# Cyber Pearl Harbor

Madison Shannon, Vincent Suillerot,

Thomas Grinberg, and Joaquin Peluffo

Dr. Bryan Reagan

April 16, 2018

On the morning of December 7, 1941 a tragedy struck. The united states naval base in Hawaii was attacked by the Japanese navy. This was a devastating surprise that no one saw coming. Over 2,000 Americans were killed in this attack and over 1,00 0 were left wounded. Vessels including planes and battleships were destroyed. Because this was extremely unexpected, the naval facility at pearl harbor was unprepared and was undefended.

Understanding pearl harbor and the extremes of the attack is crucial in understanding the term cyber pearl harbor. Cyber pearl harbor is the term that is used to describe the attack that could threaten the infrastructure and related services in the United States. The term is used so people can understand the intensity and devastation this attack would leave us with. The term was created in 2012 by the U.S. Defense Secretary Leon E. Panetta.

The agenda behind a cyber-attack this big would be to spread viruses, take control of our infrastructure, and do numerous other illegal things. If something like this was to occur it could affect many businesses, the government, and any other services that rely on it.

Cyber pearl harbor has been predicted for a long time but terrorists haven't used it yet because they go for more bloodshed and gruesome activities. Terrorist groups also are not capable of doing this right now because it would take extreme cyber skills that they don't have. Cyber Warfare is a serious problem we face and it grows each and every day. Cyber threat is growing and gets worse in time because of the advancement of technology that everyone can get their hands on.

There are four big countries that are a threat to the united states. They are Russia, China, North Korea, and Japan. North Korea launches cyber-attacks all the time including their one against Sony for their movie " the interview." These cyber-attacks leave millions of dollars in damages.

The U.S. Defense Secretary said that if we don't secure our computer systems and networks they will be on the way to destruction. There are different ways we can protect ourselves against a cyber-attack this huge. As people we can change our passwords and make them more challenging, we can put up firewalls, we can get rid of software that will allow easy access to attackers like java and flash, and we can also use system installer disks so if we do get a virus it will be easier to wipe out of computers and start again. Businesses can have encrypted cloud services, they can require 2 factor authentication, they can also have firewalls and use encrypted emails.

There are things the government can do to protect against a huge cyber-attack like cyber pearl harbor. Things the government can do is get better software, and create cyber peace. International Telecommunications Union secretary general Hamadoun Toure recently proposed the agreement of an international cyber peace treaty where parties would agree that their infrastructure would not be used, or allow it to be used, for cyber-attacks. This could be extremely helpful and be the first major step in protecting us against a big cyber-attack.

According to sixty percent of technology experts we will experience a cyber pearl harbor by 2025 and it will leave mass devastation. It is predicted to cause significant loss of life, property, and tens of billions of dollars. Cities around the world today use infrastructure systems to manage everything from sewage, water, and electricity to traffic lights. Researchers found that these systems are very vulnerable and have lots of room for cyber-attacks. It would be catastrophic if our power system was shut down. It is likely that this could happen and it would lead to mass devastation. The united states is shockingly very unprepared and that's why they refer to it as cyber pearl harbor.

If this happened, a blackout would go on for months until we knew how to fix it. Because many things rely on our power grid this would affect almost everything. We would be at a loss of running water, food, sewage, blackout and closing of banks which would lead to loss of money supply, and also loss of medical supplies. We as citizens rely on all of these things and take them for granted. We don't realize how we would all die without food and water and how the sick would die without the electricity of hospitals and their equipment.

As you can see a cyber-attack of this nature can cause a great deal of damage to the united states. We are not ready or prepared for something like this, that is why we need to start creating peace treaties and taking part in protection practices. The united states would be left at devastation with cyber Pearl Harbor and we cannot let that happen.

References:

Dunietz, J. (2017, August 23). Is the Power Grid Getting More Vulnerable to Cyber Attacks? Retrieved April 13, 2018, from https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/

Morgan, S. (2016, February 18). Major Cyber Attack On U.S. Power Grid Is Likely. Retrieved April 13, 2018, from https://www.forbes.com/sites/stevemorgan/2016/02/07/campaign-2016-major-cyber-attack-on-u-s-power-grid-is-likely/

Stavridis, J. (2017, May 15). The United States Is Not Ready for a Cyber-Pearl Harbor. Retrieved April 13, 2018, from http://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/

What is Cyber Pearl Harbor? - Definition from Techopedia. (n.d.). Retrieved April 13, 2018, from https://www.techopedia.com/definition/29052/cyber-pearl-harbor

Lewis, J. A. (2017, August 29). Opinion: The truth about a cyber Pearl Harbor. Retrieved April 13, 2018, from https://www.cnn.com/2017/08/29/opinions/truth-about-cyber-pearl-harbor-lewis/index.html