Information Technology for Peace and Security – An Emerging Research Field

CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#1-PAPER]

ABSTRACT

Technological and scientific progress, especially the rapid development in information technology (IT), plays a crucial role regarding questions of peace and security. This short overview addresses the significance, potentials and challenges of IT for peace and security. For this purpose, the talk offers an introduction to peace, conflict, and security research, thereby focusing on natural science, technical and computer science perspectives. In the following, it sheds light on fundamentals (e.g. IT in peace, conflict and security, natural science/ technical peace research), cyber conflicts and war (e.g. information warfare, cyber espionage, cyber defence, Darknet), cyber peace (e.g. dual-use, technology assessment, confidence and security building measures), cyber arms control (e.g. arms control in the cyberspace, unmanned systems, verification), cyber attribution and infrastructures (e.g. attribution of cyber-attacks, resilient infrastructures, secure critical information infrastructures), culture and interaction (e.g. safety and security, cultural violence, social media), before an outlook is given.

1. INTRODUCTION

In December 2017, an invasion of the German government network was discovered; This network links federal ministries and authorities (see Reinhold 2018a). The attackers used the Intranet of the Federal College of Public Administration and the Federal Academy of Public Administration as a gateway. This is the least secure part of the system because external participants also need to access it outside the institution, for example, for further education of the Foreign Office. Probably the first intervention should further penetrate the network. In order to gain freedom of movement on the intranet, administrative rights were claimed systematically. So far it could not be clarified whether parts of the used malware remained in the system (see Mascolo et al. 2018).

This incident is a good example of the increasing relevance of information technology for peace and security (see Reuter 2019). The innovations of scientific and technical research have always been used for military purposes and have thus strongly influenced warfare.

2. Cyberspace as a War Scene?

Violent conflicts can be conducted in different domains. In addition to land, sea, air and space, the so-called cyberspace is one of them. Therefore, the resilience of IT infrastructures is of increasing importance. Nevertheless, security strategies only insufficiently consider the specific characteristics of IT:

- Many of the actors involved (representing the group of potential aggressors) are either individuals or part of the private sector.
- The attribution of security-threatening or offensive activities is difficult because the identity of the security threat is unknown.
- Security concerns and international proliferation - that is, the proliferation of military or military technologies within and between states (see Altmann 2019) - increase the risk of military intervention as a preventive measure (see Chivvis & Dion-Schwarz 2017).
- Many technologies can also be misused as a weapon or part of a weapon system. Therefore, they are inherent in the risk of being misappropriated to harm a significant number of people. The dual-use problem (see Riebe & Reuter 2019) is of increasing relevance to IT, in particular, because the military use of IT systems and infrastructures phenomena such as cyberwar, the information war (see Ruhmann & Bernhardt 2019), (terrorist) propaganda, fake news (see Kaufhold & Reuter 2019), data espionage and hacking (see Herrmann 2019).

3. Conclusion

Existing research shows that information technology has a significant impact on warfare and military strategies. On the one hand, military forces increasingly rely on cyberspace, create capacities for offensive action in this domain, and even place it, as in the case of the United States, at the centre of future warfare. On the other hand, there is a lack of appropriate responses to questions regarding the international regulation of cyber conflicts and the current dynamics of rearmament. This circumstance is also due to the permanent ambiguity that veils cyberspace, its actors, and the operations it carries out: there are no dividing lines between internal and external security nor is it clear which cyber resources are defensive or can be assigned as open-minded.

The digital revolution also continues with network-centred warfare, which has the potential to transform warfare permanently. Attribution and verification continue to pose problems, although they are indispensable for the enforcement of international law. After all, cyber-defence faces legal dilemmas, not least due to the lack of standards regarding pre-emption, prevention and counter-operations. The peculiarities of cyberspace in the context of peace and security require a separate consideration to address the complexity and ambiguity of the field.

4. ACKNOWLEDGEMENTS

This contribution is based on Reuter et al. (2019).

REFERENCES

Altmann, Jürgen. (2019). Natural-Science/Technical Peace Research. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 39–60). Wiesbaden: Springer.

Chivvis, Christopher S., & Dion-Schwarz, Cynthia. (2017). Why It's So Hard to Stop a Cyberattack - and Even Harder to Fight Back. Retrieved from https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

Herrmann, Dominik. (2019). Cyber Espionage and Cyber Defence. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 83–106). Wiesbaden: Springer.

Kaufhold, Marc-André, & Reuter, Christian. (2019). Cultural Violence and Peace in Social Media. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg.

Mascolo, Georg, Steinke, Ronen, & Tanriverdi, Hakan. (2018, March). Die Geschichte eines Cyber-Angriffs. Süddeutsche Zeitung.

Reuter, Christian. (2019). Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg.

Reuter, Christian, Aldehoff, Larissa, Riebe, Thea, & Kaufhold, Marc-André. (2019). IT in Peace, Conflict, and Security Research. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden, Germany: Springer Vieweg.

Riebe, Thea, & Reuter, Christian. (2019). Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 165–183). Wiesbaden: Springer.

Ruhmann, Ingo, & Bernhardt, Ute. (2019). Information Warfare - From Doctrine to Permanent Conflict. In C. Reuter (Ed.), Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace (pp. 63–82). Wiesbaden: Springer.