# World War III:
## The Cyber War

*Mandeep Singh Bhatia, Lyallpur Khalsa College, Jalandhar, India*


## ABSTRACT

*"I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones." The above quote by Albert Einstein clearly forecasts the weapons of World War IV, but not anything about the weapons of World War III. What will be the weapons of World War III? How dangerous will World War III be? What will be the impact of World War III? This paper aims to answer these questions. Increasing commercial use of the Internet has heightened the security and privacy concerns. This paper shows the extent of risk to the life of an individual, country and to the whole world from cyber crime, which may lead to the cyber war. So the World War III would be the cyber war with the attacks of cyber bombs by cyber attackers. Further, this paper shows a comparison of cyber and traditional war with the after affects of both types of wars.*


*Keywords: Cyber Attacks, Cyber Bombs, Cyber Threats, Cyber War, Cyberspace, World War III*

## INTRODUCTION

The term Cyber warfare involves the units organized along the nation-wide boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means (Billo & Chang, 2004). A number of nations are incorporating cyber warfare as a new part of their military doctrine. Some that have discussed the subject more openly include the United Kingdom, France, Germany, Russia, and China (Cornish, Livingstone, Clemente, & Yorke, 2010).

Green (n.d.) the senior vice president of McAfee Avert Labs says the quote "Cyber-crime is now a global issue. It has evolved significantly and is no longer just a threat to industry and individuals but increasingly to national security." He predicted that the future attacks will be even more sophisticated. Attacks have progressed from initial curiosity probes to well-funded and well organized operations for political, military, economic and technical espionage.

The cyber war is a new kind of high-tech war, without public debate, media discussion, serious congressional oversight, academic analysis, or international dialogue. The Cyber war may be committed against the different cities, states or countries. The cyber war may intentionally harm the victim by causing the physical or mental injury directly or indirectly, using modern telecommunication technology such as Internet and mobile phones. Just like the tools of conventional warfare, cyber technology can be used to attack the machinery of state, financial institutions, the national energy and transport infrastructure and public morale (Cornish, Livingstone, Clemente, & Yorke, 2010). Hackers and other individuals trained in soft-

DOI: 10.4018/ijcwt.2011070104

ware programming are the primary executors of these attacks (Billo & Chang, 2004). These individuals often operate with the support of a country or the terrorist organizations.

The cyber war originates from the simple cyber attacks, which are likely more frequent than state-sponsored activities. These other attacks or intrusions also are unauthorized attempts to access computers, computer controlled systems, or networks. These activities can range from simply penetrating a system and examining it for the challenge, thrill, or interest, to entering a system for revenge, to steal information, cause embarrassment, extort money, or cause deliberate localized harm to computers or damage to a much larger infrastructure, such as a water supply or energy system. These cyber attacks might be referred to as hacking, cyber mischief, cyber hooliganism, personal or corporate theft, revenge, or espionage.

The biggest secret about the cyber war may be that it is very difficult or even impossible to defend the nation effectively from cyber attack. A cyber-war, in fact, would even allow smaller States, which are normally incapable of competing either militarily or economically with larger international powers, to attack the critical systems of other State targets (Mele 2010, p. 8). Cyber warfare could be the archetypal illustration of "asymmetric warfare' – a struggle in which one opponent might be weak in conventional terms but is clever and agile, while the other is strong but complacent and inflexible (Cornish, Livingstone, Clemente & Yorke, 2010).

## WEAPONS TO BE USED IN CYBER WAR

A cyber weapon is a tool that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things (Rid & McBurney, 2012). As traditional weapons, the cyber weapons can be low potential or high potential. The low potential weapons are easily available weapons used by many to play and making fun of it. The high potential cyber weapons are the modern high tech weapons in which the target is programmed into the weapon itself. It may be a learning weapon that could observe and evaluate the specifics of an isolated environment autonomously, analyze available courses of action and then take action (Rid & McBurney, 2012).

In the first decade of the twenty-first century, the U.S. developed and systematically deployed a new type of weapon, based on our new technologies. On October 1, 2009, a general took charge of the new U.S. Cyber Command, a military organization with the mission to use information technology and the Internet as a weapon. Similar commands exist in Russia, China, and a score of other nations. These military and intelligence organizations are preparing the cyber battlefield with things called "logic bombs" and "trapdoors," placing virtual explosives in other countries in peacetime (Clarke & Knake, 2010). The New York Times calls Stuxnet 'the most sophisticated cyber weapon ever deployed against another country's infrastructure' (Rid & McBurney, 2012).

The Internet security company, McAfee (2007) stated in their annual report that approximately 120 countries have been developing ways to use the Internet as a weapon, and the targets are the financial markets, government computer systems and utilities. Malicious software (malware), networks of 'botnets' and logic bombs can all be employed to navigate target systems, retrieve sensitive data or overrule command and control systems (Cornish, Livingstone, Clemente, & Yorke, 2010). Terrorist groups like Al Qaeda do make significant use of the Internet, but as a tool for intra-group communications, fund-raising and public relations. Cyber terrorist could also take advantage of the Internet to steal credit card numbers or valuable data to provide financial support for their operations (Lewis, 2002).

The cost to develop this new class of weapon is within the reach of any extremist group, criminal organization and a country. The raw materials needed to construct cyber