MIDN 2/C Ian Coffey, Brendan Lewis

Capt Rashley, USMC

Si430

5 February 2025

Lab 4 Writeup

While western intelligence agencies have a strong grasp over internet exploits that allow for mass surveillance over domestic and foreign targets, countries like China have also been developing their cyber capabilities in an attempt to match the NSA. Incidents such as Operation Aura, where Google systems were hacked by Chinese agents who spied FBI agents, demonstrate Chinese strides towards becoming a cyber threat on the world stage. However, China is far from the only country that has pursed cyber dominance in our technologically dominated world. Russia has been the hub for cyber crime and cyber warfare since the early 2000s. Much like the Chinese, the Russians lack that platform advantage that the United States has. That is to say that since the united sates is allies with so many foreign countries, we can use integrated internation systems to expand our cyber reach across Europe. Russia and China lack these strategic capabilities. With that said, Russia has a long history of making headlines on national newspapers through cyber-attacks. The famous “Not Petya” worm infected computers and encrypted its contents. This worm spread like a wildfire, causing incredible amounts of damage. Russia buy-and-large allows cybercrime to occur within its borders as long as hacker do not target Russian assets. As a result, Russia is a hotbed for cybercrime, and will continue to pose a threat in the cyber domain for years to come. While China and Russia are the two main cyber adversaries that the United States faces, there are a multitude of other countries that have their own smaller yet sophisticated cyber capabilities. Iran was able to trace the CIAs secret communications, and as a direct result, 30 CIA agents were killed. The United Arab Emirates developed malware by the name of Karma, which enabled them to spy on iPhone software. And finally, the North Koreans have very capable cyber assets, which allow them to execute attacks and release malware. When Sony released the move “The Interview” which made comedic parody off of the North Korean dictatorship, the DPRK conducted a cyber attack against Sony, releasing blackmail on Sony executives, and causing damage to internal servers. The famous WannaCry ransomware also has links to the North Koreans. Overall, if there is any clarity in the cyber domain, it is the fact that cyber warfare is here to stay, and will only grow greater in scale.