**Cyber Territory – Secret history of Cyberwarfare**

These days, whenever there’s a national election, we assume there will also be a certain amount of online interference in the form of cyber warfare – maybe even from some shady source of organized crime. But how did we get to this point? This is the story that author Fred Kaplan tells. From the early days of spy versus spy and tapped phone lines, to the modernday, seven-billion-dollar US cyber-defense program, the cyber wars have been growing fast and show no sign of slowing down. So let’s take a look at some of the bigger battles in the cyber wars – the ones that have raised the stakes and caused the US government to take notice and beef up its security.

You might think that the first people to hack into a communication network were, say, a band of pioneering computer experts who used a primitive form of the internet. However, there is a rich history of communications interception that dates back much further. During the American Civil War, for example, generals knew that their telegraph messages were being intercepted, so they would routinely issue fake orders to send the enemy on a wild goose chase. And during World War II, American and British cryptographers decoded crucial messages sent by German and Japanese forces – communication interceptions that played a vital role in the Allied victory. Then we come to the Cold War, the heyday of spies and tapped phone lines, as well as intercepted radio signals and microwave transmissions. Agents on both sides of the Iron Curtain were eager to learn what the other was capable of and intended to do. When we reach the information age – or, as some call it, the cyber age – we can see how the art of communications interception transformed into a type of warfare. At this stage, those hacking into communication lines weren’t just trying to listen in and acquire information; they were now prowling through entire computer networks. And while doing so they could erase, block and change information – anything to mislead or slow down an enemy that could be as far away as the other side of the globe. This is cyber warfare. The advent of the internet played a big role in raising the stakes of communications interception. For the first time, all of the world’s computers – even those containing top secret and classified information – were essentially connected to one big network. Even if the information is encrypted, everyone knows it’s just a matter of time before a program is developed that can break the code. During the Obama administration, the president was given daily reports on cyber attacks being conducted by nations like China and Russia. While this is unsettling enough, even more worrisome is the fact that missiles, uranium-enrichment labs and dam valves are all controlled through computers networks. This is why cyber warfare has come to be an integral part of military operations around the world. In 2009, the Obama administration created a cyber-command unit, whose annual budget rose from $2.7 billion to $7 billion in the three years after its establishment.

April 19, 1995 started off as just another day in the Alfred P. Murrah Federal Building, in Oklahoma City. But shortly after 9 a.m., a group of militant anarchists, led by a young Gulf War veteran named Timothy McVeigh, set off a bomb in the building that killed 168 people and injured another 600. All told, the blast damaged or destroyed a total of 325 buildings in the area. From this moment on, the US government was determined to crack down on terrorist attacks, especially ones that targeted federal buildings and the country’s infrastructure. It quickly became apparent that the nation needed to strengthen its cybersecurity, too. In 1997, President Clinton approved a commission to address the issue of terrorism. It was headed by Robert T. Marsh, who enlisted the help of Willis Ware. Ware was a pioneering computer engineer and the former head of the RAND Corporation, an analytical research

institute with deep ties to government security. Ware helped convince Marsh that cybersecurity was of the utmost importance. Back in 1967, Ware had written a paper called Security and Privacy in Computer Systems as a response to the US government’s desire to launch the ARPANET program. ARPA, or the Advanced Research Project Agency, was made up of scientists from around the country who were working on military weapons and defense projects. In an attempt to make it easier for these scientists to communicate with one another, computer consoles in each of the universities were hooked up to a single network: the ARPANET. Willis Ware’s paper was critical of the idea of the ARPANET. Ware worried that enemies of America might be able to break into the network and steal valuable information. But, though Ware’s paper was shared in federal circles, the consensus was that Russia and other potential threats were ill-equipped to pull off such an advanced cyber attack, and the network was formed. But 30 years down the line, after the ARPANET had essentially transformed into the internet, Ware’s concerns seemed much more justified. Computer networks and systems everywhere represented a real threat. Within its first six months, the Marsh Commission released a report that called for a far more robust cybersecurity program Dark Territ in toryhe US. But the response wasn’t what Marsh or Ware hoped it would be. Once again, the warnings fell on deaf ears, and the Clinton administration made no immediate efforts.

The Clinton administration was slow to react to the warnings of the report from the Marsh Commission. But that doesn’t mean everyone in the US government was blind to the threat of cyber attacks. In fact, during the late nineties, cyber attacks were increasingly monitored. For instance, the secretary of defense, Bill Perry, advocated for more cybersecurity, a position that drew him to a three-star general named Kenneth Minihan. Minihan, in his role as the intelligence chief at the Kelly Air Force Base, had helped devise new ways of monitoring cyber attacks. Minihan’s efforts contributed to the creation of a software called Network Security Monitoring. Invented by the computer scientist Todd Heberlein, this software detected unwanted network intrusions on open networks that connected multiple computers. So, in 1996, Perry had Minihan installed as the new director of the NSA (National Security Agency), thinking that he’d be able to push the NSA to focus more on cyber warfare and less on microwave signals and phone monitoring. Things didn’t exactly go as planned, however. At the time, the nation was embroiled in a debate over just how much network monitoring the government could do, since average civilians were part of that same network. Developments in cybersecurity were slowed to a snail’s pace. Finally, in 1997, the NSA changed the rules of the game by launching a simulated cyber attack under the code name Eligible Receiver. The aim of Eligible Receiver was to break into the Defense Department’s computer network. The NSA wanted to see how US leaders and government facilities would handle a cyber attack. Though they’d predicted it’d take two weeks, the NSA was able to penetrate the Defense Department’s entire network in a mere four days. This includes accessing the National Military Command Center, which is the unit responsible for transmitting orders from the president during wartime. This proved two big points: Clearly, the government was ill prepared for any serious cyber attack, and cyber warfare was far more dangerous than people had thought.

After the NSA’s Eligible Receiver exercise exposed the US government’s vulnerability, progress began to be made in the cyber-security field. Before the simulated attack, only a quarter of the servers at the Defense Department were connected to an intrusiondetection system (IDS). After the Eligible Receiver, they were all hooked up. But these systems, though finally put in place, weren’t run very smoothly. In fact, many command units failed to appoint anyone to be in charge of monitoring the IDS. Even if someone was in charge, many generals and military staff had no idea how the system worked. A few months after the installment of the IDS, a Defense Department general complained to Deputy Secretary of Defense John Hamre. The system must be faulty, the general said. After all, it seemed to indicate that attacks were occurring every day. The general didn’t understand that the system was actually trying to warn him; real hacks were in fact being attempted on a daily basis. More progress was made in 1998 with the establishment of the Joint Task Force-Computer Network Defense (JTF-CNF). Following a very real and effective cyber attack earlier in the year, known as the Moonlight Maze attack, the JTF-CNF was created and led by Brigadier General John “Soup” Campbell. The task force was charged with the sole purpose of protecting the computer systems and networks of the Department of Defense. It established a 24/7 watch program, as well as strict notification procedures to follow when anything suspicious happened. If this seems like a drastic response, that’s because, as we’ll see in the next blink, Moonlight Maze was a pretty serious attack.

So what exactly happened in the Moonlight Maze attack? Well, it all started at the Wright-Patterson Air Force Base, in March 1998, when personnel became aware that hackers had accessed their servers. However, since the hackers rewrote the activity log, it was not only hard to identify and catch them, it was difficult to spot their activity at all. In other words, the criminals were doing a good job of covering their tracks. After months of frustration, the intelligence team decided to try to trap the cyber attackers by using a “honeypot” – in this case, a collection of fake files made to look like real directories, passwords and usernames. The team figured it would be the perfect trap. No hacker would be able to resist the information and it would take time to browse the fake files, time during which the team would track the hacker’s IP address and figure out where the attack was coming from. When the trap was set and sprung, they discovered that the IP address was from the Russian Academy of Sciences in Moscow. Now, since it could have been a fake address or simply a point of entry for someone elsewhere in the world, the intelligence team had to investigate further. First, they were able to look at the hacker’s activity logs to learn which topics interested them. Then they checked data on recent scientific conferences and their attendees. It turned out that Russian scientists had indeed been present at conferences focusing on the – rather diverse – topics that had interested the hackers. While this suggested that the IP address was real, and that the perpetrators were Russian, it wasn’t a closed case quite yet. Someone outside of Russia could still be accessing the address remotely. The team then turned its attention to the code the hackers were using to cover their tracks. After developing new software, the team was able to break the code to reveal that it had been originally written in Cyrillic, the writing system popular in, among other places, Eastern Europe and Russia. It was enough evidence for a US delegation to travel to Moscow, where it was confirmed that the hackers behind Moonlight Maze were indeed agents of the Russian government.

During the 1990s, the nations comprising the former Yugoslav Federation were embroiled in a string of insurgencies, conflicts and battles for independence: the Yugoslav Wars. In 1995, a peace treaty was signed that was meant to end Serbia’s war on Bosnia-Herzegovina. Following that, a Stabilization Force (SFOR) consisting of members from the United States and other NATO-allied countries was established. It was stationed in the region to ensure that Serbian president Slobodan Milošević honored the treaty. As it turned out, Milošević had no intention of honoring the treaty. When he resumed aggressive actions, the SFOR reached out to a secret unit in the Pentagon called J-39. Part of the joint chiefs of staff unit, J-39 consisted of top US military chiefs, and they agreed to enlist the help of the NSA and other intelligence agencies to stop Milošević . At the forefront of strategies used by the J-39 were a series of cyber attacks. Since the Serbian air-defense system was linked to the civilian phone system, J-39 was able to hack into it. That enabled NATO’s commander, General Wesley Clark, to ascertain how the air-defense system operated and where its vulnerabilities were. J-39 was also able to intercept communications between Milošević and his accomplices and moneymen. This provided valuable information about where Milošević’s money was coming from and how his warfare was being funded. For example, some of Milošević’s biggest donations came from an owner of a copper mine. Upon getting this intelligence, J-39 contacted the donor and threatened to bomb his mine if he didn’t stop supplying Milošević with money. At first, the threat didn’t work. But when NATO forces were able to cut off electricity to the mine, the donor gave in and ceased funding the Serbian despot. In the new millennium, cyber warfare has expanded in many troubling ways. While cyber attacks have long been used to steal money or state secrets, it is now common for an attack to be motivated purely by politics. The story of one such attack begins in October 2013, at Yeshiva University, in New York. Taking part in a heated political discussion was the Las Vegas billionaire and proIsrael right-winger Sheldon Adelson. When the topic of the ongoing nuclear negotiations between Iran and the Obama administration came up, Adelson proposed the tactic of detonating a small nuclear bomb in the desert. The idea was not to cause anyone harm, but to warn Iran that the United States could, if it so desired, wipe them off the map. A few months later, in early 2014, the Las Vegas Sands Corporation, where Adelson is CEO and chairman, had its Dark Territ sysory tems hacked into by Iranians. The perpetrators successfully installed malware that destroyed 20,000 computers and all of the company’s data. The hackers also posted a prominent and clearly visible message on the company’s website, stating that it was a crime to encourage the use of nuclear weapons in any capacity. They did not, however, take even one penny of Adelson’s money. A similar cyber attack occurred later that same year. This time the aggressors were North Korean hackers and the target was Sony Pictures Entertainment. SPE was the distributor of the comedic film The Interview, which featured a fictional CIA plot to kill North Korean leader Kim Jong-un. The hackers didn’t plunder the company’s fortunes. Rather, they destroyed thousands of computers while stealing internal emails and other sensitive information, such as employee Social Security numbers, executive salary details and copies of unreleased films. They then began leaking this information to media outlets, some of which were unscrupulous enough to publish. This leak only stopped when Sony announced that The Interview wouldn’t be released. The attack had succeeded. So what can be done to stop cyber attacks? Or are they simply something we should get used to?

Even as technology continues to grow and advance in impressive ways, there is still no way to keep everyone safe and secure from cyber attacks. Surprisingly enough, today’s cyber-warfare problems are by and large the same as they were when the first hackers started to appear. What’s been happening is this: when advancements are made in network defense, the attackers make their own advancements in evading those defenses. So, despite attempts by the US government to create and install software that can detect and withstand cyber attacks, hackers are still a threat. It’s always just a matter of time before the new line of defense is penetrated. This is also the assessment given in a 2013 report by the Defense Science Board task force. They also concluded that the threat of cyber attacks will persist as long as networks are used to connect computers.

Today, our systems and networks are more connected than ever before. This has made it easier for us to communicate and coordinate, but it’s also made us extremely vulnerable. If a hacker can get into one system, there’s almost no limit to where he could go. In other words, vulnerability is inherent in network connectivity. In 2009, Secretary of Defense Robert Gates cooked up a name for the current state of cyberspace. He called it dark territory. As Gates explained, the term came from the railroad industry. Gates grew up in Kansas, and his grandfather worked as a stationmaster for the Santa Fe Railroad. At the time, railroad workers used the term “dark territory” to describe portions of the railroad tracks where signals didn’t exist and no one really knew for sure what was going on. Gates saw cyberspace in similar terms: a “train” could enter the dark territory of a network and cause catastrophic damage. And, since cyberspace is immense, it’s likely that no one would notice the devastation until it’s too late.