Committee: Disarmament & International Security

Topic: Civilian targets in cyber warfare

DEFINITION OF KEY TERMS

Cyber Warfare

The utilisation of computer technologies to disrupt the activities of a state, nation or organisation: especially the deliberate attacking of information systems for strategic or militant purposes.

Malware

Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Worms

A computer virus which replicate themselves through computer networks – damaging data on multiple computers/systems.

Botnet

A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

Trojan Horse

a program that seems to perform a useful function, but actually breaches the security of a computer: potentially a form of spyware.

Zombie Networking

A zombie network is a network or collection of compromised computers or hosts that are connected to the Internet. A compromised computer becomes a zombie that is wirelessly controlled through standards based networking protocols like HTTP and Internet Relay Chat (IRC).

CIA

The CIA is the government organization in the United States that collects secret information about other countries. CIA is an abbreviation for 'Central Intelligence Agency'.

FBI

The FBI is a government agency in the United States that investigates crimes in which a national law is broken or in which the country's security is threatened. FBI is an abbreviation for 'Federal Bureau of Investigation'.

Internet Mafia

Resembling the traditional hierarchically structured secret organisation allegedly engaging in various criminal activities, except evolved to take advantage of the internet – acting as platform of their supposed crimes.

INTRODUCTION

An issue that as consumed much of modern militant operations is the concept of Cyber-warfare; a type of modern warfare where one party deliberately penetrates the information networks of another with the intention of disrupting or damaging it. While commonly referring to the actions between nations, it can also involve non-national actors such as hacktivist groups, terrorist organizations, crime syndicates and extremists. As modern governments become increasingly reliant on information technology, the 'cyberspace' has become the new warzone of the 21st century: defined by the US Security, it is information infrastructure has become so crucial that "the incapacity or destruction of such systems and assets would have a debilitating impact on security, economic security, public health or safety, or any combination of those matters." Thus, the question at hand arises: the extent to which such warfare should affect the unsuspecting individual. Referring to incidents of such as Snowden's release of classified NSA details about the CIA: should the privacy of the individual remain a priority, or is it simply a casualty of this new form of warfare.

TIMELINE OF EVENTS

DATE	EVENT
1970	Development of early 'Worm Attacks' – currently referred to as 'Ancestor Worms'. Initiated development of further malicious software.
2003-2006	Worm viruses created in to compromise computers: initiating the first malicious botnet.
2005-2007	Internet Mafias, like the Russian Business Network (RBN) proliferate their reign on the web.
2006-Present	Hackers in China attack computers in the U.S. through the use of various malware.
August 13th 2006	Botnet Herders attach the 'Microsoft wormhole'.
January 2007	1 million computers remotely controlled network of 'zombie' computers, linked by a worm attack. The trojan in thought to have spread via email spam.
June 13th 2007	FBI operation, "Bot Roast", goes after botnet farms.
September 7th 2007	Multi-stage Botnet attack on E-Bay.
August 27th 2008	NASA provides confirmation on the discovery of a worm on laptops on the International Space Station.
November 30th 2008	Pentagon Computers were hacked by computer hackers suspected of working from Russia.
December 25th 2008	India's largest bank, State Bank of India, was hacked y a hacker group from Pakistan.
January 8th 2008	Israeli students developed a program that allows Israeli citizens to be controlled by an Israeli Hacker group that targets 'Pro-Hamas' websites.

Summer 2009	Insurgents compromise U.S. Drones. Off-the-shelf Russian software was used by insurgents to intercept live video feeds.
December 2009	Along with a Zero day attack on IE 6, 34 American companies were compromised, including Sony and Google. During these attacks intellectual property was stolen; though it is theorised to be China, they deny all involvement in such attacks.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

Russia

In 2008, Russo-Georgian War broke out. Weeks prior to the annexation of South Ossetia, 'zombie' computers allegedly already commenced attacks on government websites, including the Georgian president. This escalated into large-scale denial-of-service on both civilian and government infrastructure: information networks between the military and the bureaucracy were disrupted. Additionally civilian networks were also hacked and its contents either replicated or replaced. Thus it seemed as though this had opened up a new era of warfare where even concrete targets and infrastructure were not spared from cyberwar, a particularly severe problem given our dependence on information networks .

China and the United States of America

Both China and the US have repeatedly accused the other of cyberespionage. In 2009, the US created the US Cyber Command as an armed forces subunit in the NSA for both attack and defence. Similarly, China is believed to have both specialized military network warfare forces within the People's Liberation Army, authorising civilian hackers as part of its operations. In 2016, the Pentagon published a report asserting that China 'is using its cyber capabilities to support intelligence collection against the US diplomatic, economic, and defence industrial base sectors", which Chinese authorities denied.

Additionally, China has been conducting industrial espionage on American companies largely through the cybersphere, though no clear evidence has been presented. This shows how cyber warfare differs from conventional warfare in that it is difficult to gather compelling evidence and apportion blame.

The United States of America and Iran

The US has been accused of cyberattacks on Iran. Most notably, Iranian authorities accused the US and Israel for sabotaging Iranian nuclear capabilities, after the productivity of uranium enrichment facilities in Natanz fell by 30% in 2010. Stuxnet is a computer virus that specifically targets industrial control systems (such as power plants, water treatment facilities and gas pipelines).

BIBLIOGRAPHY

- Landesman, Mary. “Should I Worry About the Stuxnet Worm Computer Virus?” Lifewire, Lifewire, 12 Feb. 2020,

  www.lifewire.com/stuxnet-worm-computer-virus-153570.

- “What Is a Zombie Network? - Definition from Techopedia.” Techopedia.com,

  www.techopedia.com/definition/27201/zombie-network.

- Bradley, Tony. “Cybercrime Is The Modern-Day Mafia.” Forbes, Forbes Magazine, 16 Oct. 2015,

  www.forbes.com/sites/tonybradley/2015/10/16/cybercrime-is-the-modern-day-mafia/.

- Wyman, Oliver. “Global Cyber Terrorism Incidents on the Rise.” Marsh & McLennan Companies,

  www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.

- “Cyber Warfare.” RAND Corporation, www.rand.org/topics/cyber-warfare.html.

  www.rand.org/topics/cyber-warfare.html.