Discussion Paper

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

Independent Commission on Multilateralism

April 2016

Introduction

A new wave of technology is driving rapid global change. "Waves" of technological change, driven by inventions ranging from steam power to electricity to the automobile, have driven economic development and social transformation throughout recent history.[1] Some historians speak of "technological revolutions," from the first industrial revolution that mechanized production, to the second that led to mass production, to the third that automated production. It has been argued that we are now in the fourth industrial revolution, where "a fusion of technologies…is blurring the lines between the physical, digital, and biological spheres."[2] In this latest technological revolution, "new technologies" include everything from the Internet to drones to big data, and the potential applications of these technologies are rapidly expanding.

The need for multilateral cooperation in response to new technologies was recognized as early as 1865, with the creation of the International Telegraph Union (ITU). The ITU (renamed the International Telecommunication Union in 1934) became a specialized UN agency in 1947 and is the oldest existing international organization. In subsequent years, technological change has created new opportunities for multilateral cooperation in the areas of sustainable development, governance and state-society relations, peace and conflict, international security, and global governance. But at the same time, the UN and other multilateral institutions have at times struggled to keep up with the pace of change.

Any discussion of multilateral cooperation on new technologies must take a multi-stakeholder perspective. Private sector and civil society actors, in particular, have often played a leading role in developing and pioneering innovative uses of these technologies, as well as in governing their use. 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. In adapting to new technologies, the UN must determine where it can play a useful role and where existing mechanisms and other actors are better placed.

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. This integration is more advanced in some areas than in others. For example, the growing role of technology in sustainable development was highlighted in the outcomes of a number of major UN conferences in 2015. In other areas, such as peace and security, the UN is earlier in the process of integrating new technologies into its work.

This is the context in which the Independent Commission on Multilateralism (ICM) is addressing the impact of new technologies and identifying areas where the multilateral system could play a positive role. This paper does not aim to give a comprehensive overview of the landscape of new technologies. It focuses on the opportunities and challenges these technologies present and how the multilateral system, anchored in the UN, is addressing them. The objective is to offer the multilateral system concrete recommendations on applying these new technologies in key areas and developing frameworks and norms governing their use.

---

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

I. Impact on Sustainable Development

Challenges and Opportunities

The Digital Divide

The potential of new technologies, particularly information and communication technologies (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.[3] However, 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.

While 82 percent of people in developed countries use the Internet, the proportion is just 43 percent globally, 35 percent in developing countries, 11 percent in Africa, and 9 percent in the least-developed countries. According to the Millennium Development Goals Gap Task Force, "As long as more people are offline than online, it is not possible to talk about a global information society."[4] The lack of relevant content in many languages further exacerbates this divide. Mobile phone access is more widespread, with 97 subscriptions per 100 people globally, but residents of the least-developed countries still lag behind, particularly in rural areas that lack a mobile signal. In some areas, moreover, a striking gender gap in access to and use of ICTs has emerged.[5]

Improving access to ICTs in developing countries 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. Lowering prices is also critical to increasing access; despite considerable progress in reducing prices for ICTs through regulatory frameworks and increasing competition, prices remain highest in the poorest countries.[6]

Environmental Impact

While ICTs have driven economic growth, they have also contributed to environmental pollution. Storage of data in the "cloud" may seem clean and efficient, but it is stored in massive digital warehouses that require enormous amounts of energy—about 30 billion watts of electricity, roughly equivalent to the output of thirty nuclear plants.[7] In addition, new technologies are contributing to a rapid increase in the amount of electronic waste,

[3] International Telecommunication Union, "Impact of Broadband on the Economy," April 2012, p. 4.
[4] MDG Gap Task Force, "Taking Stock of the Global Partnership for Development," United Nations, 2015, pp. 68–69.
[5] GSMA Connected Women Global Development Alliance, "Bridging the Gender Gap: Mobile Access and Usage in Low and Middle-Income Countries," 2015.
[6] Ibid.
[7] 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.

which exceeded 40 million tons in 2014 and is growing by 4–5 percent per year.[8] Much of this waste is toxic and is illegally dumped in developing countries.[9]

Data for Development

Measurement is key to achieving sustainable development. Data provide benchmarks to understand what policies are failing and what new initiatives need to be implemented. 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."[10]

The same lack of resources, capacities, and opportunities that prevents broader Internet access creates similar inequalities in the quality of data in developed versus developing countries. The lack of data hurts developing countries most. Yet for all countries, regardless of income level, challenges in data collection, standardization, disaggregation, and timeliness compromise sustainable development.

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 (e.g., 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 and free. The adoption of open data, open standards, open source, and open innovation could broaden the community of analysts and policymakers committed to integrating and scaling out solutions toward the delivery of the Sustainable Development Goals (SDGs).

"Big" data present a largely untapped opportunity for sustainable development. "Big data for development" involves "turning imperfect, complex, often unstructured data into actionable information."[11] According to a report from UN Global Pulse, big data are not a panacea, but they could "allow decision makers to track development progress, improve social protection, and understand where existing policies and programmes require adjustment."[12] The success of big data in supporting development depends on support from governments and collaboration between governments, the private sector, and academics. It

[8] 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.
[9] 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.
[10] 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, available at www.undatarevolution.org/wp-content/uploads/2014/11/A-World-That-Counts.pdf, p. 2.
[11] Emmanuel Letouzé, "Big Data for Development: Challenges and Opportunities," UN Global Pulse, May 2012, available at www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf, p. 6.
[12] Ibid., p. 4.

also depends on the development and implementation of new norms and institutional frameworks for responsibly using and sharing big data.[13]

Multilateral Responses

Links between the WSIS+10 and Sustainable Development

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."[14] 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).[15]

More recently, the link between new technologies and sustainable development was 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. The WSIS+10 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."[16]

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 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 2030 Agenda also contains a commitment to "fully operationalize the technology bank and science, technology and innovation capacity-building mechanism for least-developed countries."[17] These targets have the potential to accelerate progress in the countries that need it most. Nonetheless, some critics argue that ICTs do not feature prominently enough in the 2030 Agenda.[18]

The WSIS+10 outcome document also officially endorses another global plan linking ICTs and sustainable development that the ITU adopted in 2014: the Connect 2020 Agenda for

[13] Ibid, p. 42.
[14] United Nations, *Millennium Declaration*, UN Doc. A/RES/55/2, September 8, 2000, para. 20.
[15] UN General Assembly Resolution 56/183 (January 31, 2001), UN Doc. A/RES/56/183.
[16] UN General Assembly Resolution 70/125 (December 16, 2015), UN Doc. A/RES/70/125, Art. 1.
[17] UN General Assembly Resolution 70/1 (September 25, 2015), UN Doc. A/RES/70/1, 9.b, 17.8.
[18] 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.

Global Telecommunication/ICT and Development.[19] 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 (see Annex 1).[20] Implementation of the 2020 Agenda will complement and reinforce the SDGs.

Technology Transfer Mechanisms

One challenge to multilateral efforts to promote development through technology is that these technologies are generally developed in the private sector rather than by member states. 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 (TFM) for sustainable development was launched at the UN Sustainable Development Summit in September 2015. This mechanism comprises: (1) a UN inter-agency 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 for information on existing initiatives, mechanisms, and programs.[21] This mechanism has the potential to facilitate access to technologies that will enhance the implementation of the 2030 Agenda in developing countries.

In addition, in 2010 the Conference of the Parties to the UN Framework Convention on Climate Change (UNFCCC) established a Technology Mechanism to facilitate development and transfer of technology to support action on mitigating and adapting to climate change.[22] 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."[23]

Coordinating on Data

Some agencies and actors in the multilateral system have begun to place more emphasis on unleashing the potential of data. A number of agencies such as the UN Children's Fund (UNICEF), UN Development Programme (UNDP), UN Office for the Coordination of Humanitarian Affairs (OCHA), and UN High Commissioner for Refugees (UNHCR) have endorsed open principles, which could open up the benefits of data both "small" and

[19] UN General Assembly Resolution 70/L.22, para. 25.
[20] International Telecommunication Union Resolution 200, "Connect 2020 Agenda for Global Telecommunication/Information and Communication Technology Development," 2014.
[21] UN Department of Economic and Social Affairs, "Technology Facilitation Mechanism," n.d., available at https://sustainabledevelopment.un.org/TFM.
[22] UN Framework Convention on Climate Change, *Report of the Conference of the Parties on Its Sixteenth Session*, UN Doc. FCCC/CP/2010/7/Add.1, March 15, 2011, para. 117.
[23] UN Framework Convention on Climate Change, *Adoption of the Paris Agreement*, UN Doc. FCCC/CP/2015/L.9/Rev.1, December 12, 2015, Art. 10.

"big."[24] Other platforms have informally sought to coordinate in collecting statistics, including the Global Partnership for Sustainable Development Data, a global network of governments, NGOs, and businesses partnering to make data more complete, accessible, and accurate.[25]

II. Impact on Governance and State-Society Relations

Challenges and Opportunities

Crowdsourcing

Crowdsourcing presents an opportunity to empower citizens and transform the state-society relationship. 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.[26] 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.[27] 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.'"[28]

Crowdsourcing has the potential to 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 assess their outcomes, indirectly increasing their legitimacy.[29] One recent example is Iceland's attempt to crowdsource a new constitution, which included extensive use of social media to gather feedback.[30] 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.

Networking

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

[24] UNICEF, "Principles for Innovation and Technology in Development," October, 31, 2014, available at www.unicef.org/innovation/innovation_73239.html.
[25] See Global Partnership for Sustainable Development Data, available at www.data4sdgs.org/.
[26] Daren C. Brabham, *Crowdsourcing* (Cambridge, MA: MIT Press, 2013).
[27] 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/.
[28] Jeff Howe, "The Rise of Crowdsourcing," *Wired*, June 1, 2006.
[29] Lehdonvirta and Bright, "Crowdsourcing for Public Policy and Government."
[30] 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.

technologies have often backfired, but authorities have proven that they can learn from their mistakes and use technology to their advantage. Some of these uses, such as mass surveillance, could contribute to breaking down trust between governments and citizens.

While new technologies can facilitate the rapid spread of ideas, this can have both positive and negative consequences. The easy manipulation of information and sources and the risk of viral dissemination without verification can propagate misinformation. Moreover, social media users risk finding themselves in "information cocoons" where they are not exposed to differing opinions, potentially increasing political polarization. Social media can also facilitate the spread and uptake of radical ideologies; the so-called Islamic State uses social media to recruit people from around the world.

Multilateral Responses

Open Government Partnership

Compared to sustainable development, the multilateral system has been slower 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 (OGP), which has since expanded to sixty-nine 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.[31] While still in its early stages, this partnership demonstrates the possibility of increased multilateral engagement on governance and technology.[32]

Selection of UN Secretary-General

In addition, the UN has used new technologies to increase the transparency and participatory nature of the process for selecting the next secretary-general in 2016. This process has included the use of social media and an online platform for people to ask questions to secretary-general candidates.[33] This and other such processes also provide opportunities for multilateral institutions to engage and partner with civil society.

III. Impact on Peace and Conflict

Challenges and Opportunities

Conflict Prevention

Although conflict prevention does not get the attention or funding it deserves on the global stage, this may be changing with the availability of new technological tools. 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 generate data on conflict indicators. The data generated from these tools can help

[31] Open Government Partnership, "Open Government Declaration," available at www.opengovpartnership.org/about/open-government-declaration.
[32] Jeremy M. Weinstein, "Transforming Multilateralism: Innovation on a Global Stage," *Stanford Social Innovation Review* (spring 2013).
[33] See UN Non-Governmental Liaison Service website, available at www.unngls.world/.

identify patterns associated with conflict and peace in order to better inform conflict prevention efforts, or to monitor violations of cease-fires or human rights.

However, significant hurdles to using new technologies to prevent conflict remain. These tools may not be appropriate or effective in every conflict or context. Big data, for example, come with significant risks—not just the risk of compromising privacy but also of threatening the security of individuals if the data fall into the wrong hands or that of exacerbating conflict if the digital divide parallels conflict cleavages.[34]

Peace Operations

Although new technologies have changed the way wars are fought, UN peace operations have been slow to integrate these technologies in fulfilling their increasingly complex mandates. Particularly useful for peace operations are technologies that facilitate monitoring and observation, including unarmed unmanned aerial vehicles (UUAVs), video monitoring systems, motion detectors, and satellite imagery.[35] These technologies can particularly help peace operations in the asymmetric threat environments in which they increasingly operate. The war in Syria is pushing forward exploration of many of these technological alternatives to putting boots on the ground.

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 UUAVs can improve data collection, transportation, and communication in peace operations, they also become part of the conflict dynamic, with all the attendant risks.[36] 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 connotation. Nonetheless, new technologies can benefit peace operations in many less controversial areas of their mandates, including monitoring and protection of civilians.

[34] Francesco Mancini, ed., "New Technology and the Prevention of Conflict," International Peace Institute, 2013.
[35] A. Walter Dorn, *Keeping Watch: Monitoring Technology and Innovation in UN Peace Operations* (Tokyo: United Nations University Press, 2011).
[36] Helena Puig Larrauri and Patrick Meier, "Peacekeepers in the Sky: The Use of Unmanned Unarmed Aerial Vehicles for Peacekeeping," ICT4Peace Foundation, September 2015.

Peacebuilding

New technologies also offer new opportunities for managing conflict and building peace, particularly at the local level. Beyond assisting in conflict prevention, participatory data collection and processing tools can empower communities to resist violence and recover after conflicts. ICTs can provide avenues for alternative discourse or community engagement that promote peace, and video games have been used to foster nonviolent attitudes and behaviors. However, in peacebuilding, too, these technologies bring risks. Access to new technologies is often uneven and can be manipulated by governments, and users face privacy and security risks.[37] Moreover, the same technologies that could be used to spread messages of peace could also be used to propagate messages of hate.

Multilateral Responses

The multilateral system has increasingly recognized the potential of new technologies to support peace and prevent conflict. The 2005 Tunis Commitment, a consensus statement of the WSIS, recognized the important role that ICTs can play in preventing conflicts through early-warning systems, promoting peaceful conflict resolution, supporting humanitarian action, facilitating peacekeeping missions, and assisting post-conflict peacebuilding and reconstruction.[38]

Review of UN 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 missions' ability to function, help missions execute their mandates more effectively, and streamline mission support operations. It also recommends institutionalizing innovation and continuous technological adaptation.[39]

The UN secretary-general's High-Level Independent Panel on Peace Operations (HIPPO), endorsed these recommendations, recommending 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.[40] The extent to which these recommendations are taken up remains to be seen.

Conflict Prevention Mechanisms

Efforts to use new technologies for conflict prevention have also been taken up at the multilateral level. For example, UNDP has implemented programs using new technologies to

[37] Helena Puig Larrauri and Anne Kahl, "Technology for Peacebuilding," *Stability: International Journal of Security & Development* 2, no. 3 (2013).
[38] World Summit on the Information Society, *Tunis Commitment*, UN Doc. WSIS-05/TUNIS/DOC/7-E, November 18, 2005, para. 36.
[39] Expert Panel on Technology and Innovation in UN Peacekeeping, "Performance Peacekeeping," December 22, 2014.
[40] UN secretary-general, "Report of the High-Level Independent Panel on Peace Operations," UN Doc. A/70/95-S/2015/446, June 17, 2015, para. 313.

prevent conflict and is further exploring this issue.[41] At the regional level, the Intergovernmental Authority on Development (IGAD), which includes eight countries in East Africa, launched an ICT 4 Peace project as part of its Conflict Early Warning and Response Mechanism (CEWARN).[42]

IV. Impact on International Security

Challenges and Opportunities

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.[43] 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. Moreover, conflict that takes place in the cyber domain often mirrors conflict in the physical world.[44]

New Methods of Warfare

The cybersecurity landscape becomes even more complex as new technologies reshape warfare. New technologies have made possible new methods of employing lethal force, such as armed unmanned aerial vehicles (UAVs), or drones, that pose new challenges. There is broad consensus that the use of armed drones is not in itself illegal, but there is no consensus on how to apply international law on the use of force to drones, and there is a risk that they could expand the geographical and temporal boundaries of using force. Their potential use by non-state actors raises further regulatory challenges.[45]

Lethal autonomous weapons systems, or "killer-robots," are also raising serious questions about the conduct of modern warfare and the application of international humanitarian law (IHL). The notion of the decision making process is at the heart of the IHL and as these technologies become more and more autonomous with little to no human intervention, accountability becomes more difficult to determine.

New technologies have also given rise to modern forms of hybrid warfare.[46] Many technologically advanced weapons systems are now available at relatively low cost. At the

[41] UN Development Programme, "Issue Brief: Using Technologies for Conflict Prevention," March 2012.
[42] Conflict Early Warning and Response Mechanism, "The CEWARN ICT 4 Peace Project: Use of Information Communication Technologies (ICTs) for Conflict Prevention," n.d., available at www.cewarn.org/index.php?option=com_content&view=article&id=97&lang=en.
[43] 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).
[44] Jigsaw, "Digital Attack Map," n.d., available at https://jigsaw.google.com/products/digital-attack-map/.
[45] 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.
[46] 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).

same time, more widely available technologies such as mobile phones and the Internet are increasingly used to support war efforts by facilitating communication, influencing public opinion, teaching new warfare techniques, gathering intelligence, and engaging in cyberattacks, as particularly demonstrated in the conflict in Ukraine.[47]

The growing interest and contention around the so-called "duty to hack" also raises question related to international humanitarian law and security.[48] International humanitarian law requires states to use the least harmful military means available for achieving their strategic objectives, which in the case of this theory could mean using cyber operations as the predominant least-harmful response. Such cyber operations could help avoid physical attacks that risk causing greater damage and casualties. This theory thus assigns states the "duty" to invest in offensive hacking capacities.

Multilateral Responses

Applying Existing International Laws and Norms

Given how new technologies complicate the application of existing international legal frameworks from many different vantage points, greater clarity and consensus on how to apply these frameworks is needed. As in the physical domain, a considerable role can be foreseen for the multilateral system in determining the norms and rules that govern offensive state action in the cyber domain and through new forms of warfare.

The UN has undertaken several initiatives toward this end. 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.[49] In the wake of the "Campaign Against Killer Robots," the UN Convention on Conventional Weapons (CCW) established in 2013 the Meeting of Experts on Lethal autonomous weapons systems (LAWS), involving the UN and civil society. One of the goals of these annual meetings is to figure out a way to ban LAWS and ensure that human decision making remains at the heart of lethal actions. Many say that this train has already left the station with over twenty autonomous weapon systems already in existence, but there is a need for a legal framework, and the UN could be seen as taking the lead on this issue.

Another example is the work of the consecutive Groups of Governmental Experts (GGEs) on Developments in the Field of Information and Telecommunications in the Context of International Security, established under the auspices of the UN General Assembly.[50] Though initial progress was slow, the third GGE reached a breakthrough when it

[47] 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; North Atlantic Treaty Organization StratCom Centre of Excellence, "Analysis of Russia's Information Campaign against Ukraine," 2015.

[48] 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 University Press, 2015).

[49] Heyns, *Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions*; Emmerson, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*.

[50] See, for example, A/RES/57/53, A/RES/62/17, A/RES/65/41, A/RES/68/243.

unanimously concluded that international law, particularly the UN Charter, is applicable in cyberspace.[51] This report is widely seen as indicative of an emerging consensus on the validity of applying existing international rules to cyberspace.

An additional 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 cyber-security experts brought together by the North Atlantic Treaty Organization's (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).[52] 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.[53]

A New Treaty Addressing Cybersecurity

Though the above initiatives have broken important ground, considerable work on norm development remains to be done regarding offensive state action in the cyber domain, including on issues such as cyberespionage by states and state responsibility 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 proposed a new treaty to address cybersecurity. In 1998 Russia proposed a treaty governing cyber weapons in much the same way as treaties governing nuclear, chemical, and biological weapons, although the proposal did not gain significant support. Others have argued for a more comprehensive treaty addressing cybersecurity.[54] This approach reflects existing regional efforts to address cybercrime, including the 2001 Convention on Cybercrime (also known as the Budapest Convention) among Western states, which requires parties to harmonize domestic criminal legislation and promote international collaboration in addressing transnational cybercrime.[55]

Any attempt to create new cybersecurity laws will require policymakers to address three major underlying issues. First, they will have to consider which actors to 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 distinguish between attacks by cybercriminals and attacks by cyberterrorists.[56] However, the seriousness of the threat posed by

[51] 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.
[52] 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).
[53] 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).
[54] Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," Yale Law School Faculty Scholarship Series paper 3852, 2012, available at http://digitalcommons.law.yale.edu/fss_papers/3852/.
[55] Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (2011).
[56] 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/.

cyberterrorism, as well as the use of the term itself, remains controversial.[57] 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.[58]

Second, 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.[59]

Third, policymakers must address the relationship between cybersecurity and human rights. In the Cybercrime Convention, for example, activists fear that grouping together crimes merely committed on the Internet and those for which the Internet is central 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 would likely have to be included as part of any such treaty.[60]

Confidence-Building Measures

In addition to a treaty on cybersecurity, some have proposed confidence-building measures (CBMs) as a complementary approach to addressing cybersecurity. One potential CBM is the "duty to assist," which would impose a requirement to assist victims 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.[61] 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 (CERTs) and computer security incident response teams (CSIRTSs) as building blocks, this federation would aim to make cyberspace safer and more secure.[62] Both these proposals would seek to maximize the role of all stakeholder groups rather than privileging state interests. They could also align with efforts by the World Federation of Scientists to promote the concept of cyber peace at the UN.[63]

V. Governing Cyberspace

Opportunities and Challenges

Existing Governance Systems

[57] Stuart Macdonald, Lee Jarvis, Thomas Chen, and S. Lavis, "Cyberterrorism: A Survey of Researchers," Cyberterrorism Project Research Report no. 1, Swansea University, 2013, available at www.cyberterrorism-project.org/wp-content/uploads/2013/03/Cyberterrorism-Report-2013.pdf.
[58] 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.
[59] Kovacs, "Addressing India's Global Cybersecurity Concern."
[60] Ibid.
[61] Hollis, "An e-SOS for Cyberspace."
[62] Duncan Hollis and Tim Maurer, "A Red Cross for Cyberspace," *Time*, February 18, 2015.
[63] Kovacs, "Addressing India's Global Cybersecurity Concern."

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.[64] 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.[65]

Democratic Deficit

There is growing recognition of the democratic deficit in Internet governance, and there has been some movement on this front. In addition, the realization and recognition that voices from developing countries are underrepresented in global Internet governance fora across all stakeholder groups seems to be growing.[66]

Multilateral Responses

Agreements in the WSIS

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 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."[67] 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.[68] The WSIS+10 outcome document also reaffirmed that "the same rights that people have offline must also be protected online."[69]

Role of the Multilateral System

Ever since this 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. Greater

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

[65] 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); Global Commission on Internet Governance, *Finding Common Ground: Challenges and Opportunities in Internet Governance and Internet-Related Policy* (2014).

[66] 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 developing country voices affects a wide range of sectors.

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

[68] 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.

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

involvement of the UN or other multilateral actors in Internet governance is often met with doubt, criticism, or even hostility. 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 such a shift could entail.[70]

Nonetheless, a growing number of actors recognizes that, depending on the issue and the stage of discussions, there is space for multilateralism *and* multi-stakeholderism in Internet governance. 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. In several areas, cooperation, norm development, and, ultimately, rule setting could be beneficial.

VI. Recommendations

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.

Consolidating UN Venues Dealing with New Technologies and Cyberspace

The first set of recommendations touches on cross-cutting institutional challenges that require particular attention.

- Map UN venues dealing with new technologies: The UN system is addressing and using new technologies in many ways—from integrating them into its work on development and peace to building and clarifying norms to govern and secure the Internet. The UN is far from idle, but it is creating confusion through its piecemeal approach, which spreads decision making and consultation throughout the system. By one count, nine different UN bodies have dealt with cyber issues since the 1990s, and this does not include bodies such as the UN Human Rights Council, which has started to approach these issues from a human rights angle.[71] In order to involve more stakeholders, increase efficiency, and build norms in a timely manner, the UN Secretariat should help identify the different venue where new technologies are being discussed and addressed. This would also help streamline and consolidate efforts in the UN and outside of the UN to avoid duplication.
- Identify a UN focal point on cyber issues: With ongoing efforts in regional bodies 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 that collective regional approaches to questions of sovereignty and jurisdiction will harden the stances of member states in negotiations at the UN. The appointment of a clear focal point within the UN system for particularly pressing discussions might help avoid such a situation. This focal point could also function as a test case for the establishment of other focal points as the Internet governance system evolves and more issues come up for discussion in the UN.
- Recognize and build on multi-stakeholder approaches and build partnerships with private and civil society actors: If there is greater recognition of the role of civil

[70] Cooper, "Why Growing Up Is Hard to Do."
[71] Maurer, "Cyber Norm Emergence at the United Nations."

society and the private sector in the multilateral system, it is with regards to new technologies and cyberspace that this role can most readily become a reality. While the UN has a role to play regarding new technologies and digital innovations, it is not—and never will be—in the lead. In fulfilling its role, the UN needs to build on expert input and broad stakeholder buy-in. It needs to develop far more transparent and networked forms of multilateral governance. This requires that inputs and expertise from other stakeholders are accorded far greater pride of place across the multilateral system. At the same time, it also requires putting in place checks and balances to ensure that such an opening up decreases, rather than increases, its democratic deficit. ICTs can play a role in this, too. This will require the UN to develop mechanisms that provide for meaningful participation of relevant private sector and civil society stakeholders in intergovernmental negotiations.

- Ensure coherence among new mechanisms: The Technology Facilitation Mechanism, the technology bank for least-developed countries, and the Technology Framework share the common goal of facilitating access to and transfer of technology to developing countries. These new mechanisms have the potential to accelerate progress and support the achievement of the 2030 Agenda and the Paris Agreement. But because they are disconnected from one another, there is a risk of duplicating efforts and competing for resources.

Developing New Approaches and Norms

This second set of recommendation is at a more technical level, touching on norm development and new approaches to better address the emerging challenges and opportunities created by new technologies:

- Make the UN the depository and safe-keeper of big data: The UN could help gather, collect, and store data, especially from regions where the infrastructure is not safe or sufficient. Member states could give this mandate to the UN, which would have to create and implement safeguards for the data.
- Consolidate and build analytical capacity: The UN could help provide greater analytical and statistical capacity when member states lack it. This could facilitate economic and social development, as well as gathering and analyzing necessary data on climate change. This capacity already exists but is currently spread throughout the system.
- Crowdsource international negotiations: This is a bold and nascent concept, but some issues could gain from greater public consultations. The UN could build on the lessons from previous crowdsourcing efforts, including in the process of electing the next secretary-general.
- Recognize cyberspace as “global common good”: The UN could formally recognize that cyberspace should be used for “peaceful purposes” in the interests of humanity.
- Support confidence-building measures (CBMs): The UN and other multilateral actors could put in place CBMs at the regional and sub-regional levels to ensure the security and sustainability of cyberspace.

Annex I: Connect 2020 Agenda for Global Telecommunication/ICT Development

Goal 1: Growth
Enable and foster access to and increased use of telecommunication/ICT
Targets:

- Target 1.1: Worldwide, 55% of households should have access to the Internet by 2020
- Target 1.2: Worldwide, 60% of individuals should be using the Internet by 2020
- Target 1.3: Worldwide, telecommunication/ICT should be 40% more affordable by 2020

Goal 2: Inclusiveness
Bridge the digital divide and provide broadband for all
Targets:

- Target 2.1.A: In the developing world, 50% of households should have access to the Internet by 2020
- Target 2.1.B: In the least developed countries (LDCs), 15% of households should have access to the Internet by 2020
- Target 2.2.A: In the developing world, 50% of individuals should be using the Internet by 2020
- Target 2.2.B: In the least developed countries (LDCs), 20% of individuals should be using the Internet by 2020
- Target 2.3.A: The affordability gap between developed and developing countries should be reduced by 40% by 2020
- Target 2.3.B: Broadband services should cost no more than 5% of average monthly income in developing countries by 2020
- Target 2.4: Worldwide, 90% of the rural population should be covered by broadband services by 2020
- Target 2.5.A: Gender equality among Internet users should be reached by 2020
- Target 2.5.B: Enabling environments ensuring accessible telecommunication/ICT for persons with disabilities should be established in all countries by 2020

Goal 3: Sustainability
Manage challenges resulting from telecommunication/ICT development
Targets:

- Target 3.1: Cybersecurity readiness should be improved by 40% by 2020
- Target 3.2: Volume of redundant e-waste to be reduced by 50% by 2020
- Target 3.3: Green House Gas emissions generated by the telecommunication/ICT sector to be decreased per device by 30% by 2020

Goal 4: Innovation and Partnerships
Lead, improve and adapt to the changing telecommunication/ICT environment
Targets:

- Target 4.1: Telecommunication/ICT environment conducive to innovation
- Target 4.2: Effective partnerships of stakeholders in telecommunication/ICT environment

Annex II: Annotated Bibliography

Resolutions by the United Nations General Assembly (UNGA)

UNGA Resolutions on "Information and Communications Technologies for Development"

Resolutions 62/182 (2007), 63/202 (2008), 64/187 (2009), 65/141 (2010), 66/184 (2011), 67/195 (2012), 68/198 (2013), 69/204 (2014), and 70/184 (2015)

These resolutions, passed by the UNGA from 2007 to 2015, recognize the potential of ICTs to support development. Each resolution addresses "digital divides" between developed and developing countries, gender, and the important role of governments in effectively using ICTs.

UNGA Resolutions on "Developments in the Field of Information and Telecommunications in the Context of International Security"

Resolutions 53/70 (1998), 54/49 (1999), 55/28 (2000), 56/19 (2001), 57/53 (2002), 58/32 (2003), 59/61 (2004), 60/45 (2005), 61/54 (2006), 62/17 (2007), 63/37 (2008), 64/25 (2009), 65/41 (2010), 66/24 (2011), 67/27 (2012), 68/243 (2013), 69/28 (2014), and 70/237 (2015)

From 1998 to 2015, the UNGA passed resolutions urging "states to promote further at multilateral levels considerations of existing and potential threats in the field of information security," addressing the importance of limiting threats in this field and strengthening the security of global information and telecommunications systems.

UNGA Resolution 55/2 (2000) on the Millennium Declaration

The United Nations Millennium Declaration states the importance of universal access to ICTs in paragraph 20, thus highlighting the importance of ICTs in the development process.

UNGA Resolution 69/313 (2015) on the Addis Ababa Action Agenda of the Third International Conference on Financing for Development)

Paragraph 123 of the Addis Ababa agenda calls for establishing a Technology Facilitation Mechanism, which is to be launched at the UN Summit for the adoption of the post-2015 Development Agenda. It consists of an interagency UN team on science, technology and innovation and a collaborative annual multi-stakeholder forum on science, technology and innovation for the sustainable development goals.

UNGA Resolutions on Cybersecurity

Resolutions 55/63 (2001) and 56/121 (2002) on "Combating the Criminal Misuse of Information Technologies"; 57/239 (2003) on "Creation of a Global Culture of Cybersecurity"; 58/199 (2004) on "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures"; and 64/211 (2010) on "Creation of a Global Culture of Cybersecurity and Taking of Stock of National Efforts to Protect Critical Information Infrastructures"

These resolutions acknowledge the importance of cybersecurity with the rapid advances in the use of information technology by governments, corporations, other organizations, and individuals and how the implementation of cybersecurity must adhere to the principles of democracy and the free flow of information.

UNGA Resolution 56/183 (2001)

Taking into account the rising prominence of ICTs in development and the increased need for security in the information field, this resolution endorsed the WSIS and established holding it in two phases: the first phase in Geneva (December 10–12, 2003) and the second in Tunis (November 16–18, 2005).

UNGA Resolution 59/220 (2003)

This resolution recognized the results of the 2003 Geneva Summit, the first phase of the WSIS. It included a statement of political will to "create a common desire and commitment to build a people-centered, inclusive and development-oriented Information Society" and a concrete plan of action to achieve the foundations for an Information Society for all, resulting in the **Geneva Declaration of Principles** and the **Geneva Plan of Action**.

UNGA Resolution 60/252 (2006)

This resolution recognized the results of the 2005 Tunis Summit, the second phase of the WSIS. This second phase focused on reaffirming the commitments made in the first phase and building on them through the discussion of financial mechanisms for bridging the digital gap and Internet governance. The two main documents of the second phase are the **Tunis Commitment** (paragraph 111 of which requests the UN General Assembly to conduct a review of the implementation of the outcomes of the first and second phases of the WSIS in 2015) and the **Tunis Agenda for the Information Society.** The Tunis Agenda also facilitated the creation of the **Internet Governance Forum (IGF)**, which is a forum for multi-stakeholder discussion on issues pertaining to the growth of the Internet.

UNGA Resolution 70/125 of the WSIS+10

From December 15 to 16, 2015, the WSIS held a high-level meeting (WSIS+10) to review the implementation of the outcomes of the WSIS. The outcome document highlights issues related to ICTs for development, enhanced multilateral cooperation on Internet governance, human rights in the information society, and building security in the use of ICTs.

Other Literature

Azzopardi, Myrna. "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, no. 1 (2013): 174–184.

Betts, Alexander, and Louise Bloom. *Humanitarian Innovation: The State of the Art*. United Nations Office for the Coordination of Humanitarian Affairs, 2014.

Blanco, Gabriel, Heleen de Coninck, and Laura Würtenberger. *The Technology Mechanism under the UNFCCC: Ways Forward*. Policy Brief, Climate Technology and Development, Climate and Development Knowledge Network and ECN, October 2012.

Broadband Commission for Digital Development. *The State of Broadband*. Geneva: International Telecommunication Union and the United Nations Educational, Scientific and Cultural Organization, 2015.

Centre for International Governance Innovation (CIGI). *Finding Common Ground: Challenges and Opportunities in Internet Governance and Internet-Related Public Policy*. Waterloo: CIGI, 2014.

Cooper, Mark. "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): 45–134.

Deep, Alex. "Hybrid War: Old Concept, New Techniques. *Small Wars Journal*, March 2, 2015.

Emmerson, Ben. *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.

Expert Panel on Technology and Innovation in UN Peacekeeping. *Performance Peacekeeping: Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping*. UN Department of Peacekeeping Operations, 2014.

Fleck, Dieter. "Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New *Tallinn Manual*." *Journal of Conflict and Security Law* 18, no. 2 (2013): 331–351.

Freedom Online Coalition Working Group. "Mapping Cybersecurity: A Visual Overview of Relevant Global Spaces in 2015." May 2015.

Global Commission on Internet Governance. "Toward a Social Compact for Digital Privacy and Security." Center for International Governance Innovation and Chatham House, 2015.

Hathaway, Oona A. and Rebecca Crootof. "The Law of Cyber-Attack." Yale Law School Faculty Scholarship Series, Paper 3852, 2012.

Heyns, Christof. *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*. UN Doc. A/68/382, September 13, 2013.

Hoffman, Frank G. "Hybrid Warfare and Challenges." *Small Wars Journal* 52, no. 1 (2009): 34–39.

Hollis, Duncan B. "An e-SOS for Cyberspace." *Harvard International Law Journal* 52, no. 2 (2011): 374–432.

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

Independent Expert Advisory Group on a Data Revolution for Sustainable Development. "A World that Counts: Mobilising the Data Revolution for Sustainable Development," 2014.

Internet Society. "WSIS+10 Review Process 2015: Government Positions on WSIS Implementation." October 16, 2015.

Letouzé, Emmanuel. *Big Data for Development: Challenges & Opportunities.* New York: United Nations Global Pulse, 2012.

Macdonald, Stuart, Lee Jarvis, Thomas Chen, and S. Lavis. "Cyberterrorism: A Survey of Researchers." Cyberterrorism Project Research Report no. 1, Swansea University, 2013.

Mancini, Francesco, ed. *New Technology and the Prevention of Violence and Conflict*. New York: International Peace Institute, 2013.

Maurer, Tim and Scott Janz. “The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context.” The International Relations and Security Network, Swiss Federal Institute of Technology Zurich, October 17, 2014.

Maurer, Tim. “Cyber Norm Emergence at the United Nations: An Analysis of the UN‘s Activities Regarding Cyber-security.” Belfer Center for Science and International Affairs, Harvard Kennedy School. Discussion Paper 2011-11, September 2011.

Meyer, Paul. "Gaps in Cyberspace Governance Abound, 10 Years after UN World Summit." OpenCanada.org, January 7, 2016.

NATO StratCom Centre of Excellence. *Analysis of Russia’s Information Campaign against Ukraine*. Riga: NATA StratCom Centre of Excellence, 2014.

Nye, Joseph S. “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38.

Organization for Security and Co-operation in Europe. "Drones: An Up-and-Coming Newsgathering Tool for Journalists that Must Be Safeguarded, OSCE Representative Says, Issuing Recommendations." March 3, 2016.

Puig Larrauri, Helena and Patrick Meier. *Peacekeepers in the Sky: The Use of Unmanned Unarmed Aerial Vehicles for Peacekeeping*. Geneva: ICT4Peace Foundation, 2015.

Raitasalo, Jyri. “Hybrid Warfare: Where’s the Beef?” *War on the Rocks*, April 23, 2015.

Raymond, Mark, Aaron Shull and Samantha Bradshaw (forthcoming). “Rule-Making for State Conduct in the Attribution of Cyber-Attacks.” In *Constructive Powers and Regional Security in East Asia*.

Renda, Andrea. “Cybersecurity and Internet Governance.” Council of Councils, May 3, 2013.

Saran, Samir. “International Internet Governance.” In *Indo-US Cooperation on Internet Governance and Cybersecurity,* edited by Steven P. Bucci, Lisa A. Curtis, Mahima Kaul, C. Raja Mohan, Paul Rosenzweig, and Samir Saran. New Delhi: Observer Research Foundation and Heritage Foundation, 2014.

Seton Hall University, School of Diplomacy and International Relations. "Working Paper: Why Do IGOs Tweet Differently?" June 2015.

Schwab, Klaus. "The Fourth Industrial Revolution: What It Means, How to Respond." weforum.org, January 14, 2016.

Stauffacher, Daniel, William Drake, Paul Currion, and Julia Steinberger. *Information and Communication Technology for Peace: The Role of ICT in Preventing, Responding to and Recovering from Conflict*. New York: United Nations ICT Task Force, 2005.

Synkov, Dmitriy. "Tools and Trends in Peace and Technology." #PEACETECH, March 2015.

UNHCR. “Innovation at UNHCR.” 2014.

UNICEF Global Innovation Centre. “Innovation at UNICEF.” 2014.

Van der Spuy, Anri, and Nicolas Seidler. "WSIS+10 Series: From Access to Trusted Access: Human Rights in the WSIS+10 Review." December 17, 2015.

Waugaman, Adele. *From Principle to Practice: Implementing the Principles for Digital Development.* Washington DC: The Principles for Digital Development Working Group, 2016.

World Bank Group. *Digital Dividends.* Washington DC: The World Bnank, 2016.