Journal of Intellectual Property Rights
Vol 29, November 2024, pp 472-483
DOI: 10.56042/jipr.v29i6.8468

Integration of Intellectual Property Rights and Cyber-Tech Soundness: A Pre-Requisite for National Interest

Jayanta Ghosh† and Oishika Banerji

The WB National University of Juridical Sciences, Kolkata — 700 098, India

Received: 1st February 2024; revised: 20th June 2024

Last two year's pandemic prompted a greater reliance on technology, as well as a greater usage of networked gadgets and hybrid work settings.Cybersecurity has developed into a complicated and rapidly evolving concern in the Information, Communication, and Technology (ICT) era. It seems that cyber threats will permeate every area of the economies and government infrastructures around the globe as the world's reliance on ICT increases. In fact, threats to a state's technology infrastructure that were previously unheard of, challenge national interest in the digital age. In the twenty-first century, cyber hazards are rapidly increasing and growing in the second decade. While criminals are still the ones who initiate them, other stakeholders, like foreign governments and political organizations, are also involved and may have objectives beyond money making as well. Back in 2020, the Indian government registered 1.16 million cyber security cases, a 3x increase over the previous years. Cyber-attacks in India, as in other nations, risk national security by gaining access to key government infrastructure. The scope of the cybersecurity danger is such that contemporary civilization might be described as being attacked holistically or systemically. To respond to a system-level danger, a system-level reaction will be required, so that the operations of various agencies and bodies complement each other and are mutually reinforcing, rather than competing. The current study recognizes intellectual property rights (IPR) to facilitate such requirement. The present research paper provides an insight of cyber security as a profound step towards securing the national interest, to its readers. It also makes an attempt to welcome intellectual property rights as a help towards achieving such a profound goal.

Keywords: Cybersecurity, Data Breach, Cyber Space, Intellectual Property Rights, Digital Economy

There are greater cyber risks when a country has a highly evolved digital economy and culture. This means that nations with well-developed electronic commerce and digital infrastructure will inevitably be more concerned with safeguarding the internet. There can no longer be any doubt that cyber security is an essential component of national security. The national security plan must be the foundation for a country's national cyber security policy. This is the fundamental reason why the title of this research uses the word "cornerstone." One of the things we'll be looking at in this research is the relationship between national security and national cyber security. There are now cyber security plans in most countries. Cyber-attack incidents that target people, companies, and governments globally have increased in tandem with the growing reliance on computers and Internet-based networking. In today's time therefore, ICT can be used a tool for warfare thereby posing a threat to national security.[1]

Since the main focus of intellectual property law is on intangible property, of which original ideas and concepts are the most common example—it is a distinct area of the law unto itself. Owners of original ideas are granted limited property rights under intellectual property laws. To put it briefly, "control over the products of intellectual effort" is regulated by intellectual property law. The two primary areas of intellectual property that interact with national security are trade secrets and patent law, according to Rob Farley, a visiting professor at the U.S. Army War College and senior lecturer at the University of Kentucky's Patterson School. Farley stated[2] that patent law "is important to figuring out how a state can drive innovation in its defence industrial base" on the podcast "War Room," which is produced by the U.S. Army War College. He cites the history of patent law, particularly the way the government opted to provide monopolising patents to innovators conducting research in areas that would be most helpful to national security, as proof of this claim. Farley also highlights how the American and British governments strategically used patents in the early 1900s to restrict the development and manufacture of innovations like the torpedo, specific types of weapons, and aviation

†Corresponding author: Email: joyantaghoshcool@gmail.com

technologies, as well as to stop information from being shared globally. Regarding trade secrets, Farley says that the key is for government-owned and privately held businesses to be able to keep other businesses or nations from discovering their trade secrets. This relates to the ability to shield trade secrets from being discovered by other businesses, both domestic and foreign, in the context of national interest. Naturally, this is crucial for maintaining traditional objectives of national interest like safeguarding military technology or keeping others from learning about your nation's capabilities.[3]

Cybersecurity threats have not left trademark and copyright in silos as well, taking into consideration the existing praxis that does not restrict the uninvited guest from being in its skin, inside these IPdomains. While caching, plagiarism and threat to computer software are potential examples for copyright to recognize its potential, trademark can be fundamentally seen to be walking in hand with domain names, making the overlapping areas not be 'scavenger hunts' for the unwelcomed guest. The study with the help of IP as catalysts seeks to answer the question as to whether the unprecedented present owned by cyberspace be tamed by IP as the possible night-owl and if so in affirmative, whether such can be adopted by a nation in its own interest.The cyber threat protection mechanism, which entails creating a national cybersecurity system, developing and implementing a cybersecurity strategy, bolstering security and defence sector capabilities to effectively counter military cyber threats, protecting state electronic information resources and information infrastructure from cyber-attacks, plays a significant role in this literature therefore.[4]

Viewing Cyber Security as the Tool to Safeguard National Interest

As the number of people using the Internet grows, so does the number of cyber-attacks. Many of these attacks have sad and serious consequences. It is the most popular weapon in cyberspace used for malevolent objectives, either exploiting existing weaknesses or taking use of the unique traits that are being developed. The development of more innovative and effective malware defence systems has been highlighted as a priority issue by the cybersecurity community.[5] A large part of cybersecurity is figuring out how to defend against various types of cyber-attacks and coming up with countermeasures to ensure that digital and information technologies are kept safe from intrusion while also maintaining their integrity and usability.

(i) In the context of confidentiality, this refers to the safeguarding of information against unwanted access.
(ii) Integrity refers to the ability to avoid unwanted changes or deletions.
(iii) Availability refers to the ability of systems responsible for transmitting, storing, and processing data to be accessed when and by people who require them.[6]

In fact, threats to a state's technology infrastructure that were previously unheard of challenge national security in the digital age. In today's globalized world, the internet and ICTs are undeniably crucial for social and economic advancement, serving as a vital digital infrastructure that businesses, governments, and society as a whole depend on to perform their fundamental functions.[7] The internet is a dangerous place on many levels since it is mostly an open platform. Protection of critical infrastructure, cyber-terrorism, cyber-threats, privacy issues, cybercrime, and cyber-warfare have all therefore entered the discourse on cybersecurity.[8] In the second decade of the twenty-first century, cyber risks are increasing and growing quickly.While criminal actors continue to be the driving force behind them, other parties, including foreign governments and political organizations, may be involved as well and may have goals beyond financial gain. The latter includes "hacktivism" in support of political causes, political instability, cyber-espionage, sabotage (such as Stuxnet), and even military activities.The emergence of cyber-espionage, the increasing skill of cybercriminals, and the widely reported operations of hacker collectives have all contributed to the impression that cyber-attacks are becoming more coordinated and sophisticated, which is unmistakably proof of their professionalization.[9]

Intellectual Property Rights and Cyberspace: The Vulnerable Relationship

Being a non-physical domain, cyberspace enables anyone to access data and exchange information without realizing that doing so may violate intellectual property rights. Intellectual property rights and cyber laws are inextricably linked as, in the modern world, digital content needs to be protected. Cyber concerns were not given much thought when IPR legislations were enacted, but as digital media has grown, it has become more important than ever to

safeguard authors' creations from unauthorized use so they can continue to profit from their works. As cyberspace has no boundaries and there are frequent cross-border infringements, intellectual property issues are now a global concern. As there is no absolute rule of law, it is concerning that legal conflicts about prescription, adjudication, and enforcement of the law would either fall under the purview of a court or not. As a sovereign state, a nation may enact criminal laws to punish harmful acts that are performed outside its borders but have an effect inside its borders. Courts have the authority to punish cybercriminals under universal jurisdiction in accordance with international law. Technology advancements have led to a daily growth in e-commerce, which has increased the need for businesses and organizations to safeguard IPR of online publications'. It motivates writers to disseminate and exchange knowledge, and in exchange for their published work, they get compensated. However, there is a negative tendency regarding the protection of intellectual property as e-commerce gains popularity. The following techniques are evident and are to blame for the damage they pose to intellectual property rights:

Cybersquatting

It is the act of registering, offering for sale, or utilizing a domain name with the goal of making money off the reputation of another person's brand. Essentially, this involves someone using a registered trademark's domain name maliciously in order to deceive people and profit from it. In the age of online commerce, it is now one of the ways to deceive customers and violate trademark rights. An example of cyber-squatting may be observed in the case of *Yahoo! Inc* v *Akash Arora & Anr*, in which the defendants were utilizing the name of "Yahoo" under the domain name of "Yahooindia.com" for delivering internet services. The petitioner in this case is Yahoo's owner, and for the purpose of offering services in India, they have registered the domain name "yahoo.in." In this case, the court decided that the defendant should be restrained from using the domain name "yahooindia.com" and that the petitioner should receive relief because the domain name "yahooindia.com" is misleadingly similar to and could be mistaken for the domain name "yahoo.in."

Linking

It is one technique for copyright infringement. Linking is the process by which a website enables a user to access another website without ever leaving it. Copyright infringement occurs when links to content on another website that is protected by copyright are included without the owner's knowledge. It is to be noted that copyright violations may result from duplicating any work protected by copyright, providing copies of the work to the public, or sharing the work with the public. Since linking is such a basic concept, many users think that preventing links violates their right to free speech and the ability to move about the internet. One such technique for using links for infringement is deep linking. It enables users to go straight to an internal page from the main page, avoiding the content and ads there. Although hyperlinks are not expressly forbidden by copyright law, violators who know they are engaging in unauthorized copying of protected works are prevented from creating links that aid in such copying.

Software Patent Infringement

Software, like literary and creative works, are essentially intangible properties protected by copyrights rather than patents. Programming languages are handled the same as any other basic language, meaning that copyright laws protect them even though they are not patented, like English, French, etc. Since patent law offers greater protection, many nations have been discussing whether or not to include software programming languages in its protection. With weaker patent law in force for software, infringement in the cyberspace is not only easier but a delightful treat.

In-Lining

A web page might generate a new webpage by beckoning elements from multiple sites or servers using in-line linking, sometimes referred to as in-lining. In case of in-lining, the composite page would consist of a series of links to other sites and servers. The page instructs the browser to obtain the images, graphics, etc. from the original sources when viewing the composite page.In *Leslie A. Kelly* v *Arriba Soft Corporation*,[10] a visual search engine known as ditto.com produced thumbnail images of photographs and used them to link to the original pictures. The plaintiff, a qualified photographer, took issue with the search engine duplicating thumbnails of his photos, which, once clicking, opened the full-size image in a window on Arriba's website. It was decided that the respondent had violated copyright with this activity.

To guarantee that intellectual property rights are protected and not abused even on widely used online platforms, a number of rules have been established in

several conventions, including the WIPO Performance and Phonograms Treaty, the OECD Convention on Data Protection, and the Berne Convention. The rights of an individual must also be preserved with the utmost care as the world quickly adapts to the cyberspace and lives in a virtual one. This is because it is very easy to fall victim to cybercrimes because the offender's identity stays anonymous, giving him advantages. The fact that cybercrimes are rising dramatically every day makes it evident that the laws we now have are not effective enough.

Safe Cyber Ecosystem with the Help of IPRs Read with Cyber Jurisprudence

The previously discussed vulnerabilities do not undo the possibility of IP to unravel its potential discourse in the divergent cyber environment, instead if IP is presumed to be a legal personality in itself, following it being designed with rights to be vested on its owner, revisiting its vulnerabilities will fundamentally allow it to spread its claws with rationality and decisiveness.Infringements on intellectual property rights are increasingly occurring in cyberspace. A number of actions taken by the operators of cyberspace websites led to the infringement of other website operators' rights, including intellectual property rights. It is now essential that people understand how their webpages and websites are being used illegally. As soon as we imagine such websites to be of the sovereign, it becomes a subject of national-interest security. It is the presence of IP protection on any invention or creation that safeguard and will continue doing so in light to cyber threat. The defensive attribute of IP lies in its enforceability in a court of law with competent jurisdiction either through statutory or common law remedies.

If we consider developed nations like US, the up-gaming they have been doing in regards to setting up a robust IP mechanism, stands literature lauded. A 2014 report[11] published by the Committee on Energy and Commerce, House of Representatives, 113th Congress (First Session), U.S. Government, titled, "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology", stated that there has been a rise of cyber espionage on an unprecedented scale targeted theft of confidential business information and proprietary technologies through cyber- intrusions emanating from China. The report specifically denies declaration of war, instead, promotes strategizing with elements such as defensive cyber laws reading together with existing IP regime to counter the issue in hand. This decision was reached taking into account that IP significantly contributes to the US economy thereby also encouraging innovation, serving as a fuel for accelerating economic growth.

The European Union is taking efforts[12] to combat cyber security threats as well. While IPR plays a significant role in the EU's economy, accounting for almost 50% of the EU's GDP and almost 40% of employment, it is the digital technology has grown more important in a variety of sectors, including transportation,[13] energy, health care, and finance. Even if digitalization has the potential to help solve many of Europe's problems, such as the COVID-19 quandary[14], it also exposes Europe's economy and society to cyber threats. There has been an increase in cyber-attacks and cybercrime in Europe, both in terms of number and complexity. This trend is projected to continue given that 22.3 billion devices are predicted to be connected to the Internet of Things by 2024. As a result, citizens are more likely to trust digital products and services if the cybersecurity response is improved.[15] It is equally significant to incorporate IP education into national curricula to increase public awareness and educate all key actors, starting from enforcement agencies to consumers and young innovators about IPRs in order to foster a more knowledgeable and conscious public society. This will be an attempt to aid cybersecurity legislations in current times. The EU Cybersecurity Act[16] entered into force in June 2019 and introduced:

(i) An EU-wide certification scheme.
(ii) A new and stronger mandate for the EU Agency for Cybersecurity

In December 2020[17], a new EU cybersecurity strategy was unveiled by the European Commission and the European External Action Service (EEAS). The goal of this plan is to increase Europe's ability to withstand cyber-attacks and guarantee that all people and companies have access to trustworthy and dependable digital services. Regulatory, investment, and policy instruments are all included in the new plan. On March 22, 2021[18], the Council approved conclusions on the cybersecurity strategy, emphasizing the importance of cybersecurity in creating a resilient, green, and digital European Union. For EU ministers, achieving strategic autonomy in the context of an open economy was

paramount. Encouraging the EU to make independent cybersecurity decisions will therefore strengthen the EU's digital leadership and strategic capabilities provided it also discusses how the criminal penalties for intellectual property infringements vary throughout EU nations thereby suggesting ways to improve the effectiveness and efficiency of IP enforcement processes through the use of dynamic injunctions and alternative dispute resolution methods.

Google, its parent company Alphabet, and two companies were fined a total of €250 million ($271 million) by France's competition authorities for violating an earlier agreement on the use of copyrighted content for training their Bard AI programme, which is currently known as Gemini.[19] The search engine behemoth was found to have ignored a June 2022 settlement agreement regarding the usage of news articles in its News and Discover pages as well as search results, according to the Autorité de la concurrence. Google escaped punishment by promising, among other things, to engage in good-faith discussions with news providers on payment for their content. The authority claims that Google specifically committed to giving publishers and news agencies a "transparent assessment" of their usage rights compensation and to ensuring that the talks would not interfere with "other economic relations" between Google and the publishers. Nevertheless, the authority claimed that Google had fallen short of those promises in a number of ways. First of all, it has not been transparent enough in sharing information with its representatives; it has not promptly provided the information required for the agreement's monitoring. Second, the business had confidently ignored the 2022 bindings by withholding comprehensive information on how it generates revenue from news content. Such an instance is a matter of national security and interest as manipulation of contractual licenses, by a third party, infringing statutorily vested exclusive rights, equates with pushing boundaries beyond the prescribed limit. Summarily, it is only because of the existence of IP Protection that the required action was taken thereby disclosing the potential it showcases in times of threat and vulnerability.

National Security in 2023 and Beyond: Stepping Ahead of Technology

Surprisingly[20], vastly transformed conceptions of national security will contribute to the advancement of global technology civilizations by themselves. As a result of military policy, the number of new consumer electronics products is expected to rise. Meanwhile, the line between R&D for the military and civilian sectors is becoming increasingly blurred. A very high probability exists that faster arms reduction discussions will result in further large-scale reductions in offensive nuclear weapons.As a result, the same superpowers that have invested enormous resources in military preparation and deterrence, and in establishing barriers to the globalization of leading technology—will now have to focus on the imperatives of verification.[21]

The struggle between the United States and China is the focal point of almost every international issue or field in which the two could come into contact in the twenty-first century, including sports, politics, and most importantly where the two collide in the race for technology. The race between the United States and China in the technology race has significant ramifications for national security because cutting-edge technologies like artificial intelligence (AI) have the power to significantly alter a nation's economic standing or boost its military might,[22] which could have a negative effect on rival nations. The Intellectual Property Laws and Policies that each nation has in place have a particular bearing on the technology race between the United States and China. This is because a nation's capacity to advance in the race for technological advancement depends on its ability to provide incentives and support intellectual property innovations and inventions through robust patent and trade secret protections. Notably, Chinese advances include a rise in patents, the ability to provide injunctions against patent infringement, and the establishment of specialized intellectual property tribunals with structures and procedures similar to those of Western courts.[23]

The strategic force and counterforce deterrence concept will be largely superseded by negotiated agreements. There will be a faster pace of development for remote probing devices like spy satellites. With the aid of recently created technical tools, a new dimension will be added, mutually agreed-upon, in-depth, close-up inspections of each other's production and facilities by air and land. If there hadn't been such unparalleled transparency, the potential for the opposing side to cheat would have prevented an agreement from being reached in the first place.

The tally of soldiers, tanks, and planes will be meaningless in the European theatre in the near future due to advances in technology. In terms of pure firepower, a conventional army can already outperform an aggressive conventional army. Tanks, aircraft, and military formations may all be destroyed with the use of advanced robotic weaponry.[24] NATO soldiers can interrupt Russian communications while also preventing them from jamming ours with better electronic warfare.[25]A computer-aided combat information management system enables highly targeted military operations. As a result, the military world will become more transparent, more technologically advanced, and more armed with defensive weaponry. Chips, computers, and other precise electromechanical equipment will be needed in large quantities in the future. Military computer networks, fast semiconductors, and electromechanical robots, on the other hand, do lead straight to consumer industrial items, while H-bombs[26]don't. All kinds of civilian industrial, consumer, governmental, and professional activities will benefit from their use. They are near cousins to the technical gear essential to the more efficient creation of virtually anything.

Certain international technology systems, once in place, will gradually diminish national sovereignty and autonomy. Consider, for example, electronic information networks. Material and component production scheduling, assembly, and testing, as well as labour allocation, are critical to reducing manufacturing costs and responding fast to market shifts in a timely manner for the world's largest firms.This data must be able to transit national boundaries unhindered and very instantly. Corporations who use computerized network technology will have such a clear edge over their competition that every other firm will be forced to follow in their footsteps. Countries that prohibit network growth and operation on their land risk being bypassed as a result of the rapid proliferation of networks[27]. Expect an order of magnitude growth in the velocity of company change the number of critical variables to corporate strategy, and new technical sources at the same time. Starting and running a firm means dealing with a greater variety of political issues and new sorts of corporate alliances.

It is obvious that intellectual property is a crucial and essential part of American national defence. Even though the United States has historically dominated the technological race, other world leaders like China have been able to "catch-up" in this race due to a lack of innovation or modernization in intellectual property policies within the United States. Because of Alice Corp[28]., the United States has extremely strict patent laws that have raised the bar for invention and creativity in the development of new technologies, particularly when it comes to complex ideas incorporating algorithms like artificial intelligence (AI).[29] The 21st century will see a new era of technical innovation centred on AI and related technologies. Countries who are unable to establish a presence in this rapidly expanding field of technology will suffer grave economic setbacks. Furthermore, the United States faces a serious risk from the technology's possible hostile or military applications. The rate at which intellectual property laws are changing, along with China's seeming acceptance of intellectual property theft and the United States' own intransigence in enforcing its policies, have cornered the former. The United States appears to have little choice but to enact some sort of intellectual policy shift in order to safeguard its national security and prevent falling behind in the current technology race.

In the past, we haven't purposefully used tax incentives to encourage technological advancement, but we should now.[30] Excessive consumption is encouraged, while savings are discouraged. We need to rethink our anti-monopoly rules and processes. The latter were mostly created over a century ago for a much smaller and isolated country. They are incompatible with today's sophisticated, dynamic, high-tech, global competitive society.[31]

Increase in Sophisticated Attacks: A Smart Move in the Game of Dice

DDoS attacks against Estonian websites, including those run by the Parliament, government departments, banks, newspapers, and television stations occurred in 2007[32], during a period when Russia and Estonia were embroiled in political tensions. Even though circumstantial evidence points to Russia as the perpetrator of the attacks, the Russian government has never confirmed its involvement. When a single ethnic Russian living in Tallinn became upset by Estonia's actions and decided to act alone, he was convicted guilty of the attacks by an Estonian Court.[33]

A sophisticated surveillance device was discovered in Dalai Lama's computer network in Dharamshala, India, in 2009.[34] 103 nations were found to have been penetrated by the same network, nicknamed

GhostNet.[35] Although the evidence was circumstantial, China was suspected of being the source of this monitoring network. It was also unclear if this network was maintained by a Chinese government entity or by Chinese citizens for business or nationalistic purposes.

Despite the lack of comprehensive federal law governing private-sector data activities in the United States, a network of constitutional, legislative, and institutional safeguards limit US government surveillance of US citizens, especially in the context of foreign intelligence gathering. However, the American viewpoint is less clear outside of its boundaries and among its residents. According to the United States, economically driven espionage is not admissible under the definition of approved types of government-sponsored cybersecurity (unlike cyber-attacks, for example, that impair vital infrastructure). The 2015 deal between China and the United States to ease tensions in cyberspace was predicated on a distinction that essentially allowed digital espionage as long as it wasn't carried out for financial gain. The agreement (later affirmed by the G20)[36] provided that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors". The norm suggests that cyber theft for national security reasons is still permissible while attempting to exclude "commercial" cyber theft.[37]

Cybercrime and the theft of trade secrets are strongly associated. Digital technologies have benefited innovation and information management, but they have also increased the vulnerability of intangible assets. Core value assets (such as data, customer records, security information, and intellectual property) and operational assets (such as business-critical IT services) are examples of digital assets. Trade secrets can shield assets with inherent value as the law offers these digital assets legal protection, which helps address vulnerabilities, while cyber security offers useful, business-critical protection. Using trade secrets is a strategic choice made by a company. Firms must take into account IP procedures to limit usage of their information in order to preserve a competitive advantage and protect innovations. Unlike other intellectual property, trade secrets are exempt from formal registration requirements, have an indefinite shelf life, safeguard a wide range of information, and don't need to be disclosed. Due to the broad definition of trade secrets, businesses can safeguard everything from prototypes to client lists. Trade secrets even include setbacks, including botched scientific trials and software vulnerabilities. Using trade secrets as a safeguard has the drawback that their confidentiality is essential to their application; once disclosed to the public, a trade secret is no longer one, both legally and practically.

US PolicyMakers are increasingly viewing even the personal data required to create AI and machine learning apps as a dual-use commodity with economic and national security relevance.[38] Attorney General William Barr stated[39] that while announcing the indictment of hackers who stole data on millions of Equifax customers, should know that the data has commercial value and those thefts may fuel China's development of artificial intelligence technologies as well as the production of intelligence targeting packages."[40] US actions against Chinese-owned platforms like TikTok and Chinese investment in US companies like MoneyGram and Genworth have been driven by concerns about data security and allegations regarding Chinese government access to the data of Chinese firms.

Stuxnet,[41] a computer virus designed to halt Iran's nuclear programme, damaged and perhaps destroyed centrifuges at the Natanz uranium enrichment complex in 2010 as part of the endeavour. The worm was later discovered to be a well-designed and well-executed cyber weapon that required an engineering effort that signaled a nation-state sponsor. Further investigation revealed that the worm's designers and deployers were the United States and Israel, though neither country has claimed responsibility. It's no secret that the world's main cyber powers are beset by internal conflicts when it comes to their methods to online espionage, law enforcement and data collecting.[41] Cyber-espionage is something that the US government despises, but acknowledges as a fact of world politics. The US government is having a hard time keeping its narrative straight on this issue. It's problematic for Brussels to demand more of other nations to defend Europeans' privacy rights than the EU itself can require of its own member states. Brussels Confidence in China's new privacy measures is fueled by the country's wide-ranging security and surveillance policies, which cast doubt on the value of the PRC's new initiatives.[42] If data security and national security are now almost synonymous, are

self-serving approaches still viable? Recognizing these discrepancies is the first step in dealing with the difficulty of digital cohabitation, and it is essential to understand that the only feasible method to overcome them is through legal and political measures.

The continuing negotiations regarding a successor to the EU-US Privacy Shield following the Court of Justice of the European Union's (CJEU) verdict on July 2020 in the *Schrems II case*[43]exemplifies the fundamental issue. The Privacy Shield was created to allow corporations to move data from the EU to the US while remaining compliant with the GDPR. At Schrems II, the CJEU invalidated the Privacy Shield, placing a wide range of companies' cloud services and transatlantic data transfers in peril. An absence of a comprehensive GDPR-like federal privacy law in the United States was not the court's concern.

India a Scapegoat in the Cyber Battles of World Leaders: Digging in India's Tech Laws

An essential engine of economic growth and a key pillar of Indian business and government, India's IT sector has emerged in recent years.[44] The industry improves a number of socioeconomic factors, ranging from living standards, career prospects, to that of cultural diversity, which benefits an individuals' life in India. Additionally, information technology has been instrumental in making India a global leader in business services and cutting-edge technological solutions. One of the most anxiously awaited developments in Indian cyber law is the National Cyber Security Strategy. This plan aspires to be a complete guiding doctrine for people, policymakers, and other stakeholders, as well as a follow-up to the National Cyber Security Policy of 2013.[45] The plan is anticipated to shed more light on the necessary reaction mechanisms in the government and other sectors when it comes to cyber security. For quite some time[46], the Union Government has been working on a National Cyber Security Strategy, and the entire world is watching with bated breath to see how it develops. The strategy should notify the appropriate authorities of all they need to know about dealing with cyber security implications in their operations.In order to address the latest round of national security concerns, it is imperative to have the necessary governmental authority to suppress intellectual property theft and prevent such piracy. The IT Act's many measures have also made it easier to find these malpractices. It's also important to consider if one should prioritise international or national security over human security.[47] One could observe the direct or indirect links between intellectual property and national and global security. The literary definition of human security and national and human security are intricately linked.

Interestingly, as the intellectual property rights, especially patents and trade secret have been in discussion with respect to developed nations above, it is ideal to delve into the Indian atmosphere. The Indian Patent Act, 1970 does not specifically deal with national security, but, under Section 4, it mandatorily prohibits patenting of inventions related to atomic energy. Such a provision acts as a prevention for any kind of internal threats in dynamic times. When it comes to trade secret, there is no express legislation for the same. Instead, Section 27 of the Indian Contract Act, 1872 and Non-Disclosure Agreement (NDA), are the only hope for the trade secret regime in India. Thus, it is better to state that several risks are walking alongside India's dependence on intellectual property law to safeguard national security.

When a patent is granted, the data included in the application enters the public domain and becomes a vital resource for learning about the most recent advancements in any given field. Since any government, business, or individual may readily access these documents, they appear to be an important means of technological transfer.[48] In accordance with the Copyright Act, 1957, Trade Marks Act, 1999, Patents Act, 1999, Designs Act, 2000 and Geographical Indications of Goods (Registration and Protection) Act, 1999, the Central Government has the authority to restrict or outright forbid the import and export of goods that violate the intellectual property rights of their respective owners. However, it might even be essential to deal with a variety of associated issues, like taking police action against pirates and pursuing legal action for infringement in order to carry out raids.

Last two year's pandemic prompted a greater reliance on technology, as well as a greater usage of networked gadgets and hybrid work settings. As a result, we are more technologically susceptible than we have ever been. In 2020[49], the Indian government registered 1.16 million cyber security cases, a 3x increase over the previous year. Cyber-attacks in India, as in other nations, risk national security by gaining access to key government infrastructure.

Hackers took down the Indian government's two-factor authentication system used to safeguard its email network three times last month, compromising the emails of several government personnel. Unfortunately, the perpetrators of the attack and their method of operation are yet unknown.[50]

In the last year, cybercrime, including phishing, identity theft, and fraud, has surged. However, the current laws do not adequately or comprehensively address it. The infiltration of cybercrime will most certainly continue to consolidate. As a result, stronger legal frameworks and stricter laws to combat cybercrime are even more critical. India has never had a specific data protection legislation in place. Earlier in 2021, in December, the administration presented Parliament with the Personal Data Protection Bill, 2019. In 2020, a Joint Parliamentary Committee (JPC) was actively considering the aforementioned Bill.[51]

Critical information infrastructure and other national assets are not protected by a formal essential framework that spells out the response policy in the event that they are attacked by an enemy. In 2013, the Indian government announced the National Cyber Security Policy (NCSP)[52], which included many measures for combating cyber security threats. Despite the passage of eight years, only a small portion of the plan has been implemented, and our country remains one of the most prominent targets. The lack of a comprehensive cybersecurity plan or policy is obvious and increases risk.[52] It is necessary to note that although the Data Protection Bill, 2019 was about to see the broad daylight, it was scrapped down in 2022.[53] Further, in 2023, the government came up with the Digital Personal Data Protection Act, 2023 with an aim to process digital personal data in a robust manner. Not to miss out on the development, the Act comes with yet another concern which is accumulation of unregulated powers of accessing data by the government. This concern looms around the Indian territory in present times.

Ensuring National Interests amidst the Advent of Cyber-crimes and Unrecognized Threats

ICT goods, services, and processes need to be certified to ensure that they meet rigorous cybersecurity requirements. Currently, EU nations utilize multiple security certification processes, which creates market fragmentation and regulatory hurdles. The EU has now established a single EU-wide certification system with the introduction of the Cybersecurity Act:[54]

(i) Build trust,
(ii) Increase the cybersecurity market's growth,
(iii) Ease trade across the EU.

A comprehensive collection of guidelines, technical specifications, standards, and procedures will be provided by the framework. India needs to develop and put into action a cooperative cybersecurity strategy that includes the following in order to achieve stability and security:

Robust Legal Framework

The Information Technology (IT) Act of 2000, which was passed in India in 2000, deals with cybercrime and associated offences. Regulations against cybercrime have been created under the Companies Act 2013 and the Indian Penal Code, 1860, both of which penalise crimes done in cyberspace as well. There are also sector-specific rules in place by regulators including the Reserve Bank of India (RBI), IRDA Act 1999, the Department of Transportation (DOT), and the Securities and Exchange Board of India (SEBI). As a result, the way businesses operate and crimes are committed online have vastly altered. Take, for example, the development of digital payments, which has resulted in a considerable increase in sophisticated cybercrime involving digital payment transactions. Lending firms provide consumers with rapid, frictionless payment experiences, leaving banks andother institutions in the payment ecosystem with little time to identify and respond to cyber threats. As a result, the Information Technology Act of 2000, as revised in 2008[55], will very certainly need to be changed, with cybersecurity criteria aligned with the kind of information assets managed by certain sorts of companies.

An Entity for Cyber Response

Any national organization in charge of cyberspace management should have a clear chain of authority so that all available resources may be used to their full potential. Unfortunately, no such framework exists. In India, there are a number of government entities that deal with various elements of cyber security. Cyber experts are assigned to each of our defence agencies, and even state police have cyber detectives. Experts operating under different government ministries and divisions must work together urgently to achieve a unified aim. A National Cyber Command, for example, might be formed by the Government.[53]

Need for Protecting Data

Data is a national resource, and cyberspace is where most of the data are traded. All governments and citizens that use the internet on a daily basis are required to adhere to data privacy laws. California Consumer Privacy Act covers the United States, whereas the European Union is governed by the GDPR regulations. Data has been lost by millions of Indians, however despite this, the Data Protection Bill was presented to India's Parliament in 2019 and was also taken away in August 2022. There is no denying the government's and business India's dedication to updating India's cybersecurity standards. The business sector will need to work more closely with the government in light of the increasing quantity of digital financial transactions and the current rate of cyber-attacks in India.The government's laser-like emphasis on cybersecurity readiness and awareness has the potential to transform the game.[56]

Hacking, cybercrime, terrorism and insurgency, and cyber aggression are all examples of a system-level threat to society. This is dangerous because, when it comes to cybersecurity, society as a whole does not act and respond as a cohesive system. Stakeholders remain separated and preoccupied with security within their own scope, and as a result, they fail to comprehend how their own security, or lack thereof, might harm them.[18] As a result, the business community may exclusively focus on cybercrime, despite the fact that cyber criminality increasingly employs strategies and technologies that have migrated from other fields, such as espionage. Anti-government hackers have also been known to employ cybercriminal practices. Accepting in principle that cybersecurity policy can and should be extended beyond its default settings would be the first step toward solving this broad problem.[57] The second step should be to base cybersecurity policy on a set of agreed-upon strategic and operational principles, with the following goals in mind; transforming cyberspace from a permissive, ungoverned environment into a self-governing network, increasing the costs of use by illicit actors, encouraging a comprehensive and inclusive understanding of cybersecurity across society and facilitating and ensuring legitimate use of the global ICT infrastructure.

Conclusion

The scope of the cybersecurity danger is such that contemporary civilization might be described as being attacked holistically or systemically. To respond to a system-level danger, a system-level reaction will be required, so that the operations of various agencies and bodies complement each other and are mutually reinforcing, rather than competing. However, a cybersecurity strategy that involves a large number of agencies and organizations, possibly from all sectors of society, including scientific and technological expertise, is unlikely to be amenable to central control. As a result, methods at the strategic and operational levels that are mostly self-informed, self-governing, and spontaneous are needed, as long as they are part of a larger, mutually agreed-upon framework or regime. Establishing an agile cybersecurity organization, defining a national cybersecurity doctrine, meticulous planning and de-confliction, and eventually responsiveness are all the steps in developing an active cybersecurity strategy thereby aiming to secure national security as well.

References

1 Parmar S D, Cybersecurity in India: An evolving concern for national security, https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf (accessed on 12 January 2023).

2 Morrison J, Intellectual property & national security, *University of Cincinnati Intellectual Property and Computer Law Journal*, 6 (2021), https://scholarship.law.uc.edu/ipclj/vol6/iss1/8.

3 War Room, Intellectual property rights & national security, U.S. Army War College (5 February 2019), https://perma.cc/KMH2-K94R.

4 Higgins B, The role of explainable artificial intelligence in Patent Law, *Intellectual Property Technology Law Journal*, 31 (1) (2019) 1.

5 Vakulyk O *et al.*, Cyber security as a component of the national security of the State, https://www.researchgate.net/publication/340440328 (accessed on 12 February 2023).

6 Jang-Jaccard J& Nepal S, A survey of emerging threats in cybersecurity, https://www.sciencedirect.com/science/article/pii/S0022000014000178 (accessed on 6 March 2023).

7 International Energy Agency, Data Centres and Data Transmission Networks, https://www.iea.org/reports/data-centres-and-data-transmission-networks (accessed on 20 March 2023).

8 United Nations, Leveraging digital technologies for social inclusion, https://www.un.org/development/desa/dspd/2021/02/digital-technologies-for-social-inclusion/ (accessed on 22 March 2023).

9 Achkoski J & Dojchinovski M, Cyber terrorism and cyber-crime – Threats for cyber security, https://core.ac.uk/download/pdf/35329569.pdf (accessed on 20 March 2023).

10 Europea.eu, https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf (accessed on6 March 2023).

11 *Yahoo! Inc* v *Akash Arora & Anr*, (1999 IIAD Delhi 229).

12 *L A Kelly* v *Arriba Soft Corporation*, Case No. 00-55521], US Court of Appeals for the Ninth Circuit.

13 Committee on Energy and Commerce, House of Representatives, U.S. Government, Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, 2014.

14 World Economic Forum, https://www.weforum.org/agenda/2022/12/cybersecurity-european-unionnis/#:~:text=The%20European%20Union%20is%20replacing,a%20top%20EU%20official%20said (accessed on 22 March 2023).

15 European Commission, https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/combatting-counterfeiting-and-enhancing-enforcement-intellectual-property-rights_en (accessed on 10 May 2024).

16 OECD, Digital transformation in the age of COVID-19, https://www.oecd.org/digital/digital-economy-outlook-covid.pdf (accessedon 22 March 2023).

17 Consilium, https://www.consilium.europa.eu/en/policies/cybersecurity/ (accessed on 20 March2023).

18 European.edu, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (accessed on 20 March 2023).

19 Consilium, https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/ (accessed on 20 March 2023).

20 Wahl T, Council conclusions on cybersecurity strategy, https://eucrim.eu/news/council-conclusions-on-cybersecurity-strategy/ (accessed on20 March 2023).

21 CIO, French regulator fines Google $271M over generative AI copyright issue, https://www-cio-com.cdn.ampproject.org/c/s/www.cio.com/article/2069449/french-regulator-fines-google-271m-over-generative-ai-copyright-issue.html?amp=1 (2024).

22 Ramo S, National security and our technology edge, https://hbr.org/1989/11/national-security-and-our-technology-edge (accessed on 20 March 2023).

23 Zeng F *et al.*, The Role of information systems in the sustainable development of enterprises: A systematic literature network analysis, https://hbr.org/1989/11/national-security-and-our-technology-edge (accessed on20 March 2023).

24 Iancu A &Kappos D J, U.S. Intellectual property is critical to national security, https://perma.cc/DG4H-S48L (accessed on 12 July 2021).

25 Singer J W *et al*., Property Law: Rules, policies, and practices 175 (Rachel E. Barkow *et. al.* eds., 7th ed. 2017).

26 Singer P W, Military robots and the Laws of War, https://www.brookings.edu/articles/military-robots-and-the-laws-of-war/ (accessed on 22 March 2023).

27 28Turunen A, The broader challenge of Russian Electronic Warfare Capabilities, https://www.jstor.org/stable/10.2307/resrep24241.6 (accessed on 22 March 2023).

28 Atomic archive, https://www.atomicarchive.com/science/fusion/h-bomb-basics.html (accessed on 22March 2023).

29 US Department of Education, https://nces.ed.gov/pubs98/safetech/chapter6.asp (accessed on 20 March 2023).

30 *Alice Corp* v *CLS Bank Int'l*, 134 S. Ct. 2347, 2354–55 (2014).

31 Laufman D H, Casino J M & Kasdan M J, The Department of Justice's National Security Division Chief addresses China's campaign to steal U.S. intellectual property, *National Law Rev*iew, 2021, 288.

32 UNCTAD, https://unctad.org/system/files/official-document/tir2018_en.pdf (accessed on 20 March 2023).

33 UNCTAD, https://unctad.org/system/files/official-document/ditcclp20082_en.pdf (accessed on 22 March2023).

34 NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf (accessed on 22March 2023).

35 Forest Hare, The cyber threat to national security: Why can't we agree, https://ccdcoe.org/uploads/2018/10/Hare-The-Cyber-Threat-to-National-Security-Why-Cant-We-Agree.pdf (accessed on 22 March 2023).

36 Forbes, https://www.forbes.com/2011/09/27/forbes-india-hacker-haven-cyber-crime-hot-bed.html (accessed on 22 March 2023).

37 Council on Foreign Relations, https://www.cfr.org/cyber-operations/ghostnet#:~:text=GhostNet%20was%20a%20large%2Dscale,on%20governments%20in%20Southeast%20Asia (accessed on 20 March 2023).

38 OECD, https://www.oecd.org/g20/ (accessed on 20 March 2023).

39 Williams R D, Reckoning with cyber-policy contradictions in great power politics, https://www.brookings.edu/techstream/reckoning-with-cyberpolicy-contradictions-in-great-power-politics/ (accessed on 20 March 2023).

40 OECD, https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf (accessed on 20 March 2023).

41 Department of Justice, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (accessed on 22 March 2023).

42 Ray A, Cybersecurity design engineering, https://www.sciencedirect.com/topics/computer-science/stuxnet (accessed on 22 March 2023).

43 Osborne C, Cybersecurity 101: Protect your privacy from hackers, spies, and the Government, https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/ (accessed on 22 March 2023).

44 Europe, EU, https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf (accessed on 22 March 2023).

45 Schrems II case, Case C-311/18.

46 *The Hindu Business Line*, https://www.thehindubusinessline.com/news/national/how-the-it-sector-has-emerged-as-a-pillar-of-modern-india/article32357389.ece (accessed on 23 March 2023).

47 National Cyber Security Policy, 2013, https://www.meity.gov.in/content/national-cyber-security-policy-2013-0#:~:text=1)%20To%20develop%20bilateral%20and,Agencies%20and%20the%20judicial%20systems (accessed on 22 March 2023).

48 Duggal P, India needs a dedicated Cyber Security Law, https://www.tribuneindia.com/news/comment/india-needs-a-dedicated-cyber-security-law-216669 (accessed on 22 March 2023).

49 Ramcharan R, Intellectual property and security: A preliminary exploration, contemporary Security Policy, 26 (1) (2005) 126, DOI: 10.1080/13523260500116117.

50 Patent Attorney Axel H Horns', Patents, state secrets, and the threat of terrorism, Law, http://www.ipjur.com/2003/09/patents-state-secrets-and-threat-of.php3.

51 Rana N, 3X increase in cyber-attacks results in increased budgets and attention on cyber security issues: ETILC Members, https://economictimes.indiatimes.com/news/company/corporate-trends/3x-increase-in-cyber-attacks-results-in-increased-budgets-and-attention-on-cyber-security-issues-etilc-members/articleshow/83949181.cms (accessed on 23 March 2023).

52 *Financial Express*, https://www.financialexpress.com/defence/indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need/2304053/ (accessed on 23 March 2023).

53 Rai C & Burman A, *JPC* v *PAC*, https://prsindia.org/theprsblog/jpc-vs-pac (accessed on 23 March 2023).

54 Meit Y, https://www.meity.gov.in/content/national-cyber-security-policy-2013-0 (accessed on 23 March 2023).

55 Yalavarthy A S, Aadhaar: India's National Identification System and ConsentBased Privacy Rights, https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance (accessed on 23 March 2023).

56 Hanna K T, https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008 (accessed on 23 March 2023).