Safety & Security

Cyberpeacekeeping

A New Role for the United Nations?

Walter Dorn

In the twenty-first century, cyberwar has become more prevalent than physical war. Cyberattacks and cyberconflicts are now a regular part of the global Internet, including attacks through the "Dark Web." Given hacking by adversarial states, criminal groups, and malicious individuals, new strategies are needed to manage this global problem. This paper introduces and explores the new concept of cyberpeacekeeping. Cyberpeackeepers, possibly working for the United Nations or mandated by it, could patrol and act in cyberspace just as current UN peacekeepers patrol and act in the world's conflict zones. Cyberpeacekeepers could investigate major cyberattacks and hacking events. They could help contain conflict between nations (and potentially between other conflicting parties as well), prevent escalation of cyberwars, and help catch global cybercriminals. Eventually international action could be taken to enforce new cyberrules, which are currently lacking in weakly protected cyberspace. The obstacles to such a proposal from within and outside the United Nations are addressed in this paper in order to explore feasible future roles for cyberpeackeepers.

Cyberpeacekeepers could investigate major cyberattacks and hacking events. They could help contain conflict between nations (and potentially between other conflicting parties as well), prevent escalation of cyberwars, and help catch global cybercriminals.

Cyberwar, cyberespionage, and cybercrime are now part of our planetary landscape. Unfortunately, many nations, organizations, and individuals routinely violate national and international laws in the ungoverned or weakly governed domain of cyberspace. Nations have nefariously attacked other nations not only to steal secrets, influence elections, and discredit persons, but also to bring down the Internet sites of government ministries, banks, and media. In our interconnected world, almost everyone suffers at some point from hackers who spread viruses or from nations that illegally pry into personal privacy through overreaching surveillance programs. Cyberpeacekeeping is proposed as one means to deal with various forms of cyberconflict.[1]

From Physical Space to Cyberspace

Just as peacekeeping has become an indispensable tool to deal with physical con-

Walter Dorn is professor of defence studies at the Royal Military College of Canada (RMC) and the Canadian Forces College (CFC), teaching military officers from Canada and about twenty other countries. He also works as an "operational professor" in UN field missions and assists international organizations. He served on the UN's Expert Panel on Technology and Innovation in UN Peacekeeping and as a technology expert at UN headquarters. His two most recent books are *Air Power in UN Operations: Wings for Peace* (Ashgate, 2014) and *Keeping Watch: Monitoring, Technology, and Innovation in UN Peace Operations* (UNU Press, 2011).

flict, cyberpeacekeeping can help manage cyberconflict. The world needs impartial investigators of criminal hackers and nefarious attackers, as well as protectors against attacks on electronic devices of individuals. Cyberpeacekeepers could be "deployed" by the United Nations in the digital world with specific mandates and capabilities, carrying out analogous functions as physical peacekeepers, through surfing the Internet at well-equipped computers instead of patrolling in armored vehicles. They would monitor the vague "digital borders/boundaries," prevent or warn of impending attacks, investigate violations (including cybercrises that result in widespread computer data loss endangering lives and livelihoods), and mediate between conflicting parties. They could help find acceptable terms for "cyberceasefires," develop "cyberpeace agreements" to end conflicts, and oversee "safe layers" for "netizens" to be freer from viruses and attackers. Cyberpeacekeepers could also assist with national (cyber)infrastructure development, particularly in countries that are most vulnerable, just as their counterparts in current peacekeeping engage in nation building. They could educate national cyberofficials, promote the rule-of-law more generally, and help bring more order to the weakly governed cyberspace. New norms and international agreements could be established by nations with the help of cyberpeacekeepers.

Though a mapping from traditional peacekeeping to cyberpeacekeeping is not exact, the rough analogy can extend further, with the humanitarian action of the physical peacekeepers being translated into assistance to victims of cyberattacks. The Protection of Civilians, which is now a part of twenty-first-century peacekeeping, could (as mentioned previously) translate into the defense of innocent users of cyberspace ("netizens"). Cyberpeacekeepers, for instance, could oversee "safe areas" (e.g., secure, well-guarded servers or domains) where services are better protected from attack and abuse, and offer software fixes to parties subjected to ransomware or website attacks.[2] Further extending the analogy, they could be involved in demining by removing "cybermines," the dormant malicious software activated by unwitting users, or other cyberweapons. In sum, a "virtual peacekeeping force" could help secure our increasingly vulnerable world as it becomes more digital.

UN Practice and Aspirations

The term "digital peacekeeper" is being discussed at the United Nations but with a different meaning: a physical peacekeeper—military, police, or civilian—in conflict zones equipped with advanced digital equipment, such as body cameras, night vision, advanced computer communications, and augmented-reality devices to view physical space. In the present proposal, however, cyberpeacekeeper means an authorized individual doing tasks like those described previously in cyberspace.

A deeper engagement with digital defense is already needed in regular peacekeeping operations. Given that UN missions are vulnerable to attack and cyberespionage, especially when it comes to their information about UN adversaries, countermeasures need to be taken not only to prevent escalation of parties, but also for the mission's own protection. The UN is slowly developing the necessary infrastructure and procedures to protect sensitive information and to prevent break-ins, but the cyberpeacekeeping role would be much more proactive in that sense.

There are already indications that the United Nations sees a future role for itself in cyberpeacekeeping. An example is

its recent introduction of the term "Digital Blue Helmets" (DBH), in analogy to physical UN peacekeepers (known as "Blue Helmets" because of the color of the head gear). The UN's Office of Information and Communications Technology (OICT) also writes that it is leading efforts to "enhance cybersecurity preparedness, resilience, and response."[3] These efforts, however, remain aimed at threats to the organization itself, not to the world more generally. This could be extended in the future, once a cadre of cyberprotectors is developed and the UN member states call on the UN to provide such service. OICT writes, "Ultimately the program will support the United Nations' efforts in the areas of peace and security, sustainable development, international law, human rights, and humanitarian though coordinated policy development, monitoring, response, and mitigation strategies." OICT has conducted some preliminary research on cyberthreats to the Sustainable Development Goals.[4] And under the category of "Research," OICT envisions "DBH Operations Centres" providing "interdisciplinary cybersecurity support and teaching centres that bring together specialists from around the globe to address a variety of IT-related issues."[5]

There are already indications that the United Nations sees a future role for itself in cyberpeacekeeping.

The United Nations is also examining its potential role in preventing terrorism in cyberspace. The United Nations Counter-Terrorism Centre, for instance, has plans to help requesting member states to be "better able to prevent terrorist cyberattacks, and mitigate the effects and expedite recovery should they occur."[6] The UN's Department of Peacekeeping Operations (DPKO) is already a part of the associated UN's Counter-Terrorism Implementation Task Force.[7] But efforts to counter cyberterrorism and cyberwarfare are all at a preliminary stage.

NATO is much more advanced in this domain, though it mostly sticks to research and cooperation within the alliance. It established in 2008 a NATO Centre of Excellence (COE) on Cooperative Cyber Defence as a multinational and interdisciplinary hub of cyberdefense expertise, based in Tallinn, Estonia,[8] which collects specialists from around the world to collaborate and share on cyberthreats. The COE also developed the Tallinn Manual, the first and most in-depth analysis into how international law applies to cyberattacks.[9] The center, however, exists primarily to meet the *collective defense* needs of NATO members and has no counterpart in the *collective security* regime, where the United Nations has primary responsibility for the maintenance of international peace and security (in a global sense). However, given the complexities involved, a cyberattack on one NATO country might not trigger NATO's Article 5.[10]

Fortunately, some principles do exist on the global level. The UN Human Rights Council has confirmed that "the same rights people have offline must also be protected online,"[11] while others have written about the human rights and emerging law of cyberspace.[12] The United Nations has already adopted seven principles for action on cybercrime and cybersecurity on which to build. The seven cyberpillars, adopted by the Chief Executives Board for Coordination in 2013, reflect a UN-system-wide effort to standardize policy, encouraging UN programs to help member states address "cybercrime and cybersecurity needs," and "take evidence-based action."[13]

Despite the cyberprinciples and DBH concept, the UN Secretariat is reluctant

to advance new roles for itself without being asked by UN member states to take on such positions. It is therefore necessary to increase the awareness of member states, as well as the world more generally, about the possibilities of cyberpeacekeeping. More research and consultation is needed to get a sense about how the concept might work in practice.

Much of the expertise for cyberpeacekeeping will need to come from the UN's member states. In depth knowledge of sophisticated viruses, spear phishing schemes, the "dark web," and national cyberwarfare capabilities are carefully honed capabilities that the UN does not currently possess. Just as nations already offer the United Nations their specially trained soldiers and other prized national assets, so too these nations could provide their cyberexperts on loan (secondment) to the world organization—as long as they are impartial and not instruments of narrow national interests. This is the common standard for international civil servants, seconded and gratis personnel, as well as expert panelists that currently do intense investigative work for the UN Security Council. But more is needed: a stronger international cybersecurity regime.

The Longer Term Vision: Enforceable Law

The United Nations could eventually negotiate and codify new binding standards and rules to make illegal specific types of cyberattacks, including those described in the Tallinn Manual. Moving from declarations, expert recommendations,[14] and resolutions to treaties (such as the proposed Digital Geneva Convention),[15] however, the question remains how to secure *compliance* with the rules.

At present, the main compliance mechanisms are simply the pressure of other states and the negative publicity of media reports. If more impartial UN evaluations of attacks become used, such pressure would increase. Eventually, the United Nations would need to enforce its digital decisions with the powers in Chapter VII of the UN Charter, which include the strong measure of "complete or partial interruption of . . . means of communication."[16] The Security Council could conceivably place cyberlimits on nations or organizations that use the Internet for hate crimes, for cyberwarfare, and for international cyberlaw violations more generally. Admittedly, this may be politically difficult because several nations who have engaged in cyberwar serve permanently on the UN Security Council. Enforcement is also difficult because cyberspace allows violators much room for anonymity. Still, even modest UN measures could make it more difficult for "cyberwarriors" and "cyberthugs" to carry out their nefarious activities and could eventually lead to the arrest of the extreme violators.

Should the cyberpeacekeepers themselves have the option to use force? If the analogy to the physical domain applies, the rules for ethical use of force would also carry over. The third of the three principles governing peacekeeping, in place since inception, is the use of force in defense of the mandate (and self-defense).[17] So by analogy, cyberpeacekeepers could, in theory, apply force defensively. Furthermore, the just war tradition specifies criteria for the use of force that could conceivably be applied to cyberforce: just cause (defense of self or others against cyberattack), legitimate authority (the UN Security Council or another properly constituted international organization), right intent (defense and justice), proportionality (responsive action in proportion to the threat or the magnitude of the original attack), net benefit (so the positive repercussions outweigh the negative ones), and right

conduct (according to a well codified set of "cyberrules of engagement"). It seems it is possible to construct rules for the use of defensive cyberforce.

Because quick responses may be needed to prevent or stop cyberattacks, the potential actions of cyberpeacekeepers may need to be explicitly mandated. This might include the right to block sites or accounts that launch cyberattacks or exhibit extreme breaches of Internet rules—beyond "netiquette" infractions to those committing criminal acts. For instance, when a distributed denial of service (DDoS) attack is being carried out against an innocent website or service, the cyberpeacekeeper could take measures to stop such an attack, including diverting some of the abused website queries or uncovering and stopping the electronic source. For instance, the WannaCry ransomware virus that debilitated some 200,000 computers in over 70 countries was stopped from further damage (especially in North America) because a "malware tech" in the United Kingdom activated the "kill switch" embedded in the virus's software.[18]

Where in the United Nations would such cyberpeacekeepers be placed? Given the acrimonious debates between nations in the International Telecommunications Union (ITU), it might not be the best location for a cyberpeacekeeping capacity, though the IMPACT partnership initiative showed how a new organization could be modeled on an established organization,[19] namely, the US Centers for Disease Control and Prevention (CDC). Perhaps UN headquarters in New York could take the lead, accustomed as it is to conducting impartial investigations and to the sensitivities of nations. The OICT already has a preliminary vision (DBH) and has regional technology centres in different parts of the world. Furthermore, cyberinvolvement is becoming a greater part of regular peacekeeping.[20] But at the UN, cyberpeacekeeping remains largely unexplored.

The Obstacles

So far, member states have not asked the United Nations to perform cyberpeacekeeping duties, possibly owing to the newness of the concept.[21] There may be, however, additional reasons for such national reluctance, such as fears that the UN cyberpeacekeepers might uncover and expose the secret activities of certain states in cyberspace that are closely linked to intelligence gathering and global spying. UN cyberpeacekeepers might expose a pattern of cyberattacks, not just the known and admitted ones (such as the Stuxnet "digital weapon" used to attack Iranian uranium-enrichment centrifuges[22]) but also clandestine ones.

More powerful states in the international system have been reluctant to declare a right to offensive cyber operations, even if done in response to attacks. This is a wise approach to help avoid outright wars in cyberspace. Several nations, however, still conduct cyberwarfare clandestinely; there is evidence to suggest the existence of cyberwarfare between certain countries: Russia and various countries (Georgia, Estonia, and possibly the US and several European countries); Pakistan and India; China and India; China and Taiwan; Israel and various Arab/Persian states; Qatar and Arab adversaries; North Korea and several other countries/corporations. Many of these attacks have been done through hackers who may or may not have formal affiliations with the governments that deliberately fail to prosecute them.

States that are deeply engaged in cyberespionage and cyberwarfare, such as Russia, would not want to be exposed. Some may only want the United Nations to investigate on a case-by-case basis, for example, in cases where they can be vindicated, instead

of granting the world organization the independent authority to launch its own investigations.

States that are deeply engaged in cyberespionage and cyberwarfare, such as Russia, would not want to be exposed.

The United States has invested the most in the cyberdomain, with a Cyber Command created in 2009 to complement the geographic combatant commands.[23] Since it has the most investigative power and a long record of cyberspying,[24] Washington might not wish to lose its predominance. On the other hand, the United States may not want to police the Internet, so there are possible openings for selective UN roles in "cyberpolicing."

Conclusion

Despite the need for cyberpeacekeeping, the political will of member states to take action is not yet sufficiently developed. But the idea could take hold in the collective imagination so that it can be explored when the situation warrants. At this point several steps could be taken: a group of governmental experts could be assigned the task of exploring possible roles and the UN could gradually develop its expertise in cyberforensic analysis (especially in areas where the UN already does investigations, such as human rights violations and trafficking in people, drugs, weapons, and illegal natural resources). The world organization could create a roster of national experts for potential service. Then, when the need comes, the UN will have a nucleus on which to build.

Real progress will probably come only after a cybercrisis hits the nations of the world and they realize, once again, the need to work together for global solutions to global problems. It took the Suez Crisis of 1956 for UN member states to accept the notion of armed peacekeepers, as proposed by Canadian foreign minister Lester Pearson. This first peacekeeping force allowed great powers (the United Kingdom, France) and a regional power (Israel) to withdraw from Egyptian territory as an alternative to expanding the war.

Real progress will probably come only after a cybercrisis hits the nations of the world and they realize, once again, the need to work together for global solutions to global problems.

A catastrophic cyberattack, which is quite possible (if not inevitable), would cost the world dearly since commerce, governance, and personal communications are now so deeply dependent on the Internet. Faced with a huge disaster bill and a potential for vast escalation in attacks, an investment in cyberpeacekeeping would seem like a bargain. And small steps to expand the UN architecture into cyberspace are feasible at present. The member states simply need to provide some authorization, direction, resources, expertise, and political backing. This can and should be done while preserving cyberspace as an open and essentially uncontrolled domain—a common resource for humanity.

A cyberwar of global proportions is possible. But so is cyberpeace. It is up to the world to choose the path it takes.

Notes

1. A literature review shows that cyberpeacekeeping has been proposed in several earlier publications, most notably by cyber experts

Nikolay Akatyev and Joshua I. James "Cyber Peacekeeping," in *Digital Forensics and Cyber Crime*, ed. Joshua L. James and Frank Breitinger (Cham: Springer, 2015), 126–39. Earlier authors put forward concepts including T. P. Cahill, K. Rozinov, and C. Mule, "Cyber Warfare Peacekeeping," in *Proceedings of the 2003 IEEE Workshop on Information Assurance* (New York: IEEE, 2003), 100; and Jann K. Kleffner and Heather A. Harrison Dinniss, "Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations," *Int. Law Stud.* 89, no. 1, (2013): 512–35. See also John Karlsrud, "Peacekeeping 4.0: Harnessing the Potential of Big Data, Social Media and Cyber-technology," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. Jan-Frederik Kremer and Benedikt Müller (Cham: Springer, 2014), 141–60.

2. Ransomware is malicious software that blocks access to a user's own computer system or data unless payment is made.
3. "Cyber Risk," United Nations, n.d., https://unite.un.org/digitalbluehelmets/cyberrisk.
4. OICT described potential cyberthreats to the Sustainable Development Goals as follows: (2—Zero Hunger) (cyber)attacks on food chains, supply networks and commodities trading markets; (4—Quality Education) cyber bullying and online exploitation of children; (5—Gender Equality) online human trafficking; (6—Clean Water and Sanitation; 7—Affordable and Clean Energy; and 9—Industry, Innovation and Infrastructure) attacks on critical infrastructure; (8—Decent Work and Economic Growth) attacks on critical infrastructure; corporate espionage; online human trafficking; terrorist recruitment via social media; (10—Reduced Inequalities) attacks on critical infrastructure, financial markets and institutions; online exploitation; identity theft; financial cybercrime; (16—Peace, Justice and Strong Institutions) child and illicit trafficking online, cybercrime. "Digital Blue Helmets: Activities," United Nations, n.d., https://unite.un.org/digitalbluehelmets/activities.
5. "Digital Blue Helmets: Research," United Nations, n.d., https://unite.un.org/digitalbluehelmets/research. OICT has advertised Cyber Security Expert jobs for a planned Cyber Security Operations Centre (CSOC) in New York to "deter such [cyber] attacks, and thus reduce the impact on the UN's mission and mandates."
6. "Themes & Priorities," United Nations Counter-Terrorism Center (UNCTC), n.d., https://www.un.org/counterterrorism/ctitf/en/uncct/themes-priorities.
7. "Entities," United Nations, Counter-Terrorism Implementation Task Force (CCITF), n.d., https://www.un.org/counterterrorism/ctitf/en/structure.
8. Estonia was a willing host after it suffered a massive cyber attack in 2007 on its websites and cyber infrastructure. The COE was set up to "provide a capability to assist allied nations, upon request, to counter a cyber attack." NATO summit communique, Bucharest, April 2008. The COE role is to improve cyber defence interoperability; develop policies, concepts, doctrine, and standards; enhance information security and cyber defence education; provide cyber defence support for experimentation. It also provides cyber defence subject matter experts (SMEs) to NATO, especially for cyber defence testing and validating.
9. The COE led and facilitated the drafting of the influential Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017). For more information, see "Tallinn Manual Process," NATO COE CCD, n.d., https://ccdcoe.org/tallinn-manual.html.
10. Article 5 of the North Atlantic Treaty provides for collective defence, i.e., that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." Timo Mustonen, "DefRep Analysis: NATO's Cyber Shift May Not Link to Article 5," *Defense Report*, January 6, 2015, http://defencereport.com/defrep-analysis-natos-cyber-shift-may-not-link-to-article-5/.
11. UN Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, UN Doc. A/HRC/20/L.13 (2012), 518.

12. For instance, Kleffner and Dinniss have written at length on current human rights law existing for current peacekeeping operations but do not cover the future of cyberpeacekeeping. Kleffner and Dinniss, "Keeping the Cyber Peace," 512–35.
13. Chief Executives Board for Coordination, "Summary of Conclusions, Second Regular Session of 2013," UN Doc. CEB/2013/2, January 13, 2014, https://www.unsceb.org/CEBPublicFiles/Chief%20Executives%20Board%20for%20Coordination/Document/REP_CEB_201311_CEB2013-2.pdf. The seven principles can be paraphrased as follows: (1) Cyber incidents should be dealt with in a holistic manner through criminal justice and international cooperation. (2) UN entities should aim to respond to cybercrime and cybersecurity needs in member states within their respective mandates. (3) All UN programming should respect the principles of the rule of law and human rights. (4) UN programming should focus on assisting member states to take evidence-based action. (5) Programming should foster a "whole-of-government" response. (6) Support to member states should aim to strengthen international cooperation. (7) Programming should include efforts to strengthen cooperation between government institutions and private-sector enterprises.
14. An important set of recommendations was released in 2015 in "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/70/174 of 22 July 2015.
15. The 2001 Budapest Convention on Cybercrime is the first international treaty on crimes committed via the Internet and other computer networks. It deals with things like "infringements of copyright, computer-related fraud, child pornography and violations of network security." It demonstrates some of the first measures of enforcement power through search procedures of computer networks and interception. See http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; Heidi Tworekheidi Tworek, "Microsoft Is Right: We Need a Digital Geneva Convention," *Wired*, May 2017, https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention. The speech by Microsoft president Brad Smith can be found at Microsoft, "The Need for a Digital Geneva Convention," February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#IQ5fjhKgIvqCELrA.99.
16. UN Charter, Article 41.
17. The traditional trinity of peacekeeping principles, which could apply to cyberpeacekeeping with little modification, are (1) consent of the governments involved, (2) impartiality, and (3) minimum use of force, in accordance with a defensive mandate
18. Lydia Willgress and Peter Walker, "IT Expert Who Saved the World from Ransomware Virus Is Working with GCHQ to Prevent Repeat," *Daily Telegraph,* May 15, 2017, http://www.telegraph.co.uk/news/2017/05/14/revealed-22-year-old-expert-saved-world-ransomware-virus-lives.
19. The International Multilateral Partnership Against Cyber Threats (IMPACT) bills itself as the "largest global cybersecurity alliance of its kind," including industry, academia, and 152 nations in the coalition (but not Security Council permanent members France, Russia, UK, or USA). This public-private partnership, launched at the World Cyber Security Summit (WCSS) in 2008, has trained about 2,000 cyber professionals, including computer incident response teams. ITU's Global Cybersecurity Agenda (GCA). Accessed June 12, 2017, http://www.impact-alliance.org.
20. A scenario for cyberpeacekeeping within a regular peacekeeping operation can be envisioned since some physical conflicts include a cyber dimension. Although there is no peace operation in Syria, the civil war includes entities like the Syrian Digital Army, using cyberspace to attack both cyber and physical structures. When the civilian population is under imminent physical threat by cyber actions, it stands to reason that the missions have a mandate to enter into cyberspace to protect the population.

21. The Shanghai Cooperation Organization (SCO) has proposed at the United Nations an International Code of Conduct for Information Security, updated in 2015. UN Doc. A/69/723 of 13 January 2015. But the political will does not yet exist to adopt a code of conduct. Furthermore the Code of Conduct has little in the way of verification and enforcement mechanisms or an institution to support its implementation.
22. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
23. Cyber Command is subordinate to US Strategic Command. Website: http://www.arcyber.army.mil.
24. US cyberspying (cybersurveillance) on a massive scale was uncovered in the Snowden release of information. For a summary see "Edward Snowden: Leaks That Exposed US Spy Programme," BBC, January 17, 2014, http://www.bbc.com/news/world-us-canada-23123964.