CYBER DIPLOMACY – THE CONCEPT, EVOLUTION AND ITS APPLICABILITY

Avinash KUMAR
Master's student in International studies, Christ University, Dharmaram College Post, Bengaluru, India
Kumar.avinash@isph.christuniversity.in

Abstract: This article highlights the importance of cyber diplomacy to resolve the issues arising in cyberspace. It deals with the objectives of diplomatic action in cyberspace and cybersecurity in an interdependent world. The article adumbrates on a variety of dimensions and opportunities for sustained cooperation between countries to create peace and harmony in the cyber domain. India's initiatives to deal with cybersecurity threats are also emphasized. The article has five segments – introduction, compulsions for cyber diplomacy, global efforts towards cyber diplomacy, India's attempt in cyber diplomacy, and conclusion.
Keywords: Cyberspace, Cyber Diplomacy, Cyber Ambassadors, Cybersecurity.

INTRODUCTION

World is currently undergoing a major technological revolution known as the "4th Industrial Revolution" which is transforming life as we know it (Schwab, 2017). Owing to this rapid technological progress and mindless infusion of random technological sophistication into everyday life, peace and stability of the globe is greatly challenged. This situation is further complicated by various threat actors, with varied agendas, manipulating cyberspace and its associated technologies to terrorise the world. It is therefore to handle these new forms of conflicts that arise out of the technologically sophisticated cyberspace, countries are in a need to focus their efforts into a new form of diplomacy known as Cyber Diplomacy.

Cyber Diplomacy in simple terms can be defined as the use of diplomatic tools and diplomatic thinking to resolve issues arising in cyberspace. However it is quite different from Digital Diplomacy, an equally recent concept, which refers to the use of digital tools and techniques to advance diplomatic goals. Cyber Diplomacy bridges the gaps between nations during cyberwar or cyber-attack episodes and helps to avoid escalation of a conflict into economic devastation or deadly conflict through negotiations. In this progressively changing role of the technological world, Cyber Diplomacy can be seen as a foreign policy tool in maintaining International Relations.

Therefore, this research paper aims to study the concept of Cyber Diplomacy as it exists on the global platform, followed by its perceived role in India. This paper would later articulate the need for a cyber ambassador for any country to play a vital role in minimizing the conflict arising out of cyberspace among nations through negotiations.

COMPULSIONS FOR CYBER DIPLOMACY

The concept of 'Cyber Diplomacy' came into limelight in the 21st century and this phrase was used extensively by Evan H. Potter in his book "Cyber Diplomacy: Managing Foreign Policy in the Twenty-First Century" published in 2002. Cyber diplomacy refers to exchange of grievances and getting riddance in cyberspace domain between state actors as well as non-state actors through diplomatic channels. The role of cyber diplomacy works as a tool to minimize or avoid conflict and can also work as deterrence for nations in the cyber domain in future. Cyber diplomacy mainly deals with reducing the causes and impact of cybersecurity and cybercrime issues which is boosted by the idea of cybersecurity strategies or framework of national cyberspace to form better governance within the state.

The use of diplomatic channels is not only to secure national interests in cyberspace but also to work towards the notion of confidence-building with other nations. In the last decade, many countries have adopted the policy of Cyber diplomacy as part of their respective foreign policy and have appointed 'Cyber Ambassadors' to represent their respective States and to respond to conflicts arising out of cyberspace. Nevertheless it is important to know what situational compulsions made countries to adapt the concept of cyber diplomacy into their foreign policy. As the adoption of cyber technology into everyday life was progressing leaps and bounds in the early 21st century, it revolutionised global functioning, which turned digital, as well as empowered every individual with the right skill set to threaten a much bigger player. Threats associated with the domain were also spreading rapidly, largely unchecked and due to this, countries around the world became easily vulnerable and hence a number of conflicts arose from the cyber domain for which the world was not prepared for.

For instance, in the year 2007, Estonia, a former Soviet State, faced a major cyber-attack which lasted for 22 days (27th April to 18th May). The government, the police, banks, Internet service providers (ISPs), online media, and a variety of small enterprises and local government websites were among the targets. Because Estonia was a highly networked country even back then, a widespread attack on the available public digital services had a substantial impact on everyday residents and enterprises' lives. The attackers used many known methods of cyberattacks such as email spam ping flood, UDP flood, etc resulting mostly in Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks and were considered a threat to national security.

The trigger for these cyber-attacks was a decision made by Estonian government to shift a Soviet-era monument in Tallinn to a different location that resulted in a political conflict between Estonia and Russia. Work of relocation of the monument began on 26th of April, and one day later the cyber-attacks began.

Cyber forensics on the attacks revealed that a great bulk of malicious traffic came from outside of Estonia and there was a clear indicator of Russian linguistic origins that were frequently found in the malicious communication. The Estonian state government requested Russia for "a formal investigation assistance" to track down attackers under a pre-existing Mutual Legal Assistance Treaty (MLAT) between the two countries, however this did not yield any positive

response. Nevertheless, in January 2008, one person was convicted from within Estonia for carrying out cyber-attacks in 2007. Evidence was collected against him for attacks organized inside of Estonia and resulted in his eventual prosecution.

In the aftermath of this whole episode, as part of cybersecurity and infrastructure protection, the North Atlantic Treaty Organization (NATO) performed an internal evaluation, as Estonia is a member of NATO, and hence created a strategic framework for cyber defence and established Cooperative Cyber Defence Centre of Excellence (CCDCOE) headquartered in Tallinn (About NATO). In 2013 the Centre published the Tallinn Manual 1.0 which was a major development and a direct product of 2008 cyber-attacks on Estonia from NATOs side (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013). This Tallinn Manual thus became one of the main guiding principles of cyber diplomacy for the West.

In the year 2010, on July 16th, Microsoft, MITRE Corporation, and others published a security advisory against a new malware known as Stuxnet, which was later declared as the first Cyber Weapon. It was identified that Stuxnet had infected more than 2,00,000 computers across the world, but the worst affected country was Iran. Between 2007 and 2010, the Stuxnet malware was infused into the computers of Iranian Nuclear Facility in Natanz under a secret mission codenamed "Operation Olympics Games" to sabotage the country's nuclear ambitions. Due to the malware more than 1,000 centrifuges were damaged in the Natanz facility which were important for Iran's covert uranium enrichment program to develop nuclear weapons. It was one of the first known malware to target industrial control systems, meanwhile subverting the system with the help of a Programmable Logic Controller (PLC). It was observed that around 60% of the affected companies were in Iran and it mostly targeted uranium-based infrastructure plants there. According to an estimate, this resulted in a 30% reduction in Uranium enrichment efficiency of the country which eventually led to increasing the time of Iran acquiring weapons grade Uranium.

It was identified by many analysts that such complex malware programs could only be designed with the patronage of nation states. It was ultimately deciphered that this malware attack was targeted against Siemens 7 software running in the computers connected with the Centrifuges which in turn ran the nuclear programme in Iran. This episode of Stuxnet attack not only made Cyber Weapons a reality but also resulted in complicating the existing conflict between Iran and the West, which persists till date.

Another major development in the Cyber diplomatic front at the global level was the signing of a Cybersecurity agreement between the United States and China in 2015. This bilateral Cybersecurity Agreement between the United States and China came after more than a decade long mutual allegations of cyber espionage and other cyber aggressions by the two countries. Since the wake of the 21st Century the US was crying foul about China's aggression against it in the cyber domain and was painting a cyber villain out of China. However, following Edward Snowden's revelations regarding US eavesdropping and other covert cyber operations across countries around the world including China, the cynical plans of the US got exposed. The revelation of the breadth of US spying by Edward

Snowden in 2013 further damaged US-China ties. In 2014 the US alleged that Chinese Government backed hackers had hacked into the US Office of Personnel Management database and has stolen millions of records and other documents. The US also released the names and photos of 5 allege Chinese Government Hackers an demanded with China to extradite them to the US to stand trial. However China, completely rejected all the allegations. Later in 2015, in order to remediate the broken links as well as to enhance mutual trust and stability, the world's two largest economies entered into the agreement. This deal not only marked a significant step forward in US-China ties but was also seen as a promising start for future international cybersecurity accords. This agreement aimed at preventing economically driven cyber espionage between the two nations, including theft of intellectual property and trade secrets. The US-China Cybersecurity Agreement can be termed as the first major milestone in the Global Cyber Diplomacy, though its success is highly contested.

GLOBAL EFFORTS TOWARDS CYBER DIPLOMACY

As mentioned earlier, the concept of Cyber Diplomacy is relatively new to the global diplomatic stage. Also given the high technological nitty-gritties associated with the domain, there are only very few countries which have realised the importance of this new diplomatic concept and have incorporated it within their respective foreign policies. Some of these countries which have taken a lead in this direction have also appointed a cyber ambassador as the country's representative to reach out to other nations and global platforms in order to handle the conflicts in cyberspace. A list of various countries that have appointed a Cyber Ambassador is at Table 1.

Table 1. *Countries with their Cyber Diplomats*

COUNTRIES	CYBER AMBASSADOR
Australia	Dr. Tobias Feakin
Denmark	Casper Klynge
Estonia	Heli Tiirmaa Klaar
Finland	Rantala Enberg
France	Mr Henri Verdier
Israel	Rami Efrati
Japan	Akahor Takeshi
United Kingdom	Henry Pearson

Since the adoption of the concept of cyber diplomacy in the foreign policies of different countries, they have predominantly relied upon signing of bilateral, tri-lateral and multilateral agreements on cyber security, mutual non-aggression and information sharing in cyberspace as the means to handle conflicts as well as tackle conflict of interests arising from cyberspace. At the global level, several multilateral agreements have been

signed throughout the last two decades to make cyberspace a peaceful domain, yet it is far from reality. However, one of the milestones in global cyber diplomacy arrangement begins with the Budapest Convention on Cybercrime. This arrangement, which was proposed in 2001 and came into force in 2004, is the first international convention dealing with crimes perpetrated via the Internet and other computer networks, with a focus on copyright infringements, computer-related fraud, child pornography, and network security violations. It also contains a series of powers and procedures such as the search of computer networks and interception. Its primary goal as laid forth in the Preamble is the adoption, notably via the adoption of suitable laws and promoting international cooperation of a common crime strategy to safeguard society from cybercrime. This convention is the first multilateral legally binding instrument to regulate cybercrime and is the first global cyber diplomatic agreement. The Budapest Convention is also supplemented by a Protocol on Xenophobia and Racism committed through computer systems. According to the data 66 nations have ratified the convention whereas 2 nations have not ratified the convention, but they are officially signatories of the convention (Chart of signatures and ratifications of Treaty 185, 2021). Nevertheless, this convention cannot be called truly global yet as the two largest populated countries, China and India are not signatories to the arrangement. Also, Russia, a powerful cyber actor in the globe has refused to sign the convention citing sovereignty concerns.

In 2003, the United Nations General Assembly set up a Group of Governmental Experts composed of people across the globe who have been keenly working towards cybersecurity. Since 2004, five Groups of Governmental Experts (GGE) have convened to study the threats posed by the use of ICTs in the context of international security and how these threats should be addressed. Three of these Groups have agreed on substantive reports with conclusions and recommendations that have been welcomed by all UN Member States. Although consensus was reached during the second Grouping in 2009/2010, the 2013 UNGGE might be considered as the first successful global agreement and its members agreed on the following:

- International law, in particular the UN Charter, is applicable to the cyber-sphere and is essential for an open, secure, peaceful and accessible ICT environment.
- State sovereignty applies to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.
- State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms.
- States must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-State actors for unlawful use of ICTs.
- The UN should play an important role in promoting dialogue among Member States.

This agreement was followed by a report in 2015 that persuaded all members to agree to a set of "voluntary non-binding rules." The UNGGE continued to work towards further progress after their 2015 report, but due to a disagreement over a provision asserting that

international law applies in cyberspace, it was unable to establish a consensus and issue a report in 2017. The question of whether international law applies in cyberspace is still debated at the global stage.

In 2018, an alternative to the GGE was proposed by Russia and was called Open Ended Working Group (OEWG). OEWG was designed to have much bigger membership (any of the 193 UN member states can participate) in contrast to GGE which have smaller membership (15-25 UN member states and have time-bound mandates). The US and its allies slammed Russia's plan, claiming that it misrepresented and cherry-picked wording from past GGE reports and accused Russia of divisiveness. However, the Russian representative presented the US-proposed GGE as an "exclusive club" that failed to consider the opinions of all UN members. Nevertheless both GGE and OEWG are actively functioning under the UN Office of Disarmament. The fact that countries/Blocks around the world could not even arrive at common consensus for creating a grouping that would discuss issues on cyberspace reveals the level of diplomatic maturity among nations in this field.

The European Union enacted the General Data Protection Regulation in 2016, which superseded the 1995 Data Protection Directive of the European Union. It contains requirements requiring companies to respect EU residents personal data and privacy for transactions that take place within EU member states. The GDPR also governs personal data exporting outside of the EU. The regulations are the same in all 28 EU member states, implying that businesses in the EU must adhere to a single set of rules. The GDPR is an important milestone in the cyber diplomacy front as it involves a whole region of the world of nearly 28 states, almost all private players in the cyber realm who does business in the EU, the Governments of all 28 States as well as the whole of the Internet community.

In 2011, the African Union produced a Cyber Security and Personal Data Protection Convention to provide a "credible framework for cybersecurity in Africa'' by protecting personal data, promoting cyber security, e-governance, and combating cybercrime. The Convention was supposed to be ratified during the 22nd African Union summit in January 2014, but it was postponed because many Countries were against it, arguing that it contained measures that would jeopardise privacy. The AU convened an expert meeting in May 2014 to revise the Convention considering the criticism, and the final document was ratified in July 2014.

On June 16, 2009, the Shanghai Cooperation Organization (SCO) signed its first intergovernmental agreement on information security cooperation. The agreement is unique as it commits member States to refrain from using cyber weapons against other countries and to aid third parties.

After the incident of state-sponsored cyber-attacks occurred in Estonia (2008), NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) sponsored a multi-year effort to gather input from a group of recognised experts on how international law applies to cyber events. The first Tallinn Manual was concerned with the law of armed conflict whereas Tallinn 2.0, the second Tallinn Manual, covers a considerably larger range of cyber activities, both in and out of armed conflict (Tallinn Manual 2.0 on the International Law Applicable to Cyber

Operations, 2017). In 2021, the CCDCOE is working on the Tallinn Manual 3.0 Project, a five-year project that will see existing chapters revised and new issues of state relevance will be explored (The Tallinn Manual 3.0, 2021).

Various bilateral agreements were also signed in recent years, but China-Russia Cybersecurity Cooperation agreement deems special mention. The 2015 Sino-Russian cybersecurity agreement appeared to be a step towards strengthening the overall Sino-Russian cooperation in the cyberspace domain as well. Mutual assurance on non-aggression in cyberspace and wording supporting cyber-sovereignty are two essential components of the agreement. China and Russia are expected to maintain tight technological and diplomatic ties in the coming decade. In April 2016, the inaugural Russia-China Information and Communication Technologies Development and Security Forum in Moscow showed the strengthening of Sino-Russian partnership in cyber-sovereignty.

Despite the various conventions, agreements, treaties, etc existing between nations, the threat in cyberspace is ever growing unchecked and the countries are doing very little to counter it in an effective way both technically as well as diplomatically. As countries give priority to their national interests, promises through agreements and treaties are bypassed through technological sophistication to achieve national goals. Nevertheless, the various cyber diplomatic arrangements at different levels across the globe must be looked at from an evolutionary perspective and be appreciated for its existence and the efforts behind it.

INDIA'S ATTEMPT IN CYBER DIPLOMACY

In the last two decades, India's internet and digital presence has seen an exponential growth. With an estimated 624 million users as of January 2021 (Kemp, 2021). India is the world's second biggest internet user after China. India's online population has increased rapidly at a quicker rate than any other big economy in the last decade. According to the report of IAMAI-Kantar ICUBE, India is predicted to have more than 900 million internet users by 2025 (IAMAI - Kantar ICUBE 2020 Report, 2020).

Government policies in recent years also contribute to the sudden increase in the number of internet users in the country. The Digital India programme played a great role in bringing in millions of new users into the cyberworld. However, due to the speed and scope of India's digital transition without regard for safety and security in the domain, India has become increasingly vulnerable to cybersecurity threats, and also it has become a major source and target of cyberattacks.

The fast expansion of India's Information and Communication Technology (ICT) networks has been primarily fuelled by low-cost, insecure hardware and software. Therefore, India has become one of the most targeted countries for cyberattacks by both state and non-state actors. Apart from the attack on individuals for various reasons, the country's critical information infrastructures are targeted with precision strikes especially in the financial sector and energy sector.

The 2018 Cosmos Bank cyber-attack, 2019 cyber-attack on Kudankulam Nuclear Power Plant and the 2020 cyber-attacks on India's power sector are few recent cases in point.

In response to tackle these threats, the Indian government agencies responsible for cyber security are tirelessly working and yet the number of instances and damages due to cyber-attacks are on rise. Therefore, realising the fact that cyber-attacks cannot be tackled only through technological means, India has also started taking the path of Cyber Diplomacy in recent years. The country has signed nearly 40 agreements in the field of cyber security, Information technology and Information and Communication technologies with almost 40 countries.

India is also an active member participant on the global stage on various issues concerning cyberspace governance. The country's representatives take part in the UN GGE meetings and OEWG meetings at the United Nations level. The country is also a member of almost all regional and global organisations and groupings which work towards a safe and secure cyberspace. Also having realised the importance of cyber diplomacy, the Ministry of Foreign Affairs of the Government of India has established a Cyber Diplomacy Division under it.

Despite such efforts, the country lags much behind the major players of the world mainly due to two important reasons. First, all the efforts taken by the government in cyberspace are sporadic in nature and hence there is very little or no coordination between various departments/agencies within the Government. Second, the country doesn't have a single point representation on matters concerning cyber diplomacy and hence, the interest of the nation is misrepresented at various places in different ways.

Therefore, in order for the country to become a major player in the global cyber affairs, it has to first streamline its domestic cyber governance structure thereby creating a seamless coordination, synchronization, information flow and resource rich structure. Moreover, the country can take a cue from many global players such as Australia, France, Japan and Israel and appoint a Cyber Ambassador as the single point contact for Cyber Diplomacy and foreign policy in cyber affairs for the country at all levels in the global stage. The Office of Cyber Ambassador can then work out mechanisms towards confidence building, mutual non aggressions, data and information sharing, LEA cooperation, etc with other countries of the world.

CONCLUSION

As warfare becomes more and more network centric, future wars are going to be fought in cyberspace. Therefore, in order to maintain peace and stability in the future world order and to negotiate terms between the warring parties, a new generation of diplomats are necessary with the right skills who understand both the intricacies of technology as well as the nuances of diplomacy. Cyber Diplomacy is an infusion of modern day technology and conventional diplomacy and is the right tool for the future. However, politicians, policymakers, technocrats, and even the industry associated with the domain are necessitated to adapt to this new concept in this twenty-first century. While there is a certain degree of realisation that communication and cyberspace are critical tools for improving international ties and maximising national interests, countries must find routes to equip themselves in these modern diplomatic endeavours in order to reap real benefits.

REFERENCE LIST

About NATO. (n.d.). Retrieved from The NATO Cooperative Cyber Defence Centre of Excellence. Available at: <https://ccdcoe.org/about-us/>.

Chart of signatures and ratifications of Treaty 185 (2021, June 11). Retrieved from Council of Europe. Available at: <https://www.coe.int/en/web/conventions/full-list?Module=signatures-by-treaty&treatynum=185>.

Christian (2019, November 11). Digital Diplomacy vs Cyber Diplomacy. Retrieved from Association of Accredited Public Policy Advocates to the European Union. Available at: <http://www.aalep.eu/digital-diplomacy-vs-cyber-diplomacy>.

Corera, G. (2021, April 12). Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz. Retrieved from BBC. Available at: <https://www.bbc.com/news/world-middle-east-56722181>.

Estonia fines man for 'cyber war' (2008, January 25). Retrieved from BBC. Available at: <http://news.bbc.co.uk/2/hi/technology/7208511.stm>.

IAMAI - Kantar ICUBE 2020 Report.(2020). Retrieved from IAMAI. Available at: <https://cms.iamai.in/Content/mediafiles/7d9fac50-7cac-43df-93c9-0cf34fb52403.pdf>.

Kemp, S. (2021, February 11). Digital 2021: India. Retrieved from Datareportal. Available at: <https://datareportal.com/reports/digital-2021-india>.

Murray, W. (2013, June 13). Edward Snowden's NSA surveillance revelations strain China-US relations. Retrieved from The Guardian. Available at: <https://www.theguardian.com/world/2013/jun/13/snowden-revelations-nsa-china-relations>.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Retrieved from Cooperative Cyber Defence Centre of Excellence. Available at: <https://ccdcoe.org/uploads/2018/10/Ottis2008_analysisof2007fromtheinformationwarfareperspective.pdf>.

Potter, E. H. (2002, September). Cyber-Diplomacy - Managing Foreign Policy in the Twenty-First Century. Retrieved from mcgill-Queen's University Press. Available at: <https://www.mqup.ca/cyber-diplomacy-products-9780773524514.php?Page_id=73&>.

Schwab, K. (2017). The Fourth Industrial Revolution. Retrieved from World Economic Forum. Available at: <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab>.

Stanzel, V. (2018). New Realities in Foreign Affairs: Diplomacy in the 21st Century. Retrieved from Stiftung Wissenschaft und Politik. Available at: <https://www.swp-berlin.org/publications/products/research_papers/2018RP11_sze.pdf>.

Tallinn Manual — A Brief Review of the International Law Applicable to Cyber Operations. (2019, December 06). Retrieved from The Cyber Diplomat. Available at: <https://medium.com/@cyberdiplomacy/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2>.

Tallinn Manual on the International Law Applicable to Cyber Warfare (2013, March). Retrieved from Cambridge University Press. Available at: <https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE>.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017, February). Retrieved from Cambridge University Press: <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9#>.

The Tallinn Manual 3.0. (2021). Retrieved from The NATO Cooperative Cyber Defence Centre of Excellence. Available at: <https://ccdcoe.org/research/tallinn-manual/>.

William, J. B., Markoff, J. & Sanger, D. (2011, January 15). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. Retrieved from New York Times. Available at: <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>.

Avinash KUMAR

Is pursuing Master's in International Studies at (Christ Deemed to be University), Bengaluru, India. He has interned at renowned think tanks like the Centre for Air Power Studies (CAPS) and Foreign Policy Research Centre (FPRC) in New Delhi. His research work revolves around the 4th industrial revolution, cyber security, quantum computing, and critical infrastructure protection.