Chapter 2
Reconceptualising Cyber Security:
Safeguarding Human Rights in the Era of Cyber Surveillance

Andrew N. Liaropoulos
University of Piraeus, Greece

ABSTRACT

The cyber security discourse is dominated by states and corporations that focus on the protection of critical information infrastructure and databases. The priority is the security of information systems and networks, rather than the protection of connected users. The dominance of war metaphors in the cyber security debates has produced a security dilemma, which is not sufficiently addressing the needs of people. This article underlines this shortcoming and views cyber security through a human-centric perspective. Freedom of expression and the right to privacy are under attack in the era of cyber surveillance. From a human-centric perspective such rights should be understood as a critical part of cyber security. Human rights protections need to be effectively addressed in the digital sphere and gain their place in the cyber security agendas.

INTRODUCTION

Over the past two decades, the evolution of cyberspace has impacted almost every aspect of human life. The increase in the speed, volume, and range of communications that cyberspace offers has transformed the way societies interact, how companies deliver services, and how people are governed. The Internet of Things (IOT) and Big Data are already affecting a wide range of social activities (Cukier & Mayer-Schoenberger, 2013). The cyber domain also poses a growing number of challenges to security. Critical national infrastructures are vulnerable to cyber attacks, and the global economy is exposed to the threats of cyber-espionage and cybercrime. Worms, viruses, sophisticated Distributed Denial of Service (DDoS) attacks, and spam cost the global economy billions of dollars. Cases such as the cyber attacks on the online banking system in Estonia and the use of the Stuxnet worm to harm Iran's nuclear

DOI: 10.4018/978-1-5225-5634-3.ch002

program demonstrate the crucial role of cyberspace for national security. Naturally, states have defined cyberspace in their military and security doctrines as a new domain of conflict.

The cyber security discourse is predominantly shaped by the notion of national security. The release of national security policies and governmental reports, the establishment of cyber-commands and Computer Emergency Response Teams (CERTS), the amount of money spent to defend cyberspace, and the discussion of a cyber-arms race are indicative of this trend (Kramer, Starr, & Wentz, 2009). Although this approach is to a large extent justified, it is also deficient, since it does not consider the human rights protections of around 2.7 billion Internet users (Mihr, 2014, p. 26). Over the past years, the development of Internet censorship techniques and Edward Snowden's revelations about the global surveillance carried out by the United States National Security Agency (NSA) vividly demonstrate that Internet freedom, anonymity, and personal data are constantly under attack. Citizen's communications are vulnerable to interception and surveillance (Comninos & Seneque, 2014). Therefore, cyber security should not only address the security threats against the state and the private sector, but also (if not primarily) the needs of people.

This article shifts the focus of cyber security from the protection of critical national information infrastructures to that of human rights in cyberspace. The goal is to point out the need for a human-centric approach that addresses digital human rights violations, Internet freedom, and privacy of data. The first section of the article briefly reviews the concept of cyber security and analyses the prevailing approach that perceives cyber security as a national security issue. What is the meaning of the term 'cyber security' and what is it in cyberspace that needs to be protected? The paradoxes of the cyber security dilemma reveal the misperceptions regarding the nature of threats in cyberspace and the referent object of security. The second section reviews examples of human rights violations in cyberspace. Cyber surveillance, internet filtering tools and online censorship are some of the measures used by states. The final section addresses the need for an alternative view of cyber security, one in which the human element is at the epicentre. The argument is that people should have their human rights protected, both offline and online. The unwillingness of states to endorse these rights and the lack of a global governance regime, sketch a rather gloomy picture for the future of human rights in cyberspace.

DECONSTRUCTING CYBER SECURITY

Cyberspace has become an integrated part of human society, and society's dependency upon its infrastructure is constantly increasing. When approaching a contested concept such as cyber security, the reader has to bear in mind the following. First of all, there is no explicit definition of what constitutes cyber security, partially because a universally accepted definition of cyberspace is still lacking. Cyberspace is a term whose definition is hard to pin down and is widely used as a synonym for Internet or the World Wide Web (Betz & Stevens, 2011, p. 13). A popular definition is that of Daniel Kuehl, who defines cyberspace as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies" (Kramer, Starr, & Wentz 2009, p. 28). The critical question when approaching cyber security is whether one views cyberspace as a global network that involves solely hardware, software, and information systems, or also people and the wide range of social interactions that takes place within this network.