Cyber peacekeeping is integral in an era of cyberwar – here's why

January 30 2018, by Helge Janicke

Credit: AI-generated image (disclaimer)

Cyber warfare is upon us, from interference in elections to a leak of cyber weapons from a national stockpile. And, as with most evolutions in warfare, the world is largely unprepared. Cyber peacekeeping presents significant challenges, which we explore in our research.

Any theatre of war now includes cyberspace. It has been used in targeted attacks to disable an adversary's capabilities, such as Stuxnet, where Iran's ability to enrich weapon-grade Uranium was disrupted. It can also be exploited in traditional warfare through electronic interference with intelligence and communication systems.

With little to guide nations and scant experience to build upon, many states are having to learn the hard way. In the context of warfare, it takes a long time to understand the impact of new technologies. One only need look at the example of landmines to see why. Once considered a legitimate weapon to stifle enemy movement, most countries now agree that landmines are indiscriminate and disproportionate weapons that cause civilian suffering long after a conflict has ended.

It's possible that cyber warfare holds unknown consequences that future world leaders will agree to ban for similar, gut-wrenching reasons in the aftermath.

There are, however, efforts to fill the gaps in knowledge. Researchers, such as my colleague Michael Robinson, have attempted to characterise cyber warfare to understand how it can be effectively and ethically conducted. These include efforts to create cyber warfare laws to the control and restriction of cyber weapons.

These efforts are beginning to bear fruit, with the Tallinn Manual – first published in 2013 – offering a comprehensive analysis of how existing international law applies to cyberspace.

Stop the fight

But while a large proportion of research focuses on how to conduct cyber warfare, there is very little research on restoring peace in the aftermath of an online conflict between nation states.

Just as we cannot expect a nation to spring back to peace and prosperity following years of boots-on-the-ground war, countries affected by prolonged periods of cyber warfare also need assistance to recover.

A nation's reliance on critical infrastructure brings the need to understand the damage cyber warfare can inflict on a society into sharp focus. Computer systems running essential services at hospitals, nuclear power plants and water treatment plants may be infected with advanced malware, which resists removal and prolongs civilian suffering – much like landmines persist long after a conflict ends. The physical effects of cyber weapons make cyber peacekeeping a key enabler to help bring about lasting peace.

After a conventional conflict, interventions to restore peace and security are performed on the international stage. The United Nations (UN), with its white vehicles and blue helmets, is the most widely recognised peacekeeping organisation. It has a long history of maintaining peace around the world and has evolved to match the shifting nature of warfare from inter-state to intra-state conflict over the years.

UN peacekeepers were initially ill-equipped to deal with such a change, which led to high profile failures such as Rwanda and Somalia.

With the rise of cyber warfare, peacekeepers will increasingly have to operate in this domain. But are the UN and similar organisations prepared for this expected onslaught or will they suffer a repeat of past failures, having been caught out by changes in the nature of conflict? Protracted UN cyber warfare talks fell apart last year because a consensus couldn't be reached amid suspicions that reportedly mirrored the Cold War era. Nonetheless, questions must be asked of the UN's peacekeeping strategy on its readiness to tackle cyber threats.

Peace is the word

Can existing peacekeeping activities simply be adapted for the internet, or should a completely new framework be drawn up to adequately address how to maintain or restore order online? What kind of technical obstacles will cyber peacekeepers encounter? Could they achieve something that contributes towards restoring or maintaining peace?

Disarmament illustrates these operational problems well: the destruction or confiscation of physical armoury means that assets cannot be easily replaced by a warring faction should peace efforts stall or falter. Cyber weapons are predominantly software applications that can be replicated, archived, encrypted and passed on with almost no cost or significant logistic efforts, research shows.

The effectiveness of cyber weapons diminishes once the vulnerabilities they have exploited become known, so one approach would be to publish detected cyber weapons to render them obsolete. Responsible disclosure would allow vendors to come up with fixes and give potential victims a chance to apply the patches – which can be a lengthy process.

Doing so "destroys" all cyber weapons of this kind – regardless of whether they belong to any of the warring factions. This approach has a nasty side-effect: it inadvertently leads to a proliferation of cyber weapons, because it's easier for other nations or criminals to acquire the technology before adequate protections can be put in place on a global scale. It also throws up political challenges.

Conventionality belongs to yesterday

It's no secret that the UN struggles to find money for peacekeeping contributions. The US, the largest contributor to the UN budget by far, has – under president Trump – disagreed with how the organisation is governed, and confirmed it will reduce payments to the peacekeeping budget.

If securing troops under difficult budget restrictions is already difficult, then securing highly-skilled cyber personnel in a competitive global market will be even more challenging.

And there's an additional complication: those countries conducting cyber warfare are the advanced nations, many of which already contribute the lion's share of UN funding and possess the greatest cyber expertise. Would they be willing to contribute their knowledge, wealth and people to aid their adversaries?

Conflict affects every nation, so it's in everyone's interests to have an internationally available capability to restore peace and security in the aftermath of cyber warfare.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Cyber peacekeeping is integral in an era of cyberwar – here's why (2018, January 30) retrieved 12 September 2024 from https://phys.org/news/2018-01-cyber-peacekeeping-era-cyberwar.html