Chapter 14
A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict

Christian Czosseck
Estonian Business School, Estonia

Karlis Podins
Tallinn University of Technology, Estonia

ABSTRACT

Throughout history, mankind has developed and employed novel weapons and countermeasures. Both offensive and defensive weapon systems are limited by the laws of nature. Consequently, military concepts and doctrines were designed by implicitly taking into account those limitations. The digital age has introduced a new class of weaponry that poses an initial challenge to the common understanding of conflict and warfare due to their different characteristics: cyber weapons. This article explores the crucial differences between the conventional weapon and cyber weapon domains, starting a debate as to what extent classical concepts and doctrines are applicable to cyberspace and cyber conflict. The authors propose a definition of cyber weapons being an instrument consisting primarily of data and knowledge, presenting them in the form of prepared and executed computer codes on or a sequence of user interactions with a vulnerable system. The authors describe a vulnerability-based model for cyber weapons and for cyber defence. This model is then applied to describe the relationship between cyber-capable actors (e.g. States). The proposed model clarifies important implications for cyber coalition-building and disarmament. Furthermore, it presents a general solution for the problem of the destruction of cyber weapons, i.e., in the context of cyber arms control.

1. INTRODUCTION

As conflicts have moved into cyberspace (and vice versa), a clearer understanding of cyber weaponry and its implications to conflicts becomes a necessity. The development of weapons was always part of mankind's history. Tactics evolved to suit weapons available, but from time to time new weapons revolutionised the tactics and strategies of warfare. The developments of artillery, gunpowder, aviation and weapons of mass destruction are just some examples from history.

DOI: 10.4018/978-1-4666-5942-1.ch014

These all caused dramatic changes on the face of the battlefield. But all those weapons developed so far have similar kinetic and/or thermal properties, due to the shared physical domain.

As one result of the cyber attacks on Estonia in 2007, a campaign of massive distributed denial of service (DDoS) attacks against government websites paired with hacking attempts against valuable targets such as ISP backbone routers (Evron, 2008), a new type of conflict was declared (Landler & Markoff, 2007) and hyped. In reality, hacktivism has been around already before the 2007 attacks against Estonia (Denning (2001)introduced this term already back in the early century) and politically motivated DDoS where at this point of time not entirely new as shown by (Nazario, 2009). Still media found strong and inconsistent interest in this subjects as discussed by Farivar (2009). As a consequence, cyber conflicts quickly entering the political agenda of many nations to the extent that and that Jellenc (2012) recently confirmed an arms race having started in and about cyberspace.

The term "cyber attack" is commonly used for a wide variety of malicious cyber activities aiming to achieve various objectives. Both attacker and victim can e.g. be a States, private sector (as attackers also including organized cyber crime) or groups of individuals (see Table 1).

As illustrated in Table 1, there are numerous rationales for the different actors to use cyber attacks for their benefit spanning from propaganda/ psychological operations (e.g. Israel-Palestine), espionage, censorship, information operations as part of military conflicts or even sabotage causing physical destruction to support political goals.

However, several years later we still have not seen a commonly agreed definition of cyber weapons or cyber warfare (Ottis & Lorents, 2010).

In the following section 2, central terms will be defined and a short overview of the special properties of cyber domains and cyber weapons will be given. The concepts and terminology initially used were based on those of conventional weapons or weapons of mass destruction (Sharma, 2009). Unfortunately, cyber weapons, as we will argue in this paper, follow other rules than their conventional counterparts. Thus the effects of cyber weapons on their targets are different. In 2007, a direct, destructive cyber attack on a power generator was proven possible in a real-life experiment (Herold, 2007). The prominent case like *Stuxnet*, which is assumed to have sabotaged

Table 1. Examples of cyber attacks between different groups

Attacker vs. Victim	State	Private Sector	Group
State	Stuxnet (Falliere, Murchu, & Chien, 2010), Georgia: Conventional military conflict combined with cyber attacks (Korns & Kastenberg, 2009)	DigiNotar (Denis Fisher, 2012), Saudi Aramco (Perlroth, 2012)	Censorship in Belarus (Pavlyuchenko, 2009), Russia against opposition parties (AFP, 2011)
Private sector	Ghostnet (Deibert, Manchanda, Rohozinski, Villeneuve, & Walton, 2009), Shadows in the Clouds (Bradbury & Rohozinski, 2010)	Cases of common industrial espionage	Hollywood poisoning torrents with fake releases (CERT Polska, 2012)
Group	Cyber attacks on Estonia 2007 (Ottis, 2008)	Anonymous on VISA (Pras, Sperotto, Moura, & Drago, 2010), TJMaxx credit card data theft (Jewell, 2007)	Israel-Palestine