Cyberspace Is The New Battlefield

What is cyberspace? The google definition of cyberspace is “the notional environment in which communication over computer networks occurs.” In short, it's the virtual world. Computers communicate across it. Cyberspace is global so every computer in the world communicates across cyberspace. Attacks across this giant network of computers are called cyber-attacks and are being more frequently used over the years and can cause devastating amounts of damage. It can be argued that they are the number one threat to national security of all countries and because of them, no classified info is safe and really ‘classified’. Countries are constantly ‘battling’ to try and get the most cyber power and to dominate the global cyberspace. In this essay I will be discussing whether or not cyberspace is really the new way warfare will be fought.

Cyber-attacks can cause a lot of damage and can bring whole countries to its knees. A notable cyber-attack is called Stuxnet. What was Stuxnet? Stuxnet was a computer worm. A computer worm is a type of malware that, its main ability, is to replicate itself and go to other computers at unprecedented speeds. Because of this they usually use up a lot of CPU power and bandwidth causing computers infected to slow down significantly and if a server gets infected, it can shut it down. Some worms have even been able to cause millions in damage like the Slammer worm that stuck 75,000 computers with a DoS attack in January of 2003. It caused 1 billion dollars in damage. Stuxnet used Windows Vulnerabilities that were previously unknown to Microsoft to infect computers and spread and it spread fast, it infected 200,000 computers in 115 countries. When it infected a computer, it did not do any harm to it but spread to others. Its target was Iran’s nuclear enrichment facilities. When it infected a computer, it would check to see if it was connected to a certain PLC (programmable logic controller) made by Siemens. A PLC is how a computer communicates and controls a machine. The worm would enter through what’s called a ‘zero-day’. A zero-day is a software vulnerability that can be exploited by hackers. These zero-days are not known to the creators of the software so if not patched, hackers can get into anything used by the software. Info about zero-days can be sold on the black market for upwards of $200,000. Stuxnet took advantage of 20 zero-days. How a hacker finds a zero-day is through days, weeks, and months of looking through a software’s code, uses probing applications and barrages the software with tons of reverse engineering tools just to find one small weakness or error so they can execute code inside of it. It is extremely hard to counter a zero-day attack because the vulnerability is unknown to the creators. Software and hardware such as Fireeye and Cynet can stop these attacks but with a complex enough code, they can be bypassed. What Stuxnet would then do is alter the code inside the PLC, making the centrifuges in the nuclear devices spin way too quickly for too long. This resulted in the equipment being destroyed. What the worm also did is it told the computer controlling the centrifuge that everything was fine until it registered that the equipment was destroyed. People believe that the worm was created by Us and Israeli intelligence agencies. The development of the worm was given the code name “Operation Olympic Games”. Both governments have denied their involvement in the development of the worm, but Israel did release a video in 2011 claiming that Stuxnet was one of their successes. It is estimated that it took ten programmers 2 to 3 years to complete the worm. The programmers themselves have not been identified and remain anonymous. The virus was used to stop Israel launching airstrikes on Iranian Nuclear Facilities, resulting in a war. This was the nonviolent alternative. The source code for a small part of

Stuxnet is available online due to reverse engineering but people say it’s nowhere near like having the original code.

In 2017 the world was hit with a massive cyber-attack, it was mainly targeted at Ukraine and crippled government computers, shut down banks and ATM’s, brought transport systems to a halt and caused major damage to the county’s economy. Although it was targeted at Ukraine, [footnoteRef:1]the virus also affected computer systems in Denmark, India and the United States. This malware was dubbed ‘NotPetya’ as it was part of the same family of malware called Petya. [footnoteRef:2]Other malware in this family is ‘GoldenEye’ (a cyber-attack in 2016) and newer EternalBlue based malware. All Petya malware are ransomware. It is believed that the malware [footnoteRef:3]was created by Russian Intelligence in order to cripple the economy of Ukraine. Russia and Ukraine had diplomatic tensions and they wanted to bring down the computers of the separatists loyal to the Kremlin. The malware itself is very similar to WannaCry as it locks all files and displays a message to the victim that there files have been encrypted and can only be gotten back if they send a specific amount of Bitcoin to an address. Some say it was even worse than WannaCry and that WannaCry was only a warning of what could come. [1: Ellen Nakashima, Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html, [20 March 2020]] [2: N/A, Petya (malware), https://en.wikipedia.org/wiki/Petya_(malware), [20 March 2020]] [3:]

Anyone can be affected or targeted by a cyber-attack. I have been affected by many such as COM.SURROGATE fake files, dropper.gen and many .dll files. There are a few things a person can do to stay safe whilst using their computers at home. First, make sure you are going onto trusted websites, if a person is just browsing trusted websites then they are safe, but as soon as a person enters an unsafe website they are immediately at risk of people grabbing your IP address and getting into your home network causing a potential compromise to the devices connected. When downloading files onto your computer make sure you have anti-virus software on your computer. When a person downloads a file without any sort of virus protection software, they are again at risk to hackers getting into the computer or a malware getting onto the computer. If you still think the file is unsafe but your anti-virus hasn't picked it up, then there are a few steps to take. What type of file were you downloading? If you were just trying to download a PDF or an image file and the file says it’s a .exe, .bat or .dll file then that file is almost certainly dangerous and should be deleted immediately. An exe file is an executable file. These are the most popular file types for anything. Any application usually is an exe file. But if a person creates one to cause harm it can destroy a computer by itself. A bat file or a batch file is a type of file that when opened just looks like a text file but that code inside the text file tells the Windows OS (operating system) what to do and what commands to run. They can be very useful when creating things like servers or connections but if a computer gets infected with a malicious batch very, they can do a lot of damage because it's in the OS. Also, they can be quite hard to locate as they may be able to get very deep in the computer’s files. A dll or a dynamic-link library is a file that hooks onto an executable file and only then can it execute its code. By itself it is harmless but if it hooks onto another file that can cause harm then it can be extremely dangerous to the computer. An anti-virus usually does the trick at securing your PC but if you want to go one step further you can download a VPN. A VPN or Virtual Private Network is a type of software that secures the IP address of the computer, encrypting it. When you are connected to a private network you can make websites think you are anywhere in the world meaning you can access content not available in your country, nobody can track you or

see what you are searching up because your IP is ‘spoofed’, not even your internet provider or workplace. Furthermore no one can access your network or computer when on public Wi-Fi. Hackers can use public Wi-Fi to grab anyone's IP address and get into the computers, with a VPN this stops it. VPNs are usually a bit pricey, but they are worth the buy. A few VPNs I recommend are NordVPN, Hotspot Shield or ExpressVPN.

So is cyberspace the new battlefield. It seems like it's starting to be. People are starting to combine cyber-warfare to conventional military tactics. In some cases, a cyber-attack can cause more damage than a military attack. As stated earlier, some examples are WannaCry and Stuxnet which caused millions in damages.