Origins of Cyberwarfare: How the Internet got Weaponized

Ada Peter and Ujunwa Ohakpougwu
Communications Department, Covenant University, Nigeria

ada.peter@covenantuniversity.edu.ng;
ado909@g.harvard.edu
Ujunwa.ohakpougwu@stu.cu.edu.ng

Abstract: Cyberspace was until last decade and half a perfect additional intelligence gathering tool. Within a phase of time during the spread of the world wide web, the cyberspace expanded outside the boundaries of intelligence gathering to a perfect weapon in the hands of both state and non-state actors for destabilizing or devastating the state of critical infrastructures of perceived enemy or competitors. In the heart of the storm, Social Scientists have either focused on extensive definitions and clarifications of cyberwar, others are fixated on explaining the various emerging dangers of cyber weapons on society, like the consequences of weaponizing the cyberspace against a nation's power grid, nuclear command, and control systems, neutralizing a petrochemical plant, paralyzing a government's health care or governance structure and possibilities of manipulating elections. But few, if any have considered the question which is central to this paper: How did the cyberspace evolve from an intelligence tool to a cyberweapon against critical infrastructures? The obvious answer is that the magnified global access and use of networked systems provided the perfect battle space for deploying cyberweapons. The preceding explanation is essentially correct, but it is entirely lacking in detail explaining how cyberspace became weaponized? Under what conditions was cyberspace purely an intelligence tool. Under what conditions is cyberspace weaponized? This research incorporates these and other questions into a framework through the means of a model designed to aid understanding of how the cyberspace evolve from an intelligence tool to a destructive weapon targeted at critical infrastructures. Primary sources include relatively untapped 107 Congress Laws on Cyber related legislations. From the 105th congress to the current 116th congress, 1, 177 legislations have been introduced on cyber or cyber related issues. Other primary sources include White House fact sheets, statements, press releases, President Trump's 2018 National Cyber Security Strategies, President Obama's 2016 Cyber Security National Action Plan, and cyber related executive orders, statements, and press releases from President Johnson of the last 5 US administrations.

Keywords: Cyberwar, cyberweapons, cyberspace, cyberwarfare, U.S legislations, National Cyber Security Strategies

1. Introduction

Cyberspace was until the 21st century, an additional intelligence-gathering and communication tool. As an intelligence tool, state actors collected secret or open information via covert or overt digital activities. The secret information ranged from U.S. data about the intentions and capabilities of other nations to U.S. understanding of the level of data other nations have about U.S. surreptitious capabilities and intentions. The covert activities seemed like inter-national hide and seek games, guided by self and globally initiated rules. The massive leak of NSA documents in 2005 detailing U.S. surveillance programs, accessing internet company data, eavesdropping, and tapping fiber optic cable explains how nations collected information through covert digital activities (Popovich and Chen 2013).

While it is arguable that intelligence gathering through cyber means was a weapon that provided undue advantage over allies and adversaries, at the time however intelligence gathering through cyber means lacked the sole capability of wreaking havoc without successive actions and decisions. Intelligence gathering through cyber means was by itself harmless unless used as the basis for decisions and actions that may be destructive.

However, beginning February 1990, when the era of military involvement in the operation of the internet ended, and ARPANET decommissioned, the network grew faster, access and use of the world wide web spread like an unending spider web, and the cyberspace expanded outside the boundaries of intelligence gathering to a perfect weapon in the hands of both state and non-state actors who destabilize or devastate critical infrastructures of perceived enemy or competitors. These state and non-state actors used the cyber weapon to incapacitate an adversary's national critical infrastructure, frustrate it, slow it, undermine its institutions, and leave its citizens angry or confused (Sanger 2018). Examples include the 2022 disruption of US gas pipelines, Russia's alleged use of fake social media campaigns to interfere in U.S. 2016 presidential election; the late November 2014 North Korean attack on Sony Pictures in connection to the planned release of the poorly reviewed movie *the interview;* the 2010 American *Stuxnet* attack on Iran and North Korea's weapons program, the Chinese decades-long espionage of U.S. trade secrets, and 2007 Russian attack on many of Estonian government departments, political parties, media organizations, and companies.

At the heart of the cyber weaponization storm, social scientists have focused on extensive definitions and clarifications of cyber warfare, what it means, what it entails, and whether threats can deter, or defense can