Cyberpeacekeeping: New Ways to Prevent and Manage Cyberattacks

A. Walter Dorn, Canadian Forces College, Toronto, Canada
Stewart Webb, DefenceReport, Salt Spring Island, Canada

ABSTRACT

Cybersecurity is coming to the forefront of the concerns of nations, organizations and individuals. Government agencies, banking systems and businesses have been crippled by criminal and malicious cyberattacks. There are many examples of cyberattacks in regions of tensions and armed conflict. There are no impartial international means to investigate the claims and counter-claims about cyberattacks. The international community more broadly lacks a way to deal with cyberattacks in a concerted manner. A new approach and capability should be considered for certain circumstances: cyberpeacekeeping. Peacekeeping has proven effective in physical space, and many of the same principles and methods could also be applied in cyberspace, with some adjustments. It could help prevent global attacks, and if an attack were to be successful, it could assist with recovery and conduct impartial investigations to uncover the perpetrators. The possibilities of a cyberpeacekeeping team at the United Nations to make cyberspace more secure are well worth exploring.

KEYWORDS

Cyber Operations, Cyberpeacekeeping, Cyberterrorism, Peacekeeping, Tallinn Manual

1. INTRODUCTION

1.1. The Challenge

The world is ever increasingly reliant on internet-connective technology. Computers permeate almost every facet of human life in most parts of the world, connecting people in ways that could not have been imagined, with the developing world becoming connected at the fastest rate. The level of technology and global integration is staggering even compared to just 20 years ago. This interconnectivity is a cause not only of celebration but also of deep concern for security, as what makes human life easier and more efficient also gives rise to significant vulnerabilities and threats, even the potential for a massive downfall.

Attacks on global interconnectivity have become a reality. Deliberate attacks are conducted by states or state-sponsored entities or groups or non-state and criminal actors who seek to infiltrate and bring down sites and alter the instructions that computers give to industrial machinery, such as centrifuges, dams and even electric power grids (United States Computer Emergency Readiness Team,
2018; Industrial Control Systems Cyber Emergency Response Team, 2016). Already we have seen the internet, including the parts of the deep/dark web, used to incite riots and even to influence the course of national elections. For instance, new evidence is continually emerging of Russian attempts to interfere in numerous elections, including those of the United States and France (Greenburg, 2017; Pope, 2018). Shortly before Russia invaded Georgia in August 2008, it launched a barrage of Distributed Denial of Service (DDOS) attack, making Georgian military movements and operations so much more difficult and dangerous (Markoff, 2008). The United States and Israel likely introduced malware to cause breakdown in Iranian centrifuges at Natanz. These examples show how cyberattacks have translated into kinetic damage. One problem is that, despite the effects, attribution is difficult and international means for impartial investigation are lacking. Examples of attacks are plenty, but effective responses are few and modest.

At present, the world relies on national security services and commercial companies to handle national cybersecurity, and there is no international body to provide some form of international cybersecurity. While a few countries are developing advanced cybersecurity measures, they still remain vulnerable and most countries of the world have limited capacity to respond to cyber threats. Moreover, there has not been a coordinated international effort to address cybersecurity or create measures of common or collective security in global cyberspace. With many cases of international and intranational conflict, cyberattacks have the potential of unsettling an already fragile peace. This paper seeks to explore new means of addressing cybersecurity, building on the characteristics and successes of peacekeeping in physical space. The paper proposes that the establishment and activities of a UN cyberpeacekeeping unit could lessen the threat of conflicts, help recovery, maintain balance and improve cyber relations in a wide range of scenarios. Examples from the past threats can help illustrate the threats and the types of cases where cyberpeacekeeping could help.

2. EXAMPLES AND MULTILATERAL RESPONSES

In 2007, the Estonia case demonstrated how extensively cyberattacks could affect an entire country. The attack was likely in response to the removal of a Soviet-Era statue of the Bronze Soldier of Tallinn. This showed how actions in physical space can have ramifications in cyberspace. The removal of the statue represented the shift away from Estonia’s recent Russian history and domination. Russia not only protested but, in all likelihood, supported a massive cyberattack. An impartial determination of responsibility was lacking, and Russia could easily dismiss and ignore the allegations. But it could increase its threatening power from the suspicions while also punishing Estonia severely.

The widespread and large-scale DDOS attack campaign was unleashed. Banks were shut down, government employees were unable to send emails to one another and the media found it difficult to publish stories. Regular life in Estonia turned to confusion, probably with a few final strokes of a keyboard far away. Only after much effort were computer services restored.

In consequence Estonia, which had joined the North Atlantic Treaty Organization (NATO) in 2004, offered to host a new NATO cyber defence centre. The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) was established in 2008 as a multinational and interdisciplinary hub of cyber defence expertise based in Estonia’s capital, Tallinn. 1 Although the centre was created to help meet the collective defence needs for its NATO members, the NATO CCD COE developed the world’s first, and most in-depth, analysis on the international law applicable to cyberattacks in an armed conflict situation. 2 Despite the important commentary in the Tallinn Manual on International Law Applicable to Cyberwarfare (henceforth Tallinn Manual, currently in version 2.0), the legalities of what constitutes a cyberattack and appropriate responses have not been fully flushed out yet. And the NATO COE cannot be considered an impartial investigator or upholder of any international cyber law, especially since it is biased in favour of NATO and Western countries.

A small but more important legal step had been made earlier in Europe. The Council of Europe drew up in 2001 the Budapest Convention on Cybercrime, the first international treaty
Small & Simple: Application-Specific Multi-Agent Systems
[www.igi-global.com/chapter/small-simple-application-specific-multi/5145?camid=4v1a](www.igi-global.com/chapter/small-simple-application-specific-multi/5145?camid=4v1a)

Clausewitz and the Utility of Cyberattacks in War
[www.igi-global.com/article/clausewitz-and-the-utility-of-cyberattacks-in-war/127383?camid=4v1a](www.igi-global.com/article/clausewitz-and-the-utility-of-cyberattacks-in-war/127383?camid=4v1a)