International Journal of Social Science and Education Research

ISSN Print: 2664-9845
ISSN Online: 2664-9853
Impact Factor: RJIF 8.00
IJSSER 2023; 5(2): 115-117
www.socialsciencejournals.net
Received: 02-07-2023
Accepted: 27-07-2023

Sandeep Kumar Singh
Asst. Professor (Political Science), DDU PG College, Saidabad, Prayagraj, Uttar Pradesh, India

Corresponding Author:
Sandeep Kumar Singh
Asst. Professor (Political Science), DDU PG College, Saidabad, Prayagraj, Uttar Pradesh, India

Cyber security in the era of information age

Sandeep Kumar Singh

DOI: https://doi.org/10.33545/26649845.2023.v5.i2b.167

Abstract
Cyber security has emerged as the foremost concern for the developed world's national security in this information age. Due to the interdependence of national economies and integration of financial markets and their dependence on the digital platform that they use, they have become increasingly vulnerable to the cyber threats. As there is a lack of consensus regarding Universal Cyber Convention among major actors of the world, the threat of cyber terrorism has grown exponentially. This paper examines the different aspects of cyber threats to the national security debate of India and the world in large, and has reviewed India's efforts to address these challenges.

Keywords: Critical infrastructure, cyber warfare, cyber security, cyber governance

Introduction
In the post-Cold War era, India has emerged as the most powerful country in the South Asian region both militarily and economically. Toda Indian economy ranks fourth in the world in PPP terms and has millions of mobiles and laptops with the fast broadband connectivity and 5G technologies. With the demise of communism and command economy and the advent of globalization, India has emerged as a rising power in Asia and the Third World.
However, new types of security challenges have also emerged in the shape of terrorism and irregular warfare after the end of Cold War (Baylis *et al*., 2010) [2]. As we are now living in an "Information Age" the most dangerous threat to our national security is the new phenomena of cyber terrorism. In today's world we could not imagine living without Internet connectivity and other tools of information technology like smart phones, laptops, tablets, broadband etc. The whole world economy is using the platform of information technology and other tools of the cyberspace like artificial intelligence, machine learning, block chain and cloud space.

Cyber Terrorism and the Flat World
This revolution in information technology has made our world flat by eroding geographical boundaries and making the nations of the world more interconnected an interdependent. Friedman observes that globalization has helped in making level playing field for all the consumers with the dissemination of information technology through Internet (Friedman, 2006) [4]. If Internet is being used by national governments in various sectors of critical infrastructure like banking, stock and financial markets, military servers including nuclear sites, power grids, national health infrastructure, it is also being targeted by the cyber terrorists and hackers of other states as well as non-state actors. Cyber-attacks are those covet actions of individual hackers or a rival state that targets the cyberspace or computer networks by various methods like malware software, phishing and hacking in order to breach the information system of any organization for various purposes. According to CE RT-In (Indian Computer Emergency Response Team) India has witnessed about 4 lakh and 11 lakh cyber security incidents during 2019 and 2020 respectively (Menon, 2021) [7].
In the post Galvan era, India has encountered many more cyber hacking incidents from the Chinese hacker groups on our critical infrastructure. Mumbai power outage on 12 October 2020 was case in point amid the Indian China crisis on Ladakh border (Chaudhary, 2021) [3]. New York Times has reported that a group called "Red Echo" supported by PLA was behind the attack. These cyber-attacks are not strategic but in fact they are more of a psychological in nature.

Often power grids are targeted by these hackers as they make news more viral and gain instant publicity.

There are many reasons behind the surge in cyber-attacks in the industrial developed world United States is facing this menace from Russia and China since the last decade. There are several reports that U S general elections of 2016 was interfered by Russian cyber agents (Ohlin, 2017) [8]. Russia also conducted cyber-attacks on Ukrainian power grids and other Baltic states. Iranian nuclear facilities were hacked possibly by Israeli cyber agents in 2010 "Wanna Cry" malware targeted capital and stock markets of more than 150 nations of the world in 2017.

US have often demonstrated revolution in military affairs (RMA) after the end of Cold War particularly in the Gulf War in 1991. However it is a very costly affair. We are now in the midst of information age where battles are also fought in space and cyberspace. Many nations prefer cyber warfare because they're cheap and low cost and it does not involve casualties of soldiers. Another reason for its preference is its non-attributive character which means that the country on which cyber-attack has been conducted cannot give conclusive proof about the perpetrator of cyber-crimes as Cyber weapons gives plausible deniability. There are no borders in this cyberspace and therefore it is very hard to pinpoint the origin of the attack. In modern warfare, the whole world is your battlefield and cyber warriors can cause more harm to the nation's economy than the missiles and bombs of the rival nation (Allison, 2017) [1]. US and Russia met in Geneva in June 2021 and have agreed for the creation of working groups for cyber security management between themselves.

Who Controls the Internet!

Often international cooperation in cyber warfare does not give fruitful results because of many complex issues involving cyberspace. First of all, many developed nations of the western world have different conceptions of Internet. There are different definitions of the world cyber in different part of the world. There is no agreement on the definition of cyber incident among different nations. This difference among countries about whether there should be a universal convention on cyberspace is a tricky issue. There is a lack of cyber regime in the industrial World due to the domination of private sector in the cyber world. Major World Powers like US, Russia, China, Israel and Japan accuse each other for cyber-attacks.

International law does not entail cyberspace and therefore it is very tough to govern cyberspace. The major issue of cyber security today is about the lack of cyber governance and international norms and law regarding cyber threat. The crux of the problem is the question" Who controls the Internet"? All the major servers of the Internet are located in the United States and the western world which poses the security threat to the non-western developing powers like Russia, China and India. West wants Internet open and accessible to all without any hindrances to access it whereas India and China and other developing nations want control over the data of their people which are stored in the servers of private companies of US like Meta, Google and Apple (Gupta, 2018) [5]. Cyber security challenges have increased with the rise of social media like Face book, Instagram and Whatsapp as customers share sensitive documents like videos, photos and other things that are all stored in foreign servers which can be stolen and shared illegally in the "dark web". Indian government has raised its concern about the nature of ownership of Internet and has preferred a multi stakeholder model like public private partnership (PPP) model where national governments should supervise the flow of data in the interest of their national security as well as the right to privacy of their people in general.

In today's information age, data is the new oil of the world economy. According to Harari, an Israeli historian, whoever owns the data, owns the world. The Big Tech companies of US like Google, Meta, Apple and Microsoft has acquired much power in world politics due to their control over data and expertise in handling various formats of data in their servers due to their use of modern technology of artificial intelligence (AI) and machine learning. This big data companies poses serious threat to the democratic nature of our society as new technologies like artificial intelligence and machine learning makes it easier to process big amounts of data information at one place. It can help in making digital dictatorship in the 21st century where all people of the nations are supervised by the data algorithms used by the governments like the Chinese communist government. Thus, according to Harari,"politics in the 21st century will be a struggle to control the flow of data." (Harari, 2018)

Indian Stand on Cyber Security

What does India stand on the matter of cyber security? In this information age cyber security is the bedrock of national security as Indian economy has grown multi fold in the era of liberalization and globalization. The cheap broadband or Jio Effect has added millions of customers in the cyberspace who have their own biometric identity in the form of Aadhaar. After demonetization and COVID-19 pandemic, the usage of UPI money transfer has made our economy more digital and vibrant. In India there is a lack of proper cyber governance and institutions which is a basic prerequisite for cyber security. Although India has enacted Information Technology Act in 2000 which was amended in 2008 and was further curtailed by the Supreme Court judgment regarding right to privacy in 2017, India lacks cyber hygiene (Gupta, 2018) [5].

What ails Indian cyber security is the absence of proper coordination among various ministries responsible for cyber issues. Indian cyber security industry requires massive investments for ensuring security in the critical information sectors by formulating public private partnership (PPP) in cyberspace as Indian cyber industry is heavily dependent on imported cyber appliances from the Western countries. India has to build its capabilities by investing in R&D in cyber techniques like big data analytic techniques and machine learning. Data protection is an important issue for our national security and there should be a firm stand on the issue of localization of data servers in our country (Parida, 2017) [9]. The western MNC's of US like Google, Meta, Apple and IBM should comply with Indian cyber laws and be held responsible for the manipulation of data servers located in their country. The Supreme Court judgment of 2017 which recognized the Right to Privacy under Article 21 (Right to Life) has in one way hastened the governments thinking on the development of data protection law in India. It remains to be seen how government's new proposed bill would be enforced and implemented by our government for the benefit of its citizens as data is the new currency of the digital age.

References

1. Allison G. *Destined For War.* Scribe Publications; c2017. p. 183.
2. Baylis J, Wirtz J, Gray C. *Strategy in the Contemporary World.* Oxford University Press; c2010. p. 87.
3. Chaudhary A. India plans new cyber security strategy after 'Chinese intrusions' [Internet]. The Print; c2021. Available from: https://theprint.in/tech/618062
4. Friedman T. *The World is Flat.* Penguin Books; c2006. p. 55.
5. Gupta A. *How India Manages its National Security.* Penguin Random House India; c2018. p. 311, 317.
6. Harari YN. *21 Lessons for the 21st Century.* Penguin Random House UK; c2018. p. 77.
7. Menon P. Cyber threats now sit alongside nuclear ones [Internet]. The Print; 2021. Available from: https://theprint.in/opinion/681866/ [Accessed 2022 Nov 3].
8. Ohlin JD. Did Russian cyber interference in the 2016 election violate international law? *Texas Law Review.* 2017;95:1579–2017.
9. Parida J. A stronger data protection regime for a better digital India. *Liberal Studies.* 2017;2(1).