**Forum:** Disarmament Commission

**Issue:** Addressing the Question of Cyber Warfare

**Student Officer:** Melissa Liu

**Position:** President

**Introduction**

Cyber warfare is an electronic/digital attack or series of attacks that targets a nation. It has the capacity to destroy civilian and governmental infrastructure and interfere with vital processes, causing harm to the state and detriment to the economies of the targeted nations.  The majority of the time, nation-states engage in cyber warfare by attacking other nations, but occasionally, terrorist groups or non-state actors carry out the assaults to promote the objectives of an enemy state. There have been many reported instances of cyber warfare in recent years, but there is no established definition of what constitutes an act of war in the context of cyber warfare.

There are many types of cyber warfare and many possible forms they may take. One of the main forms of cyber warfare are viruses, phishing, computer worms and malware, which are utilized to damage critical infrastructure, such as financial, public safety, and military infrastructure. It can also take the form of hacking and theft of institutions, governments, and businesses, as well as obtaining confidential information that they hold. Other forms include ransomware that seizes control systems or data, as well as disinformation or propaganda operations intended to seriously disrupt or cause havoc. One of the major forms of cyber warfare used in attacks between different governments are Distributed Denial of Service attacks which are used to flood enemy servers with large amounts of data to render them inoperable. Many countries are resorting to cyber warfare in conflicts, such as the most recent deployment of cyberattacks in the Russo-Ukrainian war. The United States, China, Russia, Israel, Iran, North Korea, and the United Kingdom are thought to have the most advanced cyberwarfare capabilities. There has been an increase in the number of cyberattacks in recent years, and these cyber superpowers have been leading the movement toward cyber warfare in conflict.

**Definition of Key Terms**

**Malware**

xxx Malicious software, or malware, such as Trojans, worms, and viruses can be used in cyberattacks. They can be installed by taking advantage of weaknesses in outdated software, being integrated with other applications, being sent as files, or, as is the case in the vast majority of instances, when a user falls for a phishing scam and opens an attachment or downloads a file that contains malware. An example of the use of malware in cyber warfare is when the Americans employed malware in 2010 to prevent Iran from obtaining uranium that might be used in nuclear weapons.

**Distributed Denial of Service (DDoS) attacks**

A Distributed Denial of Service (DDoS) attack is to render an online service inoperable by overloading it with a large amount of data coming from several sources. This form of cyberattack was employed in 2007, the year that cyberwarfare first gained widespread use, when Russia launched one to retaliate against Estonia for their decision to relocate the Bronze Soldier of Tallinn away from the city center. More than 1 million computers were used to flood Estonian governmental servers, taking down government, media, and business sites, and as a result, causing millions of euros in damage.

**Destructive Botnets**

A botnet is a network of hacked devices that have collected malware and are now under the control of a hacker. Hackers use covert channels to direct these infected bots to perform harmful tasks such as launching distributed denial of service (DDoS) attacks, distributing malicious spam, or espionage.

**Unpatched Software and Patching**

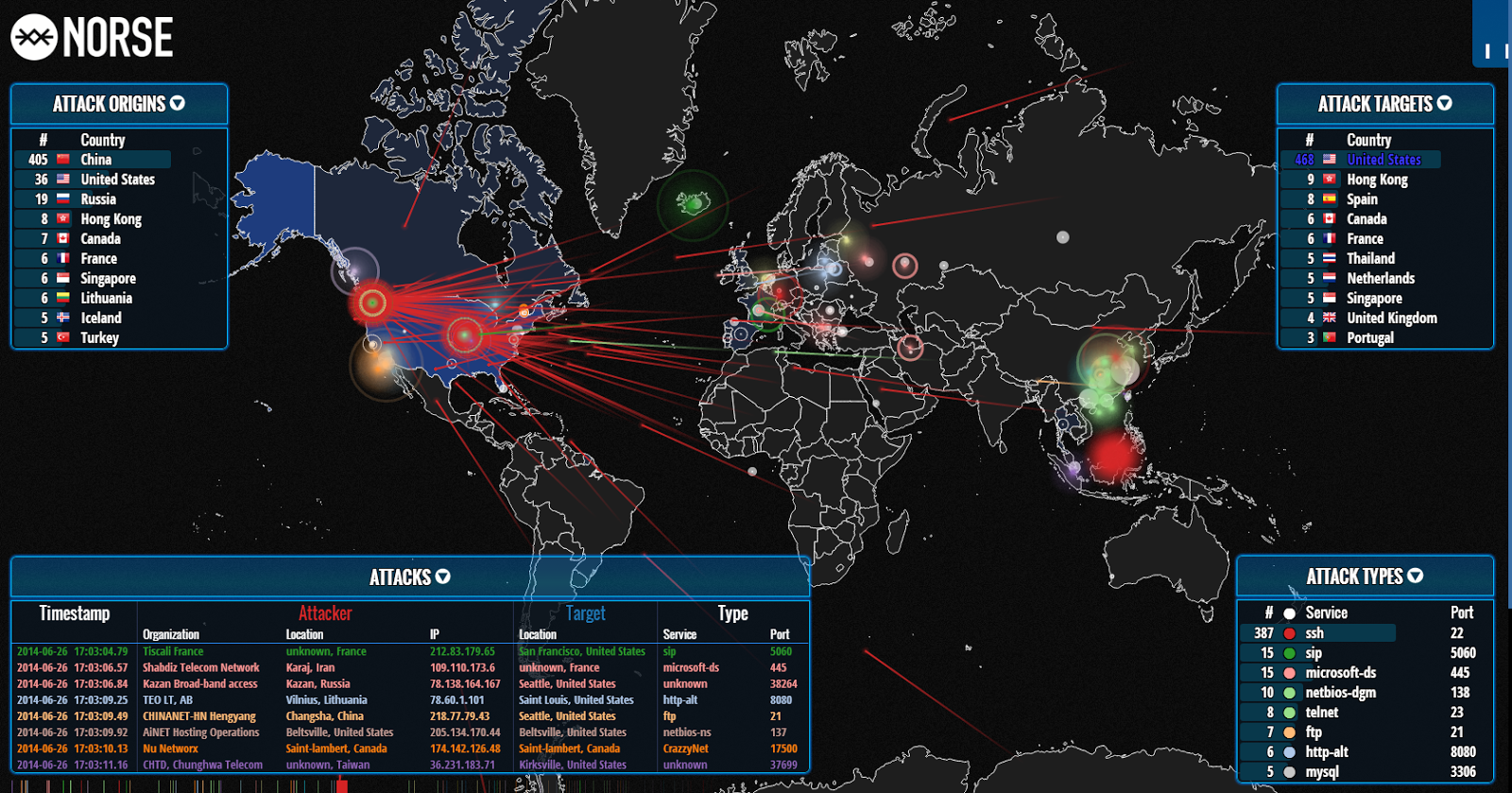
One of the biggest reasons why computers get hacked is unpatched software. Hackers are quick to begin an attack using any flaws in out-of-date and obsolete software. This takes the form of electric devices that are older or have not been updated recently. "Patching" resolves these flaws, preventing hackers from breaking into a system to steal confidential information, lock users out, or demand a ransom. If patches are not installed, it gives hackers a quick access point to networks.

**Electrical Power Grids**

By hacking into substations and intercepting communications between substations, grid operators, and electricity providers, attackers may change data on the power system. Grid operators use this information to establish power rates and maintain a balance between supply and demand. By manipulating power markets, grid hackers might profit by the millions at the expense of electricity users. They could potentially disturb the grid, resulting in blackouts.

**Background**

**Major conflicts and tensions that involve cyber warfare**



***Figure 1. A map of all known cyber warfare attacks***

***Russo-Ukraine conflict***

In the past, Russia had attacked Ukraine's infrastructure and data through cyberattacks. In 2022, further attempts were made to do so. Russia started a significant cyber effort just before the invasion of Ukraine. It appears that the goal was to destabilize Ukrainian defenses and overwhelm them. By using phishing, denial of service attacks, and exploiting software flaws, Russia attempted to interfere with services and introduce dangerous malware into Ukrainian networks. Eight different families of damaging software that Russia utilized in these assaults have been discovered. Although the assaults affected the majority of important infrastructure. The principal targets were Ukrainian government websites, energy and telecom service providers, financial institutions, and media outlets. The complete range of Russian cyber capabilities was used in this extensive strike.

***Iran-Israel conflict***

Iran's asymmetric warfare is characterized by the use of cyberspace. Cyber warfare allegedly enables Tehran to compete on an equal basis with global superpowers because of its immense power. Due to the plausible deniability provided by this weapon, Iran can avoid military responses or lessen their severity by attacking in cyberspace. The Iranian strike on Israel's water infrastructure may be a reflection of the Iranian regime's general desperation, which has already led to aggressive actions on other fronts. The strike also aims to dissuade Israel from continuing its military operations against Iranian targets in Syria and other parts of the Middle East, in an effort to oppose Israel without using force and avert a severe retaliation. The "Stuxnet" worm, which targeted Iranian nuclear facilities and was allegedly released by the West and its allies, namely Israel, is credited with starting the conflict. The worm disturbed the centrifuge in the province of Natanz.

***American accusations of cyber warfare against China***

The Chinese Communist Party has been constructing advanced systems inside the People's Liberation Army (PLA) as part of its efforts to acquire critical and confidential data from American public and private targets. The Second and Third Departments of the General Staff's PLA units are the main architects of China's major assault on seizing U.S. intellectual property. Another unit focuses its electronic warfare equipment on introducing malware into American computer networks, most likely under the Fourth Department of the General Staff of the PLA. Along with the European Union, Britain, Australia, Japan, Canada, and New Zealand, the United States publicly accused China of conducting a cyberattack and cyberespionage campaign. Further, the U.S. Department of Justice charged three Chinese security personnel and a freelance hacker with hacking several American businesses, colleges, and government institutions.

**Impacts of cyber warfare**

Cyberwarfare has far-reaching implications that could affect both citizens and industries that rely on technology or the Internet. The impacts of such attacks can vary from political instability to power grid disruption, data destruction, cyberespionage, destabilizing a regime, derailment of government initiatives, and destruction of assets, depending on the objectives of the cyberwarfare operation. Attacks committed in the name of cyberwarfare can have disastrous impacts all around and even trigger traditional warfare and conflict if the nation responsible for them is discovered. The intricacy of today's cyberwarfare software, however, makes it difficult, though not impossible, to identify the perpetrators of these cyberattacks, leaving victims with no choice but to speculate.

***Attacks on electrical power grids***

Power grid hacks may be highly impactful in interstate cyberwarfare. Modern societies depend on electricity, and the effects can be quite severe if electricity cannot be provided to the consumer. Because power is required for heating systems, law enforcement, hospitals, and other services, a true collapse may occur, potentially resulting in the loss of many lives and the destruction of infrastructure. Grids often lack adequate cybersecurity protections, which is one of the main reasons they are constantly assaulted. This is especially true when the grid makes use of IoT (Internet of Things) hardware and software, which makes it a more susceptible target for the attackers.

**Major Parties Involved**

**The Government of the United States of America:**

The United States is a major industrialized economy that depends heavily on the Internet, making it particularly vulnerable to cyberattacks. Due to its relatively sophisticated technology and huge military budget, the United States has significant capabilities in both defense and power projection. Physical systems and internet-connected infrastructure are increasingly at risk from cyber warfare. The United States continues to be constantly threatened by malicious hacking from both local and international opponents. The United States has significantly increased its cyber capabilities in response to these expanding threats. The United States was identified as the world's top cyber superpower in a 2021 report by the International Institute for Strategic Studies after accounting for its strengths in cyber intelligence. China, Russia, and Iran have been the biggest adversaries of the United States in cyber warfare.

**The Government of the Peoples’ Republic of China:**

The cyber landscape is changing as a result of China's rise to major global cyberpower. The nation boasts the largest internet user population in the world, a booming economy, and military and intelligence agencies that are becoming more and more effective. Similar to the "United States Cyber Command," China has formed a cyber division within the "Chinese Information Operation and Information Warfare." Foreign Policy magazine estimates that China has between 50,000 and 100,000 cyber professionals. There have been several claims that China is engaging in cyber warfare, mostly coming from the United States but also from Australia, Canada, Japan, and India. The US and China keep blaming one another despite it being difficult to pinpoint the source of cyberwarfare strikes.

**The Government of the Russian Federation:**

Russia's involvement in the 2016 US election makes it the most contentious nation to utilize cyberwarfare thus far. With the U.S., Ukraine, Georgia, the United Kingdom, Estonia, Kyrgyzstan, and France accusing Russia of utilizing cyberwarfare strategies, Russia may now be adopting the most aggressive cyberwarfare technique. Most recently in the Russo-Ukrainian war, cyber espionage and governmental propaganda campaigns, distributed denial-of-service (DDoS) attacks, security breaches of several NATO networks, communication jamming of Ukrainian legislation, and a campaign to rig Ukrainian elections have been the most prominent cyber activities in the Russo-Ukrainian conflict. Internet data has been used by Russian signals intelligence operations in eastern Ukraine to identify and target Ukrainian military units.

**The Government of Iran:**

After the Stuxnet virus, the Iranian government developed cyberwarfare as a defensive measure against the US and Israel. Since 2010, the Iranians have demonstrated to other countries their desire to launch cyberattacks by establishing "The Cyber Defense Command." Israel, the United States, the United Kingdom, Qatar, and Saudi Arabia have all accused Iran of being behind some of the most well-known cyberattacks, including the hacking of American banks in 2012 and the assaults against Qatar's RasGas and Saudi Arabia's Aramco.

**The North Atlantic Treaty Organization (NATO):**

In an effort to reach consensus by early 2019, the United States, Britain, Germany, Norway, Spain, Denmark, and the Netherlands--under the leadership of NATO--are developing cyberwarfare principles to instruct their forces on what justifies using cyberattack weapons more widely. The policy may change NATO's defensive strategy to one of offensive engagement with the hackers that, according to authorities, North Korea, China, and Russia employ to try to overthrow Western governments and steal technology. At the NATO Cooperative Cyber Defence Centre of Excellence, it has been said that NATO’s mindset towards cyberwarfare is shifting to have an offensive capability.

**Timeline of Events**

|  |  |
| --- | --- |
| Date | Description of event |
| July 15, 2001 | Microsoft-powered computer networks were susceptible to the Code Red worm, which targeted devices running the IIS web server from Microsoft. It was the first significant assault that was effective in attacking global enterprises. The White House’s server is among many that were disabled by the cyber attack. |
| November, 2003 | "Titan Rain" hackers, which the United States government believed were endorsed by the Chinese military, attempted to exploit vulnerabilities in U.S. military computer networks. The attack was nicknamed Titan Rain by U.S. officials and spanned over three years. |
| 2007-2008 | Distributed Denial of Service assaults damage the official network of Estonia for 22 days. The Russian government was alleged to be supporting the hackers. The president's office, the legislature, law enforcement agents, and Estonia's two largest banks were among the targets. After that, several of the Georgian government's computer networks, including those of President Mikheil Saakashvili, are taken down by distributed denial-of-service assaults in the weeks leading up to the conflict between Russia and Georgia. Companies, media, and transportation are also impacted. Georgian authorities blamed Russia for starting the attack. |
| December, 2011 | About 800 computers of government personnel, diplomats, and other entrepreneurs in Iran, Israel, Afghanistan, the United Arab Emirates, and South Africa were infected with malware named Mahdi. Users who opened the documents were at risk of having their emails and instant messages read by hackers since the virus was included in the email attachments. |
| November-December, 2014 | The computer networks of Sony Pictures were breached, and thousands of additional documents, including emails, financial data, and the private medical records of workers, were taken and made public. The United States believed North Korea was responsible for the security breach in revenge for Sony's impending release of the bizarre comedy "The Interview", which centers on a CIA plan to murder North Korean leader Kim Jong-un. Sony made the decision to postpone the movie's release. The FBI officially accused North Korea of carrying out the assault on December 19 and claimed to have substantial evidence connecting the country. |

|  |  |
| --- | --- |
| 2021-2022 | In February 2021, Ukraine accused Russia of assaulting the System of Electronic Interaction of Executive Bodies, a platform that the Ukrainian government used to distribute documents, by uploading documents that included macroscripts, which, if downloaded and activated, would cause the computer to covertly download malware that would enable hackers to take control of a computer. The Ministry of Foreign Affairs network and that of other government organizations were taken down in January 2022 as a result of a cyberattack against Ukraine. The cyberattacks correlate with the Russo-Ukrainian conflict, notwithstanding the lack of a comprehensive inquiry. Several significant Ukrainian governmental and commercial websites were knocked down by a series of cyberattacks in February 2022, both before and after Russian forces entered eastern Ukraine amid a climate of rising tensions between Ukraine and Russia. Russian assailants were blamed for the assaults by U.S. authorities, despite the Russian government's denials. |

**Previous Attempts to Resolve the Issue**

* IT Act of 2000: There is currently only one cyber law in effect in India, known as the IT Act, 2000, which was revised in 2008. Although there are a number of issues with this act that apply to circumstances involving cyberwar, this law is not particularly successful in preventing potential cyberwar. The act detailed that anyone who accesses, downloads, introduces, disrupts, or assists another person without the owner's consent on a computer system is subject to liability under the act. It further detailed that punitive penalties for crimes that fall under the category of cyberterrorism are covered by this act. If a cyberattack intends to undermine India's sovereignty, integrity, and security, it is regarded as cyberterrorism, and the offender is subject to punitive penalties.
* Cybersecurity and New Technologies Programme: The goal of the Cybersecurity and New Technologies Programme, which was established by the UN Office on Counter-Terrorism, is to strengthen member states' and commercial organizations' ability to defend against terrorist actors' cyberattacks on vital infrastructure. Should such cyberattacks take place, the project also aims to minimize their effects and recover and restore the targeted systems.
* "The Tallinn Manual": Although the issue of cyber warfare has yet to be addressed formally in international laws, the Cooperative Cyber Defense Center of Excellence (CCDCoE) published this academic guideline in 2013, in which it defined when cyber warfare violated international laws and provided several solutions on how countries may respond to serious cyber threats. There are several possible solutions to the problem.

**Possible Solutions**

To begin with, governments should perform cyber wargames, which are real-life simulations of cyber warfare, on a regular basis. During the cyber wargames, a team would act as attackers and perform cyberattacks on the target system in different and unusual ways to simulate cyberattack scenarios. This way, defenders can learn to react to attacks, protect critical infrastructure, and fix the gaps in their defense procedures, which will prepare them against future cyber warfare. The same applies to private sector businesses, as they also face the risks of cyberattacks.

Meanwhile, governments should issue national security policies in a layered approach to protect their information infrastructure if they haven't already done so. For the first step, raising awareness about cyber security is needed to improve the overall preparedness of the local community. Raising awareness is a suitable solution to almost all kinds of problems, but awareness is particularly vital in this issue of cyber warfare as it remains an unfamiliar field for the public and its importance tends to be ignored. Campaigns and informational posters are effective methods of spreading awareness in adult society. Because youths must also be made aware of the issue, the government can also collaborate with social media platforms to publish global cyberwarfare news. Even further, it may be possible for local Non-Governmental Organizations (NGOs) to establish an educational program that teaches computing skills to those interested to improve the reduce the overall vulnerability of the community against cyber attack. Then, the government should set a national cybersecurity assurance framework, and cooperate closely with private tech businesses and hackers to constantly update the system’s cybersecurity capabilities.

Since small private firms in the private sector are particularly vulnerable to cyberattacks, the government should also support them with local hackers or funds to implement measures like web application firewalls (WAF), Runtime Application Self-Protection (RASP), DDoS Protection, and other forms of obstacles to detect and block malicious traffic, as well as methods to restore business operations when facing cyber attacks.

**Bibliography**

"United Nations Convention against Corruption." *United Nations Office on Drugs and Crime*. United Nations, 2004. 13 Nov. 2009. <<http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf>>

What is cyber warfare: Types, examples &amp; mitigation: Imperva. Imperva. 9 Nov. 2021. <https://www.imperva.com/learn/application-security/cyber-warfare/>