Cyber diplomacy and cybercrime-An unholy nexus in world politics

Dr. Rupa Sen

Associate Professor, Department of Political Science HMM

College for Women, Dakshineswar, Kolkata-35

Diplomacy in International relations is resolution of problems by government and non-government agencies to strike a balance between sovereign states engaged in power politics. Diplomatic decisions are normally taken behind closed doors but the stupendous growths of communication technology have transformed the entire gamut of the activity, making it widely open and public. Technological revolution has widened the horizon of opportunities and possibilities for Governments to engage in constructive interaction with public resulting in intrusion of elements unconventional and evolving as a subject of international diplomacy. A popular outcome of the evolution is cyber diplomacy, a new component in the realm of foreign policy. However Cyber diplomacy should not be understood as just using modern means of communication; instead it should be comprehended as a crucial part of public diplomatic strategy.

Worldwide information communication and technological explosion undoubtedly influenced and enhanced life of mankind; but generated adversaries too.

Large scale use of internet facilities opened vistas of opportunities for social, economic and political benefits but the same facility emerged with the potentiality to aggravate tension in the political and military sphere leading to unwarranted misconception in relations and conflicts between nations, posing serious challenge to national and international security system. The asymmetrical and transnational nature of cyber threat, and corresponding impediments caused for political leaders, calls for accurate diplomatic effort to fight tension; because cyberspace is equally accessible to terrorists and criminals from both political and militaristic angle depending on targets fixed by perpetrators. ***Already the world is beset with four types of cyber insecurity namely cybercrime, cyber espionage, cyber terrorism and cyber warfare.*** Cyber warfare are. Largely conducted by national actors; wherein terrorist outfits need not develop malware

themselves for hacking. They may buy malware from commercial hacking crew and engage in malicious aims. Added to it access to malwares could be possible, if such groups were obliged with state sponsorship, to execute asymmetrical cyber terrorist attacks.

A few years ago Edward Snowden's revelation of cyber espionage activities of United states on NATO allies and mass surveillance upon people of America and some European countrieshad a diplomatic rendition at international level(here insiders compromised a great deal of information)This incident upholds how vulnerable the nations stand where cyber security is still not strong. This prompted many west European nations to adhere to US centric model of Governance, to prevent damaging effect to their systems inflicted by high powered nations.

Donald Trump announced his interest to harbor good relation with India soon after his presidential victory. But his anti-Indian rant and speaking in favour of Pakistan and China now persuades India to measure her steps cautiously in building diplomatic ties with America.

Candidly ambitious America seeks to promote its desired interest promoting its desired interest at the cost of manipulation or suppression. In this context, it seeks to contain the growing power of China in Asia and aims to use the regional powers like India as a platform for support. Now China is not only a close neighbor to India but also the biggest market for trade and business. On the other side China is perhaps the only country who managed to surpass America digitally. America wants Russia to prevail over China. Russia on the other hand is biggest supplier of arms to India. It enjoys close ties with Russia and strong economic ties with China (New Delhi being the largest trading partner) Pakistan exports terrorism in the area especially to India. America funds and supplies arms to Pakistan. America's only agenda is to promote its economic and political interest. Naturally its market interest with the rogue state, Pakistan, shall prevent it fromdisplaying any friendly gesture to India in its war against Pakistan for combating terrorism. Hence India needs to measure her steps toward US; unless she streamlines her own cyber capability any possibility of her maintaining a voice in world politics would remain a far cry. North Korea refuses to be complacent with United States. While China continues to be the economic lifeline of Korea. The overtures of politics compels each nation to chart out a balanced cyber diplomacy to combat possible crisis slammed by an opponent or camaflouging ally, to ensure security, peace and stability.

With societies increasingly becoming digitized a paradigmatic shift is observed in the realm of International politics. Some changes are profoundly reflected in terms of priorities acquired by hard power versus soft power. The earlier conventional modes of economic coercion or military force is now obsolete, and losing ground against more subtle and effective technique of persuasion in the form of soft power and encouraging empowerment of public opinion both within and beyond the territory of one's nation. Under the circumstance it is necessary that governments, inform and influence foreign audience to create empathy as prerequisite for achieving its policy objectives abroad and also strategic aspect of their diplomacy.

North Korea's publicised inclination to test nuclear weapons or India's digital response to Pakistan's threat of nuking or constant publicizing of news from Iran, Iraq, Syria, Turkey and host of other nations inflicted with mindless ISIS and their activities are all part of the strategy called cyber diplomacy. The dastardly covert pogroms engineered by Big powers that so long remained under cover, is popped up with the boon of advancement of technological capabilities, strengthening the scope of strategic formulations required to address a crisis. This bears a direct impact upon the unidimensional advantage enjoyed by US, in the context of diplomacy and deterrence in International relations. ***Cyber-diplomacy is a strategy wherein, a nation enjoys the opportunity of exposing actual cause of their crisis and the rogue engaged therein. Also this form of diplomacy helps a nation find global support, for its activities back home.***

This strategy also contributes largely to conventional mode of diplomacy in implementing plans and achieving objectives of foreign policy issues. It builds empathy for the country in question. If Public diplomacy of US is to spread its values and ideas internationally it is normal they adapt to mass media and growing influence of culture tied to political and social change. The ability to reach people with mass diplomacy increases with strategic communication programme designed for foreign audience and supported by wide range of technological facilities like internet talk shows, tweeting, publications etc. mediums much stronger. France has subscribed to similar diplomacy of sharing its values and ideas to carve a niche in the world forum. Culture information and communication are strategic assets in the field of security policy in Germany as well.

Moscow has a troll Army under internet Research Agency to wage a disinformation campaign in support of its invasion of Ukraine and Kremlin in general. A couple of months ago Putin nudged

a hint at Russia's role in hacking of America's Presidential election. Intel Agencies claimed that Putin himself directed a Russian influence campaign involving cyber-attacks and disinformation intended to tilt the election in favour of Donald Trump ***(Times of India dated 2nd June 2017)***

Club of Middle East countries like Saudi Arabia, UAE, Bahrain, Egypt And Yemen recently severed diplomatic ties with Qatar with the belief that the state has befriended Iran the regional enemy of the Arab world and supported terrorism in the belt following a CNN Report on 6thjune 2017, where it was alleged that Russian hackers had breached Qatars state news agency. This implied even fake news could spark a crisis anywhere in the world. If Russian hackers have done it or America falsely implicated Russia to make the news viral the result remained the same; leading to isolation of Qatar impairing its socio, economic political existence***.(Times of India dated 8th June 2017)***

Brexit Campaigner Nigel Farage is alleged to have clandestine links with FBI and Russia a belief viral in social media. All such link ups are aired to capsize the growing influence of a group or a nation, engaged in power politics; In this case it was sheer hatred simmering within liberal elites, who were unable to accept both Brexit and Trump. Similarly, the Boko Haram sect of Nigeria who kidnapped nearly 276 school girls and held them hostage for months, in 2014-15 drew attention by taking recourse to social media. It publicized the link between Boko Harams and ISIS and Al Qaida. In 2013 Syrian Army (SEA) hacked twitter account of a news agency and falsely claimed that White House was bombed and Obama injured.

Again Cyber-attacks on IT infrastructure from Estonia in 2007, the hybrid war fought in 2008 in the conflict between Russia and Georgia the cyber-attacks on Uranium enrichment programme from Iran in 2010 all denote a cyber-component. The virtual attacks following conflict between Russia and Ukraine aimed not just IT infrastructures, including military communication system of Georgia but also of Russia, European countries and NATO Allies. All the episodes beginning from war between Eastonian government and media in 2007, the German Bundestag in 2015, Ukraine's power grid in 2015 and Swedish media in March 2016 account to cyber wars. Reports said that United States collaborated with Sweden and other nations to develop hacking and surveillance tools; and assured that the devices used be more powerful than that used to attack Russia. The Swedish FRA was ensured access to National security Agency of America a powerful analytic tool called X-keyscore that would enable an internet user to find access to entire

gamut of data at his disposal. Politically and military motivated cyber wars permanently eroded mutual trust between political leaders shrouding the global ambience with suspicion and ambiguity, leaving trail of tension, competition and conflict hovering overhead***, (Ref The Swedish kings of cyber war by Hugh Eakin, New York Review 19th January 2017)***

Further the US president Donald Trump is reported to have breached a protocol with cellphone diplomacy. Leaders of Canada, Mexico and France have US President on speed dials, which proves that all such leaders have contact numbers of Trump saved for direct communication. World leaders calling up one another may appear common but in diplomatic matters where leader to leader interactions are orchestrated it is certainly a break of protocol for a president whohimself expressed distrust of official channels. More so he is the man who pilloried Hillary Clinton for lax in security for keeping an email server in her residence and generated chants of 'lock her up' for her infractions.

When the world is grappling for cyber-security, tinkering in the social media could prove disastrous for a nation. ***Typos like China steals US Navy research drone in international waters-rips it out of water and takes it to china inunpresidented act (Dec 2016) tweeted by Trump, caused shamming of the presidential post of a country the world looks upon. Secondly such irresponsible tweet could trigger unpleasant bilateral relations; thirdly such acts and information bears a direct impact not only on the economic index of that nation in question but others who are committed or dependents in the system of economic cycle. With internet infrastructure going down by few hours could catapult and cause a rupture in economy, politics and society at one go. Already Fiscal loses adhering to cybercrime and cyber wars across the globe today is alarming. The expenditure amounts to US$81 billion just in Asia Pacific region***. ***Social media has evolved into diplomacy's second self, a significant other, according to a report by Burson-Marsteller, a global PR company. It provides a platform for unwarranted communication with targeted groups.***

The Paris Agreement signed by 177 nations on climate change is due to be implemented within 2020.Cyberdiplomacy is expected to play a crucial role in keeping alive the awareness of the problem; of course to weed out the challenges, adhering to it, requires transformative technology based sustainability revolution to enable countries like China and India breathe with ease in the Asian belt at least. Cyber diplomacy has the potentiality to generate Asian public opinion to keep

China from asserting control over South China Sea. But when countries like America withdraw from their resolution of working together for a sustainable environment strategy of cyber-diplomacy ought to be applied to persuade and convince them to be back on track. With increasing use of technology as a component for military response, primarily the need is to consider the threat as seriously as a conventional one. Singapore has already deployed Cyber-diplomacy building Alliances with other nations to sweep expertise to regularly monitor and test its defence and fruitful implementation.

If cyber-diplomacy is observed as a growing strategy in the field of international politics, cybercrime, cyber warfare and terrorism are also growing rapidly, as an organised network of business, where huge number of populace are engaged directly or indirectly, threatening Governments, Business, social media etc. leaving the world in a dilemma. The unholy nexus between cyber-diplomacy and cybercrime dwindles and dodges the nations and nationalities to a destination of uncertainty.

Many Internet users indulge in nefarious acts jeopardizing peace and security of a region or state. The US produces malware, spams and viruses more than any other country in the world. It is the hub for illegal IT jobs that scams anything that profits them; yet the scammers remain free from the legal claws, often insulated and secured from distant lands by high powered influential and underworld mafias.

However recent reports hold that China has outsmarted the US by hosting web pages that install malicious programme in computers to steal private information or send spam e-mails. According to Symantec Report in 2006 Beijing was found home to largest collection of malware inflicted computers.

Infact China is the biggest threat to United States. Numerous Cyber groups are nurtured in Beijing. Many under the tutelage of the Government itself. More than 70% of US corporate intellectual property theft originates in China. Chinese military strength is still to match the impeccable competency of the US defense Unit. As an alternate path to edge over US military acumen Beijing chose to bank on commercial and Government espionage, in which they have excelled enormously. Even the US can ill afford to ignore their technological smartness, because they are still struggling and grappling to protect their technological secrets from China. The Chinese told that they have

no intention to disrespect sovereignty of nations in Cyber space, even though they focus on commercial diplomacy and participation as per international technical parameters to shape cyberspace for economic and political interests; As a nation state they too intend to fight terrorism, control regional influence and manage bilateral relation with US.

Around 150 countries were targeted recently with ransomeware cyber-attack, disrupting normalcy in both public and private life. The malware called WannaCry paralyzed computers, running factories, banks, government agencies and transport systems affecting 200000 victims in more than 150 nations. Among the worst hit was Russias interior ministry and companies including Spain's Telefonica and FedEx corps in the United States. The pirates of the cyberspace has demanded to be paid in bitcoins and threatened to release five minutes of a film of Disney Company followed by 20 minutes segment until the ransome was paid. The role of pirates and cybercriminals interfering the creative world is quiet common across the world. Very often cultural icons buckle under duress to the dictates of the digital dark world to survive financial setbacks that could ruin them forever.

Recently an attack on a plush hotel at Austria (Alpine Hotel) where computer system was locked which compelled guests to be stranded in the lobby. This incident was a novel example of an increasingly malicious and prevalent type of modern day privacy through software, called ransomeware. Ransomeware is pandemic with internet, anything can be switched on and off from computers to cameras to baby monitors. But hacking a hotel and locking people out of theirrooms is a new line of attack in the league of nefarious activities***. (TOI, 1February2017)***

Reports from the Japan's computer Emergency Response Team coordination center, a non-profit group, said that 2000computers at 600 centers in japan were crippled and hit. Companies like Hitachi and Nissan motor Company faced problems though managed later. Chinese state media announced that 29,372 institutions had been infected in the land along with hundreds of thousands of devices. Educational institutions were adversely affected because of using old computers slow in updating operating systems and security.

The Railway stations, mail delivery, gas stations, office buildings, shopping malls and government services in China were affected. Common Chinese public vented their grievance in social

networking sites. This shows greatest techno savvy country could also fall a prey to malwares and disfunctionality of the system. Similar stories followed from Indonesia, where malware locked patient files on computers in two hospitals in the capital Jakarta, causingrestlessness. The effect of the malware in India was however comparatively low as precaution for insulation from malware affliction was taken. Reserve Bank of India directed Banks to operationalize this only after software updates were completed corporate houses urged employees to back up their data and refrain from opening unfamiliar files attachments. Windows users were urged to install software upgrades and firewalls. FMCG companies Marico and Godrej issued advisories to employees asking them to guard against the malware. South Korea, Malaysia, Bangladesh and host of other countries experienced the consequence of being targetsof cybercrime, freezing their computers and causing encryption and then demanding ransom through online Bitcoin payment to unlock files. ***So the stealthy underhand of cybercrimes are constantly on the vigil undermining the positive intensions of cyber diplomacy.***

An Indian origin Google security researcher found proof suggesting that North Korean hackers may have carried out the unprecedented ransomware cyber-attacks that hit multiple nations across the globe. Researchers claimed that some of the code used in recent ransomware called Wannacry was nearly similar to the code used by Lazarus group a pack of North Korean hackers who used a similar version for the attack on Sony pictures Entertainment in 2014 and Bangladesh Central Bank last year.

Researchers found similarities between the code found within Wannacry and other tools believed to have been created by the Lazarus group. A security expert Prof Alan Woodward said that time stamps within the original Wannacry code were set to UTC+9—Chinas time zone and the text demanding the ransome used machine translated English but a Chinese segment apparentlywritten by a native.

Cybercrime has evolved into a full-fledged industry indulging into marketing, providing service, trading, financing and others. The growth of the industry fuelled by cyber currencies like Bitcoin and protective cloak for criminals provided by Technology like TOR. Increasing sophistication of the industry has lured criminals to engage in bigger crimes ranging from implementing ransomeware encrypting contents of the computer and demanding ransome to unlock the system, to exploit users engaged in publishing personal data's from various dating sites. With 1.5

million annual cyber-attack online Crime is a real threat to internet users. Thereare nearly 4000cyber attacks every day, 170 attacks every hour and 3 attacks every minute. In 2014, 47% of American adults had their personal data stolen by hackers through data breaches at large companies. In 2013, 43% companies had a data breach, in which hackers got into their systems to steal information. Data breaches targeting consumer information are on the rise, increasing 62% from 2012-13.

By the grace of social media anyone could be duped by a link posted in a twitter or facebook, or from a cloned account would easily enable a hacker to break into their computer network. Once a person compromises attack (spear phishing) could move fast through that person's friend network leading to nightmare for the targeted. According to a 2016 report by Verizon around 30% spear phishing emails were opened by targets. But research published by cyber-security firm Zero Fox showed that 66$ of spear phishing messages sent through social media sites were opened by their intended victims.

NCRB report holds that there has been an escalation of 70%rise in cybercrime in India between 2013-15; with a consistent growth of 17 18% annually.

According to NCRB Report 2014 cybercrime was a little more than 9600;while in 2013 it was somewhere around 5693.Estimates for 2015 crimes were 16000;;all targets being active participants or users of social networking sites. Large scale technological adoption with minimal awareness has led to rise in such crimes. Besides lottery and job scams are rampant that evolved as organized crimes in India. With 780 cases of cyber-crimes reported in 2015 Noida saw setting up of center for cybercrime investigation in 2016.It is essential that people learn to protect themselves, the menace would loom large with its devastating effect.

The National cyber security policy is a framework for protecting information in cyberspace, by eliminating vulnerabilities. Major clauses include greater emphasis on research and development of indigenous security, technology and effective testing and deployment. Need for Public- Private partnership visa -vis technical and operational cooperation to adopt regulations and infrastructure in conformity with International best practices policy related to cyber security facilitated the creation of new agency called National critical information Infrastructure Protection center(NCIIPC) charged with protecting assets in sensitive sectors such as finance, defence,

energy and telecommunication. Unfortunately laws formulated by Government are not binding or enforceable. Besides the budget is not enough. Telecommunications is integrated into cyberspace, since the advent of internet protocols on mobile devices, one of the primary reasons for the rise in attacks. Besides UGC directed universities (technical) and institutions to add cyber-security and information security as subject of higher studies in 2013.When common man and his life is affected by cybercrimes, can Government institutions remain unfazed? The fruitfulness of cyber-diplomacy depends on intension of leaders, rule bound administration and stable digital system because disruptions and disturbances would invariably cause turbulence and impair the objectives of nation states.

Countries across the world is trying to manage cyber related issues via existing diplomatic methods using diplomatic resources. Cyberspace seldom conforms to conventional norms of diplomacy in vogue in the 20th century. Studies show that the ability to engage in cyber war with a country in the virtual world while maintaining normal diplomatic relation in actual world can no longer be addressed by current standards.

Countries like Singapore has already adopted cyber-security measures to challenge objectives of perpetrators. They resolved to strengthen cyber-diplomacy, developing a vibrant cyber security ecosystem by educating individuals, creating jobs by developing defense of the lands critical infrastructure cyber-security talent and building international partnerships to respond to cyber threats. Singapore aims to work with ASEAN and secure the internet space of the region. They are looking forward to form a forum that would attract high ranking military and political officials…forge a dialogue with nations of ASEAN and team up for a joint mission.

The European Union now seeks to initiate proper administration and implementation of International law in cyberspace. They wish to enhance the building capacity of 3rd world nations and engage in promoting international stability and protect digital economy. China has agreed to comply and cooperate in cyber investigation to nab criminals. South Korea subscribed to active cyber diplomacy. India embarked upon the mission to spread cyber security awareness. Today America encourages countries to engage in transnational cyber cooperation and promote cyber-security.

Terrorism and crimes would continue unabated; terrorists would scale dizzy heights to discover new devices and methods of attack but to fight the mindless mayhem of a handful should still continue. ***Unless nations club together spontaneously, adhere to rules, step up public education to propagate public safe use of internet combating the unholy nexus of cybercrime and diplomacy would remain a far cry. Sailing through uncharted sea may be difficult and dangerous but surely not impossible.***

References

1. Ransomeware blow contained in India, Times of India dated 16May 2017.
2. Wannacry virus spreads to Asia, fear of new wave looms, Times of India 16May 2017.
3. Indian origin techie links cyber-attack to North Korea, Times of India dated 17May 2017
4. Notes on Diplomatic practice by Odeen Ishmael
5. The new public diplomacy: Soft power in International Relations editor Jan Mellisen, palgrave, Macmillan.
6. Cyber-diplomacy: Managing foreign policy in the 21st century by Evan H Potter(ed)
7. Cyber-diplomacy by Lindelwa Makhanya
8. Cyber-diplomacy: A new strategy of influence, Halifax Nova Scotia,May30,2003
9. Can cyber-diplomacy replace traditional diplomats and help us get a handle on world most complicated problems? by Narain D Batra. Times of India dated 27th August 2016
10. The Straits Times,Singapore,24th October 2016
11. The United states-Australia cyber dialogue: fighting cybercrime in Asia-Pacific, November 4th 2016 by Liam Nevill and Zoe Hawkins (In technology policy blog from CSIS)
12. Trump breaking protocol with cellphone diplomacy by Chidanand Rajghatta, Times of India dated jine1st, 2017.
13. Fighting ISIS in cyber age by OZ Sultan, March 17, 2017
14. The Diplomat, How China became a world class cyber power by Greg Austin dated 30th April 2015.
15. Cyber-diplomacy is the answer, Wikimedia by Oon Yeoh in Malaysia Today on September 4th 2008.

16. Cyber-diplomacy versus digital diplomacy and Terminological distinction by ShaunRlordon May 12th 2016.
17. The coming age of cyber-terrorism by Scott Stewart, VP of tactical analysis, Stratfor.
18. Is cyber terrorism the new normal? By Dan Holden, ASERT.