Emerging Cyber Attack on India's Intellectual Property: A Threat to National Security

Ayasha Firoz

Aligarh Muslim University, Aligarh

In the 20th century, national security was mainly focused on military security, but over time it expanded as a concept which required more attention and training. In the wake of cyber warfare, cyber terrorism, chemical attack, bioweapon and at the dawn of the nuclear age, defining national security solely in terms of armies fighting a set piece of battle, is not enough—it needs to be viewed beyond the physical battlefield.

National security has come to mean different things to different people. Today, there are all kinds of 'national securities' — economic security, energy security, environmental security, and even health, women's, and food security.

India's national security is incomplete without discussing India's economic security as it provides the capital to procure resources that are needed to build a comprehensive strategy on national security. Economic security must aim to protect the drivers of economic growth and reduce vulnerabilities that threatens India's economic progress. India has emerged as the 'fastest growing' major economy and is the fourth largest economy in the world. India has a mixed economy. Half of India's workers rely on agriculture, the signature of a traditional economy; one-third of its workers are employed in the service industry, which contributes to two-thirds of India's output. The productivity of this segment is possible due to India's shift towards a market economy. New Industries based on innovative ideas are coming up which contributes to India's GDP and also provides employment to many.

Under the current government, initiatives like 'Make in India', 'Startup India' and '*Atmanirbhar Bharat*' have further bolstered India's growth. Therefore, it is important to enforce the Intellectual Property Rights (IPR) in India, in an efficient way. The potential of the IPR based industry needs to be exploited properly with an aim to generate economic profit. However, with technological development, the threat of cyber crime have also become evident. Cyber attack is a global

problem with the potential to harm private businesses, government infrastructures and conventional businesses. It is easier to attack a country's economy especially through a vast cyber network. To make things worse the ongoing Covid-19 Pandemic, have increased the risk of cyber attack for money and for stealing resources.

The basic module of operation followed after stealing intellectual property from any organisation, is replicating it and then releasing the 'replicated property' in the domestic market which in turn displaces the original organisation in the global market. Historically, the country of Yemen had a monopoly on coffee, forbidding the export of its plants and seeds—their intellectual property. However, in 1616, a Dutch merchant managed to smuggle out a few coffee plants from the city of Mocha in Yemen to Holland. Holland thereafter began its coffee empire in the Dutch colony of Java from where coffee spread around the world. As a result, Yemen lost its competitive advantage and is currently one of Arab world's poorest nations. In the present 'digital' world, valuable data are stored in computers, which exposes the data to threats like hacking, sharing trade secrets, file sharing, etc. Leaking valuable data not only hampers economic competitiveness of India but puts the the national security of India at risk.

Intellectual property

"Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce".

—World Intellectual Property Organisation (WIPO)

Intellectual property contributes enormously to both— the national and state economies of India. Dozens of industries across our country relies on enforcement of their patents, trademarks, and copyrights, while consumers use Intellectual Property regulations to ensure that they are purchasing safe and guaranteed products.

The economic motivation attached to intellectual goods is expected to stimulate innovation and contribute to the technological progress of the country, which also depends on the extent of protection granted to the innovators. Intellectual Property Rights (IPR) protect the innovator by means of patents, copyright and trademarks, which enables people to earn recognition or financially benefit from what they invent or create. By striking the right balance between the

interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

Intellectual Property and National Security Concern

Cyber Threat to Intellectual Property of Big Corporates

A combination of increased global competition, digitalisation of IP, and ubiquitous internet access, have made corporate trade secrets a lucrative target for cyber criminals. Several converging factors now dramatically challenges the traditional ways that organisations had so far adopted to protect their intellectual property. The digitalisation of huge amounts of valuable corporate information and increasing interconnectivity—both inside and outside "secure" corporate networks—through multiple devices, have made IP portable and accessible. This makes Intellectual Property increasingly vulnerable, and a very tempting target to attack.

"What I see as economic espionage, to a large extent, is kind of a death by a thousand cuts... and these are being perpetrated by different actors—sometimes foreign intelligence services, sometimes by corporations, sometimes by individuals."

—Robert "Bear" Bryant, National Counterintelligence Executive, Office of the Director of National Intelligence

The theft of corporate intellectual property (IP) has received a lot of recent media attention. Cyber security breaches are largely undetected, and the economic impact of stolen trade secrets, source code, drug & chemical formulas, and product designs has become increasingly serious.

Corporate economic espionage is not a new concept— what is new is the speed, scale, and ease (a simple download to a portable device) with which cyber Intellectual Property can be stolen. Consider the following examples:

During 2008 and 2009, proprietary information from Marathon Oil, ExxonMobil, and ConocoPhillips was available to computers overseas. The information comprised 'the crown jewels of the industry' —valuable 'big data' detailing the quantity, value, and location of oil discoveries worldwide." One US metallurgical company lost technology worth around $1 billion, and which required 20 years of development. This time the cyber crime originated from China.

In 2010, Chinese turbine manufacturer– Sinovel Wind Group Company, accounted for two-thirds of American Superconductor Corporation's (AMSC) $315 million annual revenue. But in March 2011, Sinovel inexplicably stopped purchasing AMSC control systems; AMSC stock dropped 40% in one day, and 83% over the next few months. Later, in June 2011, AMSC learned that Sinovel had acquired AMSC' turbine control system source code that was stolen from its servers in Austria.

In 2010, Google revealed that it was targeted by an advanced persistent threat (APT), named "Aurora", which succeeded in accessing the company's source code repositories. Although, only an estimated 34 companies were publicly identified as targets of the attack, Joel Brenner, former Counterintelligence Chief for the Office of the Director of National Intelligence, believes that, 'thousands'' of US companies were breached—a scale that Brenner noted as evidence of China's 'heavy-handed use of state espionage against economic targets', and an 'escalation of Chinese network operations against the US'.

In 2005, 18 Israeli executives were arrested for computer espionage incidents nicknamed 'The Trojan Affair'. They had targeted competitive information from companies as diverse as retailers and high-tech manufacturers, including the Israeli divisions of Ace Hardware and Hewlett Packard Enterprise. Out of fear of stockholder or market reaction, it is clear that many IP thefts goes unreported, or worse, goes undiscovered. Unlike credit card fraud or theft of personally identifiable information (PII), there is no easy way to track stolen IP or understand as to how it has been compromised.

"There are wide-ranging attacks against commercial organizations"…. It's incumbent on organizations—be they government's or commercial enterprises or academic institutions—to understand what their crown jewels are and make sure they are protected commensurate with their value".

—Chief Information Security Officer of Motorola

To help protect IP and avoid 'death by a thousand cuts', we need to be proactive in finding the right solution.

The Cyber Threat to Military Equipment

The Defence Research and Development Organisation (DRDO) is bestowed with the responsibility to carry out research and development (R&D) related to military equipment and technologies. DRDO was set up in 1958 and is considered to be the supreme body for researching, monitoring, regulating, and administering the India Defence Research and Development Program. It is working in various areas of military technology vis. aeronautics, armaments, combat vehicles, electronics, instrumentation engineering systems, missiles, materials, naval systems, advanced computing, simulation and life sciences.

These agencies conducts experiments that involves basic research, applied research, application of the result of research, development and transfer of technology. All the undertaken research and development projects are aimed at creating a new intellectual property or developing existing forms of the intellectual property. The patent documents consisting of researched materials help to save time, resources, and provide relevant information to the researcher, at the beginning of a new project. The results of research, so obtained, calls for identification of inventions that may need Intellectual Property protection, particularly through patents. These documents, inventions and equipments rely on many systems, each of which involves computers hence exposing sensitive data to the risk of cyber attack and intellectual property theft.

There are examples wherein hackers tried to steal the Government classified document , trade route blueprints and other forms of intellectual property. Chinese hackers have stolen information of the Patriot Missile System– the F-35 Joint Strike Fighter, and the US Navy's new Littoral Combat Ship. These blueprints of US weapon and control systems were stolen to advance the development of Chinese weaponry.

It is a well-known fact that China is engaged in cyber warfare. In 2007, computer security provider– McAfee alleged that China was actively involved in cyber warfare, accusing the country of cyber attacks in India, Germany and the United States; on many other occasions, from 2007-2019, Chinese hackers tried to break into many government agencies, organisation, academic institutions, industries, etc. but however, China denied the knowledge of such attacks. One should view cyber security through the ‘prism of risk’ rather than a ‘technical prism’. It threatens national security, combating of which will require formal structures, policies and an

explicit declaration of intent. In the light of recent events, due to India-China border clash Pavan Duggal, a Supreme Court advocate and cyber law expert remarked, "there will be increased state surveillance and monitoring. One can expect digital and cyber security breaches which typically happen after such incidents. One has to be prepared for huge breaches or cyber security threats on critical networks as well".

Science and Technology

The advancement of science and technology is vital in ensuring national security, as it provides implementable solutions to difficult problems that we face in day-to-day life or to problems that has the potential to restrict overall growth of the country. Under-development in few fields of scientific research and technology has a direct impact on the development of any country's economy, infrastructure and higher education. Few such fields are mentioned below:

- Development of Nuclear Technology.
- Defence Technology.
- Development of Satellites.
- Biotechnology.
- Meteorological Science.
- Space Technology.
- Nanotechnology.

Wireless Communication

All these technologies, in turn, provides favourable conditions for the country's growth strengthens the country's national security infrastructure. The government has also created an exclusive department emphasising the development of Science and Technology, for which a separate budget is also allocated. India is one of the most fascinating destinations for technological transactions in the world and is ranked among the top five.

At present, about 27 satellites (out of which 11 facilitates the communication network) are active and operational. Furthermore, India is ranked among the top ten nations in terms of the number of scientific publications.

The Indian Space Research Organisation (ISRO) has completed its mission of developing India's independent navigation system by launching the Indian Regional Navigation Satellite

System (IRNSS – 1G).IRNSS – 1G is the seventh navigation satellite that will reduce the India's dependency on the US Global Positioning System.

India recently has become an Associate Member State of the European Organization for Nuclear Research (CERN)— the motive is to increase collaboration between India and CERN's scientific & technological efforts and also promote participation of Indian physicists, software engineers, and electronics hardware in global experiments.

- **Cyber Threat to Nuclear Technology.** Use of computers, networks and digitally stored data has created new problems for nuclear secrecy and information security.These diversified the methods available for nuclear espionage. As PW Singer and Allan Friedman states, "while computer networks are allowing groups to work more efficiently and effectively than ever before, they are making it easier to steal secrets".

  In this cyber age, espionage is the biggest challenge and therefore there is a need to protect sensitive information, weapon design and operational procedures. A much smaller aspect of the challenge, but a far greater worry, is the possibility that hackers might easily compromise nuclear systems, preventing them from working as intended, or precipitating some sort of crisis, even a launch, either directly or possibly indirectly by interfering with the data on which such systems rely.

  While the possible sabotage of nuclear systems has always been a key challenge, the Farewell Dossier, Aurora Generator Test, Operation Orchard and, most recently, Stuxnet, all demonstrated the possibility of interfering with, or damaging, nuclear systems through cyber means. The possibility that an adversary might steal nuclear secrets – be the weapon designs and capabilities or operational plans and procedures – has always been a major challenge for nucleararmed states. Indeed, the importance of nuclear espionage can be traced as far as the early 1940s when Soviet spies sought (and acquired) information on the Manhattan Project and early US nuclear bomb designs.

  Likewise, these new 'economies of scale' also allows espionage attacks that attempts to steal as much information as possible about all types of things, as also targeted attacks on specific and specialised information. However, some hackings are done to simply prove that it can be done or just to monitor what a potential enemy is planning to do.

The volume and scope of cyber-nuclear espionage have expanded exponentially. In 1991, it was feared that a group of Dutch hackers, who broke into US military networks, were searching for nuclear secrets and missile data and was planning to sell the same to Iraqi leader Saddam Hussein before Operation Desert Storm. In 1998, the Cox Report revealed that China had stolen a considerable cache of highly sensitive secrets, over several years, from the US particularly those related to the W88 thermonuclear warhead design. These type of spying, hacking, leaking of information and stealing of intellectual property(weapon design, blueprints, etc) poses direct risk to India's national security.

- ***Cyber Threat to Biotechnology.*** The world is currently going through a crucial time as we are fighting an 'invisible enemy' — Covid-19. During the two year plus course of the Pandemic, we have seen a failure and helplessness of the healthcare system, management and even the governance of developed countries. This makes us think about as to where we are really standing when it comes to healthcare, saving jobs, and controlling migrant worker's migration.

  Almost all the countries are 'racing against time' to develop 100 percent effective vaccines including India. However, in such difficult times also cyber attacks, targeting vaccine makers and healthcare institutions in India, became prevalent, according to a report by CyberPeace Foundation (CPF). A viable vaccine is a valuable piece of intellectual property; beyond the pharmaceutical formula itself, the data on testing and drug trials can be valuable for an organisation working to develop its own drug. With some countries struggling to secure an effective vaccine, such data is a tempting target. As per research by CPF, over 7 million attacks have been recorded between 01 October and 25 November 2020 on the healthcare sector based Threat Intelligence Sensors network, specifically simulated in India.

  Overall, the Research Wing at CPF has noticed a spike in cyber attacks during the Covid-19 pandemic. In October 2020, a total of 54,34,825 attacks were recorded and in November 2020, 16,43,169 attacks, on its Threat Intelligence Sensors network.The goal of these attackers was unauthorised access to information, which can include data related to research proposals, drug development, manuscripts, virus testing, clinical trials, and drug manufacturing.

"Cyber attack attempts which includes brute force and masquerading spear phishing have been identified as state-backed Russian and North Korean hackers trying to steal valuable data from leading pharmaceutical companies and vaccine researchers" said CyberPeace Foundation.Most targeted countries includes Canada, France, India, South Korea and the United States. These countries were directly involved in vaccine R&D and treatments for Covid-19.

The data so stolen could be sold in black markets to competitors who might use this information and come up with own version of vaccine to be sold at a much cheaper price. Therefore, it poses a huge risk to any country's ecomic security.

Cyber Threat to Bio based Industries

All life sciences, whether public or private, are vulnerable to cyber attacks. Bio based industries which helps in producing chemicals and materials, have similar concerns of cyber security as the chemical industry has. Bio-production relies heavily on data, on intellectual property and research, all of which needs protection so that the firms can reap financial benefits of their investments.

The health and pharmaceutical sector of the life sciences also faces issues related to patent privacy. A recent survey indicated that companies are elevating cyber security to a strategic imperative. However, the pace of protection is slow as compared to their desire to adopt digital technologies to drive innovation. Many organisations are involved in bio-production security; they range from feedstock suppliers and customers to information technology (IT) professionals from law firms and IP offices.

Cyber Threat to the IP of Educational Institutions

Educational institutions like colleges, universities, etc. are vulnerable to cyber attack. Digital platforms are used by such institutions to connect students, teachers and management, which may compromise security. It is like an open invitation to hackers. There are various motives behind attacking renowned institutions, most important being financial gains, DDoS attack, Data theft and Espionage. Many government and military projects are made in association with universities and includes research work, project model, design, structure and other valuable Intelectual Property. Such data can easily be compromised if correct measures are not taken by the institutional body.

Cyber Threat to Private Defence Sector

To uplift the economy and to become a global power, India has to increase its export and decrease its import. To achieve this, the Government first opened the country's defence sector to 49% Foreign Direct Investment (FDI) in 2014 then increased it to 74% in 2020 and 100% under the approval route, which was seen as a big step towards privatisation of the sector. These steps are taken to expand the scope of India's indigenous arms industry and to build its reputation as a self-sufficient arms manufacturer. As we are moving ahead in time there is an increase in competition between countries to achieve the status of a global power or to sabotage their opponent. India has to come up with new ideas. Defence solutions should be innovative, cost-effective and multipurpose. Here new inventions, design, research and patents, that are created, can help in the growth of the economy.

However, despite the government's best efforts, India has made little progress when it comes to indigenous defence manufacturing. The Government is well aware of the private sector being a vibrant and dynamic force, and it seems to have concluded that its military skill will remain untapped if it continues to bank on the public sector alone. However, selling most of its stakes in defence manufacturing companies is not the way to go forward as there are lot of conflict between defence manufacturers and the political and military establishment.

Furthermore, problems have increased due to privatisation. hence, allowing the private sector to completely control the defence sector, may alter the political dynamics, lead to job loss and pose a threat to defence secrecy. As arms manufacturing is in the hands of the private companies, therefore the fear of cyber threat constantly lingers. Though private companies prioritises cyber security, still there is a possibility of Intellectual property theft, data leak and even shutting down of systems and networks. Such attack damages the organisation which not only causes economic loss but also causes a loss of trust of the foreign investors. There are key economic espionage cases that we should pay attention to and take lessons from them. Few of the instances are as mentioned below.

- Xiaodong Sheldon Meng tried to sell his defence contractor fighter-pilot simulation software.
- Chi Mak, a defence contractor engineer, stole sensitive technology secret.

- Dongfan Chung an aerospace engineer, stole Boeing trade secret related to space shuttle and another related space program.
- Hanuman Jin, a software engineer, stole push talk technology from Motorola.
- Sixing Liu a defence contractor employ, stole design and performance data for an aerial guidance system.
- Liu Yuan Xuan and Robert Maegerle conspired to steal a trade secret from DuPont on chemical processing.
- Samarth Agarwal stole French highfrequency trading source code for a rival US hedge fund.

In China, besides cyber break-ins and traditional spying using human assets, it employs legal means of acquiring technology such as joint ventures, buying companies outright, partnerships with government research institutions, and hiring foreign experts and bringing them to China to work. Other undercover means include setting upfront companies that obscures its participation, etc. In today's world, without a strong market based economy, India would quickly lose its worth. We need to have a strong base of globally competitive products and services that produce jobs.

The economy must include sound government policies to promote responsible choices and reduce our debt, and grand strategies for energy and environmental sustainability, science and technology leadership (at least in some areas), human capital capabilities, manufacturing, and the industrial base.

Dr. Ronis states that there can be no question of the need to include the economic viability of our nation as a major element of national security because, "without capital, there is no business; without business, there is no profit; without profit, there are no jobs, and without jobs, there are no taxes, and there is no military capability. The viability of a nation's industrial infrastructure, which provides jobs for its people, creates and distributes wealth, and leverages profits, is essential. Without jobs, the quality of people's lives deteriorates to a point where society itself can disintegrate".

To boost the economy, the government has to focus on the potential of IP as India is a young country, with maximum number of youth who can think squarely outside.

How does it work?

In economic espionage, trade secrets are primary targets. This includes data on research and development, business plans, source code, manufacturing processes, market plans, and customer information. Since the value is in the information and innovation, both large and small companies are targeted. Even startups with breakthrough technology are vulnerable to the threat.

It can be better understood by taking an example. Currently, China and the US are not on good terms and there is a trade war going on between them. The US, on various occasions, blamed China for stealing intellectual property. There is evidence that supports US' allegations against China.

"China has institutionalized a system that combines legal and illegal means of technology acquisition from abroad", said William Schneider Jr., Former Undersecretary of State for Security Assistance, Science & Technology and Former Chair of the Defense Science Board. He also said at the DSEI Japan conference held near Tokyo that, "It is well known that China steals IP and other secrets from industries, academia and the government, but what is not so well known is how China converts the technology it acquires into their military capabilities".

The 'obtained' information (data, research etc.) is first sent to one of China's advanced science universities. They in turn apply for Chinese patents on the technology. After they acquire a patent, the government places the patents to various companies.

One of the most notable recipients is the telecommunication giant- Huawei Industries, which has been under the microscope of US regulators as the company attempts to roll out its 5G technology. It has acquired 56,000 5G and artificial intelligence related Chinese patents despite spending little on its R&D.

Economic espionage is more of a threat than standard hacking because the country is dealing with advanced attackers using advanced tactics. They are more prone to do multi-pronged attacks using electronic, physical, and social methods. Attackers are very likely to try to co-opt an insider, either directly through bribery or indirectly through social engineering. Economic espionage agents specialises in psychological techniques of 'deceit and enticement'. One big

reason could be attributed to the fact that, economic espionage is not just restricted to stealing intellectual property, but is also about acquiring the expertise to make use of it. So, employees and former employees have been lured away in violation of their employer's confidentiality and non-compete agreements. Economic espionage attackers are also willing to risk more as the nation-state as a whole is rarely harmed, even when their agents end up in prison or exile. Usually, it is the co-opted insider that often gets the harshest punishment.

What to do?

Government initiatives like '*Atmanirbhar Bharat*', 'Startup India', 'Digital India', although proved to be advantageous for startups in India, but a significant number of the Indian population are still unaware of trademark infringement and intellectual property theft. It is rightly said that "Intellectual Property has the shelf life of a banana and should be protected by law (Bill Gates).

India passed its first-ever Intellectual Protection Policy in 2016 which ensures the rights of the innovator. India's IP has seen an upward curve in the last decade which can be attributed to both— a gradual increase in awareness of IP laws (Trademarks, Patents and Copyright etc.) for industry growth and a tough competition for Foreign Intellectual Property intensive companies entering the Indian markets which aims to provide a fierce competition to their Indian counterparts.

However, as per the Global IP index, that charts the growth of IP industry among 50 global economies, India has jumped 8 places to stand at the 36th position on the list. The jump is the highest gain that any country, on the list achieved for the year 2019 and is owed to India's recognising the International Standards of Copyright Protection and the incentivising of Intellectual Property" (US Chamber International IP Index, 2019).

Even with the jump, there are certain aspects that India needs to pay more attention so that it can harness the potential of intellectual property intensive market like the UK, Australia, and USA.

Speed is crucial when dealing with IP theft

Technological advancement has made it difficult to detect the destructive trait of malware and other types of cyber attack software that are used in today's world. Cyber theft can go on for an extended period of time and companies often fail to realise that their information is being stolen.

Moreover, a competitive advantage can be missed if significant IP is stolen. So, it is important to quickly identify as to what has been stolen and thereafter assess the consequences of the. Taking these steps sets the stage for two responses. First is to identify the hackers and try to either recover your data or block them from using it in a disadvantageous way. *Second,* as discussed in the *Beneath the Surface* paper, is to quickly determine how the stolen IP can potentially be modified—or new IP developed—to regain the competitive separation, originally sought between your organisation and other players in the market. Quick identification of the theft can accelerate the targeted organisation's process of strengthening security of its IP and, if possible, developing other innovations to regain and maintain the company's competitive advantage.

Forensic Investigation is Vital when IP or Trade Secret Theft has Occurred

Forensics can serve as an important tool for several aspects of the investigation. The first is tracking of the cyber attack to determine what happened, how it happened, and what, in fact, was stolen or taken. Forensics can also help identify the data compromised , its sources, and also as to from where malware or other destructive capabilities infiltrated the system. Understanding these factors provides the basis to quantify the impacts of the theft, including ripple effects such as damaged customer relationships, lost contract revenue, and trade name devaluation; pursue and identify the theft perpetrators, and build a defensible chain of custody around the data. If the data is unrecoverable, then the investigation can support efforts to pursue legal action aimed at mitigating your organisation's losses. Encouragingly, this past Spring, the US Congress passed and the US President signed the Defend Trade Secrets Act(DTSA) of 2016, which for the first time, provides for federal criminal penalties for trade secret theft. Previously, state laws governed trade secrets. The act expands to prosecutorial damages, and recovery aspects of enforcing trade secret law, which should help to improve the company's response to such issues.

= ***Forensic Investigation Relies on Specialised Talent and Methods***

Data analytics specialists can retrieve data from compromised systems and run queries to identify patterns, isolate security breaches, and determine whether data has changed or gone missing. These professionals also help to establish the chain of custody for data, including what was stolen, as well as when and how. They understand the signatures, hallmarks of and distinctions between internal and external actors. Utilising person-to-person interviews and

analysis of computer systems & network traffic, investigating teams can determine as to whether the attack was the work of internal or external actors.

Forensic financial and accounting specialists, who understands IP and its value, are also essential. Along with their technical expertise, they can bring perspective on business processes and the competitive marketplace to quantifying damages associated with theft or infringement. They also often serve as expert witnesses in subsequent court cases, testifying about the theft of the IP or trade secrets, their value, and financial impacts of the theft.

Our take: Protecting IP requires

Employee education is important as they are often responsible for protecting the company's IP and advising the executive team on law and enforcement response. Their training should include detail on how economic espionage attackers can target both current and retired employees. Technically, we need to ensure that we are using network segmentation and least privilege to reduce the exposure of intellectual property; all-access to that information to be logged and the logs retained. Access to both, physical and electronic information, should be swiftly revoked for the terminated employees.

End Notes

1. Edwin Mansfield*, Global Dimensions of Intellectual Property Rights in Science and Technology*, , Washington, DC: National Academy Press, 1993), ch-5.
2. Sheila Ronis, "Economic Security: Neglected Dimension of National Security?" *Center for Strategic Conferencing, Institute for National Strategic Studies,* National Defense University Press, 2011.
3. The Global Innovation Index, (GII), co-published by Cornell University, INSEAD, and the World Intellectual Property Organization, 2019.
4. Sundhava Shetty, "Privatising the Defence Sector is a Dangerous Idea that will have Drastic Consequences", *The logical Indian*, 2017. Available at https://thelogicalindian.com/opinion/privatising-the-defence-sector/.

5. Himanshu Sethi, “Spike in cyber Attacks on Indian Vaccine Makers and Healthcare Institutions Report, *Business Line*, 27 November 2020. Available at https://www.thehindubusinessline.com/info-tech/spike-in-cyberattacks-on-indian-vaccine-makers-and-healthcare-institutions-report/article33192417.ece.
6. Alexander Abad-Santos, “China is Winning the Cyber War because they Hacked US Plans for Real War”, *The Atlantic*, 28 May 2013. Available at https://www.theatlantic.com/international/archive/2013/05/china-hackers-pentagon/314849/.
7. Deloitte.5 Insights on Cyber Attacks and Intellectual Property: An interview with Don Fancher, Principal, Deloitte Financial Advisory Services LLP.
8. Raymond Pompon, “Economic Espionage: How nation-state-funded ATP’s Steals Billion in Secret”, *F5 Application Threat Intelligence*, 12 June 2018. Available at https://www.f5.com/labs/articles/cisotociso/economic-espionage--how-nation-state-funded-apts-steal-billions.

About the Author

Ayasha Firoz is currently a student at the Aligarh Muslim University, Aligarh.