Chapter 11
The Double Edge of the Information Sword

Aki-Mauri Huhtinen
National Defence University, Finland

ABSTRACT

After the collapse of the Soviet Union, the West became increasingly confident that globalization, supported by an information technology network, the internet, would increase openness, liberalism, and democracy – the core values of the "free world." Western leaders knew then, just as they do now, a quarter of a century later, that the power of the internet would grow as the technology that controls its use develops. However, no development is wholly good, and the internet is no exception. It seems that the technology that has enabled us to create a "global village" where people are able to communicate in a way that is open and free, and that bypasses the encumbrances of class and ethnicity, has also brought with it a very dark underworld, an uncontrolled rhizome or meshwork, where propaganda, trolling, and hate speeches are rife. After the 2016 US elections, cyber warfare is no longer just about the technical details of computer ports and protocols. Propaganda as disinformation distributed via social media is rapidly becoming the best hacking tool.

INTRODUCTION

According to Munro (2005), media, business, politics and military organizations are increasingly reliant upon information technology, which means that technology has become a valuable resource and a deadly weapon in its own right. This naturally means that all information, whether political or economic, has become militarized and weaponized (Chong, 2013, 604). Cyber warfare, and everything it entails, from

DOI: 10.4018/978-1-5225-8304-2.ch011

corrupting adversaries' networks to spreading false information, is slowly becoming the most dangerous form of warfare. For example, the Kremlin's weaponization of information, culture, and money is an integral part of its vision for the 21st-century "hybrid" or "non-linear" war. As Gerasimov (2013) has put it: "In the 21st century, we have seen a tendency toward blurring the lines between the states of war and peace". The disinformation distribution machine as a weaponizing media domain calls for close cooperation between political leaders, private companies, and security and military intelligence agencies. It is private companies and investments that are providing the funding for troll factories to hire employees. These employees then create fake social media political groups and fake accounts, while the security and military intelligence agencies coordinate a specific targeting process against those that are the most pertinent from the online influence perspective (Summers 2018).

This paper aims to describe this extremely modern and contemporary process of weaponizing information. First, I will familiarize the reader with the theoretical concept of the rhizome (Deleuze & Guattari 1983). Then, I aim to describe the weaponizing process of information by using Iain Munro's (2005) description of information warfare. I will also integrate some quotes that aptly reflect the Kremlin's new strategic communication policy. These quotes will facilitate the reader's understanding of the rhizome process. Lastly, I will discuss the possible consequences of the phenomenon of a hybrid information environment.

The world has always brimmed with good technological innovations like the printing press, railways, roads, communication lines, and nuclear power plants. But all of these good intentions have a dark side. After the Enlightenment, the West replaced the God system with the techno-natural system in the belief that the new sword has only one good edge, which can be controlled by technological development. After the Cold War, most Western authors believed that the Internet would come to symbolize the new free world, and be controlled like a systematic subway network. At first, there were only a few dark clouds, in the shape of anonymous hackers, but now, for example, the hacker group known as Anunak, based in Russia and Ukraine, is gaining access to the internal payment systems of banks and payment providers and has succeeded in stealing millions of pounds (Flinders, 2014). At the same time, at the political level, Eastern Ukraine, for example, is rife with rioters, ready to break away from their nation's government in Kyiv. This is the message that the Kremlin may want to project to the world, and analysts believe that the Kremlin could use cyberattacks to generate further chaos and advance its objectives (Daileda, 2014). The so-called Internet Research Agency, established as a company in St. Petersburg in 2013, is actually a Russian troll factory designed to monitor political discourse in other countries. Agency employees are between 18 and 20 years old and get paid approximately 2000 US dollars per months to create fake social media accounts and blogs that disseminate disinformation to Americans (Summers, 2018).

Semiotic Brains and Artificial Minds: How Brains Make up Material Cognitive Systems

Lorenzo Magnani (2007). *Semiotics and Intelligent Systems Development (pp. 1-41).*
www.igi-global.com/chapter/semiotic-brains-artificial-minds/28935?camid=4v1a