**Assignment 2 – Cyberwar**

Nathan Ketterlinus

Fisher College of Science and Mathematics

Towson University

Towson, United States

[nketter1@students.towson.edu](mailto:nketter1@students.towson.edu)

1.d

The United States’ four major cyber adversaries are Russia, China, North Korea, and Iran.

As of today, Russia can be described as an authoritarian dictatorship. Russia’s poor human rights record is also rooted in their past with the KGB, and all the scare stories that comes with them. As for Russia’s tech development, I am not aware of any industries Russia leads. My current (uninformed) paradigm is that Russia has modern technology, although it tends to be subpar to the US’s and is usually imported from other countries, as opposed to developed in-state. Russia’s history with the US is most notable in their interaction during the cold war, when the threat of mutually assured destruction loomed overhead. There were also rumors of Russian attempts at sabotaging the 2016 election.

Today, China can be described as a socialist republic. China is such an isolated country and refuses to comment on so many matters that the common consensus is that they commit quite a few human rights violations. As for their technology development, a lot of their tech is developed in-state, and they do not allow a lot of outsider technology in. A lot of modern Chinese-American tension stems from different recognitions of the sovereignty of Taiwan.

North Korea is a totalitarian dictatorship, although they consider themselves a democratic republic. North Korea is surrounded by scare stories of human rights violations, such as government-enabled famine and propaganda bordering brainwashing. Their tech development is very far behind countries like the US. They have too much pride to use outsourced products and do not have the resources to develop anything privately. North Korea’s history with the US is hostile largely because of the Korean War, although their recent threats of nuclear warfare are also quite relevant.

Iran is an Islamic Republic. I am not too well informed about how well they uphold human rights, but I believe most violations come from the government attempting to maintain the status quo, whether by silencing reporters or stopping protesters. Iran’s tech development also cannot be too advanced as they had economic sanctions in place which prevented Iran from obtaining advanced computer parts until 2016. There have not been interactions between Iran and the US on the same scale as the other three countries, it is mostly Iran being blamed for terrorist attacks and Iran being upset about being accused.

2.c

The most common cyber crimes reported by victims are tech support, extortion, non-payment/ non-delivery of goods, personal data breaches, and phishing attacks [1].

Tech support attackers pose as legitimate tech support or government workers, then coerce victims into any number of financial traps. A common example is that instead of providing actual tech support, scammers will have victims install ransomware and then hold their device hostage. Another example is when a scammer poses as a government employee and asks for personally identifying information, only to steal it and commit identity theft. Tech support scams affected over 32,000 Americans in 2022, costing over 806 million dollars in losses [1]. Those who report tech support scams are also disproportionately made up of those over the age of 60 [1]. As discussed later, this could be for a variety of reasons, but a few notable ones include a lack of tech literacy, more valuable assets to be stolen, and more trust in people claiming to be someone they are not.

Extortion attacks involve attackers intimidating victims through threats of harm or legal action in order to steal assets. Digital extortion attacks are typically facilitated using ransomware, where victims lose access to their devices until they pay the attackers a fee. There were over 39,000 reported extortion attacks in 2022, costing 54,335,128 combined [1].

Non-payment and non-delivery attacks are straightforward to understand. Either a victim purchases a product or service, and the attackers never delivers said product or service and runs off with the money, or a victim receives a product or service and refuses to pay for it, wasting the victim’s time and labor. There were 51,679 reported non-payment attacks in 2022, accounting for $281,770,073 in losses [1].

Personal data breaches deal with victims having their personal data stolen. This can include identifying medical records, credit card information, or other costly assets. There were 58.859 personal data breach attacks in 2022, costing $742,438,136 [1].

Phishing attacks are by far the most common form of cybercrime. Phishing attacks involve attackers posing as someone credible to steal information, passwords, and subsequently money and assets. Phishing attacks are typically more sophisticated than tech support scams, as they can come from accounts that are much harder to debunk as falsified, and commonly name-drop credible figures to build their own credibility. There were 300,497 reported cases of Phishing in 2022, with a total reported cost of 52,089,159 [1].

The two most vulnerable age demographics to cyber attacks are those aged 30-39 and those above the age of 60 [1]. However, this data may be misrepresented for a few reasons. Those aged 30-39 may just be the people most willing to report when they’ve been attacked. In addition, people over the age of 60 is the largest group. While every other reported group is 10 years wide, there are many more years (and thus people able to report), in the group of 60+. Technically the under 20 group is twice as wide as the other groups, but a lot of this demographic either does not have the capital to be targeted, or does not know how to report.

The IC3’s threat overviews for 2022 include a few key attacks, including business email compromises, investment scams, ransomware, and call center fraud [1].

Business email compromises are an advanced form of phishing, where attackers infiltrate into a company’s email system or known phone numbers, and request for W-2 info, gift cards, or other forms of assets. Business email scams have a reported loss of $2,742,354,049 in 2022, over 21,832 reported cases [1].

Investment scams have victims invest their money in a company under false pretenses, such as pump-and-dump crypto coins or endorsement from an impersonated celebrity. Investment scams typically target individuals aged 30 to 49 [1]. Investment scams were the most expensive attack of 2022, costing $3,311,742,206 out of 30,529 cases.

Ransomware is software designed to make a computer unusable unless a decryption key is provided. Typically, attackers will withhold this key from victims unless a ransom is paid, while simultaneously selling data found on the computer. Disregarding the value of lost business, time, wages, files, and equipment, Ransomware is reported to have cost $34,353,237 over 2,385 cases.

Call center fraud, as described above, is when an attacker poses as a call center worker and steals credentials from victims.

3.1

The US’s main cyber adversaries are China, Russia, Iran, and North Korea

3.2

Sheldon Adelson is the CEO of Las Vegas Sands. After proposing to detonate a small nuke in the desert to warn Iran, Iranian attackers hacked his casino and defaced his website’s homepage. He is important in the conversation about cyber warfare because he shows the ease with which malicious actors can pull off destructive tasks through the internet. He also serves as a warning to everyone to be polite by presenting the ever-looming threat of being hacked for saying something controversial.

3.3

Stuxnet is a malicious worm designed to attach to specific programmable logic controllers and monitor and alter their functionality. The worm was developed by the United States in an attack against Iran’s nuclear program.

3.4

Iranian hackers got into the Las Vegas Sands casino, disabling 20,000 machines, destroying data, and vandalizing the casino’s homepage. As a sidenote, this question seems quite vague and I’m not sure if this is what’s being asked for, as it’s quite redundant with question 3.2, but I don’t know what else to have put.

3.5

Russia was accused of interfering in the 2016 elections. While there are claims of direct voter fraud, the possibility of disinformation campaigns and online propaganda campaigns seems much more realistic.

3.6

The US Cyber Command “plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries”[2].

3.7

Estonia was attacked by a mass DoS attack in 2007. The attack was motivated by disapproval of the government moving a WWII memorial. As the attack was politically motivated, it counts as cyber terrorism. Estonia is important in cyberwarfare as it serves as a reminder for how small events can be seen as justification for harmful attacks by small, independent actors.

3.8

NSPM 13 is the United States’ Cyber Operations Policy. It outlines how various segments of the government, most notably the DoD are allowed to act regarding domestic and international cyber operations, including attacks.

References

[1] “Internet crime complaint center (IC3),” Internet Crime Complaint Center(IC3) | Home Page, https://www.ic3.gov/ (accessed Sep. 10, 2023).

[2] “US Cyber Command Factsheet,” U.S. Cyber Command - U.S. Strategic Command, https://web.archive.org/web/20140416192156/http://www.stratcom.mil/factsheets/2/Cyber\_Command/ (accessed Sep. 10, 2023).