New Technology for Peace & Protection: Expanding the R2P Toolbox

Lloyd Axworthy & A. Walter Dorn

Abstract: New technological advances in areas such as digital information, algorithmic forensic data analysis, autonomous surveillance vehicles, advanced robotics, and multispectral sensors (sometimes all working together) can help avert war, introduce more effective peacekeeping and peacemaking initiatives, lessen the impact of conflict on innocent people, and help rebuild war-torn states. When international humanitarian action becomes urgent, by way of knowledge gained through such technologies, then those same peace applications can be used to reduce harmful forms of intervention and to ensure that enforcers are abiding by international law and UN guidance. An ethical failure occurs when such technologies exist to save lives, reduce risks, and secure peace, but are not employed.

One of the key challenges for the international community is to apply new technology under effective international authority to support peace. Fortunately, as will be shown, institutional reform is emerging to enable new peace strategies and new UN applications for the preventative, proactive, and protective use of new technologies. Another very promising development is the increasing technological capacity of local populations to provide for their own protection. The Norwegian Centre for Humanitarian Studies rightly asserts:

> Affected populations are the primary responders in disasters and conflict zones, and actively use information technology to self-organize, spread information about their condition, call for aid, communicate with humanitarian actors, and demand accountability. New technologies also have the potential to put responders at the center of the entire life cycle of humanitarian action.[1]

Exciting prospects lie in advancing population-centric early-warning systems to enhance prevention through the quantum leap in information tech-

LLOYD AXWORTHY, a Foreign Honorary Member of the American Academy since 2003, is Chair of CUSO International and former Minister of Foreign Affairs of Canada.

A. WALTER DORN is Professor of Defense Studies at the Royal Military College of Canada and the Canadian Forces College.

(**See endnotes for complete contributor biographies.*)

doi:10.1162/DAED_ a_00414

nology, big data collection, and analysis. These can substantially improve the ability to anticipate looming issues and enable those directly affected to become involved in a preventative response.

For example, the United Nations Development Programme (UNDP) is testing a volunteer, community-based conflict prevention and resolution approach in its Early Warning and Early Response (EWER) program in Timor Leste, where local volunteers are recruited as monitors to report on violent outbreaks or situational change. The information is fed into the EWER computer system, where regular alerts, situation reviews, and recommendations for action are produced.[2] The next step is to see how local populations can be mobilized and new technologies, such as automated surveillance vehicles, can be used to verify burgeoning outbreaks and help local populations quell incipient sources of violence and rights violations. Technology can be an empowering instrument for the protection of people.

We use the responsibility to protect (R2P) framework to present this case of technology for peace and protection. The R2P concept was a breakthrough in the world's understanding of how to deal with mass atrocities. After the horrors of Somalia, Rwanda, and Srebrenica in the first half of the 1990s and NATO's bombing in Kosovo in 1999, the international community was wrestling with what to do about future humanitarian violations and how to decide on interventions. At the beginning of the new millennium, scholars and practitioners in the International Commission on Intervention and State Sovereignty, established by Canada, adopted an ancient approach – the just war theory – to tackle the modern challenge of humanitarian intervention.

As just war theorists posited a "presumption of peace," the commissioners suggested that the international community should *not* intervene forcefully unless certain criteria were met. First and foremost, the state in question had primary responsibility for its people since "sovereignty implies responsibility." Only when the state was "unwilling or unable" to protect its population, "the principle of non-intervention yields to the international responsibility to protect."[3] But the international community should only use force after the nonmilitary options had been explored and were deemed inadequate, as enunciated in the just war criteria of "last resort." The "just cause" threshold for military intervention was "large-scale loss of life" or "large-scale 'ethnic cleansing.'" The right intention was to "halt or avert human suffering." There should be "reasonable prospects" of achieving that goal and the means should be proportionate, applying the minimum force necessary. And for "right authority" to authorize intervention, the Commission clearly pointed to the UN Security Council. It called on the Council's Permanent Five not to exert their veto power if the majority of the Council authorized forceful intervention. If the Council failed to take action, the options included authorization by the General Assembly or even regional organizations.

The Commission foresaw the problems of forceful intervention and rightly placed the priority on the *prevention* of atrocities beforehand. It also recognized the need for *rebuilding* afterward. Thus, the three "specific responsibilities" of R2P are: to prevent, to react, and to rebuild. Again, the R2P approach parallels just war thinking in proposing three phases: *ad bellum*, *in bello*, and *post bellum* (before, during, and after war/conflict). In the preventive stage, the international community must help states protect their populations by addressing both root and direct causes of conflict. To "react," it may need to assume the coercive powers of the state in order to save lives; to "rebuild," it must help create the necessary national capacity for a sustainable peace.

This R2P framework was adopted by world leaders at the 2005 World Summit. The international leaders pledged to "support the United Nations in establishing an early warning capability." This required creating some form of intelligence and analysis capability at UN headquarters. Unfortunately, the United Nations has been unable to establish such a capability despite decades of proposals and efforts within the organization. In the late 1980s, the United Nations created an Office for Research and the Collection of Information, but that office could not implement its early-warning mandate. The follow-on in the 1990s, the Information and Research Unit, was more capable because it was composed of intelligence officers from four of the five Permanent Members (excluding China). However, it was disbanded in 1999 when the developing world pushed through a General Assembly resolution to remove gratis personnel from UN headquarters, with the idea of replacing them with paid UN staff. In 2000, the Brahimi Report on UN Peace Operations proposed a UN-staffed Information and Strategic Analysis Secretariat, but this never gained the approval of the UN member states. So, apart from the desk officers who are overwhelmed with following their respective countries, UN headquarters still lacks the analytical capacity for early warning and rapid reaction. Fortunately, the evolution of intelligence analysis in field missions is more encouraging, especially with the creation of Joint Mission Analysis Centres, where information from a large number of sources is considered to create actionable intelligence to help fulfil the mission mandate. The protection of civilians mandate represents the noble but not yet achieved attempt to implement R2P in twenty-first-century UN field operations.

While political progress at the world organization has been slow and halting, technology has been advancing at breakneck speed. The information age saw the rise of the Internet, from the first website in 1991 to ten million at the end of the century to an astounding one billion websites in 2015.[4] The number of Internet users grew from three hundred million in 2000 to three billion today. The expansion of online information proved to be exponential – similar to Moore's law of doubling every two years – as data, software, and hardware have continued to play a constant game of tag. The performance-to-price ratio of computers has increased a billionfold since the early models. And the rise of mobile phones, with more subscriptions than people on earth, has meant that mobile data alone for 2014 was thirty times larger than the data exchanged through the global Internet in 2000.[5] In the twenty-first century, email and social media have revolutionized the way people connect and communicate, including in remote parts of the developing world.

In other fields, technological progress has also been tremendous, if not so dramatic. New generations of sensors have increased in range, accuracy, and user-friendliness, while decreasing in size and weight. The rapid convergence of previously separate technologies has been enhanced by miniaturization. Cameras, for example, are now ubiquitous because they are integrated into mobile phones. And new forms of robotics create innovative ways to enhance action at a distance with lesser risk.

Surely, this tremendous technological progress can be used to advance the R2P cause. Is it not part of the responsibility to apply these new technologies to protect people, to enable peace operations, and to make international interventions more accountable, effective, and safer? In this essay, we explore the ways modern technology can help implement the R2P goals to prevent, react, and rebuild, especially to help hasten the capacity of international organizations.

> The League of Nations . . . should be the eye of the nations to keep watch upon the common interest, an eye that does not slumber, an eye that is everywhere watchful and attentive.
>
> – Woodrow Wilson,
> Paris Peace Conference,
> January 25, 1919[6]

Technology provides a means to help fulfill Wilson's vision in ways unimaginable when the international organization for peace was just beginning. The information revolution of the twenty-first century can greatly assist the United Nations, even if the world organization has not yet developed the analytical capability to fully benefit. By tapping into new technologies and expanding the UN's "infosphere," the secretary general can better fulfill his or her UN Charter (article 99) mandate to warn the Security Council of "any matter which in his [or her] opinion may threaten the maintenance of international peace and security." Early warning – the first step of prevention – is information-intensive, requiring accurate observation from many sources of emerging threats and a deep understanding of the motivations behind acts of violence. The key is to combine human communication with technology-aided information-gathering on ground realities, including observation from above.

Aerospace observation, by satellite or aircraft, offers important ways to look at activities on the ground.[7] Satellite reconnaissance, once the sole preserve of the two Cold War superpowers, can now be performed by a group of image analysts with a modest budget to purchase commercial imagery. The United Nations can move from pictures for mapping (cartography) to operational imagery contained in real-time geographic information systems (GIS). Demonstrating progress, the United Nations made a major step in aerial reconnaissance with the deployment of unmanned aerial vehicles (UAVs) to the Democratic Republic of the Congo in December 2013. The unarmed UAVs have already saved lives, for instance, by spotting a sinking passenger ship in Lake Kivu, allowing UN rescue boats to launch immediately.

As shown in the Congo, UN peace operations are an important way for the international community to have a presence in conflict-prone areas. The deployment first gains the consent of the host state and usually of the main conflicting parties as well, but its mandate derives from the Security Council. Military, police, and civilian peacekeepers in modern operations help implement R2P through prevention, reaction, and rebuilding. UN field workers promote security, nation-building, rule of law, human rights, humanitarian assistance, and peace processes. In all of these tasks, technology can play a major role, with much improvement possible at the United Nations.[8]

For instance, GPS tracking would allow a UN mission to follow its vehicles in real-time, especially in dangerous areas. But the United Nations has so far been unable to set up a GPS system to keep track of its vehicles and peacekeepers in real time. The United Nations is now exploring how to upgrade its asynchronous Carlog system to a real-time system to give a current and complete picture. This would prove invaluable during ambushes and search and rescue operations, and in the retrieval of stolen vehicles.[9] Tracking the UN blue forces and civilians, for example, by their cell phone location, will make them safer and more effective. It could even usher in a new era of "precision peacekeeping," when the forces are more carefully positioned and enabled to do intelligence-led operations. The "digital peacekeeper," fully outfitted with the latest technology for positioning, tracking, sensing, and communication, can be part of the new face of peacekeeping.

The sensor and smartphone revolutions mean that new and miniaturized sensors can be included in phones and geolocated. Images and video recordings of atrocities can be captured and transmitted immediately. Some human rights organizations are exploring phones with memory-erase capabilities, so if perpetrators seize or steal their phones, the information is safely stored far away for future judicial or fact-finding purposes. For instance, the International Bar Association created the "eyeWitness to Atrocities" app for mobile cameras, designed to record video and take photos with authentication. Metadata associated with the image files specifies where and when the imagery was taken so the information can be entered as probative evidence for investigations and court cases.[10]

The amazing spread of cellphones in the world's population, with signal reception now available in some of the smallest villages of the developing world, means that the United Nations can tap into a wealth of new information sources for population-centric operations. In "participatory peacekeeping," such as that being explored in Timor Leste, the people themselves can help identify threats and criminal activity and monitor cease fires or any aberrant behavior of protagonists. Thus, human security is fostered by local communities to create a "coalition of the connected" that provides "protection through connection." Early warning reports from social media can be verified by UN observers and quick responders on the ground.

Gaining from the cellular revolution, the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo established a Community Alert Network to reach out to faraway villages in that vast country. The mission distributed cell phones and SIM cards to key local leaders who could call the mission upon seeing signs of impending danger – a drastic improvement from earlier times when villagers were told to bang on pots! UN peacekeepers can then be dispatched in response.

What matters to the protected people should matter to the peacekeepers and other interveners. For such expanded mandates, multidimensional UN operations need more than conventional intelligence; they need "human security intelligence."[11] This synergistic approach draws upon a range of human factors to build the bigger picture. It entails tracking factors relating to both "freedom from fear" (security) and "freedom from want" (development). Open-source intelligence is supplemented by active information-gathering on traditional security threats and nontraditional threats like problems with food, health, the environment, and the economy. These then need a host of technologies to address the root causes of conflict before violence escalates. While too numerous to be described in detail, some of these technologies are reviewed below.

For prevention, digital verification procedures (images, text, statistics, and other data) can reveal trend lines of potential conflicts and the buildup of preconditions for ethnic or warlord violence. Once violence has flared up, impartial evidence-gathering by peacekeepers, human rights officers, and criminal court/tribunal investigators can help determine culpability. Permanent digital evidence in the hands of international law enforcement can be a deterrent against brutal practices and corruption.

Numerous data sources, both human and technological, should be tracked in multidimensional operations. Admittedly, data fusion is a big challenge in the age of big data. But increasingly intelligent sorting algorithms help bring together both structured and unstructured data into intelligible collation and visual displays. New media journalism and social media sources can be added to sensor intelligence and direct UN observation to gain insights into "patterns of life" and the realities of the "peacekept" society. The motto "every soldier a sensor" is never more relevant than in peace operations, where observation and contact with local populations is critical. "Technological intelligence" and human intelligence are complementary since one can corroborate and help overcome the weakness of the other.

Fortunately, in the information age, knowledge of all kinds spreads fast in the interconnected world. This includes bad as well as good news. If major atrocities happen in one region of the world we can learn about them within hours. We can no longer say "we did not know so we did not act!" This new knowledge creates a stronger imperative for intervention, preferably of the proactive and preventive kind but, if necessary, also of the forceful military kind. Preventive systems can provide the information needed to determine if military force is required beyond what peacekeeping can provide. Sometimes that necessitates military intervention by international coalitions or regional alliances.

Accurate, timely information is as important to the prevention of unjust international intervention as it is to the support of a just action. The United Nations was unable, in part because of inadequate surveillance technology, to gain sufficient evidence in Iraq to stop the 2003 U.S.-led invasion. The United Nations had inspectors on the ground who did not corroborate the false claims made by the Bush administration, but they did not have enough foolproof "evidence of absence" of alleged weapons of mass destruction to halt the march to war.

By contrast, there are dire times and circumstances when the international community urgently needs to move from prevention to reaction, including force as a last resort, even against the will of the state in question. The growing capacity to assemble credible evidence and witness accounts means that decision-makers at the Security Council or regional organizations must demonstrate more substantive grounds for their decisions. Impartial data can assist the present reform effort to encourage a constructive abstention policy in the Security Council for humanitarian intervention rather than the veto. Better UN data could show if the Permanent Five votes were to meet real humanitarian needs rather than be trumped up polemic exchanges between the major powers. In other words, just war should be based on the grounds of justice and humanitarian need, not on propaganda or a special pleading of national interest.

Whatever the justifications or outcomes for forceful intervention, the international community has a responsibility to monitor those who are enforcing international law or who claim to act on behalf of humanity. Civilian casualties should, of course, be minimal, if not zero. This means watching the "enforcers" to help them maintain their responsibility *while* protecting. So the United Nations needs to have its own advanced monitoring system. As previously mentioned, this is lacking. The UN Secretariat has mostly relied on media reports to get a sense of what was going on, for instance, during interventions like the First Gulf War and the 2003 invasion of Iraq. The world organization needs many of the monitoring technologies mentioned above, including satellite reconnaissance.

During forceful interventions by coalitions, sometimes done against the will of the state, the United Nations' role is primarily humanitarian assistance. This can also benefit from technologies, for example, for protection and shelters (tough weather-proof materials), power (fuel, wind, and high-efficiency solar), communications (radios), lighting (solar-powered and motion-detecting outside tents), food safety, water purification, telemedicine, and others. Also the transport and delivery of humanitarian aid can be enhanced by asset management with radio frequency identification (RFID), tracking devices, and advanced seals and tags.

Sometimes UN peace operations themselves have taken robust enforcement action to protect civilians, even in the absence of coalition forces. At those times, some technologies proved pivotal, like the night vision equipment and aerial reconnaissance in Haiti in 2006 and 2007.[12]

After enforcement action has been taken by a coalition, an alliance (such as NATO), or a peacekeeping operation, the responsibility to rebuild comes into full play. Without proper rebuilding, conflict-prone societies may relapse into violence or civil war, as was seen in Libya and Iraq. Here again, in peacebuilding, UN technology has a role to play.

In population-centric peacebuilding operations, it is essential to communicate directly and continuously with the citizenry. The United Nations can have its own broadcasts by radio or social media to provide impartial, verified information to counter the falsehoods from former conflicting parties and the misinformation induced by the fog of war. Distribution of solar-powered and wind-up radios can ensure that the population has access to such information. The UN mission can also send and receive critical information through a text-messaging system, email, or the Internet.

UN measures are needed to counter the public propaganda strategies and misinformation campaigns of conflicting partners. The United Nations should expose false information. For instance, the Russian communication strategy in Crimea and Eastern Ukraine or the effectiveness of ISIL messaging must become a subject of focused attention with enhanced technical capacity available to UN officials and observer missions.

In the future, the United Nations might develop a capacity for cyber peacekeeping to prevent cyber wars between nations and between online actors. The Internet belongs to the people of the world and so some measure of governance is needed from the world body.

During transitional justice, before a fully empowered court system is established in war-torn countries, bodies like truth and reconciliation commissions and international tribunals can help to expose and punish crimes against humanity and war crimes. But the needed witness testimony is typically fraught with partiality and fear. Perpetrators often intimidate witnesses, and courts have difficulties finding reliable witnesses to take the stand. Fortunately, assurances can be given of visual and voice anonymity in the courtroom, achieved through face pixilation and voice-modification technology. Witness testimony can be corroborated or dismissed based on scientific and technology-based evidence, like the eyeWitness app mentioned above.

Similarly, the misbehavior by some peacekeepers, including sexual exploitation and abuse or black market activities, is a matter of deep concern and requires a solution. The capacity to monitor and provide witness verification of misbehavior can and must be explored by the United Nations using increased surveillance and reporting techniques tied to a community-based reporting system. Mandatory body cameras on peacekeepers could help prevent abuse on the job.

One of the key peacebuilding tasks after armed conflict is to clear mines and the other explosive remnants of war. Demining cries out for technological innovation. Deminers and local civilians are dying, losing limbs, and proceeding at a snail's pace because advanced detection and excavation devices are not available to them. Millions of mines remain hidden in the ground, waiting to carry out their deadly function or to be removed safely. To be sure, some research and development has been initiated since the 1997 Anti-Personnel Mine Ban (or Ottawa Convention), but these projects have mostly been unworkable, underfunded, or unexploited. The question remains: why are we still using World War II technologies, including primitive hand-held metal detectors and bayonet-style tools, to find and remove land mines when modern technologies like robotic machines can do the work independently or, at least, actively assist the deminers? The possibilities need to be explored.

In the past decade, the United States and other militaries have developed and deployed very sophisticated technologies for IED (improvised explosive device) detection and removal that have saved many soldiers' lives in Iraq and Afghanistan. Remote-controlled robots, like the Talon series, have figured large in military operations. Many of these technologies could be used for humanitarian demining, yet their technical details remain highly classified. However, there is bound to be some spillover as the companies producing the military hardware look for new markets. Meanwhile, technological advances in the medical sciences can save the lives of increasing numbers of mine victims. It is even possible to produce prosthetics with local 3D printers.[13]

More broadly, the development community has experienced a shift in thinking, allowing both security and technology tools to be used directly by locals (with training). The international community has created the Sustainable Development Goals (SDGs) to replace the largely successful fifteen-year Millennium Development Goals (MDGs). So a new look can be taken of the many ways that technology can boost developing economies while reducing pollution and greenhouse gases. New land, made available after demining, can be better harvested in a sustainable fashion. The practice of precision agriculture with UAVs, now employed by farmers in developed countries, can be transferred to the developing world. New technologies can help not only grow crops, but also bring them to market. For instance, cellphone and Internet-connected families can better determine when and where to bring their products for sale.

Technologies can help humanitarian actors boost the *post bellum* economy by providing digital payments ("mobile money" that can go where aid workers cannot) and "digital food" (e-cards to make purchases at authorized locations, rather than getting supplies off aid trucks). Electronic voting systems can help reduce the time to vote, to accurately count, and then to announce elections results, thus reducing post-election violence. Furthermore, biometrics and smart ID cards can reduce voter fraud.

These are just a sample of the amazing applications of science and technology for development and security. But the introduction of technology can also pose dilemmas and problems that need to be confronted and solved. This aligns with the basic dilemmas of intervention itself.

For some governments and international organizations, early warning itself, made easier through technology, poses a dilemma. It adds an immediate responsibility to confront the violence, whether observed or predicted, even if the means are meager and chances of success are poor. Regardless, the possibility of successful intervention is increased with early warning, and with the world watching, international accountability becomes a strong pressure.

After UN operations are deployed, the peacekeeper's dilemma is similar: when conflict situations become hot and most in need of continuous observation or robust intervention, the danger is greatest for UN personnel. Peacekeepers often have to evacuate for their own safety. Witness, for example, the short-lived United Nations Supervision Mission in Syria (2012), whose observers were fired upon and routes blocked when they attempted to leave their hotels, forcing them to return while the population continued to suffer from war and extreme resource deprivation. Technologies are available to provide a partial solution, especially unmanned air and ground vehicles (UAVs and UGVs).

Not only observation – but also force – can be applied more remotely than ever before, as seen by missiles and bombs dropped in Libya by NATO aircraft and drones during the UN-mandated operation. However, remote observation and long-range weapons raise their own set of dilemmas. The higher an aircraft (manned or unmanned) flies above its target, the less vulnerable it is to hostile fire, but the less accurate are its observations of targets and firepower. So the dilemma is: how close to get to the ground? A balance between safety in the air and on the ground needs to be achieved.

A related dilemma has arisen because of the capacity for remote viewing in real time. Sometimes officers high up the chain of command of an intervention or peacekeeping force might be tempted to direct the individual soldiers whom they observe on the screens. The "tactical general" is to be avoided because the layers of command have a purpose and because what is visible on the 2D screen cannot tell the whole story or give the entire situation on the ground.

Remote cameras on UAVs, UGVs, or in fixed positions can mean more and better viewing from mission headquarters, in safer locations "behind the wire." This might mean that peacekeepers or armed interveners are less willing to venture outside their base, even though it is vital to make contact with local populations.

This dilemma could also apply to the humanitarian community. If remote means of route reconnaissance and aid delivery are developed (such as airdropping supplies from UAVs), the humanitarians could become disconnected from the populations they serve. This problem of "bunkerization" of aid workers was seen in Somalia in recent decades, where international workers rarely left the confines of the Mogadishu airport during visits and only received reports there from local staff.

More generally, the influx of new information from remote technologies (terabytes per day from a single UAV) can lead to "information overload and underuse." When so much data is flowing it is harder to pick the images or situations most in need of viewing and analyzing. As with the problems described above, it is a question of finding the right balance. There may be too much or too little information, or the level of information could be "just right." The same is true for finding the right level of complexity of sensors.

Certain advanced technologies might prove too sophisticated or unworkable in some developing areas of the world, especially with insufficient or untrained personnel. Technology that is too advanced might not be adopted because it is too foreign for developing-world peacekeepers or for the local population. In addition, technology often requires its own infrastructure, like reliable electric power, that may not be available in conflict zones, though advances in solar power are helping. Also, devices might not be able to operate in the harsh climates found in some missions. For instance, networked computer servers need air-conditioned rooms, which are harder to keep cool under the hot sun and with intermittent power.

The expanding digital divide between peacekeeping contingents could create a "have" and "have not" distinction, though this exists in any case. The divide could further marginalize those without growing technological access. Clearly the new technology will require a new training investment at the United Nations and other international agencies to expand technological proficiency.

That some technologies can do tasks better than soldiers suggests a potential tension between humans and technologies, but on-the-ground peacekeepers remain essential and can be made more mobile and responsive with technology. Properly incorporated, technology and humans are complementary, not competitive: technology enables humans to do their job easier, better, and safer. Overstretched UN missions can better deploy their peacekeepers.

There is also a need to protect "humanitarian space," keeping the military and its technologies (particularly weapons) at a respectful distance from humanitarian actors. For instance, if surveillance imagery is shared between militaries and humanitarians, then the distinction could be blurred to the detriment of both, especially in the eyes of some conflicting parties. Similarly, some humanitarians view technology producers in the private sector as being only profit-driven, just as they view the military as being combat/enemy-centric. More often, though, industry and the military have more than one motive and more than one mode of operation, including humanitarian ones.

Similarly, some locals may view technology as Western-imposed and not organically or indigenously developed. This may mean that the technology is not adopted, and some projects could become white elephants, unless they are carefully planned and managed. Here, training and education are needed for a well-informed population.

The widely recognized problem of threats to privacy and data security also applies to UN peace operations, both for the international staff and the local population being observed. The United Nations must adopt rules for "shutter control" to know when it is inappropriate to observe or record activities of individuals and groups who pose no threat. It must also properly secure its digital resources from attack by state and nonstate hackers. The protection of people necessitates the protection of data. With effort, the ingenuity for data protection can stay ahead of the ingenuity for intrusion and destruction.

Finally, of course, the technologies themselves can be problematic, even for advanced users. There are always risks of equipment or system failures. If technology fails, overdependence can lead to a loss of capability, even more than if the technology were never deployed in the first place. If it is true that "to err is human," then "to really screw up requires a computer!" There are many additional possibilities for computer-aided human errors, but such risks can be managed by competent technicians and staff.

R2P technology should be centered on the individual human being, whose life and dignity is to be respected and protected. Human interaction remains essential between the peacekeeper and the "peacekept." In the end, peace is a human endeavor that requires the human touch. But it is also one that can be assisted, enabled, and enhanced by technology. Modern innovation can help break down the barriers of language, race, religion, borders, and time.

For effective prevention, reaction, and rebuilding, R2P missions must embrace the local population, including by social media, crowdsourcing, and more connectivity in general. "Participatory peacekeeping" is a new technology-enabled paradigm that should be embraced by the United Nations. Translation software for voice and data can help bridge the gap between the peacekeepers and the peacekept.

Despite the tremendous advantages of technology, the world organization, which represents the average of the capabilities of the world's nations, should avoid *overreliance* on technology and find a proper balance. Still, there is much to harness in the power of science for altruistic purposes. The United Nations rightly prioritizes construction over destruction and ballot boxes over bullets. All of these UN actions can be technologically assisted.

The recommendations of the UN's Panel of Experts on Technology and Innovation in Peacekeeping deserve support. The United Nations should develop technology scouts and a technology center, innovation incubators, and field-testing programs, and encourage a new category of Technology Contributing Countries (TechCCs) to help peacekeeping. Encouragingly, the United States is now seeking to be a leading TechCC;[14] as is Singapore, with its offer to design a common information management platform for UN missions.[15] We advocate an Office of Science and Technology to inform both the secretariat and member states, especially developing ones, on technological developments that impact war and peace.

The High-Level Independent Panel on UN Peace Operations presented a report on governance and strategy that was rightly supportive of the role of technology and the recommendations of the earlier expert panel.[16] The United Nations now needs to implement many of these far-reaching recommendations so that technological enhancements can be achieved in the field. The UN Secretariat in New York also needs an analytical capability to handle the vast amounts of data that come from modern technology, social media, and its field operations.

UN structures need substantial improvement to implement a tech-enabled peace. The proposal for a new Peacemaking Council for Coordination and Oversight, advanced by the Commission on Global Security, Justice, and Governance, is well worth exploring. So are the ideas for UN standby and, eventually, standing peacekeeping forces, which could give the world organization the much needed capacity for rapid reaction. Well-trained and well-equipped forces are still hard to find. Standby forces could start off as units in their own national forces but be connected through frequent exercises enabled by modern information and communications technology. They could meet several times a year so they are familiar with each other and ready for rapid deployment to the field. But that is just a transitional step.[17]

It is time for a new peacekeeping formula: a UN standing force with technological enablers, possibly robotic sensors or "bots on the ground" to assist the human "boots on the ground." While it may prove to be an exceedingly difficult political issue to tackle, the creation of such a force and such technological enablers would greatly help implement R2P. The new UN soldiers could be recruited as individuals, specially trained and technologically equipped, with mandates and abilities for early preventive responses. A comprehensive emergency response service could be based on a network of regional centers, totaling about fifteen thousand or so civilian, military, police, and judicial personnel with a broad range of skills for deployment within forty-eight hours following UN authorization. New technologies could enhance the response time and capabilities of such a force. Even now, the training and integration of UN contingents can be enhanced through Internet communication, including by adapting modern gaming technology to build useful peacekeeping-training scenarios, by improved data analysis to launch prevention initiatives and determine strategic placement, and by early engagement with local populations. These might enable R2P performance superior to ad hoc "coalitions of the willing" in conflict areas.

International diplomatic/administrative capacity needs to match the new technology tools. The United Nations should immediately develop a refreshed roster of experts who are up-to-date, communication savvy, and believe in R2P. A technology-proficient professional cadre of officers would bring new competencies to bear and create a refurbished image of the United Nations.[18]

The United Nations and regional organizations, with civil society alongside, can now move toward "smart peacekeeping and smart peacemaking," where operations are technologically enabled and intelligence-driven. Advanced systems of new technology can help bring into being Wilson's "vigilant eye" for early warning and prevention, for improving diplomatic, economic, and, when necessary, forceful action for monitoring enforcers during R2P reaction, and for local reconstruction. From the just war tradition can arise a *just peace* practice using technologically enabled operations and interventions.

It would be unethical to do otherwise when the means are so apparent and advancing so quickly.

ENDNOTES

[*] Contributor Biographies: LLOYD AXWORTHY, a Foreign Honorary Member of the American Academy since 2003, is Chair of CUSO International. He served as Minister of Foreign Affairs in the Cabinet chaired by Canadian Prime Minister Jean Chrétien, and as President of the United Nations Security Council in 1999 and 2000. He was also President of the University of Winnipeg from 2004 to 2014. He is the author of *Navigating a New World: Canada's Global Future* (2003) and *Liberals at the Border* (2004).

A. WALTER DORN is Professor of Defense Studies at the Royal Military College of Canada and the Canadian Forces College. He has served as a consultant to the United Nations and with the UN's Panel of Experts on Technology and Innovation in UN Peacekeeping. He is the author of *Air Power in UN Operations: Wings for Peace* (2014) and *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations* (2011), and editor of *World Order for a New Millennium: Political, Cultural and Spiritual Approaches to Building Peace* (1999).

[1] Kristin Bergtora Sandvik, Christopher Wilson, and John Karlsrud, "A Humanitarian Technology Policy Agenda for 2016," Norwegian Centre for Humanitarian Studies, http://www.humanitarianstudies.no/2014/08/14/a-humanitarian-technology-policy-agenda-for-2016/.

[2] As described in the Belun Project, supported by New Zealand's Volunteer Service Abroad, http://VSA.org.nz and http://belun.tl/en.

[3] International Commission on Intervention and State Sovereignty, *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty* (Ottawa: International Development Research Centre, 2001), xi, http://www.walterdorn.net/pdf/Responsibility-to-Protect_ICISS-Report_Dec2001.pdf.

[4] See Internet Live Stats, http://www.internetlivestats.com/total-number-of-websites/.

[5] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020," white paper, February 1, 2015, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html.

[6] Woodrow Wilson, "Protocol of a Plenary Session of the Inter-Allied Conference for the Preliminaries of Peace, 25 January 1919," in *The Papers of Woodrow Wilson*, ed. Arthur S. Link, vol. 54 (Princeton N.J.: Princeton University Press, 1967), 265.

[7] A. Walter Dorn, *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations* (Tokyo: United Nations University Press, 2011), http://www.keepingwatch.net.

[8] A. Walter Dorn, "Smart Peacekeeping: Toward Tech-Enabled UN Operations," *Providing for Peacekeeping No. 13* (New York: International Peace Institute, 2016).

[9] A. Walter Dorn and Christoph Semken, "Blue Mission Tracking: Real-Time Location of UN Peacekeepers," *International Peacekeeping* 22 (5) (2015): 201, http://www.walterdorn.net/220.

[10] Wendy Betts, "Closing the Verification Gap," *International Justice Monitor*, July 7, 2015, http://www.ijmonitor.org/2015/07/closing-the-verification-gap/.

[11] Fred Bruls and A. Walter Dorn, "Human Security Intelligence: Towards a Comprehensive Understanding of Humanitarian Crises," in *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, ed. Christopher Hobbs, Matthew Moran, and Daniel Salisbury (New York: Palgrave Macmillan, 2014), 123–144, http://walterdorn.net/pdf/HumanSecurityIntel_Bruls-Dorn_OSI-Book_Palgrave-Macmillan_June2014.pdf.

[12] A. Walter Dorn, "Intelligence-Led Peacekeeping: The United Nations Stabilization Mission in Haiti (MINUSTAH), 2006–07," *Intelligence and National Security* 24 (6) (December 2009): 805–835, http://www.walterdorn.net/53.

[13] For more on 3D printed prosthetics, see http://3dprint.com/tag/3d-printed-prosthetic.

[14] The White House Office of the Press Secretary, "United States Support to United Nations Peace Operations," press release, September 28, 2015, http://www.defense.gov/Portals/1/Documents/pubs/2015peaceoperations.pdf.

[15] United Nations News Centre, "UN and Singapore Agree to Develop Information Management Tool for Peacekeeping Operations," December 10, 2015, http://www.un.org/apps/news/story.asp?NewsID=52789#.VpB6ystOXm5.

[16] "Report of the High-Level Independent Panel on Peace Operations on Uniting our Strengths for Peace: Politics, Partnership and People" (A/70/95) or (S/2015/446), June 17, 2015.

[17] Commission on Global Security, Justice, and Governance, *The Crisis of Global Governance* (Washington, D.C.: The Stimson Center; and The Netherlands: The Hague Institute for Global Justice, 2015).

[18] Lloyd Axworthy, "Resetting the Narrative on Peace and Security: The Responsibility to Protect in the Next Ten Years," in *The Oxford Handbook of the Responsibility to Protect*, ed. Alex Bellamy and Tim Dunne (Oxford: Oxford University Press, 2016).