Chapter 61
Defining Cyber Weapon in Context of Technology and Law

Prashant Mali
Cyber Law Consulting (Advocates & Attorneys), India

ABSTRACT

This article describes how the interconnected world of today, or the cyber space so often called, is easily accessible through a wide array of devices and has an impact and reach beyond geo-political boundaries Owing to high levels of connectivity and the nature of E-governance activities today, the cyber space is rapidly becoming a potential global battlefield for cyber warfare among various state and non-state entities. An effective cyber weapon in this space is like an indicator of cyber power, its nature being offensive or defensive. Parameters of effectiveness and reliability range from the type of developer of the weapon, whether state or non-state to its longevity in time and technology and others like possibility of an economic implementation along with the scope of its usage. This article is aimed at analyzing existing definitions, opinions and notions about cyber weapons and defining the term cyber weapon from a techno-legal perspective, which could be universally acceptable and have characteristics of enforceability across all domains: civil, criminal & defense applications.

1. INTRODUCTION

The world is speaking of cyber warfare today with enhanced capabilities of computer systems and networks. The annual Worldwide Cyber Threats report by the Director of National Intelligence identifies politically motivated actors as a growing reason for cyberattacks (Clapper, 2015). It goes on to identify not just political but some threat vectors from smaller non-state bodies as well. Not too long ago, the United States Defense Advanced Research Projects Agency (DARPA) funded Plan X, which is a foundational cyber warfare program to develop platforms for the Department of Defense to plan for, conduct, and assess cyber warfare in a manner similar to kinetic warfare (Brecht, 2015). The understanding of cyber warfare flows from kinetic warfare in the sense that it essentially must use some weapons as well. When translated from kinetic weapons like bombs and guns, cyber warfare involves cyber weapons that could be devices or lines of code. Amassed both by state and non-state actors, cyber weapons have known to be used at multiple instances across the globe (Dunn, 2015).

DOI: 10.4018/978-1-5225-7909-0.ch061

The Internet has permeated all essential layers of our lives; the way we watch, the way we talk and entertain ourselves is all governed by the Internet (Brecht, 2015). This has opened gates for Ransomware type of Cyber Weapons like WannaCry and Petya globally because everyone ranging from deep pocketed firms to a broke restaurant server were victims. This is not just with the target victims but also with the target devices of Cyber Attacks: they range from smart power and gas utilities of the state to the IOT devices that citizens use, meaning that orchestrating a nationwide shutdown via cyber weapons is seemingly possible. Recent reports and claims suggest involvement of a nation-state in orchestrating such an attack (Cameron, 2017).

One of the biggest challenge that the law has faced since the beginning of the 20th century has been to adapt with the changes in technology: the cyberspace has been no different, rather even more challenging. There have been attempts at reaching a convention about using Information Systems in Armed Conflicts (Brown, 2006) and a treaty for the Cyber Space (Hughes, 2010) but on an International legal forum there has been no concrete discussion whatsoever. Scholars have even envisioned a cyberattacks treaty given the nature and frequency of such attacks (Moore, 2013). With all these developments picking pace, there are still irregularities in the definition of the word 'Cyber Weapon'.

Though not precise yet various scholars and experts have done their best to put forward their ideas to define the term. They have been either tested technically at some stage or legally at another, none of which has met recognition yet. Therefore, one primary object of this paper is to analyze the existing definitions and classifications related to cyber weapons and to propose a possible definition which is both technically and legally relevant. What makes it difficult to conclude a meaningful legal response to what Cyber Weapon is, is the fact that cyber warfare, cyberattacks and cybercrime are all loosely defined themselves (Hathaway, Crootof, & Levitz, 2012). Cyber War has been famously defined in a book by a US Government Security Expert as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Michael, 2010). The definition does not talk about how and up to what extent should the disruption be and what penetration qualifies as penetration enough. Another front where the definition is lacking is the possibility of involvement of a non-nation-state actor in committing an act of attack on a nation state or even upon a non-nation-state entity but causing an effect on the entire state at large. A cyberattack has been called an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it (Farhat, Mccarthy, & Raysman, 2011). But this misses the factum that a cyberattack might be aimed at just gaining access and causing disruption of some other services which are not at all cyber.

Another concern for defining any "cyber" word is the problem of non-application of a traditional principle of law to the cyber space. Often, debates arise as to why at all is there a need to define cyber weapons. There has been an assertion about the fact that in the absence of a globally accepted and clear technolegal definition, it is difficult to recognize true acts of cyber warfare, prevent attacks and demark accountabilities and legal responses (Brecht, 2015). Through this paper, it will also be clear that how International law principles can apply to instances of a cyber war with respect to cyber weapons which might not be a far-fetched occurrence.