Cyberpeacekeeping: the Challenge

By A. Walter Dorn

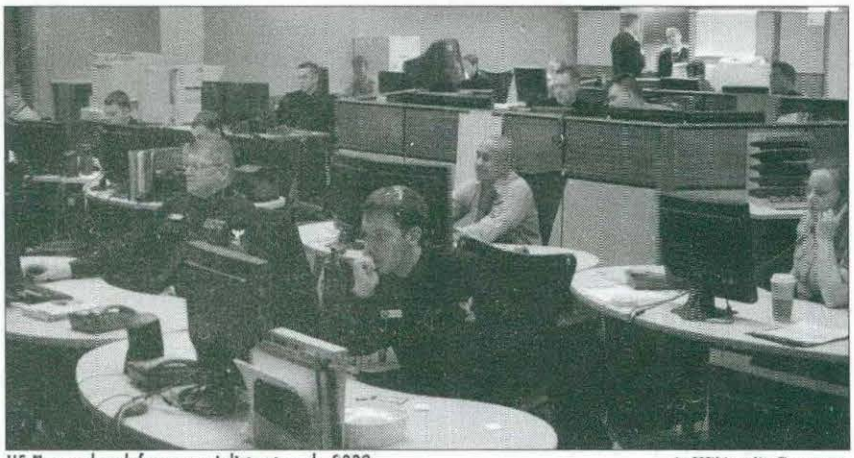
Cyberspace is virtually ungoverned. Though benefiting at least half of humanity, some nations have nefariously used cyberspace to attack other nations, steal secrets, influence elections, discredit persons, and even bring down the internet sites of government ministries, banks, and media. Almost everyone suffers at some point from hackers who spread viruses or pry into their affairs. Perhaps "cyberpeacekeeping" can become a means of dealing with the increasing problems.

FROM PHYSICAL SPACE TO CYBERSPACE

Just as peacekeeping has become an indispensable tool to deal with physical conflict, cyberpeacekeeping can help manage cyberconflict. The world needs impartial investigators of criminal hackers and nefarious attackers, as well as protectors against attacks on citizens' electronic devices. Cyberpeacekeepers could be "deployed" by the United Nations in the digital world with specific mandates and capabilities, carrying out analogous functions as physical peacekeepers, though surfing the internet at well-equipped computers instead of patrolling in armoured vehicles. They would monitor the vague "digital borders/boundaries," prevent or warn of impending attacks, investigate violations (including cyber atrocities that result in widespread computer data loss endangering lives and livelihoods), and mediate between conflicting parties.

They could educate national cyber-officials, 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.

They could oversee "safe areas" (such as well-guarded servers, properly fire-walled sites, and secure domains) where services are better protected from attack and abuse, and offer software fixes to parties subjected to ransomware or website attacks. Further extending the analogy, they could be involved in demining, removing "cyber mines," the dormant malicious software activated by unwitting users or other cyberweapons.



US Navy cyber-defence specialists at work, 2008. *via Wikimedia Commons*

The world needs impartial investigators of criminal hackers and nefarious attackers

In sum, a "virtual peacekeeping force" could help secure our increasingly digital and vulnerable world. Given that UN's current (physical) peacekeeping missions are vulnerable to cyberattack and cyberespionage, especially for spoilers and peace saboteurs, counter-measures need to be taken, not only to prevent escalation of parties from physical fighting to cyberfighting, 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, yet the UN Secretariat is reluctant to advance new roles for itself without being asked by UN member states to do so. It is therefore necessary to increase the awareness of member states, as well as the world more generally, about the idea and possibilities of cyberpeacekeeping.

The United Nations could eventually negotiate and codify new binding standards and rules to make illegal specific types of cyberattacks, such as using the internet for hate crimes, for

continued on page 30

Cyberpeacekeeping

Continued from page 27

cyberwarfare, and for other international cyber-law violations.

Admittedly, this may be politically difficult because several nations who have engaged in cyberwar are permanently in 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 "cyberaggressors" and "cyberthugs."

Because quick responses will be needed to stop cyberattacks, the cyberpeacekeepers should be explicitly mandated to be proactive. This might include the right to block sites or accounts that launch cyber-attacks or exhibit extreme breaches of internet rules. For instance, where a Distributed Denial of Service attack is carried out on an innocent website or service, the cyberpeacekeeper could take measures to stop such an attack, including uncovering and stopping the electronic source.

So far, member states have not asked the United Nations to perform cyberpeacekeeping duties, possibly due to the newness of the concept. 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 cyber-attacks.

States that are deeply engaged in cyber-espionage and cyberwarfare, such as Russia, would not want to be exposed and may only want the United Nations to investigate on a case-by-case basis, for example, in cases where they can be vindicated. Since it has the most investigative power and a long record of cyber-spying, the United States 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."

A catastrophic cyberattack, which is quite possible (if not inevitable), would cost the world immensely 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. A cyberwar of global proportions is possible. But so is cyber peace. ■

Walter Dorn is a professor of defence studies at the Royal Military College and the Canadian Forces College. (Website: walterdorn.net.) He has served as the UN Representative of Science for Peace since 1983, nad has published extensively on peacekeeping issues.

This article is a digest of a longer paper being published in the Georgetown Journal of International Affairs.