International Journal of Multidisciplinary Trends

**E-ISSN:** 2709-9369
**P-ISSN:** 2709-9350
www.multisubjectjournal.com
IJMT 2021; 3(2): 314-321
Received: 12-06-2021
Accepted: 21-07-2021

**Dr. Sanjeev Kumar**
Assistant Professor,
Chanakya Law College,
Rampur Maniharan,
Saharanpur, CCS University,
Meerut, Uttar Pradesh, India

**Corresponding Author:**
**Dr. Sanjeev Kumar**
Assistant Professor,
Chanakya Law College,
Rampur Maniharan,
Saharanpur, CCS University,
Meerut, Uttar Pradesh, India

# Cyber geopolitics and COVID-19 impact on international security

## Dr. Sanjeev Kumar

**Abstract**
Geopolitical tensions are increasingly playing out in the technology and digital space, with impacts felt across geographies and sectors. At the same time, the rapid increase in connectivity triggered by COVID-19 has added future urgency to debates regarding reliance on foreign technology and its impact on national and International security. in this environment, organizations will have maintain an understanding of the increasingly complex regulatory and Cyber threat environments in which they operate. Some observers argue the COVID-19 pandemic could be a world changing event with potentially profound and long-lasting implications for the International security environment. The long and short term view has always been a requirement for those working in cyber security. Right now, the short term involves securing remote working infrastructure, while also responding to skyrocketing COVID-19 phishing lures. The COVID-19 is a major global event that could in time sit alongside the likes of the global financial crises, 9/11 and even the breakup of the Soviet Union in shaping the Geopolitical landscape. This article explores cyber geopolitics and COVID-19 crises major challenges international and National security.

**Objectives of the Study**
**The objectives of the study are some following:**
1. To analyse the cyber geopolitics and COVID-19 crises in global pandemic.
2. To examine the COVID-19 impact on international security dimension in various countries.
3. To discuss the COVID-19 security challenges in digital world and India.
4. To understand the cyber geopolitics and COVID-19 impact on national security perspective.

**Research Methodology:** The research article is following the current trend of COVID-19 cases and the analysis which can help to development future trends. So that proper monetization and effective control measures can be implemented by the administration. This study is based on primary and secondary sources of information. Primary sources from interview in electronic mode like phone, YouTube records. The secondary sources of data collected from books, articles, magazines, would be our main resources. The methods applied in this study are current global order and national security theories, historical, descriptive, comparative & analytical.

**Keywords:** COVID-19, cyber security, global financial crises, health security, international security, technology, space war, internet trade, nation state, national security etc.

## Introduction
The novel corona virus (COVID-19) global pandemic posed new strategic challenges within the political, military, economic, social, infrastructure, information (PMESII), and intelligence domains of nation-states. The COVID-19 crises will deal a heavy blow to the global economy, but particularly to those that have heavy economic growth requirements, lie China. There are many countries who fit this category, who may be accelerating Internet Protocol (IP) theft programs in order to boost the expected state output. The cyber theft of IP has historically been aimed at acquiring next generation technologies or to leverage efficiencies in existing production techniques. The countries exiting COVID-19 crises first will be at an obvious economic advantage, and will have more capacity to implement new IP into their economies. It is worth tracking those countries from a threat perspective as they emerge the crises particularly where state ownership is prevalent. The COVID-19 pandemic has shutdown normal activity around the world since mid March 2020. Even if International relations had been in a period of relative stability before the onset of the pandemic, the consequences of the pandemic would be complex and far-reaching. Just as China was constructing as aggressive and complex plan for achieving a position of geopolitical dominance, the United States was belligerently withdrawing from its former global leadership role. There will be many geopolitical impacts of the prolonged pandemic crises.
Geopolitical tensions are increasingly playing out in the technology and digital space, with impacts felt across geographies and sectors.

At the same time, the rapid increase in connectivity triggered by COVID-19 has added further urgency to debates regarding reliance on foreign technology and its impact on national security. In this environment, organisations will have to maintain an understanding of the increasingly complex regulatory and cyber threat environments in which they operate. This paper intends to investigate and analyse the impacts of the covid-19 pandemic on Human Security, defined as an approach to national and international security that "gives primacy to human beings and their complex social and economic interactions".

**Significance of the study**

Cyber operations are significant both as a method and force multiplier to intimidate or influence the targeted state into acquiescence. These operations comprise cyber attacks that hack the digital infrastructure and networks and cognitive attacks that weaponize information to hack the hearts and minds of people in the targeted state. Recent incidents show that cyber operations could supplement broader campaigns to impose indirect pressure on government leaders and agencies of the targeted state. Wide-ranging social distancing measures are now in place around the world. This has led to a significant increase in the use of online communication by public authorities, businesses and individuals alike. Many are unknown with the use of online technology at this scale. This has presented a large, attractive and vulnerable target-set for cybercriminals to exploit.

**Cyber Geopolitics**

The long and short term view has always been a requirement for those working in cyber security. Right now, the short term involves securing remote working infrastructures, while also responding to skyrocketing COVID-19 phishing lures. Basically, it is fighting fires just to keep the organization going, while staying safe and healthy. However, we cannot forget the long term. COVID-19 is a major global event that could in time sit alongside the likes of the global financial crisis, 9/11 and even the breakup of the Soviet Union in shaping the geopolitical landscape (Terranova, 2020). Geopolitical change is a primary driver for nation-state and criminal cyber programs. From IP theft through to Information Warfare, it's worth understanding how these potential implications may unfold, some of which are addressed here.

**Cyber-Geo Matrix**

**Map 1:** World Wide Internet Connections

**Changing Balances of Power**

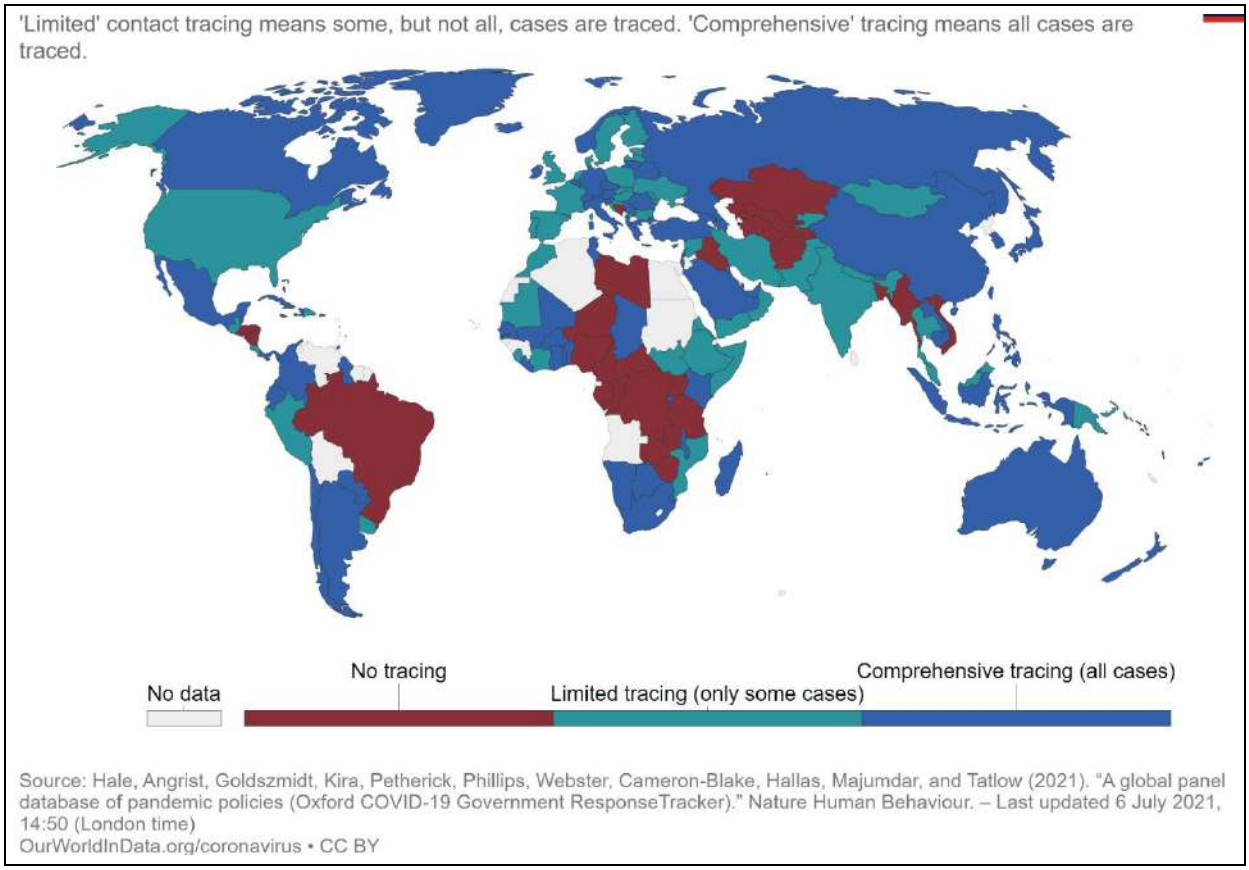
There is already a trade war between the U.S. and China, with those in Beijing seeing the U.S. attempting to derail Chinese growth, and Washington accusing China of unfair trading practices such as state subsidies. The country that can accelerate out of COVID-19 fastest will be at an advantage in this continued conflict, potentially shifting the global power nucleus. We can add to this the speculation that Russia and China may renege on import agreements in order to hit the U.S. economy while it is down, while elsewhere we have already seen in OPEC, which only adds to the uncertainty by increasing oil supply when demand is at its lowest, causing a mass sell-off of global stock (Zumbrun, 2021) [14]. China and Russia have also dispatched healthcare resources to the worst hit parts of the EU a humanitarian gesture that is admirable, which leads to consolidating influence and goodwill.

All of this together could have a substantial effect across the world, as countries scramble to the shifting landscape to secure supply chains, trading partners, and their own regional influence and security. This kind of global positioning has long been accompanied by cyber espionage (intelligence gathering), as well as the gaining of offensive cyber-footholds in critical infrastructure. This intelligence can lead to a large advantage in deploying a destructive attack in the event of conflict.

**Geopolitics of COVID-19**

Many states, as we have seen, have tried to assign physical, ethnic and racial specificities to an invisible enemy that instead in its action of contagion acts democratically without distinction of class, age, gender, nationality or religion. This is a typical phenomenon in the history of geopolitics of international health emergencies. New

diseases, as the historian William Eamon claims, bring out the deepest phobias in a culture (Eamon, 2010) [4]. In these periods people ask for reassurances, politics finds them in unfounded accusations against foreigners. The confirmation of this theory comes from the review, although not exhaustive, of the labels attributed to the pandemics that over the centuries have hit our planet. The bubonic plague, also known as the Jewish plague, broke out in Europe several times. In the mid-14th century (Eamon, 2010) [4], it caused the deaths of millions of people.




**Map 2:** Geopolitics of COVID-19 Contract Tracing Countries in July 2021

The English case is, however, an exception in the geopolitics of pandemics, which have always caused an increase in levels of discrimination and suspicion towards foreigners. In fact, the flu plague of 1918–1920 went down in history as the Spanish plague. For the simple reason that in Spain, neutral during the First World War, the press gave news of the pandemic those other European countries preferred to hide in order to appear less weak in the eyes of their opponents. The 1957–1958 flu epidemic is known as Asian because it spread mainly in Asia (Eamon, 2010) [4]. Today's pandemic will probably go down in history as the Chinese virus.

In short, while Covid-19 reaps the benefits of globalization, the governments called upon to combat it adopting national weapons, instruments and categories. In other words, governments use an anachronistic and counterproductive arsenal which, in an era in which space and time are zeroed out in favour of a high mobility, seems to be a thing of the past (Harari, 2020) [2]. It may be for these reasons that in this unprecedented and unpredictable war even the most experienced and refined political leaders have become confused between statements and denials.

A report last year from Oxford University revealed that at least 70 countries are currently using computational propaganda to manipulate public opinion on social media. Furthermore, foreign influence operations, primarily over Facebook and Twitter, have been attributed to offensive cyber capabilities from seven countries: China, India, Iran, Pakistan, Russia, Saudi Arabia and Venezuela. With elections looming worldwide, we can expect the continued manipulation of online public opinion in attempts to divide and weaken the health and economic response to the COVID-19 crisis (Alam *et al*, 2021) **[21]**. While there is little that organizations can do here (other than social media owners), the onus here falls onto individuals to think critically, avoid fake news, and understand that much of the consensus seen online is manufactured by foreign bodies with their own agenda.

**COVID-19 and Cyber Security**

At first glance, the COVID-19 pandemic and cyber security might seem like totally diverse, unrelated areas. However, the overall effects caused by either a pandemic or a cyber attack overlap in the way they affect people, including the feeling of fear and the need to protect oneself and others, as well as loss of health, wealth and privacy (Harari, 2020) [2]. The EU-funded SPARTA project recently launched a special three part podcast series that explores how COVID-19 and cyber security influence one another and the challenges involved in ensuring the safety and security of all concerned.

**Types of Cyber-Attacks**

To guide our analysis and the creation of a timeline of

COVID-19-related cyberattacks, we decided to define attacks based on their types. This definition includes cyber security by default and has inspired many international definitions of cyber-crime. The CPS guidelines categorise cyber-crime into two broad categories: cyber-dependent and cyber-enabled crimes (CPS, 2019) [10]. A cyber-dependent crime is an offence, "that can only be committed using a computer, computer networks or other form of information communications technology (ICT)" (McGuire and Dowling, 2013) [11, 12]. Cyber-enabled crimes are, "traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT)" (McGuire and Dowling, 2013) [11, 12].

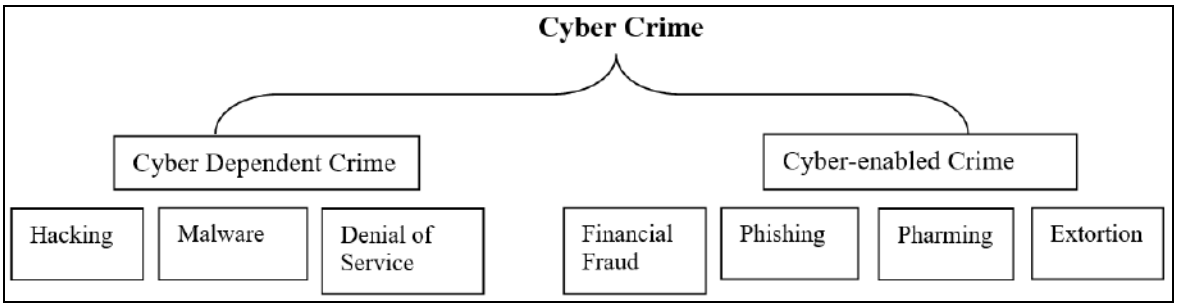



**Fig 1:** Cyber Dependent and Cyber enabled Crime

**Cyber Operations in the Grey Zone**

When Australia announced that it was facing a cyber attack campaign, it also unveiled that the attacks occurred over several months and are increasing. Cyber security experts believe that China is responsible for the attacks. Tensions between the two states rose after Australia echoed the U.S. call for an investigation into the origins of COVID-19. At the strategic level, cyber attacks multiply the pressures that China has imposed on Australia through tariffs and travel advisories claiming Asians face racial discrimination in Australia.

At the disputed Himalayan border, fighting between Chinese and Indian soldiers broke out after China increased its military presence in the area. China was reacting to India's building of more infrastructures in the disputed region. China's military escalation happened as India was struggling with its worsening COVID-19 situation. Following the incident, Chinese online media, such as the Global Times, portrayed India as the hostile actor such an effort can be viewed as an attempt to erode Indian morale. Chinese hackers have also reportedly increased cyber attacks against Indian government agencies and businesses to extract sensitive information.

In Iran, several unexplained explosions took place at sensitive locations, including the Natanz nuclear facility. In 2010, this facility sustained severe damage after Stuxnet attacked its industrial control systems. The computer worm is believed to be the creation of Israeli and the U.S. intelligence agencies. It therefore would be unsurprising if another cyberattack (a Stuxnet 2) caused the recent explosions (Harari, 2020) [2]. Undoubtedly, these explosions could add to the anxieties in Iran arising from U.S. sanctions and the worsening COVID-19 situation.

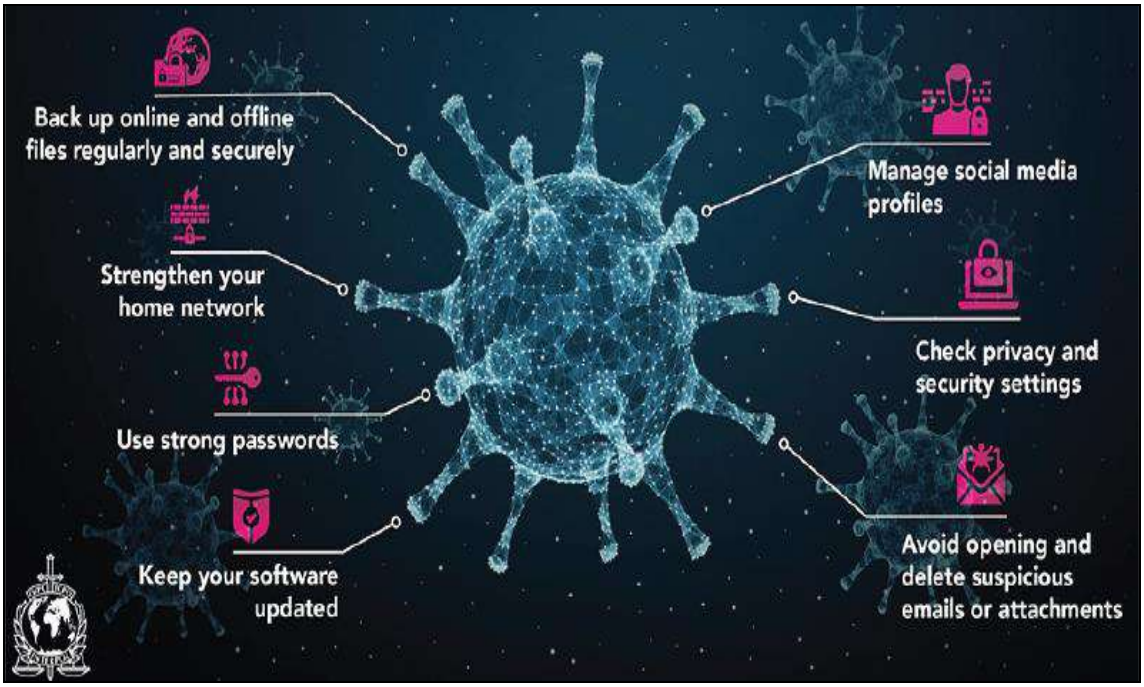
**COVID-19: The Need for New Thinking on Security**

Geopolitical tensions are increasingly playing out in the technology and digital space, with impacts felt across geographic and sectors. At the same time, the rapid increase in connectivity triggered by CPVID-19 has added further urgency to debates regarding reliance on foreign technology and its impact on national security (Terranova, 2020). In this environment, organizations will have to maintain an understanding of the increasingly complex regulatory and cyber threat environments in which they operate.

Canada is only one of the many countries that has seen China attempt to influence domestics politics, pursue aggressive cyber attacks and mount other espionage activities, all occurring before the mutual alienation worsened with the detention of Meng Wanzhou, chief financial officer of Huawei and the corresponding arrest of two Canadians as de facto hostages. China's aggressive tactics have alienated many western countries that want to see a strong counterbalance to the BRI and the so-far successful campaign to win more influence at the United Nations. Russia has become more firmly aligned with China, which could lead to close cyber cooperation between two powers with very strong but different, cyber capabilities and a strong opposition to Western alliances and norms in international relations (Alam *et al*, 2021) [21]. This competitive dynamic will not changes in the short term, but there is some hope it might in the longer term. China does not need to be a bully to be a global power and its current stance is alienating its most prosperous trading partners.

**Cyber Security Threats**

Cybercriminals are attacking the computer networks and systems of individuals, businesses and even global organizations at a time when cyber defenses might be lowered due to the shift of focus to the health crisis. The Cyber security threats also refer to the possibility of a successful cyber attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.




**Source:** Data Provide by Interpol

**Fig 2:** Cyber Security Checklist

There are a considerable number of registered domains on the Internet that contain the terms: "Corona Virus", "Corona-Virus", "COVID19" and "COVID-19". While some are legitimate websites, cybercriminals are creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware (Alam *et al*, 2021) [21].

**Types of Cyber Security Threats**

While the types of cyber threats continue to grow, there are some of the most common and prevalent cyber threats that present-day organizations need to know. They are as follows:

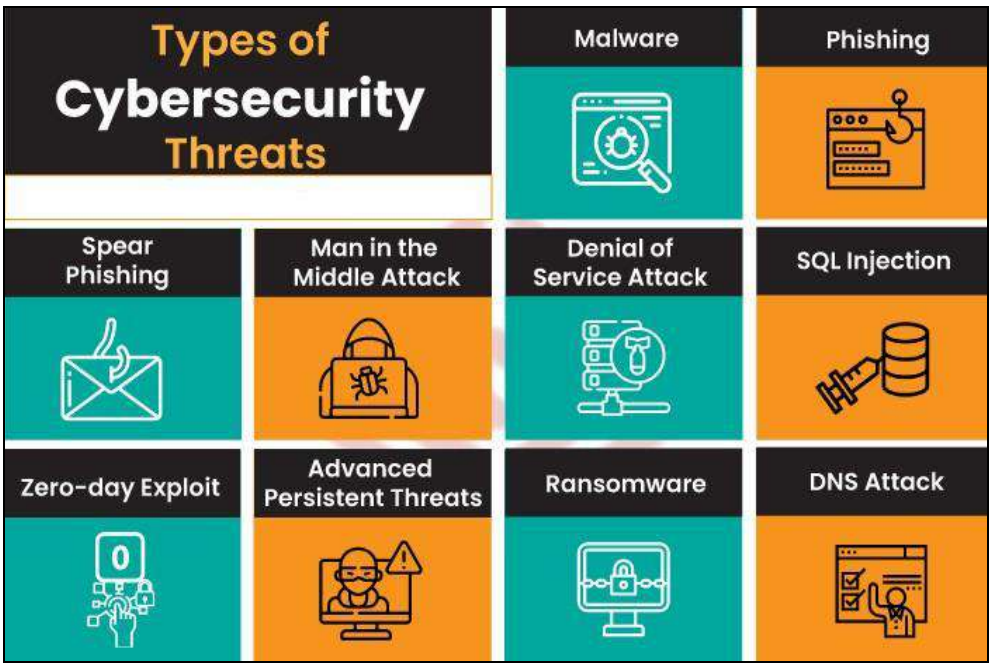



**Fig 3:** Types of cyber security threats

**COVID-19 Challenges International and National security**

The 9/11 attacks redefined the global security context on terrorism and targeted violence. Similarly, COVID-19 causes us to reconsider what composes a security threat. In the evolving security environment, it is essential to look beyond current realities and timely evaluate strategic implications and effects on individuals, states and the international system regarding pandemics. COVID-19 tests our system we live in and is a transformative reflection point that guides us through what we had as a normal before and what will be a 'new normal' after. Given its broad-reaching and global effects, COVID-19 is a game-changer that has impacted our ways of living (Alam *et al*, 2021)

[21]. This pandemic is forcing us to adapt rapidly and to explore different strategies and realities.

These are reflecting upon the strategic implications and critical effects of COVID-19 on *individuals* and *societies*, the pandemic forces us to reevaluate patterns of life. Individuals and societies around the world have been exposed to this new unknown and invisible threat that has put into lockdown millions of people and caused over a hundred thousand deaths. Global norms will be fundamentally changed, a process we are already witnessing and that places more demands on state governments (Ratsiborynska, 2020) [15]. At the same time, our way of life having been transformed by social distancing will shift people's private and professional focus to the modern opportunities offered by our high technology world. Individualism and virtual connectivity coupled with e-responsibility and data protection will mostly take hold and shape the social and cultural paradigms of our societies as a shifting power towards technological acceleration. Socially flattened and intelligent livelihood, enabled by emerging technologies, offers flexibility, connectivity and economic transformation that challenge our traditional mindset and working practices. Benefits of digital adaptation and societal inclusiveness through technological tools will lead to a forward-looking future of e-health, e-governance and e-education (Ratsiborynska, 2020) [15]. Technological opportunities and digital transformation will provide a platform for social inclusiveness, creativity and innovation that can make societies function more smoothly in times of social tensions. However, such an individual and societal interconnectivity will require a traceable measurement of risks and vulnerabilities in the digital and technological domains, complemented by a new societal culture of information literacy and digital learning.

Early warning was vital to meet an unprecedented global pandemic as COVID-19 emerged in China and began its lethal spread. With COVID-19, we have seen cyber-attacks and disinformation campaigns launched by adversarial state actors; the domestic deployment of the Canadian and Australian militaries, among other national forces, to protect vulnerable populations; the disruption and vulnerability of just-in-time global supply chains; worrying domestic political tensions and fractures in many states; and an erosion of international cooperation (Shull and Wark, 2020) [16]. All of this is taking place amid ongoing tectonic geopolitical shifts, bookended by climate change and an overdue discussion about data, tracking, commercial surveillance and the attention economy. As Patrick Walsh argues, "a first point for a post-COVID-19 policy framework is for the government and national security intelligence enterprise to move beyond the rhetoric of pandemics being a 'national security issue' to operationalizing these words in a political and bureaucratic sense" (Walsh, 2020). The UK Biological Security Strategy extolled the capabilities and systems available within the United Kingdom while calling for greater integration of effort, sustained attention to the threat and support for developing countries to help improve their capabilities (WHO, (2020). Disease outbreaks were identified as a major globalized threat to society while accidental release of a virus or deliberate biological attacks were seen as less likely. The creation of a new Joint Bio-security Centre in May 2020 [19] to act as an intelligence fusion and response mechanism is one early indicator of new thinking (www.gov.uk).

**Cyber threat on National Security during COVID-19**

Sovereign nations are equipped with wide powers to deal with what they themselves define as challenges to their national security. A strategy aimed at addressing these concerns must be underpinned by a concrete understanding of what comprises "national security", to begin with. Security risks can be categorised into two broad classes: internal (homeland) security, and external security (Alam *et al*, 2021) [21]. These threats are further classified as externally-aided internal and internally-aided external risks. Internal homeland security deals with issues related to public order within the country. In India, the Ministry of Home Affairs lists the following key issues in the country's internal security: a) terrorism in the hinterlands; b) Left Wing Extremism in specific areas; c) the security situation in Jammu and Kashmir; and c) insurgency in the northeastern states. External security, as the name suggests, is concerned about the security risks emanating from outside India's borders. In an increasingly globalised and connected world, the line between internal and external threats can get increasingly blurred.

Cyber security finds its roots in traditional military principles: many of its basic covenants have been adopted from traditional military security principles such as "need-to a know" and "least-privilege". In India, this has three interrelated elements: the unprecedented adoption of smart phone use in the country; the presence of a young and technology-savvy population, and affordable access to internet services and devices. Furthermore, the push for digitalization by the government, through flagship initiatives under the overarching 'Digital India' banner, is also a key driver of the ongoing digital transformations (www.digitalindia.gov.in). Indeed, the government's digitalization efforts have been buoyed by the restrictions on movement that were put in place to respond to the COVID-19 pandemic. Consumers are using digital applications to buy consumer durables and necessities, for telemedicine, and for connecting with their friends and family. According to the Reserve Bank of India (RBI), India is recording around 100 million digital transactions every day, with a volume of INR 5 trillion ($67 billion) (Roy, 2020). This represents approximately a five-fold increase from the 2016 levels. The RBI expects digital transactions to continue on a growth trajectory; estimates suggest an increase to 1.5 billion transactions a day worth INR 1.5 trillion by 2025 (Roy, 2020). These figures show that even as the Indian economy has suffered a slowdown because of the pandemic, the country's digital retail market has earned.

**Emerging Cyber Threats in 2021 and Beyond**

The corona virus pandemic emerged as the biggest challenge for national security, businesses and IT organizations in 2020. Amid the pandemic, the cyber threats and data breaches have grown in sophistication and volume, with the number of breaches increasing 273% in the first quarter, compared to 2019. According to Microsoft, the pandemic-related phishing and social engineering attacks have skyrocketed to 30,000 per day in the US and 35,000 per day in India alone (Admin, 2021) [20].

**Cyber Security Best Practices**

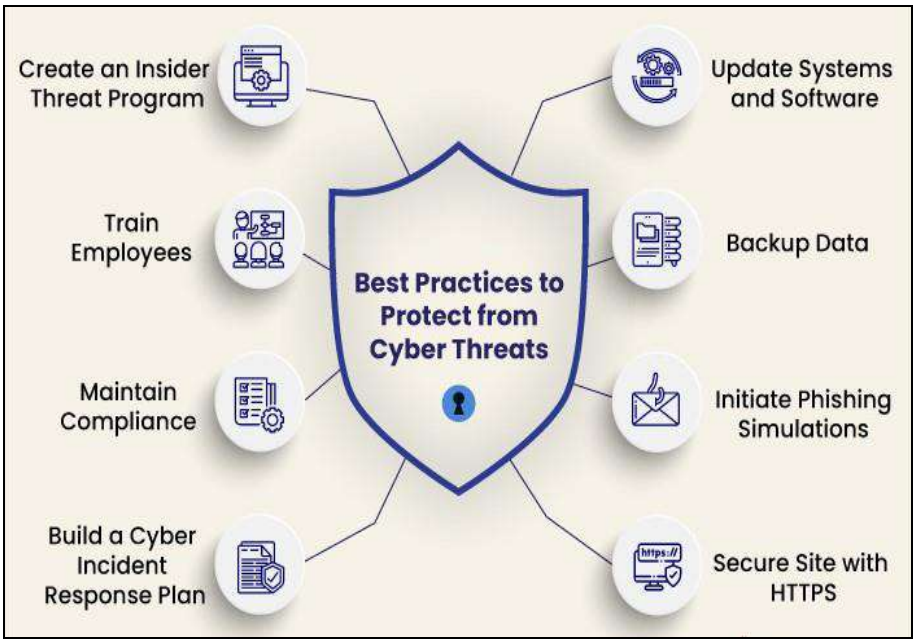



**Fig 4:** National Security protect from Cyber threats

The pandemic has ushered in a new era of cyber security. IT security professionals who raise their game and protect their companies' people, technology and data from new or heightened risks of more sophisticated cybercriminals will be crucial players in the economic turnaround.

**Concluding Remarks**

In conclusion, cyber operations could be on the rise in the post-COVID-19 reality. In regions such as Europe and parts of Asia, governments are increasingly looking to align with like-minded states to retain a global voice on technology and digital regulation, while taking more forceful steps to protect critical technology assets and infrastructure. Elsewhere, such as in Latin America and Africa, states are taking a more pragmatic view, seeking to balance competing interests. Lower-capability cyber powers such as India, Vietnam, Turkey and others will likely focus on enhancing their defensive and offensive cyber capabilities. A new national security strategy will have to address a complex threat environment and will have to shake itself loose from an overweening attention to terrorism.

COVID-19 has issued in a new age of cyber awareness as companies now send their employees to work from home with limited security. Virtual private networks (VPNs) and servers will play a significant role in cyber security of the future. This pandemic has taught us that preparation is key to successfully limiting the risks related to cyber attacks. The ability to quickly react to unforeseen events helps reduce the impact of a cyber attack. Smaller states, in particular, must do more to defend themselves amid entrenched geopolitical tensions. To that end, non-kinetic grey zone methods should also be considered despite appearing antithetical to democratic ideals. Cyberspace by nature is anarchic and should be viewed through a realist lens. Defense against threats from cyberspace requires both multilateralism (diplomacy) and deterrence. It's clear that COVID-19, and the post-crisis world, may present opportunities for cyber exploitation at all levels: nation-state, organizational, and individual. For now, the message is stay safe, and stay afloat. But soon, we may be looking at cyber in a very different way.

**References**

1. Giuseppe Terranova. Geopolitics of COVID-19: global challenge at national borders AIMS Geosciences. 2020;6(4):515-524.
2. Harari YN. The world after coronavirus, 2020. Available from: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.
3. WHO. Updated WHO recommendations for international traffic in relation to COVID-19 outbreak, 2020. Available from: https://www.who.int/news-room/articles-detail/updated-whorecommendations-for-international-traffic-in-relation-to-COVID-19-outbreak.
4. Eamon W. The professor of secrets: mystery, medicine and alchemy in Renaissance in Italy. Washington: National Geographic Society, 2010.
5. GOI. Government of India, Digital India, 2021. https://www.digitalindia.gov.in/
6. Anup Roy. Digital transactions could reach Rs 15 trillion a day by 2025: RBI, Business Standard, 2020, 22. https://www.business-standard.com/article/finance/digital-transactions-, couldreach-rs-15-trillion-a-day-by-2025-rbi-120072201431_1.html
7. Anup Roy. Digital transactions could reach Rs 15 trillion a day by: RBI, 2025.
8. Milani CRS. COVID-19 between global human security and ramping authoritarian nationalism. Geopolitical. 2020;11:141-151.
9. Zizek S. Pandemic! COVID-19 shakes the world, Cambridge: Polity, 2020.
10. CPS. Cybercrime - prosecution guidance, The Crown Prosecution Service (CPS), Tech. Rep., 2019. https://www.cps.gov.uk/legal-guidance/cybercrimeprosecution-guidance (Accessed 17 June 2020).
11. McGuire M, Dowling S. Chapter 1: Cyberdependent

crimes," Home Office, Tech. Rep., 2013. https://assets.publishing.service.gov.uk/government /uploads/system/uploads/attachment data/ file/246751/horr75-chap1.pdf (Accessed 18 June 2020).
12. McGuire M, Dowling S. Chapter 2: Cyber-enabled crimes - fraud and theft, Tech. Rep., 2013. https://assets.publishing.service.gov.uk/government/uploads /system/uploads/attachment data/ (Accessed 18 June 2020).
13. Nurse JRC. Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit in The Oxford Handbook of Cyberpsychology. OUP, 2019.
14. Zumbrun Josh. Beijing Fell Short on Trade Deal Promises, Creating Dilemma for Biden, The Wall Street Journal, December, 2021, 31.
15. Ratsiborynska Vira. Strategic security Implications due to COVID-19 Pandemic, NATO, transatlantic approaches to security and global politics at the Vrije Universiteit Brussel (VUB), 2020.
16. Aaron Shull, Wesley Wark. Pandemics: The Need for New Thinking on Security, Centre for international Innovation Governance, (CIGI), Canada, 24.
17. Patrick Walsh F. Building a Better Pandemic and Health Security Intelligence Response in Australia, Centre for International Innovation Governance, (CIGI), Canada, 2020, 24.
18. WHO. WHO in emergencies, World Health Organization, 2020. https://www.who.int/emergencies/en/
19. Joint Biosecurity Centre, Gov.uk, May 2020. https://www.gov.uk/government/groups/joint-biosecurity-centre
20. Admin. Cyber Security Threats and Attacks: All You Need to Know, Stealth Lab, December 4, 2020.
21. Alam Md. Mahmudul, Agung Masyad Fawzi, Md. Monirul Islam, Jamaliah Said. Impacts of COVID-19 pandemic on national security issues: Indonesia as a case study, Security Journal, Springer, 2021.