CYBER WAR: THE FUTURE OF CONFLICTS!

YASHVARDHAN KUMAR
18030034
BAGA 18'
JSIA

ABSTRACT

From the Information Age to the sinister Disinformation Age it is supremely necessary to understand cyber warfare as there is high human dependency on advancing information technology with the use of computer infiltrations and cyber-attacks as the internet has proved to be comprehensively untrustworthy due to the transformation of the industry. This essay focuses on the contemporary and prospect threats of 'Cyberwarfare' disrupting World Order and menacing with the critical infrastructure, data privacy rights of private and public enterprise and the Cyber Security Initiative taken by India to tackle cyber-attacks. This essay also discusses the "tech addiction" and how it plays the 'Cyber to Physical Effect' rattling protests and economic ties between nations and cause polarization globally. The latter part of the essay discusses the cyber peacekeeping processes and how international forums should prevent cyberwarfare in light of the strive for hegemony of superpowers around the globe.

INTRODUCTION

The WWW's invention in 1991, by Tim Berners Lee was the most gigantic step for technological evolution with a massive development in the Information Age which has taken a calamitous reversal to the Disinformation Age. The first ever cyber-attack in history was the Morris Worm in 1998, initiated with good intentions to determine the magnitude of the Internet, which later on took a catastrophic turn and crashed over 6000 computers with reparation costs of approximately US$1Million. World Order is exceptionally threatened today due to computer infiltrations, data privacy breach, and internet disruptions with immense use of social media platforms, highly advanced hackers' groups and phishers.

It is extremely necessary to understand the dangers and threats posed by the internet to humanity as the world revolves in the vicinity of technology, from information infrastructure regulating the telecommunication systems to factors of public life such as air, road, and from a traffic light to an airplane. This global system of internet and computers has a tremendous involvement on the private sector as well such as running businesses, exports and imports, trading, investments and stock markets. This essay will demonstrate how is cyber war the future of conflicts and how does it have a deep alliance with social media platforms amidst the immense disruption of World Order.

Russia, China, Korea and the US, along with European countries such as Ukraine, Czech Republic, etc. have some extreme cyber strategies dominating the world in this sector. Operation Titan Rain in 2003 was the first ever state-sponsored cyber-attack in the history of Internet, originated in China targeting US defense contractors, NASA and the Ministry of Defense of UK for the purpose of

gathering information of national security strategies. I would like to bring the reader's attention to "Cyber to Physical Effect", wherein the hacker gains access to the physical world through cyber-use causing catastrophic consequences. The Estonia Cyber Attack in 2007 is the most extravagant example of the above-mentioned effect in the modern hybrid warfare as a pro-Nashi Russian hacker targeted the Estonian Parliament, banks and ministries spreading misinformation and majorly influencing general public to riot against the displacement of the Soviet Bronze Soldier of Tallinn leading to a casualty.

Due to underdeveloped international organizations in cybersecurity, countries globally use cyber-attacks to disrupt sovereignty and compromise national security of other non-ally nations. Mentioning Russia, which has a Cybercrime Black Market, valued at US$2Billion annually, as nations like the US and UK recently claimed that Russia is attempting to disrupt the Tokyo Olympics in 2021, similar to the hacking of 2018 Winter Olympics as an initiative in a "worldwide hacking campaign". Moreover, about Russian interference, the US Cyber Command and Microsoft strictly stated that it detected a botnet, originated in Russia for interruption in the US Presidential Elections, forthcoming in November. Moving on to China, which has one of the largest military groups of cyber experts on the globe where 41 percent of worldwide cybercrimes are originated by the Chinese PLA. Cyber-attacks from China threaten critical infrastructure rather than cyber corporate espionage which is a high concern for nation-states, and as ex-additional Secretary from R&AW said, China's principles follow deception, stealth, ingenuity. These wholesome fact presentations represent how these powerful countries strive for hegemon and how this could be achieved by cyber-attacks and by causing national severance. The Game Theory, proven by John von Neumann is an economic field which is peculiarly interesting due to its application in computer sciences and how nation-wide decision makers apply the theory for practical and cyber strategic purposes such as the US Presidential Elections.

CYBERSECURITY IN INDIA

In 2019 from May to August, India was the most cyber-attacked country in the world, resulting in 74,998 attacks, originating in China, Slovenia, Ukraine, Czech Republic and Mexico with pertinence to the National Cyber Security Policy 2013. The consistent 2019 attacks on India awakened the Defense Cyber Agency to compose an advanced cyber strategy, culminating in the National Cyber Security Strategy 2020 which will be released later this month for security from cyber-attacks through ransomware and malware disruptions.
The Indian Army detained a Pakistan drone along the Line of Control in Jammu and Kashmir's Keran sector which shows how India should be reluctant to its regional counterparts such as China and Pakistan such as operation Sidecopy, which is a cyber espionage campaign hosted an Advanced Persistent Threat (APT) group.

The Information Technology Act 2000 circulates regulations of cybercrimes and cybersecurity for the purpose of data security, prevention from malicious ransomware attacks in India. India has faced several major cyber-attacks such as the Data Theft at Zomato and the Petya Ransomware in 2017, then moving on to the hacking of ISRO by the North Korean hacker group, Lazarus. The National Technology Research Organization (NTRO) is the primary agency designed to protect national critical

infrastructure with support from the Indian Computer Emergency Response Team (CERT-In) in analysis, forecasts and alerts on cybersecurity issues and breaches. The transformational Digital India push as well as Industry 4.0 is required to be supported by a robust cyberspace.

Chinese Army's special unit 61398 is posing severe threats to India on the borders and with respect to the banning of 118 Chinese Apps under Article 69A of the IT Act. Cambridge Analytica played a major role in the 2010 Bihar Legislative Assembly Elections to carry out an in-depth electorate analysis, wherein 355 Indian Facebook users installed the Cambridge Analytica App culminating to exposure of personal data of over 560,000 Indian users. Indian Cybersecurity agencies should be more rigorous, evolving and draconian towards cyber threats in order to protect national sovereignty and their strive for development.

THE WORM HOLE OF SOCIAL MEDIA

The worm hole of social media which is pulling humanity through it. With pertinence to social media influence on its users, I would like to highlight the "Facebook-Cambridge Analytica Scandal" as a glimpse of how private and government organizations work collectively and overpower impoverished data laws for political and profit use. The scandal was bedeviled in 2018, wherein millions of Facebook user's personal data was used for political advertising without consent in the Brexit Campaign and the US Presidential Elections in 2016 by collecting data points.

Despite facing immense criticism, the big tech names such as Google, Amazon, Twitter, Snapchat and Facebook are getting colossal as the days pass by, the entire tech industry is under a new level of scrutiny as relations between mental health and social media use are highly correlated. Plastic surgeons coined a new term called "Snapchat Dysmorphia", with young patients wanting plastic surgery to look similar to the Snapchat Filters used for selfies. In my belief, the social media tools that are being constructed stylishly have commenced to erode the social fabric of how society functions. The tech industry is full of cacophony of grievances and scandals, and misinformation leading to riots and chaos worldwide erstwhile giving rise to extremists and terrorist organizations such as ISIS to have a larger grasp of the planet and critically menacing World Order. There are several illustrations of social media influencers such as the Umbrella Movement in Hong Kong, the Protests against Abdelaziz Bouteflika in Algeria and the Black Lives Matter Movement for non-violent civil disobedience leading to social media blackouts.

I feel that the world is falling under a magical spell of "tech addiction" which is severely prevalent in today's world as tech industries are not obliging their moral responsibility to make it less addictive. Facebook, Google, Twitter, YouTube, etc. are free apps and in my perception, if the user is not paying for the product, sh/e is the product. It's the gradual imperceptible change in human behavior and perception which is the product. The Silicon Valley is a marketplace that trades exclusively in human futures, producing trillion of dollars making them the richest companies in the history of humanity also making it unprecedented as precision is ultimate at these companies. To resolve the disorientation between perceptions I would like to question that "If I search for a Versace Sneaker on Google, how

does Facebook and Instagram show me advertisements of the very same sneaker I just viewed on Google?"

CYBERPEACEKEEPING

With so much unrest around the world, and interruptions in global communication for the purpose of sensitive information, the international organizations and forums are playing a developing role in this evolution. The United Nations launched a Global Programme on Cybercrime for a united cooperation on defeating cybercrime, although some member states would not want the UN to cast inquiries into cyberattacks and espionage activities as they would themselves be at risk of disclosure. Israel is ruling the world of cybersecurity from its Silicon Valley in Wadi. DEF CON Convention in Las Vegas is very interesting to me as it is the largest hacker's convention in the world. Initiated in 1993, the convention contains hackers, students, lawyers with interests in software, robotics, wherein contests and competitions are held, called the hacking wargames. Moreover, Pentagon hosts hacking contests wherein they invite youth to hack the Pentagon and reward them with awards. Peacekeeping can also be performed by conjunction with regional groups that have cyber defense initiative. A pragmatic complication is that there is a bombarding of cyberattacks in a month's period and it is laborious to prevent those many intrusions because of the precipitate number. The United Nations' pursuit to define the criterion of cyber law on the world stage has been full of endeavors, but was not entirely profitable.

CONCLUSION

To conclude, I would state that this is just the commencement of cyber-attacks and there are many more awaiting highly. To resolve this emerging threat of cyber-attacks between the consistent strive for hegemony between superpowers, the United Nations should play a much hefty role in evolving regulations and maintain World Order. The concept of digital peacekeeping is still underdeveloped in the international world, unlike Israel, as the UN should motivate member states to undergo cyber attack prevention through aligned efforts between nation-states. Cyberattacks have previously incapacitated countries such as Estonia, and is majorly ranging in India, Israel and Pakistan to name a few. In congruence to this evolving and unprecedented domain of cyber, the United Nations need to follow an illuminating approach to sustain order or else the cyber world would transpire humanity with compliance of Robotics in the future as well.

REFERENCES

https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/

https://indianexpress.com/article/explained/explained-why-us-uk-believe-russia-is-planning-a-cyber-attack-on-tokyo-olympics-6824628/

https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06