Today's advancing technology and why prevention of cybercrimes should be priority...

Law, Crime

Introduction

With the global connectivity thanks to advancement in technology such as computers and the internet, we can be interconnected around the world from the comfort and privacy of own our home. Though with this luxury, everybody faces a lot of risks being so connected due to hackers. Cyber security has only recently became a security issue on a global scale. Due to the heavy connectivity and the rise of communication technology, this borderless exchange requires a global cooperation of monitoring to ensure safety in virtual reality. Cybercrime, whether it being traditional crimes that could be infiltrated offline or cyber-terrorism, has substantially risen over the past decade.

Background

A large range of crimes is now being perpetrated through cyberspace. Cybercrime is now a business exceeding over a trillion dollars a year.(“ Cybersecurity: A Global Issue”, 2011) Such crimes would be financial fraud, selling illegal drugs and weapons, identity theft, intellectual property violations, and the exploitation and the distribution of child pornography. These crimes not only having substantial human consequences, but now have a high economic consequence as well. As information technology becomes more integrated with physical infrastructure operations, the risk and the consequences increase substantially. According to a Norton study, threats to cyberspace have increased afflicting 431 million adult victims globally, with over one million victims of cybercrime every day. (“ Cybersecurity: A Global Issue”, 2011)

These malicious actors could potentially harm services upon the country’s (possibly the world’s) economy and affect the daily lives of millions. Cyberspace is mostly difficult to secure due to the ability of malicious actors to operate in any given location, the difficulty in reducing vulnerabilities as well as the consequences in these cyber networks, and the heavy links between cyberspace and physical systems and infrastructure. (Cybersecurity Overview, 2015)

The federal government has taken numerous steps at addressing cyber threats for their high impact. Constant enhances remain in order to protect cyber-reliant critical infrastructure such as the enhancement of cyber security air traffic control systems, the oversight of contracting IT services, implementing strategies to address the risk of federal control systems and buildings , and the improvement of security incident responses. (Wilshusen, 2015)

Though the first threat to cyberspace was in 1988 with the Morris worm, which at the time affected the world’s small nascent cyberinfrastructure, in 2007 the US Secretary of Defense email was hacked by unknown foreign intruders. Though between these two decades there have been numerous cyber-attacks on many countries besides the U. S. including Estonia, Russia, and China with various attacks such as Trojans, spyware, hacking, as well as many other forms. (“ History of Cyber-Attacks”, 2014)

The Director of US National Intelligence makes a worldwide threat assessment of the US intelligence community every year, listing the

potential dangers of the country, in 2007 cyber crimes were not on the list or anything related to cyberspace. As of 2009, cybercrimes made it onto the threat assessment, but it was at the very bottom. Within the last few years, cyber crimes have substantially risen to the top of the threat assessment proving to be one of the biggest threats not only to the United States but other countries as well. As of today, the DNI threat assessment has Cyber as the number one global threat, right above counterintelligence and terrorism. (Clapper 2015)

The DNI Threat Assessment states, “ A growing number of computer forensic studies by industry experts strongly suggest that several nations including Iran and North Korea have undertaken offensive cyber operations against private sector targets to support their economic and foreign policy objectives at times concurrent with political crises”. Many denials of service attacks (known as DDOS) has occurred on the US financial sector JPMorgan. JPMorgan announced plans for annual cybersecurity expenditures of over $250 million by the end of 2014 with the possibility of doubling the annual security computer budget over the next few years. Though this event was not the only major event that was listed on 2014 the DNI’s Threat Assessment, major companies such as Community Health Systems and Home Depot experienced security breaches from foreign hackers such as China. (Clapper, 2015)

Politically motivated cyber-attacks are growing at a quick rate. Foreign actors are developing access to the US cyber-infrastructure systems for exploiting and to cause hostile disruptions. These threatening actors

conducting cyber espionage target government, military and commercial networks typically on a daily basis. The Director of National Intelligence states; “ These threats come from a range of actors, including nation states with highly sophisticated cyber programs (such as Russia or China), nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea), profit-motivated criminals, and ideologically motivated hackers or extremists”. (Clapper, 2015) Though distinguishing between actors and non-state actors within the same country causes mass difficulty.

Analysis

In the perspective of a realist, cyberspace fits the model of a realist “ security dilemma”. Cyberspace is primarily anarchic, truly no governing body, with a limited amount of police force put into motion online. (Adams, 2001) Cyberspace is practically a new international battlefield for actors, which could potentially become one of the most dangerous strategic warfare tactics within the upcoming years.

The perspective from liberalism would be the progressiveness of the states, and their control of cyberspace but would mostly emphasize that the government alone could not secure all of cyberspace, but only certain infrastructures. Liberals would more than likely suggest an international institution dedicated solely to this security dilemma that cyberspace has inflicted. Thus gaining trust between both state and certain non-state actors in hopes of achieving lowering the crime rate in cyberspace. (Petallides, 2012)

With an approach of a constructivist, anything, especially involving politics or threat to some sort of a society, would be considered a security issue. Though constructivist highlight speech-acts, what they would consider cyber security would be different compared to the realist and the liberals perspective. (Adler, 1997) The internet hacking group (known as hacktivist), Anonymous, would be an example of constructivist in cyber-space. The group attacks what they consider to be unethical, promoting free speech, but also known to cause a lot of security breaches such as the Census Bureau database (Miller, 2015)

The perspective of historical materialism, the main approach is welfare and security for all. I believe the priority for both historical materialism and a constructivist would first be the ending of certain crimes that occur in cyberspace such as anything that potentially harms children, animals, or would put a person at actual physical risk. So with both of these view, the first set of action would be monitoring the deep web (a hard to access side of the internet that holds the most illegal activity). (Pagliery, 2014)

Realism would best cover how to securitize cyberspace. Since primarily the internet is anarchic, there are organizations and police force that monitor cyberspace, but since the internet is so big, plus the ability to cover ones trace, this makes finding illegal activity much more difficult. With past events such as the US government database security breach from a group called Moonlight Maze, which seven IP addresses from the attack originated from Russia. With little enforcement in the investigation, it’s hard to determine the motivation for the attacks, whether it was state-sponsored. But with such an

event, this resulted in more suspicion with the relations of Russia. Also to mention, the Stuxnet worm, an American cyber weapon to infiltrate the Iranian nuclear system. This malicious worm is known to be the first example of a cyber warfare attack, which would be considered a “ diplomatic nightmare”. (Drogin, 2015)

States and non-state actors could attack another with leaving little to no trace of their origin. In realism, this could break down the international trust between actors and their institutions. (Petallides, 2012)

Policy Options

Many policies involving cyber security or cyberspace as a whole in the US typically serve private sector organizations rather than protecting third parties or even the public. The United States should set up a policy focusing on severe punishment for at least domestic cybercrimes. Many cyber crimes go reported, but small amounts go investigated. Whether the report is considered to have a high impact, more investigations should be ensured to catch more perpetrators. Though the benefit would be, lowering the crimes online, the cost would be having to spend a large amount of taxpayer dollars to monitor online, whether the service web or the deep web more. A second policy option would be for the U. S. Treasury Department to create a reinsurance fund in case there is a huge data breach within the U. S. government that could potentially mess with the economy. The benefit would be the fact that the U. S. would have a nest-egg just specifically for an event that could potentially happen at any given time affecting the U. S. and potentially the world economy. This would be the best policy option.

Prediction

Cyber crimes are occurring on a daily basis, with potentially affecting over a million people. As of 2015, cybercrime, cyber terrorism, and cyber warfare are all considered to be the top worldwide threat according to the UNI Threat Assessment. Cyber security is now and will continue to have seen as major threat to countries whether in a political stance, economic stance or for the wellbeing of the general public. Cybercrimes, terrorism, and warfare will only continue to increase within the years making cyberspace just another battlefield for both actors and non-state actors. With the potential effects that cyber crimes have, this will stay at the top of the UNI Threat Assessment over the next few years.