Chapter 13
OSNs as Cyberterrorist Weapons Against the General Public

Nicholas Ayres
De Montfort University, UK

Leandros Maglaras
De Montfort University, UK

Helge Janicke
De Montfort University, UK

ABSTRACT

Conventional terrorism has been around for hundreds of years and even though its tactics and the weapons of choice have evolved over time as well as the use and deployment of weapons may have changed the root definition of terrorism has remained relatively untouched. With the advent of mass computing, cybercrime has increased year on year. This chapter will look at three differing viewpoints of cyberterrorism and its ultimate effects on society. Many industry and academic experts warn that it is only a matter of time before conventional terrorist acts will migrate to the digital arena in the form of cyberterrorism. Current literature suggests that a countries critical national infrastructure will be the main focus of attack for the cyberterrorist but this chapter will address another possible target for the cyberterrorist using a different type of cyber weapon: a mimetic virus. This chapter also looks at how a mimetic virus could use social media to spread throughout the target audience using what is known as Internet memes.

INTRODUCTION

In 1990 the National Security Council envisaged that computers could in the future be used to not only facilitate crime but as the main tool for criminal acts; 'The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb' (National Research Council, 1990). With the rise in global terrorism and the mass use of computers a new and potentially more destructive form of terrorism has come to the fore: cyberterrorism. Conventional terrorism has proved over time to be a controversial subject due to the lack of a unified

DOI: 10.4018/978-1-5225-7912-0.ch013

global definition of what constitutes an actual terrorist act. Controversy also surrounds cyberterrorism but these centre around whether a cyberterrorist attack using digital weapons can in fact have the same profound impact as conventional terrorism using traditional kinetic weapons. This chapter looks at three different viewpoints when it comes to what is a cyberterrorist and what constitutes as a cyberterrorist attack. Current literature states that if there was a cyberterrorist attack the most likely target would be against a countries critical infrastructure (CI) or critical national infrastructure (CNI) as these systems underpin a countries society and if attacked could have nationwide effects not just on services but the population as a whole. This chapter will also look at why CI /CNI may indeed not necessarily be the main focus of an attack but will show how the public could be directly attacked using a much more focused and specific kind of digital weapon.

Conventional Terrorism vs. Cyberterrorism

In order to fully comprehend the term cyberterrorism; first introduced by Barry Collin in the 1980s (Gordon & Ford, 2002) we must begin by looking at the evolution of conventional terrorism. Terrorism has always been a controversial subject, which 'has been well studied and documented' (Collin, 1997:pp 15-18) but there is a lack of a globally accepted academic or legal agreement on its true definition (Schmid, 2011). The quote "One man's terrorist is another man's freedom fighter" (Seymour, 1975) has been cited many times in relation to Middle East conflicts and uprisings in Africa and Central America (National Research Council, 1990) to name but a few. This lack of a definitive global definition is largely because the act is a highly political and emotionally charged one and governments are reluctant to agree on a legally binding definition (Hoffman, 2013). That being said there is a general global consensus that terrorism is an act which is perpetrated by individuals, groups or governments to instil fear and terror in non-combatants through the use of violence, in order to pursue a political, ideological or religious goal. In essence terrorism is the use of or threat of violence or damage to life and property with the intention of influencing a government or society through a political, religious or ideological cause. Terrorists believe they are 'legitimate combatants' fighting for their beliefs using whatever means possible in order to 'attain their goals' (International Terrorism and Security Research, 2015). Conventional terrorism has had a huge global impact in modern history. For an act to be considered terrorism the target of an attack must be non-combatants; in essence the general public. During the 1972 Munich Olympics the Palestinian terrorist organisation Black September took hostage and ultimately killed 11 Israeli athletes. The 11 victims were the direct targets of the attack but the indirect or actual target was the estimated 1 billion people who were watching the televised event around the world who were 'introduced to fear - which is terrorisms ultimate goal' (Anon, 2015). The United States went to war with the ruling Taliban party in Afghanistan with the sole intention of dismantling the terrorist organisation al-Qaeda, which was using the country to train and indoctrinate fighters, import weapons and plot terrorist actions (Zelikow, 2011). The U.S. invasion of Afghanistan was the principle reaction to the 9/11 terrorist attacks on the World Trade Centre and Pentagon (Thruelsen, 2006) by al-Qaeda. Another motive for the 9/11 attacks may have been to coerce the U.S. into a war that would incite a pan-Islamist revolution (Duran, 2002, pp. 22-42). Whatever the ultimate motive was for the 9/11 attacks it was an unlawful use of violence, motivated by ideological beliefs, which instilled fear and coerced a government in pursuit of al-Qaeda's goal.

Cyberterrorism is seen by many to be a digital extension of conventional terrorism but the act of terrorism occurs solely in cyberspace. In 2000 Dorothy Denning's testimony before the Special Oversight Panel on Terrorism is one of the most cited papers on the issue of cyberterrorism. She stated that