International Journal of Cyber Warfare and Terrorism
Volume 10 • Issue 1 • January-March 2020

A Framework for the Weapons of Influence

Miika Sartonen, Finnish National Defence University, Helsinki, Finland
Aki-Mauri Huhtinen, Finnish National Defence University, Helsinki, Finland
Petteri Simola, Finnish Defence Research Agency, Human Performance Division, Tuusula, Finland
Kari T. Takamaa, Finnish National Defence University, Helsinki, Finland
Veli-Pekka Kivimäki, Finnish Defence Research Agency, Riihimäki, Finland

ABSTRACT

The development of communications technology has enabled the internet to become a new theatre of military operations. The influence aspects of military operations in information battlespace, however, are difficult both in theory and in practice, especially concerning international law. As a result, there is a variety of national and organizational solutions of how to divide tasks and responsibilities between authorities. This asymmetry generated by different approaches and rules of conduct provides opportunities for actors with more relaxed interpretation of international law, allowing them to use weapons of influence in order to pursue military goals. In this article the authors ask whether military influence operations, just like cyber operations, could be treated as acts of war. To help militaries address the complex issue of influence operations, a framework consisting of three categories is suggested.

KEYWORDS

Attribution, Battlespace, Cyber, Information, International, Internet, Law, Rhizome, War

INTRODUCTION

The development of communications technology has enabled the Internet to become a new theatre of operations. Today it is used for commercial, political and military purposes in addition to its recreational and scientific use. The vast possibilities provided by this digital environment have not gone unnoticed, and there is a growing body of evidence showing an increasing use of the digital sphere for military purposes.

Simultaneously, the rules of military conflict seem to be challenged by the changes in the information battlespace. Especially in the Western hemisphere there is a growing feeling of losing the information war, or rather being unable to fight it. The West, proud of its technical prowess, somehow seems to struggle when it has to face the human factors of the information battlespace and some of its new frontline weapons. One of the reasons for this, we argue, is the asymmetry in how warfare, and thus the role of the military, is perceived. In the broad spectrum of influence projected on target audiences in various nations, the role of the military as an actor varies. In the Western hemisphere, militaries typically engage in armed conflict within very strict rules of conduct.

DOI: 10.4018/IJCWT.2020010103

Weapons of information, however, tend to blur the boundaries of these rules. This blurring effect can be exploited by doctrinally and digitally agile actors.

If we take a look at future battlefields, we can only expect the weapons of information to play an increasingly important part in achieving national and military objectives. In this article we suggest a new framework for military influence operations, one that we argue will in part assist militaries in both understanding and addressing the various factors contributing to the phenomenon. The key questions we ask using the framework is whether (just like cyber weapons) the weapons of information should actually be treated as weapons, and could there be similar rules of conduct for information wars as there are for "traditional", kinetic warfare? In our article we take a look at the rhizomatic information battlespace, what weapons of information look like, how they should be treated in terms of international conflict, and how their use could be attributed to an actor.

BACKGROUND

A certain utopian hype, promising to deliver more than it actually does, always accompanies the appearance of new technology. At the same time there are fears that new technologies, such as military robots, will destroy us. The communication technologies that dominate today's information battlespace are relative newcomers. Print media started in the West in around the 17th century, and the audio-visual media was largely developed during the 20th century. However, cell phones, laptops and GPS as digital phenomena are only 20-30 years old, and thus it is still quite early to estimate the long-term influence they will have on the deep culture of societies. The most important change caused by these technologies, however, is that we carry "the online" constantly in our pockets or on our wrists (Van Den Eede et al., 2017, p. xvii).

One major advantage provided by the Internet is the global reach in communications, which is an asset for anyone willing to influence large audiences. If we take a look at history, the ability to influence target audiences has always been largely defined by technology. The introduction of the aircraft allowed for propaganda leaflets to be distributed amidst the enemy combatants, and the introduction of radio and TV (or rather the mass number of receivers) allowed for propaganda to be transmitted more effectively across national borders or frontlines. The reach of these propaganda means was, however, mostly local. Equally, mitigating these means of influence was still manageable in a sense, since it was possible to physically shoot down the aircraft carrying leaflets or to compete in terms of transmitting power, using electronic warfare to limit the reach of hostile propaganda (Jowett & O'Donnell, 2012).

The ability to carry the Internet with us at all times has enabled our lives to be permeated by technology. We live in an interconnected world, of which we increasingly make sense by browsing the Internet for information and sharing our lives on social media, sharing both intentional and unconscious information about ourselves. Although the ability to choose the information we seek gives us a false sense of control, the information seeking process is not objective, as someone or something filters through the vast digital storage of billions of related topics, articles and comments for us in the form of various search engines. Additionally, the digital footprints we leave behind and our dependence on the Internet and its filters are golden opportunities for anyone who wishes to advance an agenda and shape our perceptions (Sartonen, Huhtinen, & Lehto, 2015).

The global and permeating (both in reach and fields it concerns) nature of the Internet, combined with our everyday dependence on it (including the Internet of Things, IoT, devices), means that it is difficult to "shut the Internet down", should its contents not please the local authorities. There are, of course, multiple ways of controlling the influx of information, ranging from legal and technical means to invoking social and peer pressure on the use of the Internet. Still, the sheer amount of data flowing within the Internet makes it, at least for the time being, hard to control the influences and perceptions these data flows present.