Developing Cyber Buffer Zones

2

Michael Robinson
https://orcid.org/0000-0002-4276-2359
Airbus, UK

Kevin Jones
Airbus, UK

Helge Janicke
De Montfort University, UK

Leandros Maglaras
https://orcid.org/0000-0001-5360-9782
De Montfort University, UK

INTRODUCTION

Cyberspace has become the latest domain of war(Robinson, Jones, & Janicke, 2015), where modern international actors aggressively pursue their national security and foreign policy goals(Martins, 2018). Much research has been focused upon this area, covering topics such as the ethics of cyberwarfare(Dipert, 2010), legal aspects(Baradaran & Habibi, 2017), how best to conduct military operations inside of cyberspace (Liles, Rogers, Dietz, & Larson, 2012) and how to organise and defend nations from cyber attack (Ruiz, 2017) (THIBER (The Cybersecurity Think Tank), 2013). Surveys of the literature show a vast range of additional topics, demonstrating that research interest into cyber warfare is lively and diverse (Robinson, Jones, & Janicke, 2015). Whilst it is clear that interest in cyber warfare is high, there has been less attention paid to its aftermath. What effects on societies persist after cyber warfare and do these effects stymie work to restore peace and security to conflict torn regions?

The field of cyber peacekeeping addresses these questions, looking at conflicts which contain cyber warfare through the lens of peacekeeping. In this chapter, we provide a background to cyber peacekeeping and survey existing literature. We then make a contribution to the field by developing the concept of a cyber buffer zone.

BACKGROUND

The concept of cyber peacekeeping can be traced back to an article by Cahill, Rozinov and Mule (2003). They noted that cyber warfare would likely havedevastating effects well beyond the boundaries of thecombatants and that some kind of peacekeeping capability in cyberspace would be needed (Cahill, Rozinov, & Mule, 2003). Some potential cyber peacekeeping activities were proposed, such as cyber

DOI: 10.4018/978-1-5225-9715-5.ch019

border management and monitoring/verification and their overall approach was to explore how existing peacekeeping doctrine could be mapped to cyber warfare. The topic did not receive any further attention for ten years untilKleffner and Dinniss(2013) reigniteddiscussion. They drew attention to the convergence of two significant global trends: an increase in conflicts which involve a cyber component and the increasing deployment of complex peace operations. They noted that these trends made it natural to assume that peacekeepers will find themselves asked to keep the peace in environments where the peace is threatened by cyber incidents (Kleffner & Dinniss, 2013).

Akatyev and James (2015)contributed by proposing a cyber peacekeeping model, including a set of goals and proposals of activities to perform during three stages: no conflict, conflict and post-conflict.In the no conflict stage, cyber peacekeepers work to unite efforts to keep the peace and prevent the outbreak of cyber conflict. In the conflict stage efforts are directed to orchestrating an international response and containing the harmful effects (e.g. through preventing the spread of malware or cyber weapons). Finally in the post-conflict stage, they propose that cyber peacekeepers are tasked with preventing further destruction and recovering critical infrastructure back to operation. In this regard, the model covers all three phases of warfare with the primary goal of protecting civilians.

The need for cyber peacekeeping was reinforced two years later by Dorn (2017), who states that cyberpeackeeperscould patrol and act in cyberspace just as current UN peacekeepers patrol and act in the world's conflict zones.Faced with a huge disaster bill and a potential for vast escalation in attacks, an investment in cyberpeacekeeping would seem like a bargain (Dorn, 2017).

In 2018, Robinson et al. (2018) built upon the foundations set by Cahill, Rozinov and Mule back in 2003. They reinforced the need for cyber peacekeeping with specific cases where cyber warfare would present a threat to international peace and security as defined by the United Nations. They explored how the activities of a modern multi-dimensional peacekeeping operation could be translated into a cyber warfare context, and evaluated each one according to two core criteria: value and feasibility. Any activity performed during cyber peacekeeping must bring clear value towards restoring peace and security, and must also be feasible to perform. They conclude that many of the existing UN peacekeeping activities would bring value in a cyber warfare context, but that feasibility can vary due to technical and political constraints.

Whilst such research into cyber peacekeeping is gaining momentum, further work is needed to develop the proposed activities and ideas into something practical: actions that could be concretely performed by peacekeepers in a cyber context to tangibly promote peace. The aim of this article is to contribute towards this goal by focusing on the concept of buffer zones.

FOCUS OF THE ARTICLE

In this article, we build upon the work of Robinson et al. (2018) by taking a closer examination of just one of the proposed activities: cyber buffer zones.The aim is to propose how the traditional peacekeeping activity of creating and running a buffer zone could be translated into cyber terms.To achieve this goal, we begin with a brief background of traditional buffer zones as used by UN peacekeeping. We then propose how the concepts behind a buffer zone could be translated into cyber terms, with emphasis on practical feasibility and ensuring that any proposal brings value towards peace. Data for this translation comes from both the cyber security and peacekeeping domains.