ieee.es
Instituto Español de Estudios Estratégicos

Analysis
Paper

[Visit the WEBSITE]
[Receive the E-NEWSLETTER]

37/2022 May de 2022

Javier Fernández Aparicio

**Cybersecurity in India:
bilaterality and transformation**

Cybersecurity in India: bilaterality and transformation

Abstract:

With the onset of the pandemic crisis in early 2020, which brought about a quantitative increase in the use of the Internet and its applications, plus the cybersecurity challenges that this entails, including attacks on critical infrastructure, India is facing the need to update its National Cybersecurity Policy, which dates back to 2013, developing a strategy to prevent threats from cyberspace. All this, at a time when Prime Minister Modi's government has made an effort to reach bilateral agreements on the matter with third countries, in counterweight to Chinese influence, both in the Indo-Pacific space and globally, including cyberspace, currently considered the fifth domain in the field of warfare. The war in Ukraine has strengthened this line of bilateral international commitments, influencing its cybersecurity and technology relationship with Russia. In addition, India is currently a key producer country in the growing industry 4.0 and in the entire economy that moves around it.

Keywords:

India, Cybersecurity, Cyberspace, China, Indo-Pacific, Russia

NOTE:** The ideas contained in the ***Analysis Papers are the responsibility of their authors. They do not necessarily reflect the thinking of the IEEE or the Ministry of Defence.

Ciberseguridad en la India: bilateralidad y transformación

Resumen:

Con el inicio de la crisis de la pandemia, a principios de 2020, que supuso el aumento cuantitativo del uso de Internet y sus aplicaciones, más los retos en ciberseguridad que esto conlleva, incluyendo ataques a infraestructuras críticas, la India se enfrenta a la necesidad de actualizar su Política Nacional de Ciberseguridad, que data de 2013, desarrollando una estrategia en la prevención de amenazas desde el ciberespacio. Todo ello, en unos momentos en los que el gobierno del primer ministro Modi se ha esforzado para llegar a acuerdos bilaterales en la materia con terceros países, en contrapeso a la influencia china, tanto en el espacio Indo-Pacífico, como a nivel global, incluyendo el ciberespacio, considerado actualmente el quinto dominio en el ámbito bélico. La guerra en Ucrania ha fortalecido esta línea de compromisos internacionales bilaterales, influyendo en su relación en ciberseguridad y tecnología con Rusia. Además, la India en la actualidad es un país productor clave en la creciente industria 4.0 y en toda la economía que se mueve a su alrededor.

Palabras clave:

India, Ciberseguridad, Ciberespacio, China, Indo-Pacífico, Rusia

How to cite this document:

FERNÁNDEZ APARICIO, Javier. *Cybersecurity in India: bilaterality and transformation*. Documento de Análisis IEEE 37/2022. https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA37_2022_JAVFER_India_ENG.pdf y/o enlace bie[3] (consultado día/mes/año)

Introduction

With the impact of the COVID pandemic and events in Ukraine, the geostrategic position of powers such as China and India is being analysed globally for its importance beyond the Indo-Pacific space, where both countries play a key role that undoubtedly has its continuity in the world order. The outward-looking positions of India and China reflect their own relationship, two gigantic spheres of political, economic, military and cyber power facing each other. We must remember that they are close neighbours with a common border of nearly 4,000 kilometres, the so-called Line of Actual Control (LAC), including the disputed region of Kashmir. Border incidents between India and China have been arising for decades, and of some severity in recent years, such as events on 15 June 2020 in the Aksai Chin region, which resulted in the deaths of military personnel from both countries, and which sources from India claim gave rise to a series of cyber-attacks and disinformation campaigns from China and Pakistan[1].

The rapid rise of China's presence in the Indo-Pacific, mirroring its global presence, has thus activated and led to greater closeness —although still far from close collaboration— of the countries that make up the Quad: the security forum formed by the United States, Japan, Australia and India itself[2]. Also, an Indo-US bilateral rapprochement was observed during 2015-2016, seeking to counterbalance China's pre-eminence in the region, symbolised by trade[3] and security cooperation. A contract is currently being negotiated to supply F-18 fighters for the planned Indian aircraft carrier *INS Vikrant*[4]. The role of cybersecurity is paramount within these military and defence capabilities, and cooperation between India and the United States in this area is also taking shape.

Another key factor, more internal and backed up by statistical studies, is the growing mass Internet use and importance throughout India, promoted by the government as part of the country's modernisation. This is an accelerating phenomenon since 2020.

[1] NANDINI, Navashree: India-China Faceoff: Chinese mouthpiece silent on casualties; its journalists say 5 dead (republicworld.com) (16/06/2020. Accessed on 28/04/2022). According to a government official, Chinese and Pakistani activists had started social media campaigns to allegedly spread misinformation against India. In RAIBAGI, Kashyap: India's Current Cybersecurity Policy & How It Was Impacted By COVID (analyticsindiamag.com) (05/12/2020. Accessed on 11/05/2022).

[2] HERRERA PILAR, Mikel. *El Quad en la era post-COVID: más allá del desafío chino*. IEEE Opinion Paper 102/2021. http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO102_2021_MIKHER_Quad.pdf (Accessed on 26/04/2022).

[3] JUSTER, Kenneth I: It's time for the US and India to talk trade | Foreign Affairs (foreignaffairs.com) (14/04/2022. Accessed on 26/04/2022).

[4] La India se debate entre cazas F-18 y Rafale para su nuevo portaaviones (infodefensa.com). (18/04/2022. Accessed on 26/04/2022).

Cybersecurity in India

India's global impact on Internet use is so significant that in this already populous country of 1.4 billion, its current 658 million Internet users make it the second largest country in the world, second only to China (with one billion) and double the 300 million plus of the United States.

Further evidence of the magnitude of Internet use in India is that of these 658 million users, 467 million are also social network users, which means that 33.4 per cent of the total Indian population, in practice one third, use social networks and are online. There are, however, substantial differences in this demand for the Internet, as well as a digital divide; the former is centred on large cities, whose population is 36% of the total, compared to the rural population, which will account for 65% at the beginning of 2022[5].

Precisely to alleviate this digital divide, in 2015 the government launched the 'Digital India' project, an initiative with multiple stakeholders, from the economic to the technological sector, which requires heavy investment and is a priority, as demonstrated by its direct dependence on the Prime Minister himself, Narendra Modi. 'Digital India' set out three national cyber objectives[6]:

1. Creation of a digital infrastructure for public services, reaching the entire country.
2. Establishment of a legal framework for the governance and cybersecurity of these services.
3. Digital empowerment of Indian citizens and businesses, accessing the Web from anywhere.

In practice, 'Digital India' entailed the development of several secondary projects to advance the digitisation of the administration, including defence and security, as well as connecting rural areas with fibre optics. These projects were opened to private investment for implementation. Connecting all of India's enclaves involves a titanic outlay and effort. In this regard, 'Bharat Net' is the main plan developed by the Department of Electronics and Information Technology, part of the Ministry of Communication and Information Technology, which is largely responsible for 'Digital India'. The plan aims to every Gram panchayats in the country, the basic municipal institution in India's nearly 625,000

[5] Data from January 2022. Digital 2022: India — DataReportal – Global Digital Insights (Accessed on 20/04/2022).

[6] Vision and Vision Areas | Digital India programme | Ministry of Electronics and Information Technology (MeitY) Government of India (digitalindia.gov.in) (Accessed on 24/04/2022).

villages. By the end of February 2022, 'Bharat Net' had installed more than 36,000 kilometres of fibre optics across the country, and set up nearly 105,000 WiFi hotspots[7].

One of the consequences of this expansion in rapid Internet access, from government to individuals, with a logical multiplication of downloads, applications and services, is that India must also address a vast cyberspace from a security perspective.

According to a study by Comparitech, in 2019, India ranked 15th in countries with poor cyber security. The report's conclusion is clear: India ranks as one of the least cyber-secure countries in the world, in contrast to its weight in the international arena and its importance in the Industry 4.0 economy[8]. The government has made progressive efforts in this regard over the last three years, as cyberspace is an unavoidable necessity for the country's national security.

India's national cybersecurity policy

There is a certain lack of clarity about cybersecurity regulations and competent bodies in India. The main consequences of this are overlapping powers and an almost unanimous demand from Indian society for greater transparency and centrality in this area, especially with regard to data protection and privacy of companies and individuals, as cases of cyber espionage have come to light[9].

The Indian legal framework dates back to the Telegraph Act of 1885, which allowed government authorities to access private communications and identification data, albeit under certain circumstances and always in the theoretical interest of national security. India's specific cybersecurity policy dates back to 2000, when the Information Technology Act (known as the IT Act) was enacted, regulating electronic transactions and digital communications, with an emphasis on data protection and the then emerging cybercrimes. The law provided for its periodic review by a commission of experts in different fields and has had several addenda, the last one in 2011[10].

Since 2006, this IT Act standing committee had been calling for new legislation to govern cyberspace, addressing the phenomena of cyberterrorism, cybercrime, cross-border

[7] According to figures estimated by the Ministry of Electronics and Information Technology, as reported in *Vikaspedia*, the information database maintained by the Government of India since 2014. Bharat Net — Vikaspedia (Accessed on 20/04/2022).

[8] India ranks among the worst in the world for cybersecurity. *FRPT- Software Snapshot*. February 2019:2. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=135716406&lang=es&site=ehost-live (Accessed on 09/05/2022).

[9] BAJORIA, Jayshree: RAW: India's External Intelligence Agency | Council on Foreign Relations (cfr.org) (07/11/2008. Accessed on 09/05/2022).

[10] SUBRAMANIAN, Aditi: Cybersecurity Report 2022 India (iclg.com).

cybercrime and introducing the term Critical Information Infrastructure to define for the first time a cyber resource of national security impact[11].

Recognising this increasingly urgent need for cybersecurity, in addition to responding to allegations of spying by the US National Security Agency on various Indian government officials[12], the then Ministry of Communication and Information Technology drafted the Indian National Cybersecurity Policy (INCP) in July 2013, with a key objective: to achieve a secure cyberspace in India, both for the institutional and private spheres, i.e. for all online operations by Indian citizens and businesses.

The document also included other missions such as protecting the country's critical infrastructure; preventing and responding to cyber threats from abroad; and promoting research and development of its own security technologies, so as not to depend on foreign countries or companies. A so-called ‘national ecosystem’ was created to ensure cybersecurity, designating a rapid response team to potential threats in cyberspace under the umbrella of a new agency, the National Critical Information Infrastructure Protection Centre (NCIIPC).

A single cyber command for the Indian Armed Forces was also planned, although neither the location nor the hierarchical structure of the command was defined[13].

In 2019, India's historic National Congress party, a rival to Prime Minister Modi's Bharatiya Janata Party, commissioned a report on the state of national security from prestigious retired Lieutenant General Deependra Singh Hooda, who called for a comprehensive review of the country's cybersecurity policy, along with greater investment in cybersecurity. The paper concluded that India needed a single cyber command and warned that the country's technology was ill-equipped to deal with conflicts in cyberspace[14].

Over time, as a consequence of the pandemic and the aforementioned quantitative increase in Internet use and its risks, more and more sectors have been calling for an updated National Cybersecurity Policy. Although there are some cooperative projects between the Ministry of Electronics and Information Technology and the Ministry of

[11] Cyber security framework under the IT Act in India | Ikigai Law (23/06/2020. Accessed on 05/05/2022).

[12] HARRIS, Shane: What Was Edward Snowden Doing in India? – Foreign Policy (13/01/2014. Accessed on 05/05/2022).

[13] SANJIV, Tomar: National Cyber Security Policy 2013: An Assessment | Manohar Parrikar Institute for Defence Studies and Analyses (idsa.in) (24/04/2013. Accessed on 29/04/2022).

[14] PANDEY, Shreya: The Hooda document: expanding the contours of ‘national security’ (ipleaders.in) (17/08/2020. Accessed on 12/05/2022).

Information and Broadcasting, these are more a matter of various guidelines or declarations of intent, without much practical consequence[15].

In the strict matter of defending cyberspace, the 2013 Indian National Cyber Security Policy contains guidelines to protect all Indian users —small and medium-sized businesses, plus citizens— from threats. It also promotes public awareness of the importance of cybersecurity; advocates a legal environment to prosecute cybercrime, which is not yet in place; and recommends the development of network and critical infrastructure protection plans. Finally, it calls for its own technological research, so as not to depend on an external actor and, most importantly, it calls for bilateral agreements and treaties on cybersecurity with third countries, which has been implemented[16].

India's cybersecurity infrastructure

India has a number of national bodies to ensure the cybersecurity framework for critical infrastructure, both public and private. According to his own statements, according to Prime Minister Modi, cybersecurity is a priority not only from a military or war perspective, but also because cyber threats have the potential to seriously affect society as a whole, the economy and, ultimately, the country's development[17].

There is a certain lack of clarity in the competences of the main bodies that overlook Indian cyberspace, the main centres being:

- The **National Technical Research Organisation (NRTO)**. The leading institution in the field of cybersecurity and intelligence gathering, reporting since 2004 to the National Security Adviser in the Prime Minister's Office, when it was still called the National Technical Facilities Organisation. It obtains information from a variety of sources in intelligence, data capture and collection, cryptography, space detection and surveillance, satellite intelligence, internet monitoring and the development of cybersecurity software. It transfers data to the Indian Administration, including the Armed Forces, although organically the NRTO is not related to them[18].

[15] Data Security Council of India: National Cyber Security Strategy 2020 DSCI submission.pdf (Accessed on 11/05/2022).

16 RAIBAGI, Kashyap (op. cit.).

[17] BHARDWAJ, Ananya: India to get new, 'robust' cyber security policy soon, says PM Modi (theprint.in) (15/04/2022. Accessed on 11/05/2022).

18According to statements by former NSA analyst Edward Snowden, the US security agency is actively collaborating with the NRTO as part of SIGINT Seniors Pacific (SSPAC), an international counter-terrorism platform comprising the United States, Australia, Canada, France, India, South Korea, New Zealand, Singapore, Thailand and the United Kingdom. BARUAH, Sanjib Kr: 'India joined US-led top secret alliance in 2008' (asianage.com) (10/03/2018. Accessed on 21/04/2022).

The NTRO also includes two agencies with cybersecurity competences in its organisation chart. One is the **National Critical Information Infrastructure Protection Centre (NCIIPC)**, which since January 2014 provides specific protection of critical infrastructures against cyber-attacks, including transport, telecommunications, finance, energy facilities and government institutions. Its main mission is to prevent 'unauthorised access, modification, unauthorised use or disclosure, disruption or incapacitation' of relevant information of these critical infrastructures[19].

The second centre under NTRO authority is the **National Institute of Cryptology Research and Development (NICRD)**, a cryptology research organisation dating back to 2007; its main function is secure encryption for cyber applications in critical infrastructures, both public and private.

- The **National Cyber Coordination Centre (NCCC)** is an agency created in 2014, as it was envisaged in the National Cyber Security Policy of a year earlier, as part of the Ministry of Home Affairs. The NCCC is responsible for raising awareness in Indian society about the importance of cybersecurity and coordinates the work of various state agencies in this field. Like the NTRO, it also monitors the network, acting as a theoretical 'first firewall' against cyber threats, and develops strategies to prevent cyber-attacks. It is under the authority of a national cybersecurity coordinator. In the absence of specific regulation, the NCCC has been accused of mass cyber espionage on Indian citizens[20].
- **CERT-In** is a Ministry of Information Technology and Electronics department that has existed since 2003 and is responsible, for example, for the 'Digital India' project. It issues instructions to block malicious websites, as its aim is to make cyberspace safe, but it focuses mainly on private internet service providers and companies in the country, which it tries to prevent and defend from cyber-attacks[21].
- The **Research and Analysis Wing** (RAW) is India's premier intelligence agency focused on foreign policy analysis in relation to national security, particularly in relation to Pakistan and China. Cybersecurity issues have logically become very important,

[19] National Critical Information Infrastructure Protection Centre, Government of India (nciipc.gov.in) (Accessed on 25/04/2022).

[20] NIGAM, Aditiya: Hacking India's Democracy – From Monitoring Metadata to Spying Real Time: C.P. Geevan | KAFILA – COLLECTIVE EXPLORATIONS SINCE 2006 (26/07/2021. Accessed on 10/05/2022).

[21] Indian - Computer Emergency Response Team (cert-in.org.in) (Accessed on 25/04/2022).

and proof of this is that it has its own section for technological issues. The relevance of the RAW, created in 1968 but whose roots can be traced back to pre-independence times, means that, like the NTRO, it reports directly to the Prime Minister's Office[22].

Cybersecurity incidents in India

The first incident is the increase in cybercrime in India during 2021, which includes serious allegations that various government cybersecurity agencies have been monitoring and spying on the devices of thousands of Indian citizens. In 2018, the Ministry of Home Affairs approved a directive authorising the interception of any information received or stored in official bodies, including police sources and files, which led to the directive being challenged before the Supreme Court by a citizens' platform on the grounds that it clearly violated the right to privacy.

India has not been spared the controversy over the use of Israeli Pegasus software. Some sources claim that devices of some journalists and political opponents have been spied on. To date, the matter is still being dealt with by the courts[23].

During 2021, 52% of major Indian corporations suffered some type of cybersecurity incident. The most important was the breach of the passport data of more than four million Air India passengers when the airline's data provider, SITA, was hacked[24]. In another mass cyber-attack in May 2021, the personal data of some 180 million customers of the popular restaurant chain, Domino's Pizza, were disclosed[25].

There were also cybersecurity incidents in the public sphere; for example, the COVID-19 test results of thousands of citizens were released without respect for their privacy following a cyber-attack on the Indian healthcare system's website. Another relevant personal data disclosure incident occurred in late 2020. This was the enactment by the Ministry of Agriculture and Farmers' Welfare of the so-called ‘Agriculture Acts’. Theoretically, it aimed to modernise the country's agricultural processes, including the rapid buying and selling of produce over the Internet. This procedure was contested by some of the rural population, due to the impossibility of accessing the Internet or the lack

[22] Research and Analysis Wing [RAW] - Indian Intelligence Agencies (globalsecurity.org) (Accessed on 25/04/2022).
[23] DHILLON, Amrit & SAFI, Michael; Indian supreme court orders inquiry into state’s use of Pegasus spyware | India | The Guardian (27/10/2022. Accessed on 10/05/2022).
[24] SATIJA, R.: Cyber-Attack on Air India Led to Data Leak of 4.5 Million Fliers. *Bloomberg.com*, *[s. l.]*, 2021. https://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=150446593&lang=es&site=ehost-live (Accessed on 10/05/2022).
[25] VACHHATANI, Jitesh: Domino's India faces cyber attack; data of 18 cr orders, including personal info, leaked (republicworld.com) (23/05/2021. Accessed on 11/05/2022).

of digital skills. The Ministry included an online form to access certain grants, where the personal data of the applicants had to be specified. The form contained a link that downloaded a ransomware that would disable the petitioners' computers, who would also receive a message asking for a ransom to restore the computers, while a manifesto against the aforementioned 'Agriculture Acts' was read out [26].

Another cyber risk is investment in the Indian cryptomarket, which has made it one of the world's cryptocurrency hubs by 2021. This growing Indian market is a major attraction for foreign investors, but also for fraudulent activities, whether payments for criminal activities, or a hacker from Bangladesh who had managed to obtain sensitive information from Indian government portals —a case that is still open— including some Indian political officials involved[27].

Faced with the threats of cybercrime in this field, the government is designing new provisions to stabilise the activity of this cryptocurrency market, especially from a fiscal point of view and also with regard to digital tokens, trying to reduce this highly speculative trade and, in addition, increasing public revenue in this way[28].

Indian international cooperation in cybersecurity

In the international context, since 2015, India and the US strengthened their collaboration in the fight against cybercrime, inaugurating a policy of India's international bilateral agreements on cybercrime, which have resulted in a common framework for cyber cooperation[29]. In the summer of 2016, guidelines were signed in New Delhi to share real-time information and cooperate on joint research, including on cybersecurity products, with a fluid dialogue between the responsible agencies in each country[30]. Both the United States and India seem to have a common goal on the horizon: China. It should be recalled that the US ban on imports of Chinese hardware and applications in 2020 was followed

[26] SUBRAMANIAM, Aditi (op. cit. p.8).

[27] BANERJEE, Swagata: Priyank Kharge targets BJP over alleged Bitcoin Scam: 'Why was Hacker granted bail?' (republicworld.com) (10/11/2021. Accessed on 11/05/2022).

[28] Investment in Indian crypto market will rise - Oxford Analytica Daily Brief (oxan.com). (07/04/2022. Accessed on 21/04/2022).

[29] Joint Statement—2016 United States-India Cyber Dialogue. *Daily Compilation of Presidential Documents*, *[s. l.]*, p. 1–2, 2016. https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=118809843&lang=es&site=ehost-live (Accessed on 11/05/2022).

[30] Framework for the U.S.-India Cyber Relationship - U.S. Embassy & Consulates in India (usembassy.gov) (30/08/2016. Accessed on 10/05/2022).

by the same restriction in other countries, including India, which is an example of a digital and trade war between the two countries[31].

This type of bilateral cybersecurity understanding has been repeated with other countries. In 2018, the Israeli and Indian prime ministers signed, among other agreements, a cooperation agreement on cybersecurity. A year earlier, a memorandum of understanding on cybersecurity was signed between India and Spain, taking advantage of Prime Minister Modi's visit to Spain in May 2017. This roadmap is the seed for an Indo-Spanish alliance in this area, which also includes technological cooperation[32].

In the Indo-Pacific region, cybersecurity saw closer ties between India and Australia, with a bilateral strategic partnership in 2020, where one of the priorities was common cybersecurity for both countries. In addition, Indo-Australian technology company partnerships were also sought to address cybersecurity and the partner economy from a joint perspective, with a focus also on potential cyberthreats from China[33].

In October 2021, senior representatives from 25 countries, including Southeast Asian countries grouped in ASEAN, the United States, the European Union and India, met in a virtual session to take common action against ransomware, recognising that this cybercriminal practice is one of the most significant threats on a global scale. The meeting established a principle of agreement to involve both the public and private sectors in all countries, and agreed on the need to raise awareness of this and other cyberthreats and the need for protection[34].

Impact of the Ukraine conflict on relations with Russia and China

The ongoing conflict in Ukraine and India's ambiguous stance towards Russia has raised questions (as it refrained from condemning Russian aggression in the UN resolution on the matter) that also spill over into the field of cybersecurity. In September 2021, the two

[31] ALDAMA, Zigor: Primero EEUU y ahora India: la guerra digital contra China que está rompiendo internet (elconfidencial.com) (03/07/2020. Accessed on 11/05/2022).

[32] Spain-India Council Foundation: *Spain-India Report 2020*. Document 5. Science, technology and innovation. Madrid, 2020. http://www.spain-india.org/files/documentos/2021_DOC_5_INFORME_ESPANA_INDIA_(3).pdf (Accessed on 25/04/2022).

[33] PANKAJ, Jha & STAR, Shaun: *India–Australia. Defining New Horizons of Engagement*. Strategic Analysis, 45:5, 411-430 (2021). DOI: 10.1080/09700161.2021.1965344 (Accessed on 10/05/2022).

[34] Significance of India's Act East Policy and Engagement with ASEAN | Manohar Parrikar Institute for Defence Studies and Analyses (idsa.in) (07/12/2018. Accessed on 12/05/2022).

countries met to agree on a joint policy, along the lines of other bilateral agreements, to prosecute cyberspace crimes that affect them both[35].

While this somewhat ambiguous Indian position may appear to be an element of dissent, at least within the Quad group of countries, it is most likely a minor discrepancy with respect to the other major challenge of Chinese hegemony[36].

For decades, Russia and India have been close partners in securing each other's interests, both regionally and globally. New Delhi recently allowed Moscow to invest in Indian public debt funds, imported more Russian oil, and today may be considering an alternative payment system for its imports and exports that would circumvent international sanctions on Russia for its invasion of Ukraine[37]. For their part, Indian companies participate in the Russian technology ecosystem, and today's mass exodus of Western technology companies from Russia further opens a door to expand Indian participation in other markets, such as the cloud computing segments —taking advantage of Google Cloud and similar companies having discontinued their services— or smartphone business activities. However, the current situation is highly complex and changing in this Indo-Russian technological and commercial relationship[38].

Regarding China, as we have discussed, India has a strategy to strengthen the country's cybersecurity in the face of alleged Chinese intrusions that, according to some sources, could have attempted to affect several critical infrastructures, such as the stock exchange or power supply[39].

The technological relationship between the two countries has taken a considerable turn, also as a result of India's attempt to export its products and services in relation to Industry 4.0, and not to depend on the foreign market, especially China.

Prior to 2020 and over the previous five years, China had invested heavily in the Indian technology sector as a prelude to its Belt and Road Initiative (BRI), China's strategy to invest Chinese capital in the infrastructure of several foreign countries, including those in

[35] Russia, India ready to cooperate on cybersecurity. *Russia & CIS Military Newswire* (07/09/2021). https://www.proquest.com/wire-feeds/russia-india-ready-cooperate-on-cybersecurity/docview/2569687422/se-2?accountid=32797 (Accessed on 11/05/2022).

[36] CHANDRASHEKHAR OAK, Niranjan: Quad and the Ukrainian Crisis (idsa.in). Issue Brief MP-IDSA 22/03/2022 (Accessed on 26/04/2022).

[37] IVASHENTSOV, Gleb A.: *Russia-India: Strategic Partnership, Not Alliance*, Strategic Analysis (2020). DOI: 10.1080/09700161.2022.2039579 (Accessed on 12/05/2022).

38 Western sanctions alter Russia's technology strategy - Oxford Analytica Daily Brief (oxan.com) (12/04/2022. Accessed on 21/04/2022).

[39] CHAUDHARY, A.: China Hacking Concern Revives India Focus on Cybersecurity Plan. *Bloomberg.com*, [s. l.], 2021. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=149132917&lang=es&site=ehost-live (Accessed on 12/05/2022).

the Indo-Pacific, launched in 2013[40]. So far, it is estimated that nearly $4 billion has been invested by Chinese entities in technology companies, apps and start-ups developed in India[41].

The first tensions between the two giants arose in 2017 over Chinese investment in Pakistan's economic corridor through disputed Kashmir, which led to India's refusal to include its own representative in the BRI forum, a true sign of the Modi government's rejection of this expansive Chinese policy in a region that has always been unstable and conflictive[42]. The new geostrategic landscape opened up by the pandemic crisis and the war in Ukraine has further strained the Indo-China relationship, as we saw at the beginning, including some border incidents, a shared reticence that also has its repercussions in the technology sector, trade and, of course, cyberspace threats.

Conclusions

In the area of cybersecurity, India has yet to revise its 2013 national cybersecurity strategy to bring it in line with the changing times. With hundreds of millions of users surfing in cyberspace, both in the public and private spheres, such an overhaul seems an unavoidable priority in the short term.

Yet India is increasingly committing resources to cybersecurity, cyber espionage and preventing cyberspace threats to critical infrastructure, sometimes taking advantage of a legal limbo concerning data protection and privacy of its citizens.

Despite the existence of various cybersecurity bodies, there is no central, unitary command that coordinates them, although the National Technical Research Organisation stands out for its competences.

On the international scene, there has been a strong partnership with the United States on cybersecurity since 2016, followed by a series of bilateral agreements between India and a number of countries, including Russia. In cyberspace, a confrontation with China can be observed, reflecting the struggle between the two countries in the Indo-Pacific and

[40] Since May 2018, the World Bank has been engaged in monitoring the BRI with standards on trade, investment, debt, procurement, environmental impact, poverty reduction and the state of global infrastructure. In RUTA, Michele: Belt and Road Initiative. *World Bank Brief* (29/03/2018). https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative?cid=EXT_WBEmailShare_EXT (Accessed on 28/04/2022).

[41] BHANDARI, Amit; AGARWAL, Aashna & FERNANDES, Blaise: Chinese investments in India - CIAO (ciaonet.org). *Gateway House: Indian Council on Global Relations* (Report No. 3, Map No. 10. February 2020. Accessed on 28/04/2022).

[42] DARSHANA, M. Baruah: India’s Answer to the Belt and Road: A Road Map for South Asia - Carnegie India - Carnegie Endowment for International Peace (08/2018. Accessed on 28/04/2022).

globally. These bilateral agreements in India are aimed at preventing cyber threats, primarily from China.

Finally, we must also take into account the growth of Industry 4.0 in India, including a multitude of companies dedicated to the manufacture of hardware and its components, software, applications, etc., which increasingly represent an important part of the Indian economy, a major global supplier and in open competition in international markets, especially with regard to China.

Javier Fernández Aparicio
IEEE Analyst.