Yale Law School, 2012, available at http://digitalcommons.law.yale.edu/fss_papers/3852/ .

[68] Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (2011).

guish between attacks by cybercriminals and attacks by cyberterrorists.[69] However, the seriousness of the threat posed by cyberterrorism, as well as the use of the term itself, remains controversial.[70] In considering this question, the UN Working Group on Countering the Use of the Internet for Terrorist Purposes concluded that cyberterrorism is not yet a threat serious enough to warrant separate legislation.[71]

If policymakers put in place different rules for different actors, they must be able to attribute each act to determine which set of rules applies. Attributing cyberattacks is difficult, however, and simply determining an attack's source may not be enough to determine who is responsible. If governments are too careful to attribute, this could undermine attempts to hold those violating laws accountable.[72]

In developing new legal frameworks, policymakers must address the relationship between cybersecurity and human rights. Big data comes with significant risks to human rights—not just the risk of compromising privacy but also of threatening the security of individuals if the data falls into the wrong hands or of exacerbating conflict if the digital divide parallels conflict cleavages.[73] While in many developed countries the notion of data privacy revolves around "the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them," in conflict areas privacy can be a question of life or death.[74]

In addition, activists fear that grouping together crimes merely committed on the Internet and those for which the Internet is central, as in the Convention on Cybercrime, opens the door to content controls. This highlights questions about the extent to which a new cybersecurity treaty would be able to safeguard human rights around the world. Existing guidance on human rights in the digital age developed within the UN system or by international NGOs would likely have to be included as part of any such treaty.[75]

The International Committee of the Red Cross (ICRC), UN OCHA, and UN Global Pulse have all created guiding principles for privacy and protection that could be incorporated into multilateral normative or legal frameworks.[76] The idea behind these principles is not to overregulate the system, which would be detrimental to cyber activists, who can often thrive in environments hostile to real-world grassroots movements; the goal is to address the fact that "privacy, access, and use remain key concerns for all actors looking to leverage big data for different ends."[77] All stakeholders need to establish checks and balances on the use of big data to ensure human rights are protected.[78]

In addition to determining what new legal and

[69] Anja Kovacs, "Addressing India's Global Cybersecurity Concerns: Norm Development, Regulatory Challenges, Alternative Approaches," Internet Democracy Project, August 18, 2015, available at https://internetdemocracy.in/reports/addressing-indias-global-cybersecurity-concerns/ .

[70] Stuart Macdonald, Lee Jarvis, Thomas Chen, and S. Lavis, "Cyberterrorism: A Survey of Researchers," Swansea University, 2013, available at www.cyberterrorism-project.org/wp-content/uploads/2013/03/Cyberterrorism-Report-2013.pdf .

[71] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," Harvard Kennedy School Belfer Center for Science and International Affairs, September 2011.

[72] Kovacs, "Addressing India's Global Cybersecurity Concerns."

[73] Mancini, ed., "New Technology and the Prevention of Violence and Conflict."

[74] Kevin Roebuck, *Internet Privacy of Data and Information: High-Impact Strategies* (La Vergne, TN: Lightning Source, 2011).

[75] Kovacs, "Addressing India's Global Cybersecurity Concerns."

[76] See ICRC, "Rules on Personal Data Protection," January 2016, available at www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection ; UN OCHA, "Humanitarianism in the Age of Cyber-Warfare: Towards the Principled Use of Information in Humanitarian Emergencies," October 2014, available at https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf ; and UN Global Pulse, "Privacy and Data Protection Principles," available at www.unglobalpulse.org/privacy-and-data-protection-principles .

[77] Mancini, ed., "New Technology and the Prevention of Violence and Conflict."

[78] Alistair Croll, "Big Data Is Our Generation's Civil Rights Issue, and We Don't Know It," in *Big Data Now* (Sebastopol, CA: O'Reilly Media, 2012).

normative frameworks are needed, policymakers also need to consider how existing international law applies to cyberspace. For example, growing interest and contention around the so-called "duty to hack" raises questions about the relationship between cybersecurity and international humanitarian law. International humanitarian law requires states to use the least harmful military means available for achieving their strategic objectives, which leads some to identify cyber operations as the least harmful response. Such cyber operations could help avoid physical attacks that risk causing greater damage and casualties, hence the "duty" to invest in offensive hacking capacities.[79]

The UN has undertaken several initiatives to increase the clarity of how existing international law applies to cyberspace. One example is the work of the consecutive Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, established under the auspices of the UN General Assembly.[80] Though initial progress was slow, the third Group of Governmental Experts reached a breakthrough when it unanimously concluded that international law, particularly the UN Charter, is applicable in cyberspace.[81] This report is widely seen as indicative of an emerging consensus on the validity of applying existing international rules to cyberspace and is being used as a reference document in other multilateral organizations such as the OSCE.

Another major initiative was the development of the Tallinn Manual on the International Law Applicable to Cyber Warfare. This manual was created by a group of international law and cybersecurity experts brought together by the NATO Cooperative Cyber Defence Centre of Excellence to consider *jus ad bellum* (the laws for engaging in war) and *jus in bello* (international humanitarian law).[82] Although the manual is nonbinding and left a number of important issues unresolved (e.g., where the threshold of serious damage lies), the manual is considered an important attempt to determine how international rules apply to cyberspace.[83]

To complement legal approaches to securing cyberspace, some have proposed putting in place confidence-building measures. In this area, the OSCE is developing confidence-building measures "to enhance security and stability in the cyber domain and reduce the risks of conflict stemming from the use of [ICTs]." These include sharing information and appointing governmental focal points on cybersecurity.[84] But ambitions on implementing confidence-building measures vary greatly among different organizations, and few concrete measures have been implemented.

One potential confidence-building measure is the "duty to assist," which would impose a requirement to assist victims (states or individuals) facing serious harm. This would avoid the challenge of attribution, as the severity of harm, rather than its source, would determine whether to provide assistance.[85] Building on this concept, others have proposed a global cyber federation of nongovernmental institutions committed to providing independent, neutral, and impartial assistance to the Internet and its users. Using existing computer emergency response teams and computer security incident response teams as building blocks, this federation would aim to make cyberspace safer and more secure.[86] Both these

[79] Duncan B. Hollis, "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" in *Cyberwar: Law and Ethics for Virtual Conflicts*, edited by Jens David Ohlin, Kevin Govern, and Claire Finkelstein (Oxford: Oxford University Press, 2015).

[80] See, for example, General Assembly Resolutions 57/53 (December 30, 2002), 62/17 (December 5, 2007), 65/41 (January 11, 2011), and 68/243 (December 27, 2013).

[81] Group of Governmental Experts, *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, June 24, 2013.

[82] Myrna Azzopardi, "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on Its Treatment of Jus Ad Bellum Norms," *ELSA Malta Law Review* 3 (2013).

[83] Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual," *Journal of Conflict & Security Law* 18, no. 2 (2013).

[84] See www.osce.org/secretariat/cyber-security .

[85] Hollis, "An e-SOS for Cyberspace."

[86] Duncan Hollis and Tim Maurer, "A Red Cross for Cyberspace," *Time*, February 18, 2015.

proposals would seek to maximize the role of all stakeholder groups rather than privileging state interests, such as by aligning the efforts of the World Federation of Scientists and of the UN to promote the concept of “cyber peace.”[87]

Adapting to New Forms of Physical Warfare

Beyond cyberspace, policymakers must also consider the relationship between international humanitarian law and new forms of physical warfare. Many technologically advanced weapons systems are now available at relatively low cost, giving rise to new forms of hybrid warfare.[88] As in cyberspace, new forms of physical warfare expose gaps and shortcomings in international laws and norms.

This is particularly true for armed unmanned aerial vehicles (UAVs), or drones. There is broad consensus that the use of armed UAVs is not in itself illegal, but there is no consensus on how to apply international law on the use of force to UAVs. There is a risk that armed UAVs could expand the geographical and temporal boundaries of the use of force, and their use by non-state actors raises further regulatory challenges.[89]

Lethal autonomous weapons systems, or “killer robots,” also raise serious questions about the application of international humanitarian law. The notion of decision making is at the heart of international humanitarian law, and as these technologies become more autonomous with little to no human intervention, accountability becomes more difficult to determine.

As in cyberspace, a considerable role can be foreseen for the multilateral system in applying existing international laws and norms to new forms of physical warfare. For example, the UN special rapporteur on extrajudicial, summary or arbitrary executions and the UN special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism have both issued reports to clarify the applicability of international law surrounding the use of armed drones.[90] In the wake of the Campaign to Stop Killer Robots, in 2013 the UN Convention on Conventional Weapons launched an annual Meeting of Experts on Lethal Autonomous Weapons Systems involving the UN and civil society. The 2016 meeting reflected a general understanding that states should be held accountable for the actions of such weapons in accordance with international law.[91]

[87] Kovacs, “Addressing India’s Global Cybersecurity Concerns.”

[88] Alex Deep, “Hybrid War: Old Concept, New Techniques,” *Small Wars Journal*, March 2, 2015; Frank G. Hoffman, “Hybrid Warfare and Challenges,” *Small Wars Journal* 52, no. 1 (2009).

[89] Christof Heyns, *Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions*, UN Doc. A/HRC/26/36, April 1, 2014; Ben Emmerson, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UN Doc. A/HRC/25/59, March 10, 2014.

[90] Ibid.

[91] UN Office at Geneva, “Recommendations to the 2016 Conference Submitted by the Chairperson of the Informal Meeting of Experts,” available at www.unog.ch/80256EE600585943/(httpPages)/37D51189AC4FB6E1C1257F4D004CAFB2?OpenDocument .

Conclusions and Recommendations

The UN is eternally playing catch-up to a rapidly evolving wave of technological change. Since these new technologies are revolutionizing our societies, the UN should also use them as agents of change to promote its core objectives. That said, the UN should be realistic in determining where it can be a norm setter and where it is better suited to be a user. For example, international governance of the Internet has largely taken place outside of the UN. Since most technological innovations have been developed by the private sector and civil society, it is vital to involve these actors in efforts to harness technology as an enabler for positive change.

While it may be unrealistic to expect the UN to be at the forefront of technological innovation, it has a unique role to play in promoting dialogue, enabling partnerships, highlighting best practices, and supporting decision making and norm setting. The UN is already undertaking this role in a number of areas. Through the ITU and the implementation of the 2030 Agenda on Sustainable Development, for example, the UN is convening more dialogues and increasing the number of partnerships on the links between technology and sustainable development. Through initiatives such as ICT4Peace, the private sector and other stakeholders are becoming more involved in the work of the UN. The fact that in May 2016 the vice-president of Microsoft was invited to make a presentation to the Security Council during a debate on counterterrorism, where not long ago only member states and parties to the issue would be welcome, is a step in the right direction. The UN has also been active in supporting the recognition of the Internet and big data as global public goods.

For the multilateral system, and the UN in particular, to make progress on the range of issues touched upon above, the UN and its member states should take several important actions.

Consolidate a Multilateral Space for Innovation and New Technology

The UN should help enable and consolidate the space for all stakeholders, above all the private sector, to meet and partner in addressing crosscutting challenges. Many such forums already exist, but they are spread throughout the UN system and are often difficult to navigate, especially for non-state actors.

1. **The secretary-general should identify a UN focal point on cyber issues.** With ongoing efforts to improve cybersecurity through regional bodes such as NATO, the Organisation for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS), and the Council of Europe, there is a risk of a plurality of regional initiatives without global standards. The appointment of a clear UN focal point on cyber issues would consolidate the UN's currently disjointed approach and make it a more credible player on an issue that demands greater international engagement.

2. **The UN Secretariat should map UN venues dealing with new technologies.** By one count, ten different UN bodies have dealt with cyber issues since the 1990s, not including bodies such as the UN Human Rights Council that have started to address cyber issues in their specific area of work.[92] This piecemeal approach is

[92] Maurer, "Cyber Norm Emergence at the United Nations."

confusing and spreads decision making and consultation throughout the system while excluding outside partners. Mapping the venues where new technologies are being used could identify good practices and needs, thereby helping streamline and consolidate efforts to more effectively use technology to achieve the UN's objectives.

3. **The UN Secretariat should ensure coherence among new mechanisms.** The Technology Facilitation Mechanism for sustainable development, the Technology Bank for Least Developed Countries, and the Technology Framework for climate change share the common goal of facilitating access to and transfer of technology to developing countries. These new mechanisms need to be connected to one another to accelerate progress toward achieving the 2030 Agenda and the Paris Agreement without duplicating efforts and competing for resources.

4. **The UN Secretariat should create a "cyber and innovation compact" with the private sector and civil society.** Nowhere is there a greater need to fully recognize the role of civil society and the private sector in the multilateral system than in the area of technological innovation. Inputs and expertise from these actors should be accorded far greater pride of place across the multilateral system. A formal forum for cooperation with the UN would be a step in the right direction.

Recognize the Internet and Big Data as Global Public Goods

The UN should formally recognize the Internet and big data as global public goods by developing norms and new approaches to better address the challenges and opportunities they present and to ensure they are used for peaceful purposes.

5. **Member states should recognize cyberspace as a global public good.** This could be done through a General Assembly resolution declaring that cyberspace should be used for "peaceful purposes" in the interests of humanity.

6. **Member states should establish a UN-guaranteed depository as a safe-keeper of big data.** Member states could mandate this body to help collect, structure, and store data, especially from regions where the infrastructure is not safe or sufficient. Establishment of this body should involve a multi-stakeholder process to create and implement safeguards for the data, incentivize the private sector to partner with the UN, identify ways to overcome firewalls, agree on protocols for extracting and sharing data as needed, and enable data philanthropy.

7. **The UN Secretariat should consolidate and build its analytical capacity.** The UN could help provide greater analytical and statistical capacity when member states lack it. This could facilitate economic and social development and contribute to gathering and analyzing necessary data on climate change. This capacity already exists but is currently spread throughout the system.

8. **The UN Secretariat and member states should support and integrate confidence-building measures.** Based on the report of the Group of Governmental Experts on cybersecurity, the UN Secretariat, through its focal point on cyber issues, should work with member states to develop a strategic approach to implement these measures. This approach could focus on putting in place confidence-building measures at the regional and subregional levels to ensure the security and sustainability of cyberspace.

Annex 1: ICM Personnel

Co-chairs

HE Mr. Kevin Rudd, *Australia* (Chair)

HE Mr. Børge Brende, *Norway*

HE Ms. Hannah Tetteh, *Ghana*

HE Mr. José Manuel Ramos-Horta, *Timor-Leste*

HE Ms. Patricia Espinosa Cantellano, *Mexico* (2014–July 2016)

Ministerial Board

HE Mr. Jean Asselborn, *Luxembourg*

HE Mr. Mevlüt Çavuşoğlu, *Turkey*

HE Mr. Stéphane Dion, *Canada*

HE Ms. Aurelia Frick, *Liechtenstein*

Sh. Khaled Al Khalifa, *Bahrain*

HE Mr. Sebastian Kurz, *Austria*

HE Ms. Retno Marsudi, *Indonesia*

HE Mr. Heraldo Muñoz, *Chile*

Sh. Abdullah Al Nahyan, *UAE*

HE Ms. Netumbo Nandi-Ndaitwah, *Namibia*

HE Mr. Sameh Shoukry Selim, *Egypt*

Geneva Ambassadorial Board

HE Ms. Marianne Odette Bibalou, *Gabon*

HE Ms. Regina Dunlop, *Brazil*

HE Mr. Alexandre Fasel, *Switzerland*

HE Ms. María Fernanda Espinosa Garcés, *Ecuador*

HE Mr. Jean-Marc Hoscheit, *Luxembourg*

HE Ms. Nazhat Shameem Khan, *Fiji*

HE Mr. Steffen Kongstad, *Norway*

HE Mr. Ajit Kumar, *India*

HE Ms. Saja Majali, *Jordan*

HE Ms. Marta Maurás Pérez, *Chile*

HE Ms. Rosemary McCarney, *Canada*

HE Mr. François Xavier Ngarambe, *Rwanda*

HE Mr. Vaanchig Purevdorj, *Mongolia*

HE Mr. Amr Ramadan, *Egypt*

HE Mr. Carsten Staur, *Denmark*

HE Ms. Yvette Stevens, *Sierra Leone*

HE Mr. Thani Thongphakdi, *Thailand*

HE Mr. Roderick van Schreven, *Netherlands*

HE Mr. Obaid Salem Al Zaabi, *United Arab Emirates*

New York Ambassadorial Board

HE Mr. Amr Abdellatif Aboulatta, *Egypt*
HE Mr. Brian Bowler, *Malawi*
HE Mr. Harald Braun, *Germany*
HE Mr. Yaşar Halit Çevik, *Turkey*
HE Mr. Vitaly Churkin, *Russia*
HE Mr. Vladimir Drobnjak, *Croatia*
HE Mr. Einar Gunnarsson, *Iceland*
HE Mr. Mohamed Khaled Khiari, *Tunisia*
HE Ms. Lana Zaki Nusseibeh, *UAE*
HE Mr. Antonio de Aguiar Patriota, *Brazil*
HE Mr. Geir O. Pedersen, *Norway*
HE Mr. Amrith Rohan Perera, *Sri Lanka*
HE Mr. Nawaf Salam, *Lebanon*
HE Mr. Fodé Seck, *Senegal*
HE Mr. Karel van Oosterom, *Netherlands*
HE Mr. Christian Wenaweser, *Liechtenstein*
HE Mr. Jean-Francis Régis Zinsou, *Benin*

Vienna Ambassadorial Board

HE Mr. Luis Alfonso de Alba, *Mexico*
HE Ms. Olga Algayerova, *Slovakia*
HE Ms. Bente Angell-Hansen, *Norway*
HE Mr. Abel Adelakun Ayoko, *Nigeria*
HE Mr. Mark Bailey, *Canada*
HE Ms. Maria Zeneida Angara Collinson, *Philippines*
HE Mr. Mehmet Hasan Göğüş, *Turkey*
HE Mr. Philip McDonagh, *Ireland*
HE Mr. Rajiva Misra, *India*
HE Mr. Michael Adipo Okoth Oyugi, *Kenya*
HE Ms. Marion Paradas, *France*
HE Mr. Kairat Sarybay, *Kazakhstan*
HE Mr. Gonzalo de Salazar Serantes, *Spain*
HE Mr. Khaled Abdelrahman Abdellatif Shamaa, *Egypt*
HE Ms. Christine Stix-Hackl, *Austria*
HE Mr. Claude Wild, *Switzerland*

Convener

Terje Rød-Larsen, President,
International Peace Institute

The Ministerial and Ambassadorial Board lists include attendees at the ICM Ministerial and Ambassadorial Board meetings.

ICM Secretariat

Hardeep Singh Puri, Secretary-General
(September 2014–March 2016)

Barbara Gibson, Secretary-General

Adam Lupel, Vice President, IPI

Els Debuf, Senior Adviser

Ariun Enkhsaikhan, Research Assistant

Omar El Okdah, Senior Policy Analyst

Warren Hoge, Senior Adviser

Jimena Leiva Roesch, Senior Policy Analyst

Youssef Mahmoud, Senior Adviser

Nadia Mughal, Digital Content Producer

Andrea Ó Súilleabháin, Senior Policy Analyst

Véronique Pepin-Hallé, Adviser

Asteya Percaya, Intern

Anette Ringnes, Research Assistant

Rodrigo Saad, External Relations Coordinator

Margaret Williams, Policy Analyst

IPI Publications

Albert Trithart, Associate Editor

Madeline Brennan, Assistant Production Editor

IPI Web and Multimedia

Jill Stoddard, Director of Web & Multimedia
and Web Editor

Thong Nguyen, Program Administrator

Hillary Saviello, Social Media Officer

Annex 2: ICM Policy Papers

This is one in a series of fifteen issue-specific policy papers that the Independent Commission on Multilateralism (ICM) is publishing over the course of 2016 and 2017. These papers cover in greater detail issue areas addressed in ICM's September 2016 report "Pulling Together: The Multilateral System and Its Future." The fifteen policy papers (not in order of publication) are as follows:

Armed Conflict: Mediation, Peacebuilding, and Peacekeeping

Climate Change and the 2030 Agenda for Sustainable Development

Communication Strategy for the UN Multilateral System

Engaging, Supporting, and Empowering Global Youth

Forced Displacement, Refugees, and Migration

Fragile States and Fragile Cities

Global Pandemics and Global Public Health

Humanitarian Engagements

Impact of New Technologies on Peace, Security, and Development

Justice and Human Rights

Social Inclusion, Political Participation, and Effective Governance

Terrorism and Organized Crime

The UN, Regional Organizations, Civil Society, and the Private Sector

Weapons of Mass Destruction: Non-proliferation and Disarmament

Women, Peace, and Security

Annex 3: Participation in Consultations

Retreat: October 23–24, 2015 (Greentree Estate, Manhasset, New York)

Keynote Speaker

David Kirkpatrick, *CEO and Founder, Techonomy Media*

Participants

Muhammad Anshor, *Deputy Permanent Representative, Permanent Mission of the Republic of Indonesia to the United Nations*

Aloísio Barbosa de Sousa Neto, *Permanent Mission of Brazil to the United Nations*

Jeanne d'Arc Byaje, *Deputy Permanent Representative, Permanent Mission of the Republic of Rwanda to the United Nations*

Els Debuf, *Adviser, Independent Commission on Multilateralism*

Walter Dorn, *Professor of Defense Studies, Royal Military College of Canada*

Vladimir Drobnjak, *Permanent Representative, Permanent Mission of the Republic of Croatia to the United Nations*

Dirk Druet, *Technology and Innovation Focal Point of the Policy Planning Team, UN Departments of Peacekeeping Operations and Field Support*

Wilfried I. Emvula, *Permanent Representative, Permanent Mission of the Republic of Namibia to the United Nations*

Ariun Enkhsaikhan, *Intern, International Peace Institute*

Camille François, *Fellow, Harvard Berkman Center for Internet and Safety*

Helani Galpaya, *CEO, LIRNEasia*

Barbara Gibson, *Deputy Secretary-General, Independent Commission on Multilateralism*

Christina Goodness, *Chief of Peacekeeping Information Management, UN Departments of Peacekeeping Operations and Field Support*

Warren Hoge, *Senior Adviser for External Relations, International Peace Institute*

Justin Kosslyn, *Product Manager, Google Ideas*

Anja Kovacs, *Project Director, Internet Democracy Project*

Jimena Leiva Roesch, *Policy Analyst, International Peace Institute*

Adam Lupel, *Director of Research and Publications, International Peace Institute*

Youssef Mahmoud, *Senior Adviser, International Peace Institute*

Peter Janos Major, *Chair, Commission on Science and Technology for Development, UN Conference on Trade and Development*

Jānis Mažeiks, *Permanent Representative, Permanent Mission of the Republic of Latvia to the United Nations; Co-facilitator, WSIS+10*

Paul Meyer, *Senior Advisor, ICT4Peace Foundation*

Nadia Mughal, *Digital Content Producer, Independent Commission on Multilateralism*

Thong Nguyen, *Program Administrator, International Peace Institute*

Omar El Okdah, *Senior Policy Analyst, International Peace Institute*

Véronique Pepin-Hallé, *Adviser, Independent Commission on Multilateralism*

Hardeep Singh Puri, *Secretary-General, Independent Commission on Multilateralism*

Florian Reindel, *Political Counsellor, Permanent Mission of Germany to the United Nations*

Jorge Alberto Restrepo Torres, *Director, Conflict Resource Analysis Center*

Anette Ringnes, *Research Assistant, International Peace Institute*

František Ružička, *Permanent Representative, Permanent Mission of the Slovak Republic to the United Nations*

Rodrigo Saad, *Program Assistant, Independent Commission on Multilateralism*

Riadh Ben Sliman, *Deputy Permanent Representative, Permanent Mission of Tunisia to the United Nations*

Patrick Vinck, *Director, Peace and Human Rights Data Program, Harvard University*

Public Consultation: May 12, 2016 (IPI, New York)

Discussants

Vladimir Drobnjak, *Permanent Representative, Permanent Mission of the Republic of Croatia to the United Nations*

Robert Kirkpatrick, *Director, UN Global Pulse, Executive Office of the Secretary-General*

Véronique Pepin-Hallé, *Senior Adviser, Independent Commission on Multilateralism*

Patrick Vinck, *Assistant Professor, Department of Global Health and Population, Harvard Humanitarian Initiative, Harvard T. H. Chan School of Public Health*

Moderator

Barbara Gibson, *Deputy Secretary-General, Independent Commission on Multilateralism*

IPI Personnel

Issue Area Lead: Véronique Pepin-Hallé

Cover Photo: Drone carrying life buoy, December 30, 2015.
Chesky_W/iStock Photo.

Suggested Citation:
Independent Commission on Multilateralism, “The Impact of New Technologies on Peace, Security, and Development,” New York: International Peace Institute, May 2017.

www.ipinst.org
www.icm2016.org

The **INTERNATIONAL PEACE INSTITUTE** (IPI) is an independent, international not-for-profit think tank dedicated to managing risk and building resilience to promote peace, security, and sustainable development. To achieve its purpose, IPI employs a mix of policy research, strategic analysis, publishing, and convening. With staff from around the world and a broad range of academic fields, IPI has offices facing United Nations headquarters in New York and offices in Vienna and Manama.

IPI

INTERNATIONAL
PEACE
INSTITUTE

777 United Nations Plaza
New York, NY 10017–3521
USA
TEL +1-212 687-4300
FAX +1-212 983-8246

Freyung 3, 1010
Vienna, Austria
TEL +43-1-533-8881
FAX +43-1-533-8881-11

51-52 Harbour House
Bahrain Financial Harbour
P.O. Box 1467
Manama, Bahrain
TEL +973-1721-1344

www.ipinst.org

www.theglobalobservatory.org