Moving Forward EU-India Relations

The Significance of the Security Dialogues

edited by
Nicola Casarini, Stefania Benaglia and Sameer Patil

Edizioni Nuova Cultura

Output of the project "Moving Forward the EU-India Security Dialogue: Traditional and Emerging Issues" led by the Istituto Affari Internazionali (IAI) in partnership with Gateway House: Indian Council on Global Relations (GH). The project is part of the EU-India Think Tank Twinning Initiative funded by the European Union.

EU Public Diplomacy and Outreach in India and in the SAARC

First published 2017 by Edizioni Nuova Cultura

for Istituto Affari Internazionali (IAI)
Via Angelo Brunetti 9 – I-00186 Rome – Italy
www.iai.it

and Gateway House: Indian Council on Global Relations
Cecil Court, 3rd floor
Colaba, Mumbai – 400 005 India

ISBN: 9788868128531
Cover: by Luca Mozzicarelli
Graphic composition: by Luca Mozzicarelli

Table of Contents

Abstracts

1. Maritime Security and Freedom of Navigation from the South China Sea and Indian Ocean to the Mediterranean: Potential and Limits of EU-India Cooperation

by *Nicola Casarini*

Abstract: Maritime security is of increasing importance for the EU and India. The two partners are affected by both traditional and non-conventional security challenges, including piracy, human and drug trafficking and maritime terrorism. This led the EU to launch Operation Atalanta and the Indian Navy to carry out anti-piracy patrols in the Gulf of Aden. However, a far greater threat could arise from traditional power politics, i.e. inter-state conflict which could result in a blockade of key maritime routes, in particular in the South China Sea which is currently under the spotlight as territorial and maritime tensions have steadily increased, not least in light of China's growing assertiveness in the area. These evolving security dynamics should therefore invite EU and Indian policy makers to begin considering maritime policy and collaboration beyond the Indian Ocean – which so far has been the focus of their cooperation – to include the waters stretching from the Indo-Pacific to the Mediterranean, through the South China Sea, the Indian Ocean, the Arabian coasts, the Horn of Africa, the Red Sea and the Suez Canal. This Eurasian maritime space is also the area covered by China's new Maritime Silk Road which presents India and the EU with formidable opportunities, but also significant security challenges.

2. Maritime Security and Freedom of Navigation from the South China Sea and Indian Ocean to the Mediterranean

by *Vice Admiral Anil Chopra*

Abstract: Tackling traditional challenges of maritime security and maintaining freedom of navigation in the Indian Ocean region has assumed greater salience for both India and the EU. However, India has not viewed EU as a significant regional maritime player, save for limited counter-piracy operations. The EU has also not highlighted India's concerns on terrorism in its neighbourhood, or done enough to contain the very real possibility of an interstate conflict which can threaten regional stability. As a way forward, India and EU must focus on coordinating efforts to address maritime piracy, crime and terrorism through greater intelligence sharing and developing a common Maritime Domain Awareness. They should also collaborate on capacity-building in the Indian Ocean region and concentrate on issues like disaster management, early warning systems, maritime tourism and the Blue Economy.

3. India-EU Cooperation on Cyber Security and Data Protection

by *Sameer Patil, Purvaja Modak, Kunal Kulkarni and Aditya Phatak*

Abstract: India and Europe face common cyber threats – critical infrastructure protection, deep web, cyber crimes, espionage (commercial and strategic), and online radicalisation. Yet, cooperation between the two remains inadequate at present. A related issue has been the differences on India's data adequacy assessment which has posed difficulties for the Bilateral Trade and Investment Agreement negotiations. Therefore, India and the EU need to adopt a pragmatic approach towards addressing their cyber security challenges by fostering practical cooperation between their respective law enforcement agencies for cyber forensics and cyber intelligence sharing, establishing a dialogue on "Smart Cities," forging PPPs to raise encryption standards and promoting research on emerging technologies such as TOR and crypto currencies.

4. EU-India Cooperation on Cyber Issues: Towards Pragmatic Idealism?

by *Patryk Pawlak*

Abstract: As the two biggest democracies in the world, the European Union and India share many values and principles. Yet, their cooperation in several policy areas is undermined by suspicions resulting from questions about each other's real intentions and discrepancies between official discourse and concrete policies. The field of cybersecurity cooperation is not immune to these dilemmas. For instance, this is the case in their respective approaches to the multi-stakeholder model of Internet governance, sovereignty in cyberspace and the protection of human rights online (including the right to privacy). In an effort to overcome these differences, this paper calls for "pragmatic idealism" in EU-India relations that could be implemented through network diplomacy that reinforces trust and institutional dialogue needed for closer cooperation. The paper suggests that such network diplomacy could be particularly fruitful in fostering relationships between local authorities and cities, research communities, cyber respondents and track 1.5 diplomacy.

5. EU-India Cooperation on Space and Security

by *Isabelle Sourbès-Verger*

Abstract: As far as security is concerned, space definitely stands out as a critical emerging issue. Space is considered part of the "Sector Policy Cooperation" in the Agenda 2020 endorsed at the latest EU-India Summit on 30 March 2016, but is not included within the Security section even if it may contribute to some of those objectives. Setting aside the national dimension in defence matters, space cooperation represents an optimal choice for the EU-India Security Dialogue, especially considering global security issues such as climate change, natural disasters, the environment, water management, migrant flows, piracy and terrorism. This paper provides insight into the role and place of cooperation in Indian and EU space policies. It then examines the main opportunities for developing space

cooperation towards security on Earth. This raises the issue of security in space while taking into account natural and human threats as a new challenge for the EU-India Dialogue. An analysis of current opportunities will provide policy recommendations in order to initiate a deeper dialogue on this increasingly important dimension of EU-India cooperation.

6. Potential and Challenges of India-EU Space Cooperation

by *Chaitanya Giri*

Abstract: India-EU space cooperation predates the formation of the EU. At present, the bilateral space collaboration is nascent largely due to the EU's limited autonomy over its space programme. However, astro-geopolitics, an inevitable successor to geopolitics, requires confidence-building and further strengthening of bilateral linkages. It is important for India and the EU to engage in "scientific diplomacy" and regular multi-track dialogues to include space experts and private space companies from both sides. They can also cooperate on creating space situational awareness and exchanging knowledge and data on crisis management in space. Collaborating on joint ground stations such as Europe's ground station projects in Chile and new ground stations in India provides another opportunity to take forward the partnership.

7. India-EU Defence Cooperation: The Role of Industry

by *Sameer Patil, Purvaja Modak, Kunal Kulkarni and Aditya Phatak*

Abstract: Since 2004, India and EU have established multiple dialogue mechanisms, which convey a sense of common understanding on broader security dynamics, but for most part their approaches on key security issues have diverged. On defence, India has forged closer ties with the individual European countries than it has with the EU as a whole. India's military modernisation and "Make in India" offer many opportunities for the European defence companies in land, air, naval, and electronic sys-

tems. To realise those opportunities, EU should expand its political and strategic engagement with India by establishing specialised dialogue mechanisms including a Defence Trade meeting allowing defence companies from India and the EU to discuss possible collaboration, understand India's technological priorities and evaluate risks from the EU's dual-use technology regime.

8. EU-India Defence Cooperation: A European Perspective

by *Stefania Benaglia and Alessandro R. Ungaro*

Abstract: When looking at the European Defence and Technological Industrial Base (EDTIB) from India – where competition among global defence suppliers is fierce – there is a clear need to step up European coordination and integration. There are a number of mechanisms the European Union can put in place to stimulate fruitful competition amongst its defence providers and prove the value of EDTIB as a whole. Additionally, EU-India security dialogue can be enhanced by boosting coordination among EU Member States. This paper provides recommendations on how industrial cooperation in the defence sector can serve as a driver to enhance EU-India defence and security cooperation.

9. EU-India: Starting a More Adventurous Conversation

by *Shada Islam*

Abstract: Twelve years after they launched their strategic partnership, the EU and India appear ready to take their relationship into new and potentially more adventurous, exciting and mutually beneficial directions. The summit in March 2016 marked the beginning of a more mature and politically relevant dialogue between the EU and India. Implementation of the different priorities set out at the March summit, however, will require time, energy and effort to keep up the momentum. High-level summits should be held regularly – instead of at four-year intervals – so that

leaders can maintain contacts and build better relations. New areas of cooperation, including in the security sector, must be strengthened and quickly lead to real action. Given their different histories, identities and priorities, the EU and India will continue to disagree on many issues. Such differences, however, must not become an obstacle to better relations.

Introduction

Relations between India and the European Union (EU) have been growing in quantity and quality in the last two decades. Alongside the economic dimension, the political and security elements of the relationship have emerged as the most promising area for further collaboration between the two sides.

The basis of their political cooperation was laid in the Joint Political Statement of 1993 and the 1994 Cooperation Agreement, which took relations beyond trade and economic cooperation. In 2004, the two sides established the EU-India Strategic Partnership, based on the shared values and principles of democracy, the rule of law, human rights and the promotion of peace and stability. At the 13th EU-India Summit held in Brussels on 30 March 2016, leaders from the two sides adopted a Joint Declaration and endorsed the EU-India Agenda for Action 2020 which builds on the achievements of the 2005 Joint Action Plan, moving the relationship into the political and security-related policy domains.

Upgrading the policy dialogues on security cooperation is indeed an area which has the potential to significantly move forward the EU-India strategic partnership. The Agenda for Action 2020 states that the EU and India should: (i) strengthen their cooperation and work towards tangible outcomes on shared objectives of non proliferation and disarmament, counter-piracy, counter-terrorism and cyber security; (ii) deepen existing cooperation and consider cooperation in other areas mentioned in the EU-India Joint Action Plan, including promoting maritime security and freedom of navigation in accordance with International law (UNCLOS); (iii) enhance space cooperation including earth observation and satellite navigation for the strengthening of interaction between the India Regional Navigation Satellite System and EU's Galileo as well as joint scientific payloads.

In the framework of the EU-India Think Tank Twinning Initiative – a public diplomacy project aimed at connecting research institutions in Eu-

rope and India funded by the EU Delegation to India- a select pan-European and Indian group of experts was tasked by the Rome-based Istituto Affari Internazionali (IAI) and the Mumbai-based Gateway House: Indian Council on Global Relations (GH) to conduct research and provide policy recommendations on: (i) Maritime security and freedom of navigation; (ii) EU-India cooperation on cyber security and data protection; (iii) Space policy and satellite navigation cooperation; (iv) EU-India defence cooperation: the role of industry; and (v) EU-India relations: the challenges ahead.

Below are the joint recommendations presented for consideration to the EU and Indian policy makers.[1]

1 Maritime security and freedom of navigation

Nicola Casarini, Head of Programme Asia, Istituto Affari Internazionali, Rome
Vice Admiral Anil Chopra, Distinguished Fellow, International Security and Maritime Studies, Gateway House, Mumbai

Research questions: Are there conditions for expanding EU-India cooperation in the waters stretching from the Indo-Pacific to the Mediterranean? What are the implications of the changing dynamics in the South China Sea and of China's maritime ambitions for the EU-India maritime security relations? Is there room for a joint EU-India response?

Key policy recommendations

- Establish an EU-India High Level Dialogue on Maritime Cooperation. The two partners should move their partnership to a new level by broadening the scope of their current anti-piracy dialogue to other functional areas, including an assessment of the opportunities, and challenges of China's 21st century Maritime Silk Road initiative for both the EU and India;
- Conflict prevention in the Indo-Pacific is critical for both EU and India.

[1] For full list of policy papers and additional information on the initiative, please refer to the project webpage: http://www.iai.it/en/node/6650.

Hence, they should forge diplomatic cooperation to curb rogue states with the potential to do harm or escalate tensions;
- Develop interoperability and increase coordination between the EU NAVFOR and the Indian Navy, particularly in the field of maritime surveillance, counter-piracy, disaster relief efforts, as well as training and military exercises;
- Support freedom of navigation in the Indo-Pacific. This could be achieved by creating an EU-India Joint Working Group tasked to assess their respective interpretations of freedom of navigation, in view of the eventual issuing of joint declarations on the South China Sea.

2 EU-INDIA COOPERATION ON CYBER SECURITY AND DATA PROTECTION

Sameer Patil, National Security Fellow, Purvaja Modak, Researcher, Kunal Kulkarni, Senior Researcher, Aditya Phatak, Senior Researcher, Gateway House, Mumbai
Patryk Pawlak, Policy Analyst, European Parliament Research Service and member of the GFCE Advisory Board, Brussels

Research questions: What are the Indian and EU priorities on cyber security? How can the EU-India cyber security policy dialogue be advanced? What are the threats to critical infrastructure and business? How can the private sector and public sector jointly develop solutions to protect against cyber-attacks? How to counter the deep web?

Key policy recommendations

- Promote cyber threat intelligence sharing. European countries should be forthcoming in sharing their experiences with India on lessons learnt from past incidents, as part of the capacity building of the law enforcement agencies;
- Increase interaction between the Europol's E3C and India's proposed National Cyber Coordination Centre. Both sides could share their best practices and work on minimum standards for security and cyber forensics;

- Facilitate the creation of a Cyber Action Task Force at the international level. This proposed agency could be aligned with the CERTs in each country for coordination and information sharing;
- Develop cooperation on regulating the behaviour of non-state actors in the cyber space.

3 SPACE POLICY AND SATELLITE NAVIGATION COOPERATION

Isabelle Sourbès-Verger, Senior Research Fellow, Centre Alexandre Koyré, EHESS, Paris
Chaitanya Giri, Visiting Scientist, Solar System Exploration Division, NASA Goddard Space Centre, Greenbelt, MD, United States

Research questions: What is the state of EU-India space cooperation after the two sides signed an agreement on the joint development of Galileo (Europe's global navigation satellite system) in 2006? What are the prospects of further EU-India collaboration on space technology? What is the role of the aerospace industry? How to enable collaboration between Indian and EU space agencies/institutions on research, development and operations?

Key policy recommendations

- Establish a Joint Working Group to assess potential for collaborative projects on space surveillance;
- Increase coordination on crisis management by exchanging data on (almost) real-time information;
- Develop synergies between the EU's and India's scientific projects focusing on research and innovation in space.

4 EU-INDIA DEFENCE COOPERATION: THE ROLE OF INDUSTRY

Sameer Patil, National Security Fellow, Purvaja Modak, Researcher, Aditya Phatak, Senior Researcher, Kunal Kulkarni, Senior Researcher, Gateway House, Mumbai

Stefania Benaglia, Associate Fellow; Istituto Affari Internazionali, New Delhi; and Alessandro Ungaro, Researcher, Istituto Affari Internazionali, Rome

Research questions: What is the current state of EU-India defence cooperation? What are the most promising areas for cooperation between the Indian and EU defence companies? How can European companies contribute to the 'Make in India' initiative and stimulate Indian manufacturing? And what will be the benefits for the European defence companies?

Key policy recommendations

- Enhance EU's visibility and internal coordination on defence matters. This could be achieved by posting a permanent Security Advisor to the EU Delegation in New Delhi and appointing a desk officer in the European External Action Service in charge of coordinating European defence initiatives in India;
- Develop a normative framework for Government to Government (G2G) relations. This will give further meaning and content to the EU-India strategic partnership;
- Promote India-EU joint military exercises. India already holds military exercises with some individual EU member states. This could be taken to the next level by organising EU-India joint exercises for HADR and/or SAR operations, thus contributing to the interoperability between the two sides' military forces;
- Establish an India-EU Defence Trade Dialogue with the aim to help in evaluating the opportunities and challenges, of the EU's dual-use technology regime.

5 EU-INDIA RELATIONS: THE CHALLENGES AHEAD

Shada Islam, Director, Europe and Geopolitics, Friends of Europe, Brussels

Research questions: What is the current state, and future prospect, of the EU-India strategic partnership? What are the main challenges ahead?

Key policy recommendations

- Given their different histories, identities and priorities, the EU and India will continue to disagree on many issues. But differences must not become an obstacle to relations. In order to stay the course, both sides will have to avoid being distracted by other priorities and concerns. In order to keep their relations vital and relevant, the EU and India must continue to dialogue on all important matters of bilateral, regional and global concern. Having worked hard to establish the groundwork for a stronger and more diversified relationship, India and the EU must now demonstrate a determination to move forward and engage with each other over a sustained period.

1.

Maritime Security and Freedom of Navigation from the South China Sea and Indian Ocean to the Mediterranean: Potential and Limits of EU-India Cooperation

Nicola Casarini[*]

In the EU-India Agenda for Action 2020 adopted on 30 March 2016, it is clearly stated that the EU and India should

> strengthen cooperation and work towards tangible outcomes on shared objectives of [...] counter-piracy [...] Deepen existing cooperation and consider cooperation in other areas mentioned in the EU-India Joint Action Plan, including promoting maritime security [and] freedom of navigation in accordance with International law (UNCLOS).[1]

Maritime security is of increasing importance for the EU and India. The two partners are affected by both traditional and non-conventional security challenges, including piracy, human and drug trafficking, and maritime terrorism. Acts of piracy and terrorist activity continue to disrupt the sea lanes connecting the South China Sea to the Mediterranean, through

[*] Nicola Casarini is Head of Asia Programme at the Istituto Affari Internazionali (IAI). This paper is based on academic research and interviews with officials and experts. It has also benefited from the author's involvement in a number of policy-oriented conferences on Asia's security held in Europe and Asia. The author wishes to thank Lorenzo Mariani, Research Assistant in the Asia Programme at IAI, for his help during the research process.

[1] EU-India Agenda for Action-2020, 30 March 2016, http://www.consilium.europa.eu/en/meetings/international-summit/2016/03/20160330-agenda-action-eu-india_pdf.

the Indian Ocean, the Arabian coasts and East Africa. Incidents of piracy reached alarming levels in 2007-2008, leading the EU to set up Operation Atalanta and the Indian Navy to begin carrying out anti-piracy patrols in the Gulf of Aden.

The EU has a vested interest in a stable environment in the Indo-Pacific, given the importance of markets in the Far East for European industry. For India, the sea lanes of communication are crucial for its commercial and energy security.[2] More than 90 percent by value of India's trade is transported by sea.[3] In recent years, India's major maritime security concerns have not only been related to non-conventional issues, but also to traditional threats coming from Pakistan and China, as featured in the latest Indian Maritime Security Strategy released in late 2015.[4]

A far greater threat could indeed arise from traditional power politics, i.e., state-to-state conflict which could result, for instance, in a blockade of key maritime routes. The South China Sea is currently under the spotlight as territorial and maritime tensions have steadily increased among the resident countries. China, Vietnam, the Philippines, Malaysia and Brunei all have competing claims. China has backed its expansive claims with island-building and naval patrols. While the US has declared several times that it does not take sides in territorial disputes, the Obama administration has deployed military ships and planes near disputed islands on what it calls Freedom of Navigation Operations (FONOPs), to ensure access to key shipping and air routes. India has also stepped up its involvement in the South China Sea, while Europe has become preoccupied with the growing tensions in the area that could jeopardize its economic and strategic interests in the Far East.

This study asks the following questions: (a) How could the EU and India work together to ensure free movement of trade and freedom of navigation from the Indo-Pacific to the Mediterranean – i.e., the maritime area stretching from the Western Pacific to the Eastern shores of Africa,

---

[2] Kavalam Madhava Panikkar, *India and the Indian Ocean. An Essay on the Influence of Sea Power on Indian History*, London, Allen & Unwin, 1945. See also Robert D. Kaplan, *Monsoon. The Indian Ocean and the Future of American Power*, New York, Random House, 2010.

[3] Indian Department of Defence, *Annual Report 2015-2016*, March 2016, p. 28, http://www.mod.gov.in/forms/List.aspx?Id=57&displayListId=57.

[4] Indian Ministry of Defence and Indian Navy, *Ensuring Secure Seas: Indian Maritime Security Strategy*, October 2015, https://www.indiannavy.nic.in/node/14305.

including the Arabian coasts, the Horn of Africa and the Red Sea, reaching the Mediterranean via the Suez Canal? (b) Is Beijing's new Maritime Silk Road – which traverses all the abovementioned waters and coasts – and growing assertiveness likely to impact, and to what extent, the business and security interests of Europe and India? (c) Is there the political will to upgrade and expand the EU-India counter-piracy policy dialogue to a fully fledged and structured maritime security cooperation mechanism that would address issues such as maritime governance and freedom of navigation, including the prospect of joint "freedom of navigation" operations in concerned areas?

The first part examines the maritime security strategies of the EU and of India, including discussion of their respective policies to fight piracy and maritime terrorism. The second part focuses on China's new Maritime Silk Road and the evolving security dynamics in the South China Sea, including discussion of European and Indian responses to those new dynamics. The third section is devoted to an assessment of the current military balance in the Indo-Pacific and the prospect for the emergence of a multilateral security framework. The last section offers a number of policy recommendations for consideration by those EU and Indian policy makers committed to fostering their security dialogue in the years ahead.

1.1 Europe's maritime strategy

In June 2014, the EU released its first ever Maritime Security Strategy[5] which clearly stated that Europe's maritime interests are fundamentally linked to the well-being, prosperity and security of its citizens and communities, as some 90 percent of the EU's external trade and 40 percent of its internal trade is transported by sea. Europe's economic security depends on open, safe seas and oceans for free trade, transport, tourism and ecological diversity, as well as for economic development.[6]

[5] Council of the European Union, *European Union Maritime Security Strategy* (11205/14), 24 June 2014, http://data.consilium.europa.eu/doc/document/ST-11205-2014-INIT/en.

[6] European Commission and High Representative of the Union, *For an Open and Secure Global Maritime Domain: Elements for a European Union Maritime Security Strategy* (JOIN/2014/9), 6 March 2014, p. 2, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52014JC0009.

The EU has identified a number of maritime security threats, including: (i) territorial maritime disputes, acts of aggression and armed conflict between States; (ii) maritime piracy and armed robbery at sea; (iii) terrorism and other intentional unlawful acts against ships, cargo and passengers, ports and port facilities and critical maritime infrastructure, including cyber-attacks on information systems; and (iv) cross-border and organized crime including seaborne trafficking of arms, narcotics and human beings. To address these threats, the EU has launched a number of missions in the last years.

In December 2008, the EU launched the European Union Naval Force (EUNAVFOR) Operation Atalanta, which was recently extended by the European Council until December 2018.[7] It has a number of objectives, including "the deterrence, prevention and repression of acts of piracy and armed robbery off the Somali coast."[8] Operation Atalanta operates in coordination with NATO's counter-piracy mission Operation Ocean Shield, the multi-national counter-piracy mission Combined Task Force 151 (CTF-151)[9] and independently deployed ships from, for instance, Russia, India and China. European countries participate in all of these operations, shifting between the different outfits on an irregular basis and sometimes acting alone.

Participation in EUNAVFOR goes beyond EU member states; its composition changes constantly due to the frequent rotation of units and its configuration varies according to the monsoon seasons in the Indian Ocean. However, it typically comprises approximately 1,200 personnel, 4-6 surface combat vessels and 2-3 maritime patrol and reconnaissance aircraft (MPRA). In addition to EUNAVFOR units, a considerable international military maritime presence is deployed in the area, consisting of the Combined Military Forces (CMF), NATO (Operation Ocean Shield) and independent national units from countries such as China, India, Japan, South Korea, Russia and others, all committed to counter-piracy, but with varying mandates and mission objectives.

---

[7] Council of the European Union, *Council Decision (CFSP) 2016/2082 amending Joint Action 2008/851/CFSP on a European Union Military Operation to Contribute to the Deterrence, Prevention and Repression of Acts of Piracy and Armed Robbery Off the Somali Coast*, 28 November 2016, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32016D2082.

[8] Ibid.

[9] For more information see the Combined Task Force official website: http://wp.me/P1248M-g.

In July 2012, the EU launched EUCAP Nestor, a civilian mission which assists host countries develop self-sustaining capacity for enhancement of maritime security. At its launch, EUCAP Nestor was mandated to work across the Horn of Africa and the Western Indian Ocean.[10] As of the end of 2015, following a strategic review of the mission, activities focus solely on Somalia (including Somaliland), with the Mission Headquarters currently located in Mogadishu.[11]

Counter-piracy efforts are a response to the larger concern of securing energy supplies in the western part of the Indian Ocean as oil tanks pass through the Strait of Hormuz and then the Suez Canal. Yet, the operations also serve to protect trade in goods, as cargo ships cross the Indian Ocean to reach the East Asian markets. Some of the biggest trading partners of the EU are located along the Eurasian coastline. Operation Atalanta – as well as the adoption of the EU Maritime Security Strategy in June 2014[12] – demonstrates the EU's commitment to addressing security challenges in a vast area that stretches from the Indian Ocean to the Suez Canal through East Africa.

Alongside the EU, some individual member states have also stepped up their involvement in maritime security issues. France, for instance, adopted in December 2014 its own maritime policy paper, the *National Strategy for the Security of Maritime Areas*, which includes the assertion that Paris is ready to enlarge the scope of its maritime operations in Asia to include freedom of navigation operations.[13] In the last years, France has held a number of joint naval exercises with India – for instance, the Varuna in 2010 – where the two navies would prepare to secure and re-open, if blocked, the sea lanes of communication in the Indian Ocean.

It remains to be seen whether other European maritime powers would

[10] Council of the European Union, *Council Decision 2012/389/CFSP on the European Union Mission on Regional Maritime Capacity Building in the Horn of Africa (EUCAP NESTOR)*, 16 July 2012, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32012D0389.

[11] EEAS, *EUCAP Nestor Mission Headquarters Moved from Djibouti to Mogadishu*, 2 October 2015, https://www.eucap-nestor.eu/en/press_office/news/1324.

[12] Council of the European Union, *European Union Maritime Security Strategy*, cit.

[13] French Government, *National Strategy for the Security of Maritime Areas*, 22 October 2015, http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2016/01/strategie_nationale_de_surete_des_espaces_maritimes_en_national_strategy_for_the_security_of_maritime_areas.pdf.

be willing to follow France, going beyond counter-piracy operations – so far limited to the waters off the Horn of Africa – to further engage with Asian partners, including the prospect of joining freedom of navigation operations in the Indo-Pacific. India, for instance, has joined the US-led freedom of navigation operations in the South China Sea since 2014, given the strategic significance that New Delhi accords to its surrounding waters.

1.2 India's maritime strategy

Prime Minister Narendra Modi views the Indian Ocean as a foreign policy priority, with maritime dominance apparently the goal as India seeks to confront piracy and terrorist activities – but also to counter China's expansionist policies in the area and keep Pakistan in check. Modi's first visit outside Delhi after his swearing-in ceremony was to go aboard the Indian aircraft carrier Vikramaditya off Goa in June 2014.[14] It is noteworthy that India is the only power in Asia (excluding the US) to possess such a landing platform.

In March 2015, Modi unveiled a four-part framework for the Indian Ocean, focusing on: (i) defending India's interests and maritime territory, in particular countering terrorism; (ii) deepening economic and security cooperation with maritime neighbours and island states; (iii) promoting collective action for peace and security; and (iv) seeking a more integrated and cooperative future for sustainable development.[15]

New Delhi's "blue water" ambitions were first outlined in its 2007 Maritime Security Strategy, after which it acquired a number of capabilities, including amphibious surface ships and nuclear-powered submarines. In 2013, New Delhi launched its first indigenous naval communication satellite, which further enhanced its capacity to monitor the entire Indian Ocean. In the wake of the 2008 Mumbai attack, India established the Sagar Prahari Bal, a maritime force protection group with 1,000 marines and 80 patrol boats, sustained by a maritime special operation unit, the

[14] Rahul Roy-Chaudhury, "Five Reasons the World Needs to Pay Heed to India's New Maritime Security Strategy", in *The Wire*, 22 December 2015, p. 2, https://thewire.in/?p=17741.

[15] Ibid.

2,000-marine Special Forces Marine Commando.[16] The development of these units suggests that India takes the threat of maritime terrorism and asymmetric warfare seriously. more integrated and cooperative future for sustainable development.

Pakistan, India's long-time rival, lacks the conventional naval forces to challenge New Delhi. With 10 frigates and 8 submarines, Pakistan has some ability to protect its coastline and inhibit an adversary's seaborne manoeuvrability. However, recent and likely future investment in Chinese-supplied frigates, missile craft and submarines could improve Pakistan's maritime protection capabilities.[17]

China's emergence as a major air/sea power – and also a potential source of aid to Pakistan – presents India with an ominous challenge. In its latest defence white paper (May 2015), the Chinese government outlined the importance of power-projection capabilities, emphasizing the requirements for offensive and defensive air operations, and "open seas protection."[18] Since 2008, China has sent nearly two dozen naval expeditions to the Indian Ocean, including Chinese nuclear submarines, ostensibly to counter piracy but implicitly to project its influence in the region.[19] Moreover, China is the largest arms supplier to India's neighbours and since 2013 the People's Liberation Army Navy (PLAN) has started an impressive programme of expansion, including port construction and upgrades at several locations around the Indian Ocean such as Karachi and Gwadar (Pakistan), Chittagong (Bangladesh), Kyaukpyu (Myanmar), and Hambantota and Colombo (Sri Lanka).[20]

Given these dynamics, it is not surprising that New Delhi and Beijing

---

[16] Anthony H. Cordesman and Abdullah Toukan, *The Indian Ocean Region. A Strategic Net Assessment*, Lanham, Rowman & Littlefield, August 2014, p. 244, https://www.csis.org/node/25176.

[17] International Institute for Strategic Studies (IISS), *The Military Balance 2016*, Abingdon, Routledge, 2016, p. 279.

[18] Chinese Ministry of National Defense, *China's Military Strategy*, May 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805_4.htm.

[19] Mohan Malik, "India's Response to the South China Sea Verdict", in *The American Interest*, 22 July 2016, http://wp.me/p4ja0Z-ACJ.

[20] International Center for Strategic Analysis (ICSANA), Gwadar Port: Implications for GCC and China, 2014, http://www.icsana.com/index.php?option=com_content&view=article&id=433&catid=9&Itemid=561&lang=en. Ruchir Sharma, *The Rise and Fall of Nations. Forces of Change in the Post-Crisis World*, New York, W.W. Norton & Co., 2016.

increasingly compete in the Indo-Pacific, especially as they scramble for energy resources and sea lane protection. India's suspicion about China's expansionist policy is not new. It dates back to the mid-2000, when Beijing developed a geo-political strategy, the so-called "string of pearls", consisting of a series of port facilities in Pakistan, Bangladesh, Sri Lanka, Myanmar, the Seychelles and the Maldives aimed at securing Chinese maritime interests in the area. These facilities were seen in New Delhi as an act of "encirclement". The "string of pearls" has now been revitalized and subsumed within Beijing's 21st century Maritime Silk Road – an initiative through which Beijing seeks to promote economic ties with the countries concerned, but also further its political influence and military presence.[21]

1.3 China's new Maritime Silk Road: Implications for the EU and India

China's new Silk Road, consisting of the Silk Road Economic Belt and the 21st century Maritime Silk Road – also known as the One Belt, One Road (OBOR) or simply the Belt and Road initiative – was unveiled by President Xi Jinping in late 2013. It is China's most ambitious geo-economic and foreign policy initiative in decades, aiming to connect China to Europe through South East Asia, Central Asia, the Indian Ocean, the Middle East and East Africa, covering areas hosting 70 percent of the global population, holding 75 percent of known energy reserves and generating 55 percent of the world's gross national product (GNP). The stated aim of this grandiose initiative is to boost connectivity and commerce between China and 65 countries traversed by the Belt and Road.[22]

China's total financial commitment to this initiative is expected to reach 1.4 trillion dollars in the coming years. Beijing has already committed around 300 billion dollars in loans and trade financing, a sum which includes a 40 billion dollar contribution to the Silk Road Fund for infra-

[21] Eva Pejsova, "Scrambling for the Indian Ocean", in *EUISS Briefs*, No. 4 (February 2016), p. 2, http://www.iss.europa.eu/publications/detail/article/scrambling-for-the-indian-ocean.

[22] Nicola Casarini, "When All Roads Lead to Beijing. Assessing China's New Silk Road and its Implications for Europe", in *The International Spectator*, Vol. 51, No. 4 (December 2016), p. 95.

structural development and 100 billion dollars in capital allocated to the China-initiated Asian Infrastructure Investment Bank (AIIB).

China's Maritime Silk Road was first charted during President Xi Jinping's visit to Southeast Asia in October 2013. The road takes inspiration from historical maritime trading routes connecting coastal China to the Mediterranean, through the South China Sea, the Indian Ocean, the Arabian coasts and East Africa. China's new sea-based Silk Road is taking the form of a network of ports and other coastal infrastructure projects. This grandiose initiative is driven by the Chinese government in conjunction with some giant state-owned enterprises. For instance COSCO, China's biggest shipping line, has taken minority stakes in terminals in Antwerp, Suez and Singapore and a majority stake (67 percent) in Piraeus Port in Greece, where it plans to invest 350 million euros over the next ten years, including building a dock that can handle mega-ships. China Merchants Holdings International has invested massively in Colombo (Sri Lanka) and has stakes in the port of Gwadar (Pakistan).

Securing Eurasia's sea lanes of communication has become a strategic priority for China, whose military has recently been granted the right to build logistics facilities in Djibouti. The base is expected to contribute to anti-piracy operations in the area, but also to protect China's strategic assets and cargo ships directed towards (or coming from) the European ports.

The Mediterranean has a key role to play in China's Maritime Silk Road, as the EU is today Beijing's most important trading partner. Between 2000 and 2015 Chinese trade towards the south of the Mediterranean grew tenfold, exceeding 50 billion euros and doubling in value each year. Today, China is the second trade partner for the area after the US and the first in terms of percentage growth rate.[23] China's growing interests in the area have led Beijing – together with Moscow – to hold their first ever joint military drills in the Mediterranean Sea in May 2015.

The doubling of the Suez Canal has further contributed to increasing China's strategic interest in the area. China already owns 20 percent of the Suez Canal Container Terminal, running one of the biggest terminals in Port Said, right at the entrance of Suez.[24] Beijing is also planning to

[23] SRM, *Italian Maritime Economy 2016*, Naples, Giannini, 2016, p. 15, http://www.srm-maritimeconomy.com/?p=17090.

[24] Ibid.

build or own (even partially) similar ports and logistics facilities in Iran and Saudi Arabia, after having invested massively in the Pakistani port of Gwadar, which is expected to be connected through a modern highway network to China's Xinjiang province, giving the landlocked Chinese region access to the Indian Ocean. There are also plans for a high-speed rail link running alongside the road as well as the construction of oil pipelines that, through Gwadar, will bring supply from the Gulf to Western China. These projects are part of the China-Pakistan Economic Corridor (CPEC), first announced during Xi Jinping's state visit to Islamabad in April 2015.[25]

The CPEC is China's largest overseas investment project to date with an estimated value of 46 billion dollars. It consists of extensive investments in Pakistan's transport, telecommunications and energy infrastructure which will, when terminated, extend for about 3,000 km, linking the port of Gwadar to the city of Kashgar in China's northwestern Xinjiang province, thus opening up new routes for Middle Eastern oil and gas.[26]

It is at this geo-political juncture that the development of China's Maritime Silk Road clashes more acutely with India's strategic priorities. Not only is Beijing investing massively in Pakistan, China's thirst for natural resources from the Middle East creates a challenge for New Delhi which is heavily reliant on imported oil and gas. A second point of friction is the South China Sea, where China's assertiveness and activities – such as island building not in accordance with international law – are a source of concern not only for India but also for the EU, raising the question as to whether, and to what extent, Brussels and New Delhi could join forces in upholding rules-based order in the area.

1.4 European and Indian perspectives on evolving security dynamics in the South China Sea

In July 2016, after more than three years of deliberation, the Tribunal at the Permanent Court of Arbitration in The Hague rendered the Award in

[25] Nicola Casarini, "When All Roads Lead to Beijing", cit., p. 100.

[26] Ibid.; Omar Alam, "China-Pakistan Economic Corridor: Towards a New 'Heartland'?", in *LSE South Asia Centre blog*, 16 November 2015, http://wp.me/p6htYG-1qM.

the Arbitration between the Philippines and China,[27] making it clear that China's extensive historical rights claims to maritime areas within the so-called "nine-dash line" are incompatible with the UN Convention on the Law of the Sea (UNCLOS) and therefore illegitimate. The Tribunal also underscored that none of the land features claimed by China qualify as an island – status that would in turn warrant the claiming of an exclusive economic zone under UNCLOS.

China strongly condemned the verdict, declaring it null and void, and questioned the legality of the Tribunal itself. China's refusal to recognize the Tribunal's ruling has prompted other claimants to reinforce their actions and the United States to intensify its so-called freedom of navigation operations to deter China from adopting even more confrontational policies in the future, such as declaring an Air Defence Identification Zone (ADIZ).[28]

Following the ruling by the Hague Tribunal, Federica Mogherini, the EU's High Representative for Foreign Affairs and Security Policy, issued a declaration stating the need for the parties to the dispute to resolve it in accordance with international law, including the United Nations Convention on the Law of the Sea (UNCLOS).[29] Also some individual EU member states have intervened in the debate.[30] France, which is the only European nation with an Asian-Pacific military projection, has expressed an interest in leading EU patrols to sustain freedom of navigation in the South China Sea – an eventuality that is being considered by other European maritime powers such as Italy, Spain and the Netherlands. The United Kingdom, while reiterating its support for UNCLOS and the rule of law, has refrained however from any direct condemnation of Beijing, for fear of irritating the country with which the new cabinet in London is keen

[27] Permanent Court of Arbitration, *The South China Sea Arbitration (The Republic of the Philippines v. The People's Republic of China)*, 12 July 2016, https://pca-cpa.org/en/news/pca-press-release-the-south-china-sea-arbitration-the-republic-of-the-philippines-v-the-peoples-republic-of-china.

[28] Gregory B. Pooling et al., "Judgment Day: The South China Sea Tribunal Issues Its Ruling", in *CSIS Critical Questions*, 12 July 2016, https://www.csis.org/node/37159.

[29] European External Action Service (EEAS), *Declaration by the High Representative on behalf of the EU on the Award rendered in the Arbitration between the Republic of the Philippines and the People's Republic of China*, 15 July 2016, http://europa.eu/!vT73kP.

[30] Emanuele Scimia, "Europe Can't Save the South China Sea", in *The National Interest*, 24 July 2016, http://nationalinterest.org/node/17092.

to negotiate a free trade agreement. Germany, whose economy is significantly interconnected with that of China, has tended to shy away from any involvement in the South China Sea, also in light of Berlin's reluctance to join military missions in Europe's neighbourhood. Besides issuing a declaration of principles, there is not that much that the EU can do in the South China Sea – an area that has now become the playground for rivalry among great powers.

While Europe is largely a bystander, India has been increasing its involvement in the region in recent times, given that 55 percent of the country's trade passes through the South China Sea[31] – and several of India's island territories, such as the Andaman and Nicobar islands, are located at the western bottleneck of the Straits of Malacca.[32] India has clearly voiced its interest in promoting freedom of navigation in the area and in the peaceful resolution of territorial disputes between Beijing and its maritime neighbours, in an attempt to create strategic opportunities for the littoral states as well as faraway countries like the US and Japan which seek to deter China from dominating the Indo-Pacific.

In the aftermath of the Hague ruling, a joint statement issued by the Indian and Japanese Defence Ministers (on 14 July 2016, following the annual Indo-Japanese Defence Ministerial Meeting) urged parties to "show utmost respect for the UNCLOS" and expressed the two countries' "concern over recent developments," with particular reference to Chinese actions such as the landing of planes on artificial islands.[33] In December 2015, a joint statement by Indian Prime Minister Narendra Modi and Japanese Prime Minister Shinzo Abe had called all parties to "avoid unilateral actions" in the South China Sea "that could lead to tensions in the region."[34] Tokyo and New Delhi have also agreed to deepen their overall

[31] Rajeev Ranjan Chaturvedy, "South China Sea: India's Maritime Gateway to the Pacific", in *Strategic Analysis*, Vol. 39, No. 4, 2015, p. 360-377 at p. 364, http://dx.doi.org/10.1080/09700161.2015.1047218.

[32] Ibid., p. 361.

[33] Indian Ministry of Defence, *Joint Statement after the meeting Between Raksha Mantri and Japanese Defence Minister*, New Delhi, 14 July 2016, http://pib.nic.in/newsite/PrintRelease.aspx?relid=147097.

[34] Indian Ministry of External Affairs, *Joint Statement on India and Japan Vision 2025: Special Strategic and Global Partnership Working Together for Peace and Prosperity of the Indo-Pacific Region and the World*, New Delhi, 12 December 2015, http://www.mea.gov.in/bilateral-documents.htm?dtl/26176.

military cooperation by setting up a Maritime Strategic Dialogue and conducting the annual India-US-Japan trilateral maritime exercise dubbed Malabar.

Besides Japan, New Delhi has also reached out to Vietnam and the Philippines, publicly supporting them in their disputes with Beijing. In September 2016, India signed a deal to base its ships in Vietnam and supply fast patrol boats to Hanoi, a contract worth 100 million dollars.[35] And New Delhi continues to cooperate with Vietnam on hydrocarbon exploration in the South China Sea. In bilateral declarations with Manila, New Delhi has acknowledged the region as part of the West Philippines Sea, refuting the Chinese position.[36]

As part of its "Act East" policy, India has thus increased coordination, both military and diplomatic, with those Asian nations that also see China as a challenge. New Delhi is currently negotiating the sale of the BrahMos cruise missile to Vietnam and frigates and patrol craft to the Philippines, while forging military-to-military ties and economic and trade links with Indonesia, Malaysia, Thailand and Singapore.[37] Finally, with the United States, India has issued a number of high-level joint statements where the two powers have declared their support for freedom of navigation and overflight in the South China Sea. This indicates that the Modi government is no longer afraid of siding with the US to counter China.[38]

1.5 The maritime balance of power in the Indo-Pacific

The main security challenge today in the Indo-Pacific is how to accommodate China's growing military capabilities with the existing order dominated by the US. The pace of China's military modernization is staggering. Since the turn of the century, it has commissioned more than 30 modern

[35] Indian Ministry of External Affairs, *Joint Statement between India and Vietnam during the visit of Prime Minister to Vietnam*, Hanoi, 3 September 2016, http://www.mea.gov.in/bilateral-documents.htm?dtl/27362.

[36] See, for instance, India's Ministry of External Affairs, *Joint Statement: Third India-Philippines Joint Commission on Bilateral Cooperation*, New Delhi, 14 October 2015, http://www.mea.gov.in/bilateral-documents.htm?dtl/25930.

[37] Mohan Malik, "India's Response to the South China Sea Verdict", cit.

[38] Ibid.

conventional submarines, 14 destroyers, 22 frigates and about 26 corvettes, assets that are supported by satellites, radar, air defence systems, ballistic missiles and cyber capabilities.[39] Although China's military development is changing the maritime balance of power, it is likely that the US will remain the strongest naval power in Asia for the foreseeable future.

In March 2015, the US released a new maritime strategy,[40] reflecting concern over the ongoing developments and fielding of anti-access/area-denial capabilities, particularly by China. The strategy introduced a new functional ambition, "all domain access," acknowledging the increasingly contested nature of, in particular, space, cyberspace and the electromagnetic spectrum.

From Djibouti, the US military secures the Red Sea and controls its operations in the Gulf of Oman, while the US naval base in Diego Garcia houses both army and marine brigades, long-range bomber operations, the replenishment of naval surface combatants, and the strike and special operations capabilities of guided-missile submarines.[41] Diego Garcia's location and relatively insular position enable US power projection throughout the Indian Ocean by long-range strategic bombers, as well as through surface warships, including aircraft carriers, cruisers, destroyers, frigates and fast attack nuclear submarines.

While the EU does not have military capabilities in the Indian Ocean, some member states do. France, in particular, has a longstanding presence in the western Indian Ocean, maintaining a naval base (Pointe des Galets) on its island department of La Réunion, east of Madagascar. Djibouti remains economically and militarily close to France. In addition, the UAE now hosts a French military base in Abu Dhabi, encompassing three military camps: a land base, a naval base, and an air base near Al-Dhafra. Finally, the overseas department of Mayotte is home to a 270-strong garrison of the Légion étrangère.[42]

---

[39] Jonathan Holslag, "Why the US policy on South China Sea only helps China", in *South China Morning Post*, 21 August 2016, http://www.scmp.com/week-asia/politics/article/2006225/why-us-policy-south-china-sea-only-helps-china.

[40] US Navy, *A Cooperative Strategy for 21st Century Seapower*, March 2015, http://www.navy.mil/local/maritime.

[41] Andrew S. Erickson, Ladwig C. Walter III and Justin D. Mikolay, "Diego Garcia and the United States' Emerging Indian Ocean Strategy", in *Asian Security*, Vol. 6, No. 3 (2010), p. 215.

[42] Bruno de Paiva, "France: National Involvement in the Indian Ocean Region", in *Fu-*

The United Kingdom also has a number of strategic interests – and assets – in the area: the Biot military complex in Diego Garcia, in conjunction with the United States; an army barracks in Brunei; a logistical and refuelling facility in Sembawang, Singapore; Gorkha recruitment centres in Nepal; and a naval command post in Bahrain that connects the Gulf with its Mediterranean air and naval facilities.[43] London has traditionally invested both politically and financially in the Five Power Defence Arrangements (FPDA), a series of defence relationships established by multi-lateral agreements between the United Kingdom, Australia, New Zealand, Malaysia and Singapore.

Europe's defence industry increasingly looks towards Asia when it comes to arms sales and technology transfers. EU member states continue to sell military equipment in the region. Competition exists among European defence companies, of course, but even more so between EU and US defence manufacturers for acquiring shares of Asia's buoyant procurement budgets. Europeans have developed a strong market presence in South and South-East Asia, especially in sales of naval units (submarines, frigates, corvettes).[44] France, for instance, has sold Scorpène-class submarines to both India and Pakistan in the past, while six French Scorpène-class submarines are currently being built in Mumbai for the Indian navy.[45]

Europe's growing industrial defence interests in South and South-East Asia have, however, gone hand in hand with EU efforts towards supporting existing – as well as creating new – regional multilateral cooperation frameworks for addressing maritime security issues.[46]

---

ture Directions International, 5 December 2011, http://www.futuredirections.org.au/?p=1300.

[43] W. Lawrence S. Prabhakar, *Growth of Naval Power in the Indian Ocean. Dynamics and Transformation*, New Delhi, National Maritime Foundation, 2016, p. 61, http://www.maritimeindia.org/View Profile/Growth of Naval.pdf.

[44] Nicola Casarini, "The European Pivot", in *EUISS Alerts*, No. 3 (March 2013), p. 2, http://www.iss.europa.eu/publications/detail/article/the-european-pivot.

[45] Cameron Stewart, "Our French Submarine Builder in Massive Leak Scandal", in *The Australian*, 29 August 2016.

[46] Lee Cordner, "Progressing Maritime Security Cooperation in the Indian Ocean", in *Naval War College Review*, Vol. 64, No. 4 (Autumn 2011), p. 68-88, https://www.usnwc.edu/Publications/Naval-War-College-Review/2011---Autumn.aspx.

1.6 Old and new multilateral security frameworks

The oldest multilateral security framework in the region is the Indian Ocean Rim Association (IORA), formerly known as the Indian Ocean Rim Initiative and Indian Ocean Rim Association for Regional Cooperation (IOR-ARC). It is an international organization consisting of coastal states bordering the Indian Ocean. The IORA, which has a Coordinating Secretariat located in Ebene, Mauritius, increasingly discusses issues related to maritime cooperation and the "blue economy" and as such is ideally situated to be a dialogue partner of the EU.

Yet, the most effective multilateral maritime security construct has been, since 2008, the Indian Ocean Naval Symposium (IONS) which brings together the navy chiefs of 35 littoral countries and includes China as an observer. A brainchild of India's commitment to promote maritime cooperation in the area, the IONS is constructed along lines similar to the Western Pacific Naval Symposium (WPNS). As a voluntary initiative that seeks to increase maritime cooperation among navies of the littoral states of the Indian Ocean, the IONS has so far focused discussions on maritime information sharing, transnational crime and drug trafficking, as well as interoperability in case of search and rescue exercises.[47]

The IONS would be an ideal partner for Europe, which in the last years has been investing heavily in maritime security in the western Indian Ocean, building the capacity of local maritime agencies and enhancing maritime situational awareness to counter piracy, as well as other transnational security threats.

The EU has bolstered the implementation of the International Maritime Organization Djibouti Code of Conduct (DCOC), signed by 21 coastal states on the Western Indian Ocean rim. Brussels has also lent support to the creation of three information-sharing centres in Kenya, Tanzania and Yemen, and helped in setting up the Regional Maritime Training Centre in

[47] Pradeep Chauhan, "The Criticality of the IONS Maritime Security Construct", in *CIMSEC Articles*, 25 May 2016, http://wp.me/p2moGg-6AY. See also Rahul K. Bhonsle, "India's Maritime Cooperative Security Architecture", in *Mantraya Briefs*, No. 2 (3 April 2015), http://mantraya.org/?p=462. For more information on IONS, see the official website: http://ions.gov.in/about_ions.

Djibouti.[48] In 2013, the EU launched the MASE Programme (with a budget of 37.5 million euros), whose aim is to ensure coordination and continuity between its various capacity-building projects in the Indian Ocean, as well as its inland economic development and governance projects. According to the EU, 80 percent of the budget (over 80 million euros) of the Indian Ocean Commission (IOC) is currently underwritten by Brussels.[49] The IOC aims to foster regional capacity building in fisheries management, small island state development and marine biodiversity protection. Finally, in 2015 the EU launched the Critical Maritime Routes in the Indian Ocean, an initiative that seeks to enhance maritime situational awareness throughout the Indian Ocean by providing technical assistance to coastal states in the realms of information sharing, capacity building, and operational policies and governance.[50]

Europe's commitment to maritime security is an opportunity for India, a country that aims to be a "net security provider" in the Indian Ocean.[51] Both Brussels and New Delhi have significant stakes in securing the sea lanes of communication. Building on the IORA and IONS, the EU and India could join forces to promote an effective multilateral cooperation mechanism in the region to address maritime security issues, including exploring the possible synergies between the EU's Blue Growth Strategy and India's Blue Economy Plan.[52]

However, the evolving security dynamics in the Indo-Pacific, including China's growing assertiveness and rising tensions in the South China Sea, should invite EU and Indian policy makers to begin considering their maritime policy dialogue and cooperation beyond the Indian Ocean to include the vast area stretching from the Indo-Pacific to the Mediterranean, through the South China Sea, the Indian Ocean, the Arabian coasts, the Horn of Africa and the Red Sea, and the Suez Canal. This vast Eurasian

[48] Eva Pejsova, "Scrambling for the Indian Ocean", cit., p. 4.

[49] Ibid.

[50] Ibid.

[51] Pradeep Chauhan, "India as a Net Security-Provider in the Indian Ocean and Beyond", in *CIMSEC Articles*, 29 April 2016, http://wp.me/p2moGg-6s7.

[52] Vijay Sakhuja, "Blue Economy: An Agenda for the Indian Government", in *CIMSEC Articles*, 19 September 2014. http://wp.me/p2moGg-3nC. See also Vijay Sakhuja, "Harnessing the Blue Economy", in *Indian Foreign Affairs Journal*, Vol. 10, No. 1 (January-March 2015), p. 39-49, http://www.associationdiplomats.org/publications/ifaj/Vol10/10.1/10(1)-ejournal.html.

maritime space – from the Far East to the Mediterranean – is also the area covered by China's new Maritime Silk Road, which presents India and the EU with both formidable opportunities and significant security challenges. To move forward their security dialogue on maritime issues, EU and Indian policy makers could therefore consider the following policy recommendations:

- *Develop a joint understanding on maritime governance and freedom of navigation in the area stretching from the Indo-Pacific to the Mediterranean*. This could be achieved by creating an EU-India Joint Working Group tasked to assess their respective interpretations of UNCLOS and freedom of navigation – also with a view towards the eventual issuing of joint declarations.
- *Increase coordination between EUNAVFOR and the Indian Navy*. EUNAVFOR is arguably the most successful and longstanding EU military mission so far, and has enabled European navies to cooperate with Indian military naval units, including in the Contact Group on Piracy off the coast of Somalia. Based on this experience, the two partners could work more closely in the field of maritime surveillance, counter piracy, disaster relief efforts, as well as training and military exercises.
- *Establish an EU-India high-level dialogue on maritime cooperation*. This could be created by deepening and broadening the scope of their current anti-piracy dialogue by including other functional cooperation areas as well as research programmes and initiatives linking Europe's Blue Growth Strategy and India's Blue Economy Plan. The EU-India high-level dialogue could also be used as a platform for exchanging views, best practices and lessons learnt, including in naval military and peacekeeping operations, as well as for exploring the possibilities for the EU to become a dialogue partner with IORA and IONS.
- *Promote a multilateral security culture and framework*. By building on existing arrangements and platforms – such as IORA and IONS – Brussels and New Delhi could join forces to create a structured multilateral security mechanism with the aim of addressing maritime security and freedom of navigation in the region, exploring ways to promote UNCLOS as the basis for maritime governance, and reducing potential rivalry and tensions in the area.

2.

Maritime Security and Freedom of Navigation from the South China Sea and Indian Ocean to the Mediterranean

Vice Admiral Anil Chopra[*]

The IAI has produced a well researched and comprehensive paper on the prospects of Indo EU cooperation in maritime security. They have raised a number of pertinent questions that will take this dialogue forward.

This effort to explore India-EU maritime cooperation stems from the EU-India Agenda for Action 2020, adopted on 30 March 2016, which, inter-alia, calls for "promoting maritime security [and] freedom of navigation in accordance with international law (UNCLOS) […] and fight against trans-national organised crime."

The IAI paper clearly articulates the European Union's vested interest in the maritime stretch from the South China Sea and the Indian Ocean to the Mediterranean, which I will henceforth refer to as the "Indo-Pacific," as this term encompasses the specific maritime domain that stretches from the Western Pacific to the Eastern shores of Africa, including the Horn and the Red Sea.

I propose to comment on the paper in the following order:

- aspects of maritime security;
- the Indo-Pacific and its flashpoints;

[*] Vice Admiral Anil Chopra is Distinguished Fellow, International Security and Maritime Studies, Gateway House. He was the former Commander-in-Chief of the Western Naval Command, the Eastern Naval Command, and former Chief of the Indian Coast Guard. Gateway House Research Team: Vice Admiral Anil Chopra, Sameer Patil (Project Director and Fellow, National Security, Ethnic Conflict and Terrorism), Purvaja Modak (Project Manager and Researcher), Aditya Phatak (Senior Researcher), Nandini Bhaskaran (Editor), Manjeet Kripalani (Executive Director).

- the EU and the Indo-Pacific;
- India's maritime perspective;
- China and the Belt and Road Initiative;
- prospects of Indo-EU maritime cooperation.

2.1 Maritime security

As highlighted in the IAI paper, there are four principal threats to maritime security. These are: armed conflict between states; maritime piracy and robbery; maritime terrorism; and lastly, cross-border organised crime, including trafficking of people and illegal goods by sea. I would like to add a fifth, which is transgression and poaching in exclusive economic zones (EEZ) and non-adherence to UNCLOS (United Nations Convention on the Law of the Sea).

The term, "maritime security," has different connotations for different nations in a specific geographical region. This is particularly so when it comes to littoral and non-littoral states using a body of water, such as the Indian Ocean. Regional nations have to factor into their security calculus traditional state-to-state threats, possible military conflicts, and safeguarding of the EEZ, whereas non-littoral and extra-regional players need not be concerned in this regard. India's maritime security concerns in the Indo-Pacific are therefore fundamentally different from the EU's.

World trade flows through the sea lanes of communication, or SLOCs, and what could disrupt it the most is state-to-state conflict, such as that hypothetically between Saudi Arabia and Iran, or between India and Pakistan.

A conflict or war at sea leads to blockades of ports; collateral damage by way of likely sinking of, or damage to, neutral vessels; possible destruction of marine infrastructure and general increased risk to all maritime activity. Shipping is further affected by increase in freight and insurance rates, and re-routing costs.

Conflict prevention in the Indo-Pacific is therefore critical for both the EU and India, and diplomatic cooperation is required to curb rogue states with the potential to do harm or escalate tensions.

The other threats – piracy, terrorism, crime – can be, and have often,

drawn suitable multinational responses, such as those witnessed in the defeat of Somali piracy in and around the Horn of Africa, and the EU and India can certainly come together to enhance regional maritime governance in the Indo-Pacific, as clearly mandated by the United Nations and the International Maritime Organization.

2.2 The Indo-Pacific

The Indo-Pacific construct underscores the fact that the Indian Ocean has replaced the Atlantic as the world's busiest and most strategically significant trade corridor. It carries approximately two-thirds of global oil shipments, half its container traffic, and one-third of bulk cargo. This vast maritime expanse is witness to many intractable and ongoing conflicts between states, and also others involving non-state entities.

The imbroglio in the South China Sea and tensions in the East China Sea have every likelihood of sparking a conflagration through miscalculation by any of the powers in the region, including the US. The recent moves of Philippine President Duterte may well lead to the informal formation of American and Chinese blocks in Southeast Asia, which has thus far avoided such a dangerous division. Much will now depend on the strategy and actions of the new administration in Washington.

Japan too may feel the need for naval rearmament and general militarisation since 90 percent of its energy imports flow through the China Seas. The situation on the Korean peninsula only adds to the possibility of military confrontation in the region.

In comparison to these geopolitical concerns, the threat that piracy poses in this area is insignificant, especially as regional nations have established an effective anti-piracy and intelligence sharing network and institutionalised it through the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia. But there remains every likelihood of terrorists sinking large vessels due to the blockage of the Malacca Straits or other narrow waterways.

West of the Malacca Straits, shipping enters the calmer waters of the Bay of Bengal and the south Arabian Sea, along sea lanes whose essential safety lies in the hands of a capable and growing Indian Navy, which is the

Net Security Provider in the central Indian Ocean, not least because of its favourable geography and reach. This open ocean passageway is relatively immune to pirates, terrorists and hijackers, and would be vulnerable only in case of conflict between states.

Further west, the situation again becomes fragile. The many conflicts bordering the Persian Gulf, the Gulf of Oman, the Gulf of Aden, the Red Sea, and the vital straits of Hormuz, Bab-el-Mandeb and the Suez Canal, could all spill over into the ocean. This would be further exacerbated if the US indeed "pivots" out of the area in any significant fashion. The resultant maritime power vacuum could invite aggressive power plays by some regional actors in West Asia.

2.3 The EU and the Indo-Pacific

The IAI paper has encapsulated the EU's maritime initiatives and programmes, and its extensive engagement with African and island nations. From the Indo- Pacific perspective, the European Union is yet to be seen as a composite security entity, despite its naval participation in anti-piracy efforts through Operation Atlanta and the EUNAVFOR since 2008. This is perhaps because it was evident that the maritime force, fielded by the European Union, was specifically for combating piracy, and also perhaps because it was the first time that naval forces under the EU flag had ventured East of Suez.

On the other hand, individual European nations, especially in the United Kingdom and France, have had a military presence in the Indo-Pacific for centuries, and therefore Europe's involvement with the region has been seen in terms of their presence. Moreover, these two nations have territorial outposts, and consequent high visibility in the Indian Ocean Region (IOR). Even these two countries have mostly restricted their maritime activity to the western Indian Ocean, from Reunion Island and the island nations of the Indian Ocean, through the African East Coast to the Arabian Peninsula and the Persian Gulf. In the central Indian Ocean, both these navies have focused on port visits and interoperability exercises with the Indian Navy on a regular basis. There has been minimal European presence in the eastern Indian Ocean and east of Malacca.

The spurt in EU maritime activity since 2008 – as evident in the EUCAP NESTOR, MARSIC and CRIMARIO programmes too – has strengthened the European Union's security profile in the western Indo-Pacific. The EU's maritime security strategy, released in 2014, clearly recognises that its well-being and prosperity are linked to the maritime domain, and specially to open and safe seas for free trade. Towards this end, the Indo Pacific has now naturally come to occupy centre-stage for the EU. Not only does the EU source significant energy supplies from this region, but increasingly, the majority of its trade passes through these waters, to and from the economic powerhouses and emerging economies of the resource-rich Indo Pacific.

However, the contours of the European Union's Common Security and Defence Policy, and its military and security architecture are yet to crystallise, and this may well be delayed due to Brexit. It is also not clear whether Operation Atlanta will continue beyond 2016. It is, however, apparent that the European Union would like to continue to maintain a standing quick-reaction naval force, which could be deployed in the western Indian Ocean for general maritime security in the region. Should this become a fact, such a force would be available for interaction with other maritime forces deployed in the same area. It would be natural for such a EUNAVFOR to forge ties with the Indian Navy, in the interests of interoperability.

2.4 India's maritime perspective

India went through a few centuries of sea blindness, but in a comparatively short period of 70 years since winning independence, it has gone from almost negligible maritime capability to fashioning a professional, three-dimensional blue water navy, and raising a large and effective Coast Guard. This capability – besides its centrality in the Indian Ocean and Indo Pacific – enables it to be an extremely effective force of stability and a maritime security provider across the entire region.

India is also committed to overhauling and expanding its maritime infrastructure, and investing substantially in its EEZ, fisheries and deep sea mining. Furthermore, it is actively participating in the maritime development of its immediate neighbours and other nations of the IOR littoral

through project "Security and Growth for All in the Region," quite aptly, the acronym SAGAR meaning "ocean" in Hindi.

The IAI paper has succinctly highlighted India's concerns. China's desire for economic gains from markets and resources in the Indian Ocean is understandable, But India believes that the China-Pakistan Economic Corridor and Gwadar port could well destabilise the region by giving direct access from China's mainland to the mouth of the Persian Gulf, especially if the US were to downsize in the Middle East. Similarly, ports in Bangladesh or Myanmar that have been constructed or are being controlled by the Chinese could ruffle the calm waters of the Bay of Bengal. India does not consider Beijing's forays into the Indian Ocean an "ominous" challenge, and neither is it overtly concerned with the "string of pearls," or the Belt and Road Initiative (BRI), as it is now called.

India hopes to see a vibrant blue economy and effective maritime governance in the Indian Ocean Region through the Indian Ocean Rim Association and promote collective action for peace and security through the Indian Ocean Naval Symposium.

2.5 China and the Indian Ocean region

Eighty percent of China's energy imports transit through the Indian Ocean and the Malacca Straits. This clearly strategic vulnerability, often referred to as Beijing's Malacca Dilemma, has propelled China to seek greater involvement with the nations of the IOR littoral through economic engagement and by increasing the People's Liberation Army (Navy) or the PLA(N) deployment in the Indian Ocean. The IOR offers both resources and markets for the gigantic Chinese economy. The BRI is but a manifestation of these vital requirements for Beijing.

The smaller and less developed states and island nations of the IOR are but naturally absorbing what Beijing had to offer by way of financial assistance and infrastructure development. This does not automatically translate into facilitation of China's strategic or military ambitions in the area. These nations are not beholden or militarily vulnerable to China the way that similar nations of Southeast Asia are. On the contrary, the excessive presence of Chinese personnel in many of the smaller nations has

seen the emergence of a social and political backlash in the public discourse and media, with concerns about a new form of colonialism being openly expressed by the opposition and national commentators.

It is India's belief that it would be better for the region – and for China – if infrastructure projects were distributed to multinational consortia of private and public companies. India is attempting to compete with Japan in the development of maritime infrastructure, as evident in Bangladesh and Iran. This is certainly a field in which the EU can contribute by being part of the maritime development agenda which has seized the region, and there is every possibility of India and the EU cooperating in this regard.

Beijing's generally aggressive approach is disquieting, but its economic initiatives and presence in the IOR need not be viewed with alarm. Whether the Chinese economy can bankroll the ambitious BRI over a long stretch of time is as yet a question mark. Social and political unrest prevailing in the host countries should not hinder the completion of many of the projects through time and cost over-runs. The financial viability of the projects is also a factor to be taken into consideration: for example, Hambamtota port in Sri Lanka, developed entirely by the Chinese, is not breaking even and will incur substantial losses.

As far as military presence is concerned, suffice it to say that the Indian Ocean is not the South China Sea, and there are severe logistical and operational vulnerabilities when deploying significant naval forces at long distances from the homeland. It takes many decades and much soft power to shape a distant environment for enabling maritime operations. As mentioned earlier, the only concern relates to possible PLA(N) bases on the Asian mainland in the IOR. An alarmist approach regarding China thus needs to be avoided.

2.6 India-EU maritime cooperation

There are many areas of maritime cooperation which are possible between India and the EU. Given their shared values and common objectives in the Indo-Pacific, maritime security coordination and cooperation between the two sides would help make the seas free and safe for continued global prosperity.

Primarily, the EU and India must work more closely diplomatically to prevent the outbreak of an armed conflict in the Indo Pacific. The EU must recognise that India is a major force for the good in this vast maritime arena, and given its capability and centrality, the only responsible regional guarantor of stability. Both sides must work actively to remove minor irritants in their relationship.

From India's perspective, the EU has displayed an inadequate appreciation of the factors, including terrorism, which India has to contend with in the neighbourhood. Cooperation in this area must begin with the EU developing a more nuanced understanding of India's security concerns, abjuring its customary hyphenated perspective so far.

India and the EU can cooperate in three distinct areas:

- Firstly, by coordinating their efforts to address maritime piracy, crime and terrorism. This would call for greater intelligence sharing and developing a common Maritime Domain Awareness picture pertaining to these threats.
- Secondly, by strongly adhering to and supporting the tenets of UNCLOS, and coordinating on all aspects of maritime governance as applicable to the high seas, the EEZ and the SLOCs.
- Lastly, developing maritime infrastructure and the blue economy in the region to prevent any monopolistic outcomes, possibly beginning with the Indian Ocean Commission initiative.

To do so, we concur with all three policy recommendations outlined in the IAI paper. The modalities for taking this forward call for further elaboration and discussion.

3.

India-EU Cooperation on Cyber Security and Data Protection

Sameer Patil, Purvaja Modak, Kunal Kulkarni and Aditya Phatak[*]

Advances in information technology (IT), accompanied by the decreasing costs of computing, have created opportunities for using technology for the benefit of humanity. But, the same advances have also engendered security challenges for many countries. This includes the problem of formal attribution or pinning a cyber attack on a specific entity or location, since such attacks are routed through multiple global servers. Taking advantage of this, some states have tried to use the cyber domain to pursue their geopolitical ambitions. Cyber war, or what some states conceptualise as an "information war," has now become the most significant form of non-kinetic warfare.

The problem of attribution, along with the growing number of cyber incidents, is complicated by the absence of a global cyber security regime or norms for state behaviour in cyber space. It is further compounded by the ambiguity of the capabilities of major cyber powers – such as the US, Russia and China – to launch offensive and defensive cyber operations. Moreover, given the low technological entry barriers – anyone with a basic background in computers can acquire the skills to hack networks –

[*] Sameer Patil is Fellow, National Security, Ethnic Conflict and Terrorism, at Gateway House. Purvaja Modak is Researcher and Assistant Manager, Research Office, Gateway House. Kunal Kulkarni is a former Senior Researcher at Gateway House. Aditya Phatak is Senior Researcher, Gateway House. Methodology followed for this paper is deskesk research and interviews with officials of the Government of India and of the Delegation of the European Union to India, lawyers specialising in data protection issues, cyber security analysts, and representatives of Indian and European IT companies operating in India.

even non-state actors such as terrorist groups, hackers, organised criminal gangs, hacktivists are exploiting cyber space for their own purposes.

In the past few years, cyber threats have become sophisticated and nuanced. A majority of cyber attacks have targeted personal and commercial computer networks, but their consequences are no longer restricted to these levels. In 2009-10, the Stuxnet malware, allegedly designed by the US and Israel, attacked Iran's Natanz nuclear facility, affecting its reactors.[1] Before reaching its designated target, it also infected the computer systems of a host of manufacturing sites worldwide.[2] As a result, cyber space and the threats emanating from it have become a focus area for many countries, including India and the European Union's member states.

3.1 Multiple cyber security challenges

For India, cyber threats have multiplied after a few of computer systems in the public and private sector in India were infected by the Stuxnet malware in 2010. Exploiting the same vulnerabilities in those computers (which operated on the Siemens systems) as it did in Iran, the malware infected computers across India at facilities like power plants and national oil pipelines in Gujarat and Haryana; but other than this, no major disruption was reported.[3] Yet, these disruptions made India the third largest victim of the Stuxnet virus, after Iran and Indonesia.[4]

India's predominant cyber security concern is the protection of Critical Information Infrastructure (CII)[5] – telecommunication networks, air

[1] Ellen Nakashima and Joby Warrick, "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say", in *The Washington Post*, 2 June 2012, http://wpo.st/Hr8W2.

[2] Eric Byres, Andrew Ginter and Joel Langill, *How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems*, Tofino Security White Paper, February 2011.

[3] Pierre Mario Fitter, "Stuxnet Attack Wakes India Up to Threat to Critical Infrastructure", in *India Today*, 5 September 2012, http://indiatoday.intoday.in/story/stuxnet-cyber-war-critical-infrastructure-of-india-ntro/1/216107.html.

[4] Jarrad Shearer, "W32.Stuxnet", in *Symantec Security Response Blog*, updated 26 February 2013, https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[5] Critical information infrastructure means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

traffic, signal management, nuclear reactors, power plants, oil pipelines – which are required to be functional at all times. The weakest links in the protection of this critical infrastructure are Supervisory Acquisition and Data Control (SCADA) systems, which are used to manage the operations of these facilities. A majority of SCADA systems used in India were installed 20-30 years ago, in the pre-internet era. They were therefore not built to deal with the network-based threats or cyber attacks of today.

Table 1 – Major cyber incidents affecting Indian and European computer systems

Year	Incident	Implications
2007[6]	Estonian websites targeted by a Distributed Denial of Service (DDoS) attack.	The attack, suspected to have been carried out by Russia, disabled the websites of the government, political parties, news organisations, and banks.
2010	Stuxnet malware infects Indian computer systems.	The malware infected many computer systems in India including the Supervisory Control and Data Acquisition (SCADA) systems at power plants and oil pipelines. No other adverse impact was reported.
2011	Duqu virus hits European computer networks.	The Duqu virus, similar to Stuxnet, targeted a specific number of organisations in Europe; it was used to steal information that could be utilised to attack the Industrial Control Systems (ICS).
2013	DDos attack on Spamhaus' Domain Name system (DNS) servers (located across Europe).	The attacks, the result of a business dispute (between Spanhaus, a company that filters spam, and Cyberbunker, a web-hosting company), disrupted internet services in Western Europe.
2016	Computer systems at the state secretariat of Maharashtra, India, infected by a ransomware.	The attack targeted the revenue and public works departments of the Maharashtra state government, but no substantial damage to the systems was reported.

Source: Gateway House research, based on data collected from media reports.

This vulnerability spans CII in the public as well as private sectors. It is complicated by the lack of trust between the state and the private sector. The lack of trust is the product of multiple factors, but mainly because the private sector thinks that the government does not have the technical

[6] The year such large-scale and massively disruptive attacks were carried out for the first time anywhere in the world.

capability to counter cyber threats, and the government sees the private sector as not being sensitive to national cyber security concerns. Besides, private sector entities are reluctant to share the vulnerabilities of their computer systems, fearing that other private sector competitors may find a way to exploit their weakness.[7] As a result, both sides are unable to do enough in terms of joining hands to counter cyber threats.

Confidential data from India's Computer Emergency Response Team (CERT) reveals that hundreds of attacks on India's SCADA systems occur annually; anecdotal evidence suggests that their scale and frequency has been increasing over the years.[8]

Europe too is grappling with this vulnerability. A malware named Duqu, similar to Stuxnet, targeted European companies in 2011. It stole data that could be utilised to attack the Industrial Control Systems. Another instance had occurred in 2007 with a series of cyber attacks on websites of the Estonian government, the country's political parties, news organisations, and banks,[9] allegedly to achieve Russia's larger political objectives.

Except for the infections caused by Stuxnet, India has not witnessed an attack at the same level as that on Estonian websites in 2007. ButIndia remains a major target of hostile countries (such as Pakistan and China) and rogue elements (including cyber extortionists and organised crime syndicates). The country's government servers and commercial entities are clearly at the receiving end of data breaches[10] and espionage attacks for stealing confidential official and commercial data. According to Fire-

[7] Sameer Patil, "India's Vulnerable SCADA Systems", in *Gateway House Articles*, 17 June 2014, http://www.gatewayhouse.in/?p=52186.

[8] Sameer Patil, Interview with Indian government officials, New Delhi, December 2013.

[9] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia", in *The Guardian*, 17 May 2007, https://gu.com/p/xvm3k/stw.

[10] Verizon, *2016 Data Breach Investigations Report*, 19 May 2016, p. 10, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf. For the purpose of this paper, data will mean the following: (a) Government-related information and databases in electronic form including their confidential emails and contact details of officials, and national security-related information; (b) Commercial information and databases in electronic form including confidential emails, business and product development plans; and financial information such as passwords, bank account or any payment instrument details; and (c) Personal sensitive information such as physical, physiological and mental health conditions; sexual orientation; medical records and history; passwords and biometric details.

Eye, a private American cyber security firm, India was the target of a decade-long espionage operation through the Advanced Persistent Threat (APT)-30 vector, carried out by a China-based group, which was most likely state-sponsored.[11] Several media reports have also pointed that India was the fifth-most spied-on country by the PRISM surveillance programme of the United States' National Security Agency.[12]

With the growing sophistication of snooping technology and the wider recurrence of and malicious social media engineering attacks, cyber-enabled espionage has acquired more worrying proportions. Europe faces the same challenge; it too has been a sustained target of espionage operations – primarily attributed to Russia and China – for stealing commercially valuable and intellectual property data. Extensive assessments from private American cyber security firms FireEye and Mandiant have noted that Europe has witnessed data breaches since 2004 attributed to the APT-1 and APT-28 vectors (suspected to be from China and Russia).[13]

3.1.1 Cyber threats from non-state actors

India and Europe face another potent cyber threat from the "deep web" or the hidden internet, which hosts thriving digital black markets that sell stolen personal data, malware, sensitive trade secrets, stolen bank and credit card information, firearms, and controlled substances and narcotics – which cannot be bought in an open market.[14] These are powered by crypto currencies such as Bitcoin, which complicates the challenge of the deep web for a country's security establishment. The anonymity offered by the deep web has, in turn, contributed to the growth of cyber crimes,

---

[11] FireEye, *APT30 and the Mechanics of a Long-Running Cyber Espionage Operation*, April 2015, https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

[12] Glenn Greenwald and Shobhan Saxena, "India among Top Targets of Spying by NSA", in *The Indu*, 23 September 2013, http://www.thehindu.com/news/national/article5157526.ece.

[13] Mandiant, *APT 1. Exposing One of China's Cyber Espionage Units*, February 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; FireEye, *APT28: A Window into Russia's Cyber Espionage Operations?*, October 2014, https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf.

[14] Sameer Patil, "The 'Deep Web': New Threat to Business", in *Gateway House Articles*, 6 January 2015, http://www.gatewayhouse.in/?p=69321.

which increased by 40 percent annually during 2012-2014 in India.[15] American internet security firms McAfee and Symantec estimate that the annual cost of cyber crimes to the global economy is between 375 billion dollars (333.57 billion euros) and 575 billion dollars (511.47 billion euros), with 594 million people affected globally.[16] Annually, cybercrimes cost India around 4 billion dollars (3.56 billion euros) and Europe around 13 billion dollars (11.56 billion euros).[17] For Europe, this threat emanates primarily from Eastern Europe.

One of the major black market platforms on the deep web was "Silk Road." It was shut down in 2013 by the US government, but not before generating revenues worth 1.2 dollars billion (1.07 billion euros) between 2011 and 2013.[18] Silk Road's activities were dominated by buyers and sellers from North America and Europe, but the site also had users from India.[19] For terrorist groups that always look for new technologies, the deep web's black market is an ideal platform to purchase arms and smuggle drugs, and to raise funds.[20] No hard evidence of such activity is available at present, but it is speculated that the weapons used during the Paris attacks of November 2015 were sourced from the deep web.[21]

For India and Europe, the use of social media and cyber space by terrorist groups for spreading their propaganda has emerged as a serious challenge. This is exemplified in their security establishments' efforts to counter the terrorist group Daesh, located in Iraq and Syria. For India, the

---

[15] Indian Ministry of Home Affairs, *Setting up of Expert Study Group for Tackling Cyber Crimes*, 24 December 2014, http://pib.nic.in/newsite/PrintRelease.aspx?relid=114013.

[16] Center for Strategic and International Studies (CSIS) and McAfee, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014, p. 2, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf. US Federal Reserve rate as on 1 October 2016 (1 dollar: 0.89 euro). For updated estimates, see: Symantec, *2016 Norton Cybersecurity Insights Report*, November 2016, https://us.norton.com/cyber-security-insights-2016.

[17] Symantec, *2013 Norton Report*, http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx.

[18] US Department of Justice, U.S. v. Ross William Ulbricht, 27 September 2013, https://publicintelligence.net/silk-road-complaint.

[19] Sameer Patil, interview with cyber security professionals, Mumbai, December 2014.

[20] Gabriel Weimann, *Terror on the Internet. The New Arena, the New Challenges*, Washington, US Institute of Peace Press, 2006, p. 137-138.

[21] Stefan Candea et al., "How EU Failures Helped Paris Terrorists Obtain Weapons", in *Spiegel Online*, 24 March 2016, http://spon.de/aeH1l.

Daesh is a different challenge from those it has encountered earlier, like the Lashkar-e-Taiba and the Indian Mujahideen. Both these groups used the internet for recruitment and propaganda, but their focus was on domestic issues such as riots and Kashmir.[22] However, Daesh's brutal violence in Iraq and Syria, its reliance on "lone wolves" for executing attacks outside West Asia, and its social media blitzkrieg focusing on propaganda and recruitment, has opened up new avenues of online indoctrination of vulnerable youth. Given Daesh's vast social media effort worldwide, with approximately 38 unique multimedia propaganda events per day,[23] a coordinated counter response is required from the countries that are impacted, and which spans across all sectors (public, private, and civil society).

For India, inadequate awareness among the government and people of cyber security issues, and a lack of preparedness to respond to cyber incidents, deepens the challenges of cyber space. For instance, law enforcement agencies (LEAs) in India lack the capacity and cyber forensic skills that are required to gather digital evidence, which is a basic requirement in combating cyber crime.

The absence of boundaries in cyber space means that the computer systems of India and Europe are negatively impacted by cyber incidents occurring outside their territories. This was evident in the case of Stuxnet, and in 2013 when suspected Eastern European hackers stole bank and credit card information, mostly that of European consumers, from the servers of Nasdaq and US companies including, J.C. Penney and 7-Eleven.[24]

3.2 Opportunities for India-EU cyber security cooperation

Despite these common threats, cyber security cooperation between India and the EU remains inadequate at present. Both sides began cooperat-

[22] Sameer Patil, interview with Indian government officials, New Delhi, July 2016.

[23] Charlie Winter, Documenting the Virtual Caliphate, Quilliam Foundation, 2015, p. 5, https://www.quilliamfoundation.org/?p=9011.

[24] Andrea Peterson, "Why Stolen European Credit Card Numbers Cost 5 Times As Much As U.S. Ones", in *The Washington Post*, 29 July 2013, http://wpo.st/fxOW2.

ing on cyber security issues after the 2010 Brussels Summit, where they agreed to closer cooperation and mutual assistance in this field.[25] Initial steps were limited to a bilateral consultation on cyber security and cybercrime. Subsequently, in May 2015, consultations were upgraded to a Cyber Dialogue, within the framework of the bilateral Security Dialogue.

The bilateral cyber engagement takes place at four levels:

1. The Cyber Dialogue, which lacks a security focus because it covers a wide gamut of areas including issues related to internet governance. Discussed therein are training programmes for India in the field of IT and security, assessments of cyber crime, enhancing cooperation between CERTs, and cooperation on the R&D front.
2. There are discussions within the Counter-terrorism Dialogue on the use of cyber space by terrorists. At the operational level, CERT-India has a working relationship and collaboration with CERTs in Europe and with CERT-EU.
3. India and the EU have a Joint Information and Communications Technology (ICT) Working Group, set up in 2000,which has held nine rounds of meetings so far.[26] It includes representation from the government as well as industry. Themes discussed by this group include internet governance, and ICT research and innovation.
4. India also has bilateral security dialogues with countries such as France, UK and Germany, which encompass discussions on cyber security issues.

Recently, the bilateral engagement in this sphere received a boost after the India-EU Summit in Brussels in March 2016. The summit's joint statement highlighted the links between the "Digital India" initiative and the EU's "Digital Single Market" strategy, through increased cooperation in cyber security, ICT standardisation, and internet governance, research and innovation.[27] The EU-India Agenda for Action 2020 has, among other

[25] EU-India Joint Declaration on International Terrorism, 10 December 2010, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/foraff/118405.pdf.

[26] European External Action Service, *EU-India Relations*, 29 March 2016, http://europa.eu/!Up34bw.

[27] Joint Statement: 13th EU-India Summit, Brussels, 30 March 2016, http://www.consilium.europa.eu/en/meetings/international-summit/2016/03/20160330-joint-statement-eu-india_pdf/.

goals, mentioned strengthening cooperation and working towards tangible outcomes on various areas including cyber security.[28]

It is in these areas listed above that India and the EU have significant opportunities for cooperation in cyber security.

Domestically, India is stepping up its cyber focus through many initiatives:

- In 2013, India announced a broad policy framework in the form of the National Cyber Security Policy (NCSP). Then, the National Critical Information Infrastructure Protection Centre (NCIIPC)[29] was set up in 2014, as a response to the challenge of CII protection. The Centre works with the public and private sectors for plugging gaps in their computer systems. In 2015, the government created the post of a National Cyber Security Coordinator to synchronise efforts on cyber security issues at the national level.[30]
- The Indian government and industry are also engaged in capacity building of law enforcement agencies through awareness raising, training programmes, and enhancing cyber forensics skills. To counter indoctrination and the use of cyber space by terrorists, the LEAs are setting up social media labs (such as one in Mumbai) as an experiment in public private partnerships to monitor social media.[31]
- In 2015, the Indian government launched a flagship programme called "Digital India," aimed at improving governance and citizen-centric services by harnessing IT.[32] Another flagship project, "Smart Cities Mission," intends to utilise technology to improve the infrastructure of the country's cities.[33] Big data management will be at the heart of these

[28] EU-India Agenda for Action-2020, 30 March 2016, http://www.consilium.europa.eu/en/meetings/international-summit/2016/03/20160330-agenda-action-eu-india_pdf.

[29] Indian Ministry of Electronics and Information Technology, *Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules*, 2013, 16 January 2014, http://meity.gov.in/sites/upload_files/dit/files/GSR_19(E).pdf.

[30] Varun Aggarwal, "Gulshan Rai Becomes First Chief of Cyber Security; Post Created to Tackle Growing E-threats", in *The Economic Times*, 22 April 2015, http://ecoti.in/zSxQVY.

[31] "Mumbai Gets Country's First 'Social Media Lab'", in *The Hindu*, 17 March 2013, http://www.thehindu.com/news/national/article4516705.ece.

[32] See the website of the Indian Ministry of Electronics & Information Technology, *About the Programme*, http://www.digitalindia.gov.in/content/about-programme.

[33] See the website of the Indian Ministry of Urban Development, *Strategy*, http://

projects. IT and the Business Process Management sector is also one of the focus areas of the "Make in India" programme.[34]

At the same time, New Delhi has put cyber security concerns on India's diplomatic agenda. For example, in the last two years, India has initiated cyber security cooperation with many countries, including Mongolia, Australia, Vietnam, Canada, Malaysia, Singapore, the UK, and Japan. It has also intensified cyber security cooperation with countries such as the US (through an Agreed Framework for Cyber Security Cooperation) and Russia (by signing an information security agreement).

Meanwhile, in the military domain, the three wings of the Indian armed forces are at advanced stages of integrating network-centric warfare capabilities, and are increasing the awareness of cyber threats and cyber-enabled espionage among their personnel.

Europe too has taken initiatives in the cyber domain:

- The continent as a whole took the first step in 2001 to evolve a common strategy for cyber crimes in the form of the Council of Europe's Budapest Convention on Cybercrime.[35] (India opposes this Convention. The detailed position of India is outlined in Appendix 3).
- In 2013, the EU published its Cybersecurity Strategy, its first comprehensive policy document on the issue.[36]
- In June 2016, the European External Action Service released the Global Strategy for the EU's Foreign and Security Policy document which outlined the EU's efforts in protecting against cyber threats, while striving for an open and safe cyber space.[37]
- Organisationally, the EU has been at work since 2004 when it established the European Union Agency for Network and Information Security (ENISA) to work with member states and the private sector in

smartcities.gov.in/writereaddata/Strategy.pdf.

[34] See the website of Make in India, *IT and BPM*, http://www.makeinindia.com/sector/it-and-bpm.

[35] Council of Europe, *Convention on Cybercrime*, 23 November 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[36] Raluca Csernatoni, "Time to Catch Up: The EU's Cyber Security Strategy", in *European Public Affairs*, 4 March 2016, http://wp.me/p38b3I-11u.

[37] European External Action Service, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, 28 June 2016, p. 21, http://europa.eu/globalstrategy/en/language-versions.

the field of information and network security. To counter cyber crimes, in 2013 Europol specifically set up the European Cyber Crime Centre (EC3),[38] which is the one-point source for all data regarding cyber crimes and threats.

In the military domain, the European Defence Agency has put forward cyber defence as a priority area. The 2016 Strategy has also emphasised enhancing cyber security cooperation with core partners such as the US and the North Atlantic Treaty Organization (NATO).[39]

3.3 Impact of EU's dual-use regime on cyber security cooperation

A potential dampener for enhanced India-EU cyber security cooperation is the Wassenaar Arrangement and EU's dual-use regime.

Since the 2008 attacks on Mumbai, India has initiated important internal security measures designed to respond better to terrorist activities. One such measure has been the installation of mass surveillance systems such as the Central Monitoring System for counter-terrorism purposes. India is utilising its IT base to develop domestic solutions for setting up these systems, but many of these technologies also need to be imported off-the-shelf. This presents an opportunity for India-EU cooperation.

But India will certainly not receive the full benefit of any agreement with EU on the sharing of cyber security know-how because of the EU-wide application of the restrictions placed by the Wassenaar Arrangement, the multilateral export control regime governing the worldwide export of arms, and dual-use goods and technologies, which all EU countries adhere to.[40]

In December 2013, the Wassenaar Arrangement was amended to include controls on the export of "intrusion software," a key element of sur-

[38] See Europol website, *European Cybercrime Centre - EC3*, https://www.europol.europa.eu/node/50.

[39] European External Action Service, *Shared Vision, Common Action: A Stronger Europe*, cit., p. 21.

[40] See the website of The Wassenaar Arrangement, *Abut Us*, http://www.wassenaar.org/about-us.

veillance systems.[41] These amendments to the Arrangement's dual-use and munitions lists were spearheaded by the major EU members – UK[42] and France.[43] The EU has included the control lists of the Wassenaar Arrangement in its legislation and practices – the Wassenaar's Dual-Use Goods and Technologies List is included in the Common EU List of Dual-Use Items[44] (including the "intrusion software"), while its Munitions List is mirrored in the Common Military List of the EU.[45] The EU and its member states are thus committed twice over to applying stringent standards of export control for dual-use technologies.

Sure, the amendment to the Wassenaar Arrangement may have been intended to prevent the export of surveillance mechanisms to authoritarian governments and regimes worldwide, but the amendment has disadvantaged India specifically, which is not a member of the Arrangement. India therefore finds itself in a weakened position when dealing with the EU and its member states as a consumer of dual-use technologies. The amendment can also potentially work against India in the case of any bilateral cyber security disagreement.

3.4 Data protection issues impinging on India-EU ties

The EU has stringent and elaborate data protection and privacy laws, which have been linked to human rights. The European Court of Human Rights has observed that the protection of personal data falls under the

[41] The Wassenaar Arrangement, *List of Dual-use Goods and Technologies and Munitions List*, 8 December 2016, p. 73, http://www.wassenaar.org/control-lists; US Bureau of Industry and Security, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 20 May 2015, https://www.federalregister.gov/d/2015-11642.

[42] UK Government, *United Kingdom Strategic Export Controls Annual Report 2013*, 17 July 2014, https://www.sipri.org/databases/national-reports/United%20Kingdom.

[43] Tim Maurer, "Internet Freedom and Export Controls", in *Carnegie Briefings*, 3 March 2016, http://ceip.org/2jzPoci.

[44] Commission Delegated Regulation (EU) 2015/2420 of 12 October 2015 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items, p. 15, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32015R2420.

[45] Council of the European Union, *Common Military List of the European Union*, 21 April 2015, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52015XG0421(05).

ambit of Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home, and correspondence.[46]

The principal EU legal instrument on data protection is Directive 95/46/EC of 1995, which states the rules for processing and transfer of personal data, including international transfers.[47] The provisions of this Directive, relating to the international transfer of personal data, affect India directly, specifically Article 25, which specifies the criteria for a country to be declared as having adequate protection.[48] In May 2010, Graham Greenleaf, an Australian professor who studied India's data protection regime as part of a EU-commissioned study, presented his findings to EU. He concluded that India's provisions for data protection cannot be regarded as adequate as per the EU's standards.[49] The EU's concern is the security and confidentiality of personal data, including preventing any unauthorised access to such data,[50] which can be potentially used by cyber criminals.

After the invalidation of EU-US Safe Harbor agreement in October

[46] European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, June 2014, http://fra.europa.eu/en/node/9534.

[47] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eurlex.europa.eu/legal-content/en/TXT/?uri=celex:31995L0046. In April 2016, the European Council adopted a new single law on data protection i.e. Regulation (EU) 2016/679, repealing the existing Data Protection Directive 95/46/EC. This Regulation will apply from 25 May 2018 to the EU member states. The Regulation also contains adequacy requirements but this has not been examined for the purposes of this paper.

[48] It states that "adequacy" should be assessed on a case by case basis "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations." Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

[49] Graham Greenleaf, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Country Studies: India*, May 2010, http://ec.europa.eu/justice/data-protection/document/studies.

[50] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32016R0679.

2015 by Court of Justice of the European Union, the European Commission and the US Department of Commerce came up with a revised framework (EU-U.S. Privacy Shield) in July 2016, as a legal means to transfer personal information between the EU and US businesses. The legality of Privacy Shield was threatened after civil society challenged its legitimacy to satisfy concerns arising out of mass surveillance by the US government. The EU decision to persist with the implementation of the Privacy Shield, despite its widely acknowledged inadequacy to protect against mass surveillance by the US, clearly implies the EU viewing cross border data flows as a trade matter, not a privacy issue.

The Data Security Council of India (DSCI), the main industry body working on data protection issues in India, has argued against the heavy handed stringent regulation governing data flows. It has also pointed out that the EU has denied India a framework similar to the United States for data flows.

The DSCI contested Greenleaf's report and responded to this EU-commissioned paper with a White Paper in January 2012.[51] It strongly argued that the regulatory changes brought in by the amendment to India's IT Act, 2000, have significantly closed the perceived gap in the regulatory and enforcement mechanisms for privacy protection. It said that these changes have made the country eligible to qualify as providing "adequate protection" from the EU Directive's standpoint (a table summarising the DSCI White Paper on the EU commissioned paper is in Appendix 4). However, some legal experts in India are of the opinion that the amendments to the IT Act, 2000, are weak and do not provide effective protection.[52]

The DSCI's position is echoed by the Indian government, which also insists that India has adequate data protection laws under the IT Act, 2000, along with its amendments and rules. Together, the government asserts, these provide a comprehensive legal framework for privacy and data protection.[53]

---

[51] Data Security Council of India, *White Paper. EU Adequacy Assessment of India*, 7 January 2012, https://www.dsci.in/node/1328.

[52] N.S. Nappinai, "Technology Laws", in *Lexis Nexis*, 2017 (forthcoming).

[53] Indian Parliament-Lok Sabha, Unstarred Question No. 3202: Legislation for Data Protection, 16 March 2016, http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=31968&lsno=16.

The differences over India's data adequacy status have also featured in the India-EU Bilateral Trade and Investment Agreement (BTIA) negotiations, which began in 2007. So far, 16 rounds of negotiations have been held, the last one in 2013.[54] Since then, the talks have been suspended due to differences over market access and procurement related issues[55] and India's demand for "data secure" status from EU.[56] India has linked this demand to trade, arguing that without such a status it will be difficult for both sides to engage in cross-border trade in services.However, the European Commission insists that the issue of data protection adequacy should be separated from the BTIA talks.[57] India and EU have discussed setting up a Joint Expert Working Group (JWG) to bridge differences on India's data adequacy or come up with alternative solutions agreed upon by both the parties;[58] its status remains unknown. Incidentally, in 2013, the EU had done another study which had acknowledged the progress made by India in data protection regulations. However, the report, for unknown reasons, concluded that India did not have adequate data protection laws.[59]

While the BTIA talks remain stuck, other related complications have arisen. Some countries like Japan and South Korea are harmonising their data protection regimes with the EU's standards of data protection in order to increase engagement with the EU.[60] This is putting further pressure on India and Indian companies to raise their standards.

Legal experts in India are of the opinion that the evolution of a global privacy and data protection regime is being driven, to a large extent,

---

[54] Indian Parliament-Rajya Sabha, Unstarred Question No. 1934: Delayed Talks on India-EU FTA, 11 May 2016, http://164.100.47.234/question/annex/239/Au1934.pdf.

[55] See the European Commission website: Trade > Policy > Countries and regions > India, http://europa.eu/!HU47rD.

[56] Indian Ministry of Commerce and Industry, *Anand Sharma Asks EU to Declare India Data Secure*, 17 October 2012, http://pib.nic.in/newsite/PrintRelease.aspx?relid=88472.

[57] See NASSCOM website: *EU-India FTA Discussions Gather Steam*, https://shar.es/1OESlD.

[58] Indian Ministry of Commerce and Industry, *Sharma and Gucht Review India-EU BTIA Negotiations*, 30 May 2013, http://pib.nic.in/newsite/erelcontent.aspx?relid=96316.

[59] This report is not in the public domain. Gateway House was informed about this report during the interview with the DSCI representatives, who have seen a copy of this report.

[60] Kunal Kulkarni, interview with DSCI representatives, Mumbai, September 2016.

by EU regulations. These are bureaucratic, with cumbersome and sometimes incomprehensible regulations, and are therefore creating difficulties for countries such as India. While there can be a broad agreement on privacy principles, the implementation of those principles should be left to each country, which can adapt regulations as per local socio-cultural attitudes to privacy.[61] The experts recognise that India does have enforcement problems but that the country is taking steps to address these concerns.

In particular, in 2016, India passed the Aadhaar Act (Targeted Delivery of Financial and Other Subsidies, Benefits and Services),[62] which provides for a unique identification number to those residing in India for targeted delivery of subsidies, benefits, and services. The Aadhaar Act contains a separate chapter titled "Protection of Information" by which the Unique Identification Authority of India, established under the Act, is obligated to ensure the security of information about individuals. It restricts the sharing of this information and penalises any unauthorised access of such information.[63]

3.5 Policy recommendations for India-EU cyber security cooperation

For deepening India-EU cyber security cooperation, it is necessary to look at EU's cyber cooperation with other countries and understand the range of issues covered:

- EU-US: The EU and the US work in close coordination on cyber-related issues, both bilaterally and in multilateral fora. An annual vibrant US-EU Cyber Dialogue discusses cyber security, data protection and

[61] Kunal Kulkarni and Purvaja Modak, interview with lawyers and DSCI representatives, Mumbai, September 2016.

[62] Indian Ministry of Law and Justice, *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*, 26 March 2016, https://uidai.gov.in/images/the_aadhaar_act_2016.pdf.

[63] However, concerns have been raised in respect of confidentiality and disclosure provisions in the Aadhaar Act. See Elonnai Hickok and Amber Sinha, *Salient Points in the Aadhaar Bill and Concerns*, The Centre for Internet and Society, 21 March 2016, http://cis-india.org/internet-governance/salient-points-in-the-aadhaar-bill-and-concerns.

internet governance issues, as well as confidence building measures and capacity building in third countries.[64] They also have a Working Group on Cyber security and Cybercrime, which focuses on cyber incident management, public private partnerships on security of critical infrastructure, raising awareness, and cyber crime.[65]

- EU-China: The EU has a similarly active cooperation with China. Both sides have deliberated and discussed cyber crimes, innovation and cooperation on "Smart Cities Mission," 5G technology, broadband, etc. Many of these issues are also of salience for India.

While the path to creating trust and evolving deeper India-EU cooperation is indeed long and winding, as India's cyber security cooperation with the US has shown, if India and the EU demonstrate their intent to advance cooperation with patience and perseverance, the true potential of the relationship will be realised.

Measures to further cooperation on issues of cyber security and data protection are suggested in Table 2.

[64] The White House, *Fact Sheet: U.S.-EU Cyber Cooperation*, 26 March 2014, http://go.wh.gov/axF72A.

[65] European External Action Service, *Fact Sheet: EU-US Cooperation on Cyber Security and Cyberspace*, 26 March 2014, https://eeas.europa.eu/statements/docs/2014/140326_01_en.pdf.

Table 2 – Policy recommendations for deepening India-EU cooperation on cyber security and data protection

Policy recommendation	Guiding principles
Cyber security	
JWG on cyber security	The Cyber Dialogue must be carried forward with regular meetings. It should also include discussions on the use of social media by terrorists, given the pervasiveness of the threat.
Public-private partnership (PPP) for mitigating cyber threats	The PPP should leverage the expertise and experience of private sector ICT companies. India has a strong IT base, with Indian IT and business process management companies exporting more than 100 billion dollars (88.95 billion euros) annually.[66] Moreover, major European ICT companies are already active in India. Therefore, it is imperative for these companies to be an important element in addressing cyber threats. The expertise of these companies can be used to raise strong encryption standards, promote cyber security research, and create cyber security professionals. Their engagement should also focus on creating a network or platform where they can report the cyber attacks they face. This will certainly contribute to the resilience of computer systems in India and Europe.
Cyber crime and the deep web	
Fostering cooperation between the LEAs	An important part of cyber crime investigations is the collection of evidence. Therefore, despite their differences on the European Cybercrime Convention, India and the EU must foster practical cooperation between their respective law enforcement agencies and also with Europol for evidence collecting methodologies. This can be done by designating nodal agencies/officials to access digital evidencein timely manner. This cooperation should also include real-time sharing of information between both sides. As part of this engagement, India and the EU can create standards on sharing information and uniform methods of reporting cyber incidents.
Sharing lessons on their respective investigations of deep web-related cases	The challenge of cyber crime and the deep web cannot be tackled alone. A multi-jurisdictional approach is a basic requirement. Besides, solutions to the problem of the deep web are not necessarily restricted to the technology domain, and traditional investigation methods remain valid. In this context, law enforcement agencies in India and Europe can share lessons on their respective investigations of cases related to the deep web.
Interaction between the Europol's E3C and India's proposed National Cyber Coordination Centre	The Europol's E3C and India's proposed National Cyber Coordination Centre should have a formal working relationship in order to tackle cyber crime. Since the E3C also works on critical infrastructure protection, this interaction can also plug gaps in that domain, and both sides can share their best practices and work on minimum standards for security of the CII.
Informal technical cooperation among the LEAs	As against the flourishing ecosystem of the deep web, governments are still limited by silos in their responses to counter the online black markets. Technical cooperation among the Indian and the European LEAs can also be forged informally to collect the IP addresses of computers in the deep web as a first step, just like Project Honey Pot.[67]

[66] See the website of Make in India, *IT and BPM*, cit.

[67] See the website of the Project Honey Pot, *About Project Honey Pot,* https://www.projecthoneypot.org.

Data protection and privacy	
Understanding Indian sensitivities on privacy issues	The EU needs to understand that every country has different socio-cultural attitudes to privacy. Hence, rather than pushing to make EU regulations a global benchmark, Brussels can work out an agreement on privacy principles with New Delhi that leaves the implementation of those principles to India's policy establishment.
Bridge differences on India's data adequacy issue	Data protection laws in India are yet to be declared as adequate by the EU – this, when done, will allow the transfer of personal data. With other countries increasingly moving towards harmonising their laws with EU regulations, the pressure will mount on India – not only from the EU but also from other countries too – to increase its standards. Moreover, the new EU Regulations on data protection will come into effect in 2018. Therefore, despite the stalled BTIA negotiations, both sides must continue to work on data adequacy issues and resolve their differences.
Digital India and Smart Cities Mission	
Dialogue on smart cities	The EU co-funded European Business and Technology Centre (EBTC) has recently become a partner in Pune and Navi Mumbai's "Smart Cities" plans.[68] Instead of individual cities in India signing memorandum of understanding (MoU) with the EBTC, India and EU can set up a separate dialogue for "Smart Cities." The EU has a similar dialogue with China.[69] ENISA's work on cyber threats to smart cities should be a part of these discussions.[70]
Collaboration between Ministry of Electronics and Information Technology (MEITY) and ENISA on Internet of Things (IoT) Infrastructure in India	The IoT is still in its infancy in India, but the MEITY has recently come up with a draft policy on the IoT. Considering the criticality of the IoT and its link with "Digital India," this paper proposes a collaboration between MEITY and ENISA on IoT as ENISA has recognised various cyber security challenges arising due to the IoT.[71] The ENISA as an advisory and training outfit can also help build human resources for handling IoT infrastructure and services in India.
Capacity building	
Increasing awareness on cyber security issues	While cyber threats keep evolving, the basic response to mitigate these threats remains simple. Cyber hygiene is the key to awareness. India and the EU can host a "Cyber security awareness month" similar to the "EU-US cyber security awareness raising month"[72] of October 2015.

[68] "PSCDCL and EBTC Sign MoU for Knowledge Sharing and Technical Cooperation", in *India Infoline News*, 26 September 2016, http://www.indiainfoline.com/article/news-business/pscdcl-and-ebtc-sign-mou-for-knowledge-sharing-and-technical-cooperation-116092600130_1.html; Smart Cities Project, *NMMC signed MoU with EBTC for Navi Mumbai Smart City*, 6 December 2015, http://www.smartcitiesprojects.com/navi-mumbai.

[69] See the website of the EU-China Smartcities: http://eu-chinasmartcities.eu.

[70] See the website of the European Union Agency for Network and Information Security (ENISA): *Smart Cities*, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-cities.

[71] Evangelos Ouzounis, *Securing Europe's IoT Devices and Services*, presentation at Validation Workshop, Berlin, 16 October 2015, https://www.enisa.europa.eu/events/copy_of_enisa-workshop-on-cyber-security-for-iot-in-smart-home-environments/1-enisa-securing-europes-iot-devices-and-services/view.

[72] "Joint Elements" from U.S.-EU Cyber Dialogue, Washington, 8 December 2015, http://europa.eu/!Fd64Xr.

Cyber security research	The EU is expected to spend 500 million euros for research on cyber security and hopes that the private sector will spend three times that amount on the same.[73] Some of that research can focus on studying the cyber threats in emerging economies such as India. In particular, the existing technical capability of India on crypto currencies is inadequate. Therefore, research on these currencies and their financial and security implications must be undertaken. For this, the private sector in India and Europe should also involve the academic and scientific community. For instance, the Bombay Stock Exchange has joined hands with the Indian Institute of Technology-Kanpur for setting up a Cyber Security Centre of Excellence.[74]
Cyber forensics	The Verizon 2016 Data Breach Investigations Report states that India has witnessed a number of data breaches.[75] Surprisingly, Indian law enforcement agencies have not been able to detect even a single attack or breach. This is a worrying factor since the time taken to detect a breach is increasing while the time taken to respond and prevent the loss of control of a system is decreasing. This is primarily due to a lack of adequate cyber forensics capacity – skill sets and infrastructure – of the Indian LEAs. The EU can play an important part in building this capacity for India.
Cyber threat intelligence sharing	European countries must be forthcoming in sharing their experiences with non-European powers such as India on lessons learnt from past incidents. This can be a part of the capacity building of law enforcement agencies.
Joint simulation labs	The EU can help India set up simulation laboratories and testing facilities for carrying out controlled experiments.[76] Also, since the private sector is at the forefront of technologies, including the "deep web," rather than government bodies, these facilities should have representation from the European private sector too.
Global cyber security cooperation	
Pushing for a global agreement on the protection of critical infrastructure from cyber attacks	Since both India and the EU have seen the consequences of cyber attacks on the CII, they must take the lead in facilitating a global agreement for protecting critical infrastructure from cyber attacks by engaging with like-minded parties (such as the US, Australia, Israel, and others).
Regulating the behaviour of non-state actors in cyber space	A big challenge for state actors in cyber space is to regulate the cyber capabilities of non-state actors. India and the EU can take the lead in developing an international consensus on dealing with non-state actors and thereby contribute to global cyber security cooperation.
Creating a Cyber Action Task Force	Given the criticality of a cyber threat and the lack of a dedicated global cyber security organisation, India and the EU can facilitate the creation of a Cyber Action Task Force, an organisation similar to the Financial Action Task Force (Paris), which works on combating money laundering and terrorist financing. The Cyber Action Task Force can consist of senior policy makers, and private sector and technical experts, who work to establish a set of norms and best practices. This proposed agency can be aligned with the CERTs in each country for coordination and information sharing.

[73] Peter Sayer, "EU Plans $2B Investment in Cybersecurity Research", in *PCWorld*, 5 July 2016, http://www.computerworld.com/article/3090891.

[74] Purvaja Modak, interview with a representative of the Bombay Stock Exchange, Mumbai, September 2016.

[75] Verizon, *2016 Data Breach Investigations Report*, cit., p. 10.

[76] Purvaja Modak, interviews with representatives from the Indian private sector and Cyber Security professionals, Mumbai, September 2016.

Conclusion

The ability and capacity of the cyber saboteurs to think and act across multiple jurisdictions remains the biggest challenge in countering cyber threats; more so because the governments responding to these cyber threats are hampered by their respective national jurisdictions. So, even if a country is prepared to mitigate cyber security challenges, the challenge of unforeseen risks still exists, which necessitates cooperation.

India and the EU must adopt a pragmatic approach to cyber security cooperation by assessing areas of common concern and expeditiously sorting out their differences, mostly on data protection. Data transfer and sharing is the key to tackling the issues that are encountered within the cyber domain. The efforts in this context cannot be limited to government and regulators. Businesses must also contribute and cooperate in mitigating cyber threats.

Enhanced cyber security cooperation between the two sides will potentially have a beneficial effect in other domains of India-EU defence and security cooperation.

Appendices

Appendix 1. Factsheet on India-EU cyber cooperation

Cooperation with the EU: Platforms for cyber cooperation between India and the EU

- Joint ICT Working Group, set up in 2000, comprising G2G and B2B level dialogues focusing on internet governance, ICT research and innovation
- Cyber Dialogue at the G2G level covering security and internet governance issues
- Cooperation between CERT India and the CERT-EU

Table 1.1 – Cooperation with the individual EU member states

Country	Engagement
Estonia	- 2014: MoU signed by India and Estonia for capacity building in the sphere of e-government for five years
France	- 2000: MoU on mutual cooperation in ICT signed by India and France - 2003: MoU signed by India and France for establishing a Indo-French Cyber University for information exchanges in the fields of education, training, transfer of technology, and research - 2013: India-France agreed to collaborate on ICT cluster, open data and cloud computing - 2013: First round of the India-France cyber dialogue held in Paris
Finland	- 2010: Agreement signed for cooperation in the field of information security
Germany	- 2013: India and Germany held consultations on cyber issues - 2015: India and Germany signed an MoU for security cooperation for countering terrorism, including online terrorist propaganda - 2016: India participated in the technology exhibition CeBIT 2016 at Hannover to promote the “Make in India” campaign in the electronics and IT sectors
Poland	- 2015: India and Poland agreed to cooperate in the areas of capacity building, skill development, R&D and innovation in emerging technologies
Sweden	- 2016: India and Sweden endorsed the creation of a new JWG on Digital Technologies and Economy
UK	- 2015: India-UK Cyber Dialogue in October 2015 - 2016: India and the UK signed anMoU for cooperation on countering the cyber attacks both countries face; the agreement includes exchange of knowledge and experience in detection, resolution, and prevention of security-related incidents

Source: Gateway House research, based on the data obtained from the Government of India’s Ministry of External Affairs and Ministry of Electronics and Information Technology.

Appendix 2. Steps taken by India and EU to address cyber security threats

Table 2.1 – Policies implemented by India on cyber security and data protection

Act/Policy	Year	Details
Cyber security		
National Cyber Security Policy	2013	It aims at protecting the information infrastructure in cyberspace, reducing vulnerabilities, building capabilities to prevent and respond to cyber threats and minimising damage from cyber incidents. The objective is to create a secure cyberspace ecosystem, strengthen the regulatory framework, and launch a comprehensive national awareness programme on the security of cyberspace.
Data protection		
Information Technology Act (with a 2008 amendment)	2000	It elaborates on offenses, penalties, and breaches and outlines the justice dispensation systems for cyber-crimes and provides for the constitution of a Cyber Regulations Advisory Committee.
Right to Privacy bill	2014	The bill extends the right to privacy to all residents of India. It defines nine specific privacy principles: i) notice ii) choice and consent iii) collection iv) limitation v) purposes limitation vi) access and correction vii) disclosure of information viii) security ix) openness and accountability. It requires authorisation by the relevant state authority for the collection and processing of sensitive personal data. An earlier version of this bill was under consideration in 2011, but it lapsed.
Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act	2016	It provides for, as a part of good governance, efficient, transparent, and targeted delivery of subsidies, benefits, and services to individuals residing in India by assigning of unique identity numbers to such individuals.

Source: Gateway House research, based on data obtained from the Government of India's Ministry of Electronics and Information Technology and The Centre for Internet & Society, a Bengaluru-based NGO.

Table 2.2 – Policies implemented by Europe on cyber security and data protection

Convention/Policy	Year	Details
Cyber security		
Budapest Convention on Cyber crime (with an Additional Protocol in 2003)*	2001	It is the first international treaty seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. It also sets out procedural law issues related to cyber crime. In addition, the Convention contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties.
Cyber Security Strategy of the European Union	2013	It sets out the EU's approach to preventing and responding to cyber disruptions and attacks. It details a series of actions to enhance the cyber resilience of IT systems, reduce cyber crime, and strengthen the EU's international cyber security policy and cyber defence.
Directive on security of network and information systems	2016	This directive provides legal measures to boost the overall level of cyber security in the EU by ensuring member states' preparedness, cooperation among all the members by setting up a cooperation group, and a culture of security across sectors – all of which are vital for the economy and society. Businesses in the sectors identified by member states as operators of essential services will have to take appropriate security measures and notify serious incidents to the relevant national authority.
Data protection		
Directive 95/46/EC	1995	It was formulated for the "Protection of individuals with regard to the processing of personal data and on the free movement of such data." It applies not only to the processing of personal data but also to transfer of such data, including international transfers. It lays down the criteria for a country to be declared as having adequate protection.
Data protection directive, Regulation (EU) 2016/679	2016	This regulation will replace Directive 95/46/EC (General Data Protection Regulation). It seeks to harmonise the protection of the fundamental rights and freedoms of human beings in terms of processing activities and to ensure the free flow of personal data between member states. It will come into force from 2018.

Source: Gateway House research, based on data obtained from the official websites of the EU, European Union External Action, European Commission, and the Council of Europe.
* The Budapest Convention is from the Council of Europe.

Table 2.3 – Agencies of the Government of India working on cyber security and data protection issues

Agency	Year	Details
IT security		
Centre for Development of Advanced Computing	1988	The premier R&D organisation in the IT and electronics, working on strengthening national technological capabilities. It works in close junction with the MEITY.
CERT India	19/01/2004	Works under the MEITY and is a nodal agency dealing with cyber security threats. It aims to strengthen the security-related defence of the Indian internet domain. CERT India has a working relationship with the CERTs of other countries.
Ministry of Electronics and Information Technology	2012	Promotes e-governance for empowering citizens, promoting the growth of the electronics, IT and information technology-enabled services (ITeS) industries, and enhancing India's role in internet governance. It also focuses on developing human resources in this field, and promoting R&D.
National Critical Information Infrastructure Protection Centre (NCIIPC)	2014	The nodal agency for taking all measures, including associated R&D, for the protection of CII in India. The NCIIPC has identified 12 macro sectors as critical infrastructure sectors, zeroing in on the most vulnerable infrastructure facilities in the public and private sectors; it coordinates with other relevant agencies.
Cyber crime		
Indian Cyber Crime Coordination Centre / National Cyber Coordination Centre	Proposed	The creation of the centre has been recommended to fight against cyber crimes. It has been accepted, in-principle, by the Ministry of Home Affairs (MHA). The centre will work on online cybercrime reporting, cybercrime monitoring, setting up of forensic units, capacity building of the police, prosecutors and judicial officials, promotion of R&D, etc.

Source: Gateway House research based on data obtained from the Indian Ministry of Electronics and Information Technology, Computer Emergency Response Team, and the Centre for Development of Advanced Computing.

Table 2.4 – Government agencies in the EU working on cyber security and data protection issues

Agency	Year	Details
IT security		
European Union Agency for Network and Information Security (ENISA)	2004	Works closely with EU member states as well as private firms to strengthen network and information security as an advisory agency. It looks into matters of information privacy, security issues related to software and hardware products, security solutions for firms and governmental agencies on managing the risks arising out of online information. It is not a law enforcement agency and does not regulate the operating of rules and regulations regarding network security.
CERT-EU	(Pilot project 2011) September 2012	An IT solution agency which helps EU organisations run their cyber operations, helping them fight cyber threats. It serves as the internal IT security team of the EU, comprising IT experts from the main institutions of the EU. It cooperates with CERTs in member states, as well as with private IT firms.
Cyber crime		
European Cyber Crime Centre, Europol	January 2013	Acts as a law enforcement agency and deals with cyber crimes in EU member states. It focuses on areas like cybercrimes committed by organised criminal groups. It acts as the one-point source for all data regarding cyber crimes and threats that can emanate from across Europe and the world. Also acts as an investigating agency assisting investigations by member states by helping them on technical and forensic issues regarding cyber security.

Source: Collated and analysed by Gateway House, based on data obtained from the official websites of the European Union Agency for Network and Information Security, Computer Emergency Response Team, and EUROPOL.

Appendix 3. India's position on the European Convention on Cybercrime, 2001

India, in principle, agrees with the necessity to fight and counter cyber crime. Therefore, it does not does not fundamentally contest the Convention and rather uses it as a guideline for reforming the county's national legislation. India has incorporated most of the substantive provisions of the Convention in its IT Act through the amendment in 2008.[77] But the Convention remains unacceptable for India because of the following reasons:

- *Drafting process*: India has generally opposed treaties that have been drafted without its consultation. Therefore, India, along with China and Brazil, has argued that the Convention remains a treaty drafted by Europe, reflecting its priorities.[78]
- *Implications of Clause 32 (b) of the Convention for India's sovereignty*: India is particularly opposed to this clause, which talks about "trans-border access to stored computer data with consent or where publicly available" and specifically states that a party may, without the authorisation of another party, "access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."[79] This clause has grave implications for any country's sovereignty and therefore India has deemed it to be discriminatory.
- *The China factor*: India also believes that the Convention in its present form is insufficient in tackling the cyber crimes that it faces, predominantly originating from China. Signing the Convention will therefore not solve India's problems, and China too has not signed the Convention.

---

[77] Indian Ministry of Electronics and Information Technology, *Information Technology Act*, 2000, http://meity.gov.in/content/information-technology-act.

[78] S. Shalini, "Budapest Convention on Cybercrime – An Overview", in *The CCG Blog*, 3 March 2016, http://wp.me/p3PRi6-k5.

[79] Cybercrime Convention Committee, *T-CY Guidance Note # 3, Transborder Access to Data (Article 32)*, 3 December 2014, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.

Appendix 4. Summary of the DSCI White Paper on the EU Adequacy Assessment of India's Data Protection

Points raised by the EU-commissioned paper	DSCI's position
Content principle: Purpose Limitation-use and disclosure	
There is no specific limitation on the ability of companies or the government to collect personal information, except in relation to credit information. Furthermore, the IT Act 2000 does not impose limitations on the internal use of personal information by the organisation collecting such information.	It may be noted that the report by the EU assessing India's adequacy was released in 2010, prior to the enactment of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules).[80] These Rules were enacted by the central government of India vide powers under section 43A of the IT Act 2000. The Privacy Rules, specifically Rule 4 (1)(iii), 5 (1), 5(2) (a), 5 (3), 5 (5) now bring specific content with respect to the privacy principle of "purpose limitation." The Privacy Rules require collection of information for a lawful purpose connected with a function or activity of the collector of information, and require the information collected to be used only for the purpose for which it has been collected.
With regards to the IT Act 2000 and its 2008 amendment, the EU observes that they cover only a small part of what is usually covered by privacy and data protection laws. According to the EU, the IT Act 2000 does not deal specifically with data protection, and core concepts such as "personal data/information," "processing," "disclosure," and "consent" are not defined.	The Privacy Rules define "personal information" and "sensitive personal data or information." Rule 5 requires entities to take written consent "regarding purpose of usage" before collecting information. It also binds the companies not to collect information unless it is necessary for the stated purpose. Rule 6 requires companies to acquire prior consent before "disclosure of information" to third parties, and disallows the third party from further disclosure.
Content principles: Data quality and proportionality principles-collection limitations, deletion/preservation of data	
Indian law cannot be considered to provide adequate protection in relation to the collection of personal information.	Rule 5 (1) and (2) of the Privacy Rules address the requirements of this privacy principle, obligating companies to take consent for the purpose of usage before collection of information. It also stipulates that the information collected should be for the lawful purpose, and collected only if the information is necessary for the purpose.

[80] Indian Ministry of Communications and Information Technology, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,* 11 April 2011, http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.

The EU raises concerns regarding the deletion of personal data when it is no longer necessary to retain the same for the legitimate purpose for which it was collected.	Rule 5(4) of the Privacy Rules clearly stipulates that sensitive personal data or information shall not be retained for any length of time longer than is required for its lawful purposes.
Content principles: Transparency	
The IT Act 2000 does not impose obligations on private sector organisations to disclose details of their practices.	The Privacy Rules obligate a body corporate[81] that collects, receives, stores, processes, deals in, or handles information to provide for a privacy policy regarding such information, including personal sensitive data. Rule 4 requires entities to maintain "clear and easily accessible statements of its practices and policies" in the public domain so as to make them easily available to the providers of information; this includes publishing the privacy policy on the website of the company.
Content principles: Security	
The 2010 report examined Indian laws to assess whether they meet the security principle of adequacy. The principle requires technical and organisational security measures by the data controller that are appropriate to the risks presented by the processing. The report says that no such security standard exists.	This was addressed by Rule 8 of the Privacy Rules, which requires companies to have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational, and physical security control measures. The rule states that the international standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such accepted standard. If the members of any industry association are following any standard other than the IS/ISO/IEC codes of best practices for data protection, then the same needs to be approved and notified by the central government for effective implementation.
Another aspect affecting India's adequacy, according to the EU, is the lack of an encryption policy from the central government as required by section 84A of the IT Act 2000.	The DSCI stated that the Department of Information Technology is in the process of notifying an encryption policy designed to significantly address the information security concerns of businesses as well as consumers. (Update: In 2015, the Indian government had published a draft encryption policy, but it was later withdrawn due to heavy criticism from the civil society and public at large about the stringent provisions related to retaining and storing data such as retaining the instant messenger messages for at least 90 days).

[81] "Body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; Explanation to section 43A of the Information Technology Act 2000.

Content principles: Onward transfer	
The EU report raised concerns on the lack of laws restricting the transfer of personal data out of India (onward transfers).	This concern has been addressed by Rule 7 of the Privacy Rules, which allows transfer of sensitive data to any company or person within or outside India only if the same level of data protection is maintained by such company or person. Further, the transfer is allowed only for the performance of the lawful contract and when the provider of information has consented to data transfer.
Content principles: Rights of data subjects (access, rectification and opposition)	
The EU principles of adequacy also require the data subjects be given certain rights such as: - Informing of data subjects at the time of collection - Right to obtain a copy of all data relating to him/her that are processed - Right to rectification of those data where they are shown to be inaccurate - Right to object to the processing of the data relating to him/her	The Privacy Rules stipulate intimating (providing notice), publishing policies, and making practices transparent to the data subjects. Rule 5(6) requires companies to permit the data subjects to review the information provided to ensure that information is correct, and if found to be inaccurate or deficient, is corrected. Rule 5(7) allows the data subject to withdraw their consent at any time by writing to the body corporate.
Adequacy assessment: Procedural and enforcement mechanism	
The EU assessed the procedural and enforcement mechanisms in India with regards to data protection, primarily from five perspectives: (i) Independence and functions of supervisory authorities; (ii) Role of courts; (iii) Provision of appropriate redress to the injured parties; (iv) Delivery of a good level of compliance; (v) Provision of support and help to individual data subjects.	The EU observes some positives with India's procedural and enforcement mechanism but maintains that it has gaps and overall is not adequate. The Indian position, as stated by DSCI, is that the Indian courts along with quasi-judicial authorities such as the Adjudicating officer (under the IT Act 2000), do meet these requirements. Appropriate redress and support is provided to aggrieved parties and data subjects by the IT Act and the Privacy Rules, along with Article 32 of the Constitution(which rovides,extensive powers to the Supreme Court of India to enforce Constitutional rights).

Source: Data collected from the Data Security Council of India.

4.
EU-India Cooperation on Cyber Issues: Towards Pragmatic Idealism?

Patryk Pawlak[*]

4.1 The EU and cyber diplomacy: A forward-looking player?

The friction between value-based foreign policy and a pragmatic and action-oriented approach has always been part of the debate about the EU's global role. It should not come as a surprise, therefore, that even in such a seemingly unexciting policy area as cybersecurity the emotions become high with any mention of human rights online or state control over the Internet. It is true that because cybersecurity is inherently linked to ensuring the resilience of networks that underpin the proper functioning of Internet-based platforms, the overly technological language of the debate may discourage some from joining the conversation. But more often than not, cybersecurity is also about building and maintaining robust and resilient human networks grounded not in the seabeds like fiber-optic cables but rather in mutual trust and cooperation between various communities that shape cyberspace – be it as policymakers, engineers, law enforcement agents or simple users. This observation is even more pertinent in the case of international cybersecurity cooperation where the dynamic advances in technology development might lead to misunderstandings and conflicts due to different regulatory frameworks or a suspicion of malicious activity. At the same time, the broad array of threats to national

[*] Patryk Pawlak is Member of the Advisory Board of the Global Forum on Cyber Expertise (GFCE). The views set out in this article are those of the author and can in no way be taken to reflect the views of the GFCE Advisory Board or the GFCE.

security or our societies posed by states, criminal networks or terrorist organizations call for practical cooperation. The dark side of the Internet is only a part of the explanation why cooperation despite the differences is essential. The growth of Internet-related and mobile technologies has fundamentally transformed our way of life and contributed towards economic growth. Economic benefits of Internet-related technologies are expected to reach between 8.1 trillion dollars and 23.2 trillion dollars annually by 2025.[1]

The EU Global Strategy presented in June 2016 recognizes the tension between values and pragmatic approach to cooperation in cyberspace. The Strategy expresses the EU's wish to become a "forward-looking cyber player [by] protecting our [the EU's] critical assets and values in the digital world, notably by promoting a free and secure global Internet."[2] To that aim, the EU will rely on its cyber diplomacy and capacity building cooperation with partners as well as seek agreements on responsible state behaviour in cyberspace based on existing international law. However, to be able to fully implement its vision of open, safe and secure cyberspace – as pronounced in the EU Cybersecurity Strategy[3] – the European Union needs to grapple with several developments that will shape cyberspace in the future and will impact the EU's capacity to pursue its policy objectives.

First, the number of Internet users has grown over a thousand-fold from just 3 million in 1990 to over 3.2 billion in 2015 and is expected to reach 4.7 billion by 2025.[4] Most of this growth is happening in the developing countries and emerging economies. The growing online population of these countries has already translated into calls for a more fair and

[1] James Manyika et al., *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy*, McKinsey Global Institute, May 2013, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies.

[2] European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, 28 June 2016, p. 42, http://europa.eu/globalstrategy/en/language-versions.

[3] European Commission and European External Action Service, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN/2013/1), 7 February 2013, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52013JC0001.

[4] Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends", in Anna-Maria Osula and Henry Rõigas (eds.), *International Cyber Norms. Legal, Policy & Industry Perspectives*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, February 2016, p. 129, https://ccdcoe.org/node/956.html.

representative distribution of control over cyberspace, including by the Government of India.

Second, the digital environment and threat landscape are changing too: state and non-state actors increasingly exploit vulnerabilities in cyberspace to gain an advantage over their competitors and adversaries. The transborder nature of cyber threats puts additional pressure on the EU's capacity to fight cybercrime and protect its assets in the cyber domain. The experience so far has shown that an effective fight against cybercrime is impossible without cooperation between law enforcement agencies and judicial bodies – often based in countries with inadequate legal and institutional frameworks, including about the protection of civil rights and fundamental freedoms. Such an environment will put additional pressure on the European Union to engage in a complex balancing exercise between competing values such as freedom of expression and freedom from fear in the case of counter-radicalization efforts or protection of privacy and safe/secure use of the Internet for economic or social activities.

Finally, the progressing militarization of cyberspace and the reliance on new systems of state-owned cyber weapons accelerate the cyber arms race and competition for "digital supremacy." Therefore, the EU will face some hard choices concerning its cyber capabilities as well as future alliances in this domain. One issue that requires in-depth reflection is the EU's posture about defensive and offensive capabilities. At the same time, as the barriers to access to cyber capabilities decrease, the risk of a conflict resulting from misunderstandings and miscalculation is growing. Establishing whether a cyber attack constitutes an armed attack if the use of force is legitimate (*jus ad bellum*), and how force can be employed (*jus in bello*) is still a subject of debate among international legal scholars and policymakers.

4.2 Incredible India: More than a slogan

The EU Cybersecurity Strategy acknowledges that "preserving [an] open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners"[5] with a particu-

[5] European Commission and European External Action Service, *Cybersecurity Strategy of the European Union*, cit., p. 14.

lar focus on like-minded partners that share EU values. In that sense, the relationship with India represents a specific challenge and an opportunity. With 1.25 billion people or 17.5 percent of the world's population, India is the biggest democracy in the world. And it is one of the most diverse too as home to eight major religions, over 4,600 castes, and 22 federally recognized languages in use. At the same time, the online population in India is expected to reach 708 million by 2025 – numbers that have almost doubled compared to 2015.[6] Still, that implies that less than a half of the India's projected 1.46 billion population[7] will have access to the Internet. India is also the world's seventh largest economy in terms of gross domestic product (GDP), and has become the world's fastest growing large economy. The EU is India's biggest trading partner, accounting for 13 percent of India's overall trade, ahead of China and the United States.[8] In 2015, the value of EU exports to India amounted to 38.2 billion euros, which made it the EU's ninth largest trading partner. The total value of EU-India trade stood at 77.6 billion euros in 2015 while trade in commercial services has quadrupled in the past decade. The EU is also the largest investor in India. Beyond trade relations, India is also one of the greatest contributors of forces to the UN peacekeeping operations. Since 1948 it has participated in 44 missions with close to 180,000 troops including both police and military forces.

Recognizing the importance of the India in the global system, the bilateral EU-India summit organized in March 2016 reaffirmed the commitment of both sides to give new momentum to the bilateral relationship. The EU-India Agenda for Action 2020 endorsed at the summit[9] will serve as a joint roadmap for the India-EU Strategic Partnership, including towards strengthening cooperation and working towards tangible outcomes on

[6] David Burt et al., *Cyberspace 2025. Today's Decisions, Tomorrow's Terrain*, Microsoft, June 2014, p. 3, https://blogs.microsoft.com/microsoftsecure/2014/06/02/cyberspace-2025-todays-decisions-tomorrows-terrain.

[7] UN Department of Economic and Social Affairs (UNDESA), "Total Population - Both Sexes", in *World Population Prospects. The 2015 Revision*, July 2015, https://esa.un.org/unpd/wpp/Download/Standard/Population.

[8] European Commission DG Trade, *European Union, Trade in Goods with India*, November 2016, http://trade.ec.europa.eu/doclib/html/113390.htm.

[9] European Council, *EU-India Summit: Joint Statement, Agenda for Action and Joint Declarations*, 30 March 2016, http://europa.eu/!kq76NY.

some shared objectives, including cybersecurity. Acknowledging the progress achieved in the EU-India Information and Communication Technologies (ICT) dialogue, the section of the Agenda for Action devoted to ICT policies includes several specific proposals.[10] The primary focus of the ICT section is on exploring synergies between the "Digital India" initiative and the EU's "Digital Single Market." This concerns in particular cooperation on economic and regulatory issues (e.g., market access), ICT standardization, Internet governance, research and innovation as well as innovative start-up companies. It also entails making good use of the annual Joint ICT Working Group and Business Dialogue. The new Startup Europe India Network (SEU-IN), funded through the Partnership Instrument, is a flagship initiative implemented under the Agenda 2020. It aims to enhance cooperation and foster growth, investments and collaboration between the major stakeholders from the pan-European and Indian start-up ecosystems (i.e., start-ups, scale-ups, investors, incubators, innovation agencies, universities and other relevant change-makers). Cybersecurity is among the ten core areas covered by the network's activities. Also, the Agenda includes commitments to work towards the exchange of expertise and best practice in cybersecurity, the Internet of Things, cloud computing and e-governance; discussion on simplification of a co-financing mechanism for research and innovation in mutually agreed areas of IT; and promotion of the IT industry.

The primary platform for cooperation, sharing information and exchanging best practices on cross-cutting external cyber issues, in particular those linked to bilateral and multilateral relations in cyberspace, is the EU-India Cyber Dialogue.[11] One of the main components of the dialogue is devoted to consultation on politico-military and international security issues, including norms of state behaviour in cyberspace, application of international law, and confidence building measures. The EU and India share the conviction that norms of responsible state behaviour in cyberspace and developing Confidence Building Measures (CBMs) are essential for international stability. Both sides also agree that recommendations

[10] UN Group of Governmental Experts, *Report on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), 22 July 2015, http://undocs.org/A/70/174.

[11] Patryk Pawlak, "Cyber Diplomacy: EU Dialogue with Third Countries", in *EPRS Briefings*, June 2015, p. 5-6, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)564374.

in the 2015 report of the UN Group of Governmental Experts (UN GGE) should serve as a starting point for any future discussions, including on CERT-to-CERT cooperation, exchange of points of contact or enhanced information sharing about national cybersecurity strategies and policies. Consultation on involvement of the EU and India in various regional and international organizations is also pursued through the cyber dialogue. In that context, India's bilateral cooperation with ASEAN and the ASEAN Regional Forum (ARF) is particularly valuable for the EU as it aims to promote more actively the development of CBMs in the region, similarly to the process undertaken in the OSCE context to reduce the risks of escalation, misperception and miscalculation.

India and the EU are also keen on advancing cooperation on bilateral issues such as developing a closer cooperation on cyber-related research and development, in particular about cybercrime and digital forensics techniques. The protection of critical infrastructure is also gaining importance in bilateral contacts in light of India's increasing reliance on SCADA and industrial control systems and the expertise required for their secure operating. In addition, the EU and India suffer a substantial economic loss due to cybercrime which implies a potential for cooperation, for instance by strategic agreements with Europol (i.e., such agreements are already in place between Europol and Bosnia and Herzegovina, Russia, Turkey and Ukraine). While India's expertise in the field of ICT and cybercrime is on the rise, there is still room for improvement. For instance, India could benefit from the EU's assistance in training law enforcement and justice professionals on many issues, including forensics and investigative techniques. Such cooperation is also possible through capacity building projects coordinated by the Council of Europe with EU funding, however India has so far not expressed interest in pursuing this option. Finally, the agenda of EU-India dialogue includes consultations on capacity building in third countries to enhance cybersecurity, fight cybercrime and increase access to and use of ICTs and the Internet for social and economic development. Cooperation on the last point could prove particularly fruitful and could take a more strategic dimension in the future given that India is a laboratory for innovation about the use of ICTs for stimulating social and economic growth. Programmes such as *e-Choupal* could help identify useful lessons for the EU and support its ambition to strengthen the link between cybersecurity and development in its partner countries.

4.3 India's cyber policies: A swing state?

Despite the similarity of approaches in several cyber-related areas, the scope of EU-India cooperation has been undermined by the three concurrent debates about the multi-stakeholder model of Internet governance, cyber-sovereignty and the protection of human rights online. India's interpretation of these issues has been evolving, leaving the EU without a clear perspective on bilateral and regional cooperation on cyber issues.

4.3.1 Multi-stakeholder approach and accountability

The basic premise of the multi-stakeholder model is that it assigns responsibility for the future of the Internet to a broader community including governments, the private sector, civil society and technical experts. This vision has been promoted and supported by liberal democracies, including the EU. India is an active participant in the debate about the future of the Internet. It officially expressed its commitment to the multi-stakeholder model at the Net Mundial conference in São Paulo in 2014. However, commentators have noted a rather narrow interpretation of this concept by the Government of India and have criticized its potential implications.[12] It needs to be mentioned that the multi-stakeholder model itself has been criticized by stakeholders – both governmental and within the community – who, while recognizing its value as an organizational principle for cyberspace, find it vague and difficult to translate into practical measures. Consequently, the notion of multilateralism in Internet governance – an approach whereby major decisions are taken by states in a multilateral setting – emerged as a complementary concept, including in the Indian discourse. In light of the growing complexity of cyber threats and vulnerability of the critical public infrastructure, there has been a growing acceptance – also among the EU member states – of a higher role for governments compared to other stakeholders, especially faced with phenomena such as jihadi radicalization online.

[12] Anja Kovacs, "Is a Reconciliation of Multistakeholderism and Multilateralism in Internet Governance Possible? India at NETmundial", in *Internet Democracy Project Reports*, 4 September 2014, https://internetdemocracy.in/?p=2254.

4.3.2 Sovereignty in cyberspace

Concurrently, the debate is underway concerning governments' control over "their" cyberspace as an expression of sovereignty. The 2015 report by the UN GGE confirmed that "state sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."[13] However, despite the general agreement on the application of this principle of international law, it is still unclear what such provision means in practice, for instance with regard to uncooperative jurisdictions in cybercrime investigations or for relations with countries which commit abuses of human rights online. Linked to this is the question of perceived lack of transparency and accountability of the existing mechanisms through which decisions about cyberspace are taken. The position expressed by the Government of India on numerous occasions demonstrates confidence that "India is well-poised and willing to play an important and constructive role in evolving the global Internet governance ecosystem."[14] The challenge of ensuring greater transparency and accountability of governance in cyberspace is clearly visible in India's rather cautious approach to initiatives like the Budapest Convention, the Tallinn Manual or the Global Forum on Cyber Expertise – all of which are considered as "Western projects."

4.3.3 Protection of human rights online

Finally, an issue that obscures EU-India cooperation is the level of protection of human rights online in India, which is partly linked to the debate about privacy and data protection. Despite the commitment to the protection of human rights, India's repeated usage of the "Internet kill switch," usually during a period of anti-government demonstrations and in the absence of a comprehensive privacy bill,[15] makes such cooperation

[13] UN Group of Governmental Experts, *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, cit., para. 27.

[14] Statement by Vinay Kwatra at NETmundial welcome remarks, São Paulo, 23 April 2014, p. 61-65, http://netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Welcome-Remarks-en.pdf.

[15] Anuj Srivas, "India No Haven for Net Freedom But It Did Not Oppose UN Move on

complicated. India's stance in the debate about the UNHRC resolution[16] on the promotion, protection and enjoyment of human rights on the Internet was also ambivalent.[17] One area that has suffered considerably is EU-India cooperation in the fight against radicalization online and against the misuse of social media. Although high on India's agenda, this aspect has not taken off due to the EU's concerns about potential abuses by the government.

Of course, the EU's dialogue with India is not unique in the context of the EU's relations with other international partners. As a matter of fact, the whole international community is currently debating these issues and similar discussions are taking place with China, Japan, South Korea and the United States. The peculiarity of the EU-India dialogue, however, lies in the EU's recognition of the important role played by India and the keen interest in working together, on the one hand, and its incapacity to come up with a new, innovative approach to shaping this relationship in the future, on the other.

4.4 Understanding the limits of EU-India cooperation

Despite overarching agreement on the main security challenges and principles that govern inter-state relations,[18] including the governance of cyberspace, cooperation between the EU and India suffers from two major impediments that could be summed up as "guilty by association" and "principles-policy gap."

4.4.1 Guilty by association

Even where a trust-base exists, it is often the victim of anti-European sentiments in India or suspicion about India's real agenda among its Euro-

Internet Rights", in *The Wire*, 6 July 2016, http://thewire.in/49131.

[16] UN Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet* (A/HRC/32/L.20), 27 June 2016, http://undocs.org/A/HRC/32/L.20.

[17] Anuj Srivas, "Jammu & Kashmir Has Lost 18 Days of Mobile Internet Access over Last Four Years", in *The Wire*, 15 April 2016, http://thewire.in/29857.

[18] Samir Saran et al., *Prospects for EU-India Security Cooperation*, New Delhi, Observer Research Foundation, November 2016, http://www.orfonline.org/?p=27277.

pean partners. Neither perspective can be dismissed as irrational. Discussions with Indian government officials and experts – like the EU-India Security Dialogue hosted by Gateway House and the International Affairs Institute – suggest that Indian anti-Europeanism is mostly driven by association of the EU policies with the interests of the United States and by the perceived unequal treatment of the EU's other partners. From the Indian perspective, the EU's stance on the adequacy finding of the Indian data protection regime is unfair given the large concessions that the EU has made towards the United States.[19] This sentiment – and the perception that the views of the developing countries and emerging economies are not adequately represented at the global level, as mentioned earlier – has pushed India to reject some of the potentially beneficial initiatives. For instance, in the bilateral Cyber Dialogue with the EU, India has signalled the lack of sufficiently qualified and certified experts who could testify in the courts. Such expertise and training are available within the capacity building provided by the EU's programmes in the fight against cybercrime, such as the Global Action on Cybercrime Extended (GLACY+)[20] that is implemented by the Council of Europe in compliance with the Convention on Cybercrime (henceforth the Budapest Convention). India, however, has not ratified the Budapest Convention – which it considers a US-driven project prepared without any consultation with a broader international community. For similar reasons, India is not part of the Global Alliance against child sexual abuse online. The European Union, on the other hand, is concerned about the ongoing Indian engagement with countries like Russia and China, especially within the BRICS context. Even though India officially endorses many of the principles that the EU stands for, some of its declarations send mixed messages. For instance, the GOA Declaration adopted at the 8th BRICS Summit reaffirms the paramount importance of principles such as political independence, territorial integrity and sovereign equality of states, the settlement of disputes by peaceful means, non-interference in internal affairs of other countries as well as respect for human rights and fundamental freedoms, including the right to priva-

[19] Sameer Patil et al., *India-EU Cooperation on Cyber Security and Data Protection*, Paper presented at the IAI-GH Rountable Discussion, Mumbai, 7 November 2016.

[20] See the Council of Europe website: *Glacy+*, http://www.coe.int/en/web/cybercrime/glacyplus.

cy. However, a rather questionable interpretation of these principles by Russia or China may raise doubts on India's views.

4.4.2 Principles-policy gap

Another issue that limits EU-India cooperation is the perceived gap between the values each side claims to uphold and how they are translated into concrete policies and actions. India's record on the protection of civil liberties[21] is often brought up in this context. For instance, the government has passed laws that criminalize peaceful expression despite the fact that respect for this and other fundamental freedoms is assured in the Constitution of India. Human rights defenders also argue that the government uses laws such as the sedition provisions of the penal code, the criminal defamation law, and legislation dealing with hate speech to silence any criticism of the government. Concerning cyber issues, as a strong advocate of the protection of human rights online and offline,[22] the European Union finds India's policy towards Internet shutdowns and blockage of social media problematic, even though it recognizes India's sovereign right to govern cyberspace within its territory. India, on the other hand, considers the EU's criticism unjustified given that several member states – including France and the United Kingdom – have significantly strengthened their control over the Internet as an element of the fight against terrorism.[23] In addition, the EU's concessions towards the United States – even in the aftermath of the Snowden revelations – are difficult to understand from the Indian perspective.

4.5 A "Pragmatic Idealism" through Network Diplomacy

The discussion presented in this analysis suggests that the main issue undermining EU-India relations is a persistent crisis of confidence and trust

[21] Human Rights Watch, *World Report 2016*, January 2016, p. 302, https://www.hrw.org/world-report/2016.

[22] Council of the European Union, *EU Human Rights Guidelines on Freedom of Expression Online and Offline*, Foreign Affairs Council meeting, Brussels, 12 May 2014, http://www.consilium.europa.eu/en/workarea/downloadAsset.aspx?id=15782.

[23] Freedom House, *Freedom on the Net 2016*, November 2016, p. 12-13, https://freedomhouse.org/report/freedom-net/freedom-net-2016.

on both sides, despite political declaration to the contrary. As a result, possible gains from a closer EU-India cooperation are lost. It is therefore crucial that both sides invest in initiatives that, on the one hand, improve the mutual understanding of each other's positions and, on the other hand, move practical and goal-oriented cooperation behind a political bracket in search of common denominators. Either way, EU and India need to recognize that security culture plays an important role also in the case of cybersecurity cooperation. Therefore, while acknowledging that strengthening the culture of cybersecurity is an important objective globally, one also needs to recognize that there is no single cybersecurity culture and that cultural sensitivities need to be better understood and decisions taken in a spirit of "pragmatic idealism."

This paper suggests that fostering learning and a trust-building dimension in the EU-India relations may significantly contribute to advancing cooperation. Consequently, in addition to traditional diplomatic avenues, this paper proposes that the EU and India should invest in network diplomacy[24] by reinforcing additional channels of cooperation that may contribute towards building the trust-based institutional fabric needed for a closer cooperation:

- *Local authorities and cities*: Most initiatives so far have focused on intergovernmental cooperation with little attention to strengthening cybersecurity cooperation between local governments, city councils, etc. In that sense, the infrastructure created by the World Cities Programme might be used to expand cooperation to include ICT security and critical infrastructure protection and cooperation on smart cities.
- *Research community*: The India-EU Joint Steering Committee meeting held in November 2015 in Delhi paved the way for a further strengthening of cooperation in research and innovation, and developing concrete solutions to common societal challenges such as water, health, energy and ICT. The exchange of good practices and lessons on the use of ICT for development and cybersecurity might help identify valuable pathways for advancing cooperation in this area, both bilaterally and in multilateral venues.
- *Cyber respondents*: Both the EU and India organize regular cyber exer-

[24] Patryk Pawlak, "Network Diplomacy in Digital Networks", in *Digital Debates. CyFy Journal 2015*, June 2015, p. 67-72, http://www.orfonline.org/?p=16184.

cises but their participation in individual initiatives has to date been non-existent. It is, therefore, worth exploring modalities under which such participation could be facilitated. In addition, regular contacts between specialized cybersecurity agencies and operators of critical infrastructure should be encouraged.

- *Diplomats and analysts*: Investment in track 1.5 and track 2.0 diplomacy has proven to be a useful measure in forging a better understanding between the EU and other global partners. Therefore, stronger support for such initiatives between EU and India could yield unexpected positive outcomes, including potential spill-overs to other development countries or groupings like BRICS. In that sense, both sides could gain a better understanding of their respective cybersecurity cultures and sensitivities with regards to international debates about cyber norms or the application of international law in cyberspace.

While these initiatives may appear to be low profile due to their apolitical nature, their implementation will require a lot of good faith and commitment on both sides. For the EU, it also implies the need for a more strategic use of instruments such as public diplomacy, better coordination of funding between different Commission services, and finally strong political commitment that will allow for more flexibility in the search for mutually acceptable solutions.

5.

EU-India Cooperation on Space and Security

Isabelle Sourbès-Verger[*]

Space technology is a full-fledged element of the Strategic Partnership[1] concluded at the fifth EU-India Summit held in November 2004.[2] It is specifically mentioned in the first section entitled "Economic Sectoral Dialogues and Co-operation" in the initiatives supported by the Joint EU-India Action Plan.[3] Ranked sixth in the 2005 Plan, it ranked ninth three years later in the 2008 Revised Plan.[4] It is considered as part of the "Sector Policy Cooperation" in the Agenda 2020 endorsed at the latest EU-India Summit on 30 March 2016,[5] but is not included within the Security section even if it may contribute to the achievement of some of those objectives. This positioning could be viewed as unexpected and merits examination. Indeed, space technology plays an increasingly decisive role in

[*] Isabelle Sourbès-Verger is Director of Research at the Centre Alexandre Koyré, Paris. The author wishes to thank Martin Sarret (Research Assistant) and Raymond Ghirardi (Cartography). This paper is based on academic research and interviews with officials and experts.

[1] European Commission, *An EU-India Strategic Partnership* (COM/2004/430), 16 June 2004, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52004DC0430.

[2] Council of the European Union, *Fifth India-EU Summit* (14431/04 Presse 315), The Hague, 8 November 2004, http://europa.eu/rapid/press-release_PRES-04-315_en.htm.

[3] Council of the European Union, *The India-EU Strategic Partnership Joint Action Plan* (11984/05 Presse 223), 7 September 2005, http://europa.eu/rapid/press-release_PRES-05-223_en.htm.

[4] Council of the European Union, *Global Partners for Global Challenges: The EU-India Joint Action Plan (JAP)*, 29 September 2008, http://europa.eu/rapid/press-release_PRES-08-277_en.htm.

[5] EU-India Agenda for Action-2020, 30 March 2016, http://www.consilium.europa.eu/en/meetings/international-summit/2016/03/20160330-agenda-action-eu-india_pdf.

life today, as well as in the world economy, and both the EU and India are currently developing ambitious space programmes for Earth observation (EO), communication and navigation.

As far as security is concerned, space definitely stands out as a critical emerging issue. It is widely recognized that satellites are essential tools to foster development, to monitor natural resources, and to address disaster preparedness and mitigation. They are also crucial to support communication, to master advanced technologies and even to nurture innovation. To a large extent, they are a matter of priority because of the need for stability and the safeguarding of national interests.

At the political level, space programmes are a key feature of the national and international image of any State. From this point of view, the contribution of space to security is crucial. Setting aside the merely national dimension in defence matters – a complex issue on the EU side due to the sovereignty of Member States – space cooperation represents an optimal choice for the EU-India Security Dialogue, especially considering global security issues such as climate change, natural disasters, the environment, water management, but also migrant flows, piracy and terrorism.

Moreover, as India and Europe are increasingly dependent on space assets, security in space has become a growing concern owing to natural and human threats: micrometeorites, debris, space weather and even weaponization. With regard to the latter issue, it should be noted that both Europe and India put particular emphasis on preservation of the peaceful uses of space. This could lead to the opening of a new discussion area for mutual benefit.

It is true that India and Europe have strong experience in cooperation on space matters through the Indian Space Research Organization (ISRO), the European Space Agency (ESA) and many national Member States' space agencies. Their primary expertise lies in research and technology-related issues and their intervention is requested for well-defined programmes. However, it would be appropriate to take into account their experience at the level of the EU-India Dialogue.

This paper provides an insight into the role and place of cooperation according to Indian and EU space policies (section 1). Then, it examines the main opportunities for developing space cooperation towards security on Earth (section 2). This raises the issue of security in space as a new

challenge for the EU-India Dialogue (section 3). An analysis of opportunities and challenges in the current context favourable to cooperation will follow (section 4). Political recommendations form the final part of the paper.

5.1 The prominent role of cooperation in building the space capabilities of India and Europe

From the 1980s onwards, Europe and India have enjoyed the status of space powers. Both of them have acquired space capabilities through cooperation, which remains a key element of their space strategies, unlike other countries such as China.

By the 1960s, European countries had established the foundation for cooperation agreements aimed to back up national programmes. Their newly designed framework includes two dimensions. On one side, the European Space Research Organization (ESRO), built upon the European Organization for Nuclear Research (CERN) model, is tasked with promoting scientific research and satellite development. On the other, the European Launcher Development Organization (ELDO)'s goal is to develop a launcher built with British, French, Italian and German contributions. The creation of a common space agency was only decided in 1973. The European Space Agency was charged with promoting R&D in the use of space for peaceful purposes – which essentially constitutes the ESRO's scientific programme – and to steer optional launcher development programmes. Thus, ESA Member States have independent launchers – Ariane and Vega – and can participate in joint European programmes while pursuing their own cooperation programmes within and outside of Europe. The European model of governance in space matters has proven to be efficient over the course of 50 years, with each State building its own partnerships depending on how much it is willing to invest. In the process, States consider the stakes in terms of industrial policy as the number of awarded industrial contracts depends on their financial contribution. Such a model could be a source of inspiration for EU-Indian cooperation and the implementation of dedicated programmes, jointly developed in areas where pooling resources is of prime importance, such as global monitoring.

Cooperation is also an overarching element of the building of India's space capabilities as its potential value was identified at an early stage as necessary for the development of the country based on the "leapfrog principle," whereby the country is catching up economically by skipping inferior technologies through the promotion of high tech industries. The Indian government advocated the construction of an international launch base in Thumba, for the purpose of acquiring the basics of space technology at the Thumba Equatorial Rocket Launching Station (TERLS) under the aegis of the UN and UNESCO while allowing the international community to conduct experiments with sounding rockets to study the terrestrial environment.[6] This was an essential step for India to acquire hands-on experience with launch activity. This interaction enabled ISRO to include launcher technology in its range of capabilities. Similarly, the principle of cooperation is a characteristic feature of India's approach to satellite technology. In the Cold War context, India's non-aligned status allowed the multiplication of partnerships with Russia, the US and other European countries, including France, depending on its needs and the circumstances. In a parallel process, its willingness to get involved in international institutions – UN, UNESCO – allowed the country to gain experience in a kind of cooperation that is not solely based on national interests. The maps below (Figures 1 and 2) give an overview of the diversity of cooperation conducted in space by India and Europe. As we can see, European-Indian cooperation is far from being exclusive but remains visible in numerous programmes and includes several space-sector actors at the European level.

Europe and India have a longstanding history of cooperation between space agencies, at the bilateral level, notably with France and the French National Space Agency (Centre national des études spatiales, CNES)[7] which is one of the oldest partners of ISRO, but also with ESA and the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT). However, the only direct interrelationship between Europe and India concerns the Galileo programme, where cooperation does not seem to be working so well.

[6] TERLS's strategic position in regard to the magnetic equator allowed particularly interesting experiments for the study of the Earth's magnetic field.

[7] Ajey Lele, "Space Collaboration between India and France: Towards a New Era", in *Asie.Visions*, No. 78 (September 2015), https://www.ifri.org/en/node/10311.

Figure 1 – Map of India space cooperation

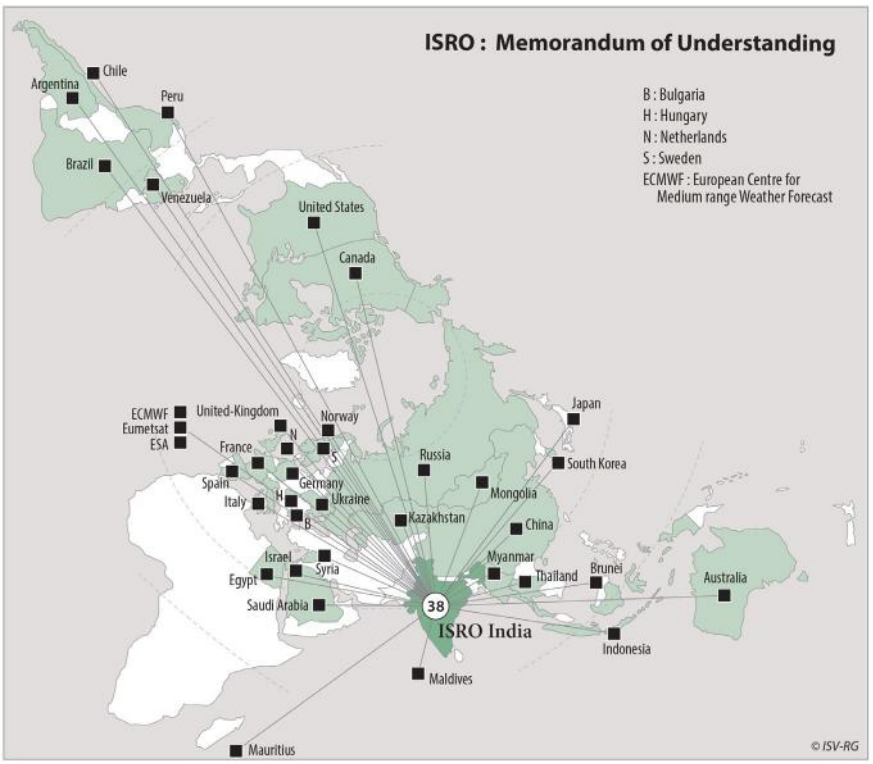


Figure 2 – European worldwide space cooperation

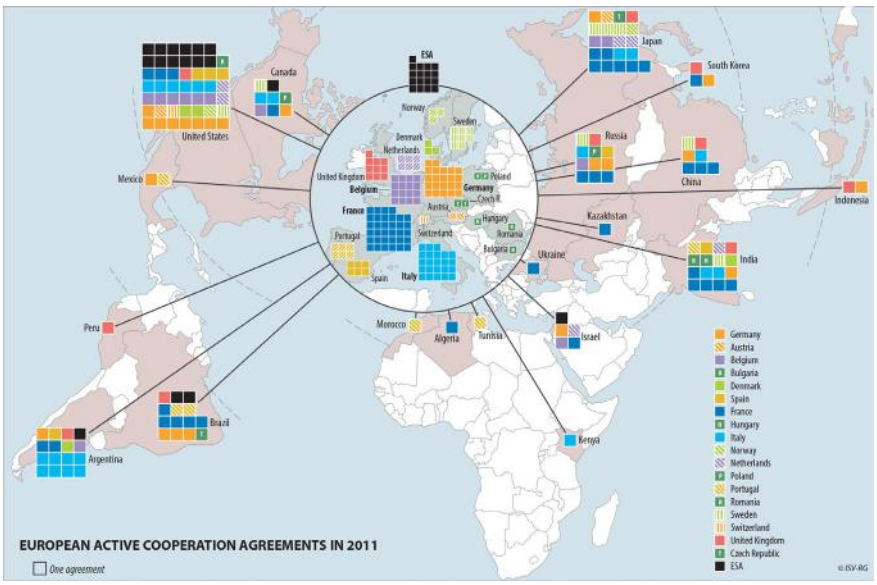
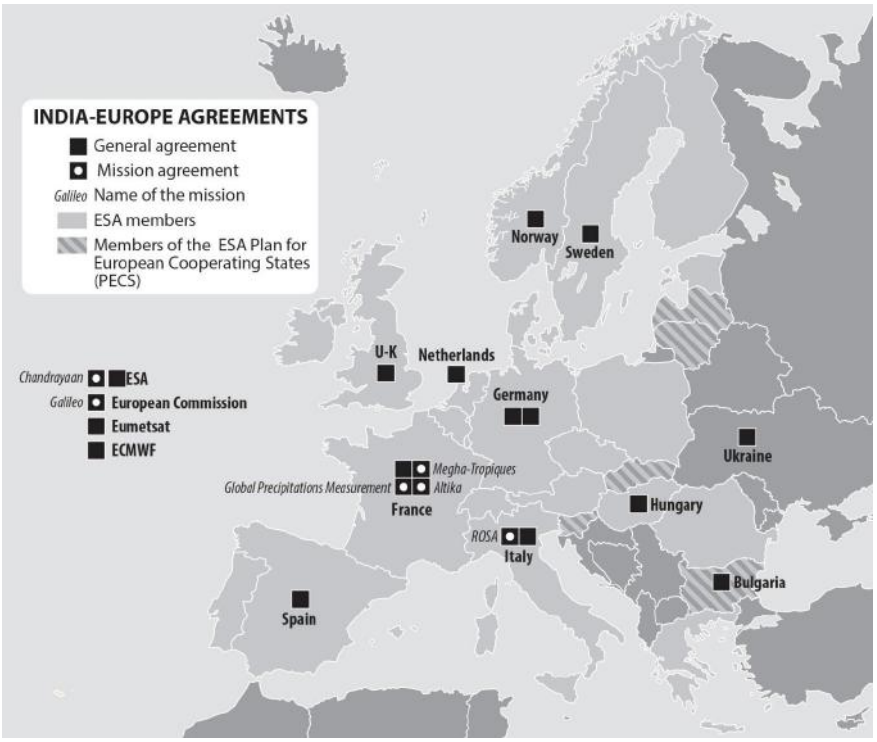


Figure 3 – Current cooperation agreements between European partners and India



This issue brings us back to the characteristics of the EU-India partnership and its limitations. Whereas diplomatic channels were established at the beginning of the 1960s and formalized in the 1994 Cooperation Agreement, they essentially dealt with business and development issues. Since the first bilateral summit held in Lisbon in 2000, diplomatic relations between the parties progressively developed through regular political dialogue, economic exchanges, annual summits and regular ministerial, senior official and expert-level meetings. The implementation of the Strategic Partnership in 2004, the Joint Action Plan in 2005 and the Country Strategy Paper for EU-India relations 2007-2013[8] display India's willingness to interweave economic relations with political and strategic considerations. In these documents, there is a wide range of topics to be observed, including trade and investment, science and technology, eco-

[8] European Commission, *India Country Strategy Paper 2007-2013*, March 2008, https://eeas.europa.eu/india/csp/07_13_en.pdf.

nomic and development cooperation, and security. Space capabilities can be put to use for most of these areas, and yet they are not mentioned. This might stem from the belief that space programmes' technicality ought to be directly handled by national agencies or ESA and not be taken into consideration at the EU level, possibly for lack of suitable community powers.

In fact, the capabilities of space systems could be better integrated in EU-India relations with an approach that includes the main challenges identified in the EU-India Dialogue.

5.2 The use of satellites to enhance national and international security

The European Security Strategy Policy published in 2013[9] acknowledges the need for an international order that is more multilateral and a greater involvement of new emerging powers such as India. Furthermore, Europe, for reasons due to its singular political structure, has to rely on its soft power capability.[10] In parallel, since the Lisbon Treaty, Europe has more agency in space matters. The communication "Towards a Space Strategy for the EU" adopted in 2011[11] makes it clear that European Space Policy should be considered as "a response to the social, economic and strategic challenges that we [Europe] face."[12]

This approach is compliant with the Indian government's approach that always has sought to promote space as a means to bring India back into the concert of nations as envisaged by Vikram Sarabhai, the father of the Indian space programme. This vision is shared by senior officials and chairmen at ISRO: "But we are convinced that if we are to play a meaning-

[9] European Council, *A Secure Europe in a Better World. European Security Strategy*, 12 December 2013, https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

[10] Annegret Bendiek and Christian Wagner, "Prospects and Challenges of EU-India Security Cooperation", in Shazia Aziz Wülbers (ed.), *India-EU Relations. A Critique*, New Delhi, Academic Foundation in association with EuroIndia Centre, La Rochelle, 2008, p. 167.

[11] Adopted by Council of the European Union on 31 May 2011, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/122342.pdf.

[12] European Commission, *Towards a Space Strategy for the European Union That Benefits Its Citizens* (COM/2011/152), 4 April 2011, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52011DC0152.

ful role nationally, and in the community of nations, we must be second to none in the application of advanced technologies to the real problems of man and society."[13] This political alignment is all the more important to take into consideration as India is seriously considering the development of systems not only for civil but also military uses,[14] which marks a strategic shift from the initial Indian space programme that did not include the military dimension.

Indeed, for a long time India's position on military space came in line with the 1967 Outer Space Treaty which promoted the use of space for peaceful purposes.[15] The definition of "peaceful" itself was a continuing source of debate for 20 years, as several countries considered that the wording completely excluded military satellites, while others considered it did not include humanitarian military missions, as "peaceful," according to them, was to not be interpreted as "civilian" but as the opposite of "offensive."

India's political shift can be understood by the general acceptance of the presence of military satellites as force multipliers but without direct offensive capability. For instance, the US has the biggest fleet of military satellites, followed by Russia and an increasing number of European countries such as France, Germany, the UK, Italy and Spain but also China.[16]

India's new stance[17] is compliant with the upgrading of its capabilities and explains the increasingly prominent role accorded to space assets by the military and intelligence. ISRO itself acknowledged that its effort

---

[13] Vikram Sarabhai quoted in P.V. Manoranjan Rao, "No Ambiguity of Purpose: The Indian Space Programme", in P.V. Manoranjan Rao (ed.), *50 Years of Space. A Global Perspective*, Hyderabad, Universities Press Pvt Ltd, 2007, p. 215.

[14] Rajeswari Pillai Rajagopalan and Arvind K. John, "A New Frontier: Boosting India's Military Presence in Outer Space", in *ORF Occasional Papers*, No. 50 (January 2014), http://www.orfonline.org/research/a-new-frontier-boosting-indias-military-presence-in-outer-space.

[15] Rajeswari Pillai Rajagopalan, "India's Changing Policy on Space Militarization: the impact of China's ASAT Test", in *India Review*, Vol 10, No. 4 (October-December 2011), p. 354-378.

[16] Isabelle Sourbès-Verger, "Strategic Space, a Variable-Geometry Concept", in Ajey Lele and Gunjan Singh (eds.), *Space Security and Global Cooperation*, New Delhi, Academic Foundation in association with the Institute for Defence Studies and Analyses, 2009, p. 61-74.

[17] Ajey Lele, "Indian Armed Forces and Space Technology", in *India Review*, Vol 10, No. 4 (October-December 2011), p. 379-393.

to build the high-resolution Technology Experiment Satellite (TES) programme in record time was motivated by the need to meet operational requirements of military forces during the Kargil conflict against Pakistan in 1999.[18] In the same vein, the telecommunications satellite launched in 2013 was meant to be put to use by the army.[19]

When it comes to the military use of space, the EU sits on the fence as well. The EU is in charge, with ESA – whose position on the civilian nature of such programmes has also shifted since the mid-2000s for pragmatic reasons – of the management of the two "dual-use" programmes, namely the Galileo constellation of navigation satellites and the Copernicus constellation of EO satellites.

Europe's military strategy essentially consists of bi- or multilateral cooperation mechanisms set up by Member States to share data related to national sovereignty, generated by military systems. The beginning of the 2000s saw an emphasis on maximization of satellite data programming, along with an effort to make national systems complementary for the sake of efficiency, through the establishment of an operational framework on the notion of common operational needs (known by its French acronym BOC, "Besoins opérationnels communs"). At the European level the Torrejón Satellite Centre – created in 1991 under the auspices of the Western European Union – became the European Union Satellite Centre (SatCen), an Agency of the Council of European Union in 2001.[20] It is considered an essential asset for the strengthening of the Common Foreign and Security Policy, especially for crisis monitoring and conflict prevention, as it provides products and services resulting from the exploitation of data including satellite imagery.[21]

An international conference on space security and cooperation was

---

[18] P.S. Goel, "Operational Satellite of ISRO", in P.V. Manoranjan Rao (ed.), *From Fishing Hamlet to Red Planet. India's Space Journey*, Noida, HarperCollins India, 2015, http://www.isro.gov.in/node/3122.

[19] GSAT-7 was launched for the Indian Navy in August 2013.

[20] Council Joint Action 2001/555/CFSP of 20 July 2001 repealed by Council Decision 2014/401/CFSP of 26 June 2014, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32014D0401.

[21] Jean-Pierre Darnis, Anna Veclani and Valérie Miranda, *Space and Security: The Use of Space in the Context of the CSDP*, Brussels, European Parliament, November 2011, http://www.europarl.europa.eu/thinktank/it/document.html?reference=IPOL-SEDE_ET(2011)433834.

held in 2007 on the initiative of two institutes: the Institute for Defence Studies and Analysis (IDSA, New Delhi) and the Centre for Defence and International Security Studies (UK). It was also a first step in bringing together European and Indian academics and experts on the issue.[22] The opening address was given by A.P.J. Abdul Kalam, former President of India and a very distinguished space scientist. The question he addressed was quite simple: "Can space cooperation lead to space security?" and his concluding remarks advocated the introduction of a World Space Vision for 2050 steered by a World Space Council to lay the foundations for a fairer planet.[23]

From a down-to-earth perspective it is worth mentioning that the introduction of reconnaissance satellites is pivotal to understanding international security on arms control and the signature of the SALT and ABM agreements in 1972 and 1978. The idea of leveraging space technology as a tool for international stabilization led several European countries and Canada to seek the international community's support at a time when only the US and the former USSR had such capabilities.[24] The problematic nature of the issue was still being debated at the beginning of the 1990s when the US was the last country to have a permanent global monitoring system – Russia's spending cuts having put an end to its programmes.[25] The improvement in image sensors and the wide commercial distribution of satellite imagery marked the dawn of a new era with the creation of Spotimage in France, commercializing Spot imagery (10 m) from 1985 onwards, the 1995 launch of India's first civilian satellite, the IRS-1C, with a resolution lower than 5 m and last but not least, the creation of American private companies with satellites offering metric resolution in 2000.

While the world is facing a growing number of security issues iden-

[22] The conference, entitled "Space Security: Scope and Prospects for Global Cooperation", took place in New Delhi on 13-14 November 2007.

[23] A.P.J. Abdul Kalam, "Can Space Cooperation Lead to Space Security?", in Ajey Lele and Gunjan Singh (eds.), *Space Security and Global Cooperation*, New Delhi, Academic Foundation in association with the Institute for Defence Studies and Analyses, 2009, p. 21-28.

[24] See the unsuccessful French ISMA, Canadian PAXSAT A&B, Swedish Tellus proposals made at the UN in the 1978-1981 period.

[25] Isabelle Sourbès, "Overhead Imagery for Arms Control and Disarmament Purposes: a European Perspective", in Steven Mataija and J. Marshall Beier (eds.), *Multilateral Verification and the Post-Gulf Environment. Learning from the UNSCOM Experience*, Toronto, York Centre for International and Strategic Studies, 1992, p. 187-198.

tified in the Joint Agenda 2020 (see section 4), the multiplication of EO systems of increasing performance and the enhancement of Europe's and India's own competencies should allow the promotion of an effective co-operation scheme in which political mechanisms, abiding by the principle of sovereignty, would complete each other's capabilities and would allow both countries to benefit from a network of multi-sensor systems offering a tremendous flow of images and reduced delays in data delivery.

5.3 Space security challenges, a new topic for the EU-India partnership

As mentioned above, satellites are instrumental for improving natural resource management, enabling national and international infrastructure and contributing in a decisive way to technological, scientific, strategic and even soft power capabilities. Their upkeep is thus a key concern and priority. However, satellites are not only subject to natural threats (meteorites, space weather effects[26]) but also human threats such as space debris generated by launch activity and anti-satellite technology (ASAT). The number of European and Indian satellites is already high. Moreover, this trend is on the increase. India announced the launch of 20 satellites within the next two years. For its part, with the launch into orbit of the Galileo and Copernicus constellations, the EU will own the largest number of European satellites. Therefore, security in space is a topic of growing interest for both India and the EU, and the ability to monitor the space environment has become crucial. Indeed, space surveillance (also known as Space Situational Awareness, SSA) is a true political and technical issue. It is meant to protect space assets from risk of in-orbit collision and curb emerging threats stemming from the weaponization of space.

On the diplomatic side, the EU tried to deal with the issue by proposing a draft International Code of Conduct (ICoC) meant to frame a global effort for space security. From the European perspective, the ICoC initiative was a turning point as it expressed a position that was common to all

[26] The effect of space radiation on satellites varies depending on the period and solar wind, hence the necessity of better understanding the phenomenon to forecast its fluctuations.

the players, some of which having only recently begun to take interest in the question. This approach promoted the "rules of the road in space" for greater transparency, and a more concrete regulation through the Technical and Scientific subcommittee of the Committee on Peaceful Uses of Outer Space (COPUOS). The idea was to offer an alternative to the Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT), submitted to COPUOS by Russia and China and which the United States firmly opposed, by considering a broader perspective on security centred on topics less controversial than space weapons, such as debris.[27]

The contents of the Code were unrestrictive as it only required respecting existing treaties and principles, implementing measures aimed at minimizing the risk of collision and interference with other objects or space activities as well as the creation of new debris, refusing actions that could endanger or destroy objects in space and accepting transparency and confidence measures (TCBM) such as launch notifications, base visits, etc. This proposal raised criticism by India and other countries on several accounts: it did not clearly forbid space attacks, although the right to self-defence was explicitly mentioned, it did not express a common approach on the aim of space activities, and it had no restrictive dimension. It shared a certain number of flaws with the Hague Code of Conduct (HCoC),[28] mainly the risk that future activities by new entrants be limited, for instance.

A second version published in March 2014 took the feedback into consideration. It clarified the aim of the initiative: to guarantee the "security, safety and sustainability of space activities,"[29] making an explicit reference to prevention of an arms race. However, the procedure being conducted outside the UN framework remained a problem. The new consultation that opened in 2016 finally resulted in an admission of failure and a re-

[27] Gerard Brachet, "The Security of Space Activities", in *Non-Proliferation Papers*, No. 51 (July 2016), https://www.sipri.org/node/3705.

[28] HCoC is a non-binding proposal to limit missile proliferation. For more information, see the official website: http://www.hcoc.at.

[29] Ajey Lele, "Deliberating the Space Code of Conduct", in Ajey Lele (ed.), *Decoding the International Code of Conduct for Outer Space Activities*, New Delhi, Pentagon Security International in association with Institute for Defence Studies and Analyses, 2012, p. 20, http://www.idsa.in/node/10440.

turn to discussions within the UN in accordance with India's stance. If the legitimacy of the EU to undertake such an initiative unilaterally may be questioned, it could offer a starting point for a new proposal made jointly with India. At least, this option can be discussed as part of the disarmament and non-proliferation part of the EU-India Dialogue (see section 4).

This political approach has an inherently technical component. The development of Space Situational Awareness (SSA) is a key issue for independent information on any kind of potential threat.[30] At present, the United States Space Surveillance Network is able to track more than 19,000 objects, and Russia is improving its system although on a smaller scale, while China is developing its own surveillance network. In Europe, some national capabilities exist and the process of developing a common network is in motion both in ESA[31] and in the EU, with the aim of being recognized as a full player on the field of space surveillance. India has begun to consider the acquisition of such a system,[32] as well as the pooling of systems with Europe, whose geographical position is advantageous in terms of complementarity.

5.4 Opportunities and challenges for EU-India cooperation

The Joint Statement issued at the end of the 13th EU-India Summit includes several points about security cooperation issues.[33] Although space is not mentioned, it deserves consideration on many levels. The EU-India Agenda for Action 2020 released at the same meeting explicitly includes space as an area of cooperation in the section entitled "Global issues/sec-

[30] European SSA focuses on three main areas: space weather (SWE), near-Earth objects (NEO) and Space Surveillance and Tracking (SST). Its aim is to give Europe an independent capability to watch for objects and natural phenomena that could harm satellites in orbit.

[31] Heiner Klinkrad et al., "Europe's Eyes on the Skies. The Proposal for a European Space Surveillance System", in *ESA Bulletin*, No. 133 (February 2008), p. 42-48, http://www.esa.int/esapub/bulletin/bulletin133/bul133f_klinkrad.pdf.

[32] ISRO is already using the Multi-Object Tracking Radar (MOTR) to detect debris.

[33] European Council, *EU-India Summit: Joint Statement, Agenda for Action and Joint Declarations*, 30 March 2016, http://europa.eu/!kq76NY.

tor policy cooperation." However, space technology is not identified as a tool to meet several objectives.

Opportunities for space cooperation should be seriously considered and were in fact identified in regard to the points put forward in these policies, but they do not intersect throughout the documents. They can be divided into two categories according if they are directly or indirectly related to security issues.

Opportunities directly related to security issues *stricto sensu*:

- contribution to the establishment of security cooperation: use of EO system, setting up a collaborative network of space surveillance;
- crisis management: data exchange for almost real-time information;
- international security in international fora: collaboration on issues related to the weaponization of space.

Opportunities related to global security issues at the core of the Agenda for Action 2020:

- climate: introduction of programmes based on EUMETSAT's cooperation model and of scientific projects focusing on research and innovation;
- environment: pooling of satellite optic and radar imagery;
- sustainable development: use of remote sensing and telecommunications satellites for better natural resource and major risk management.

Other dimensions of security considered in broader terms should also be included, such as:

- business opportunities in the defence industry: ensuring the continuity of cooperation programmes in satellite manufacturing but also development of joint ventures in the start-up sector;[34]
- digital: development of telecommunications satellites following a classical model or the Space 2.0 philosophy of constellations of small satellites;
- foreign policy aimed at reaching stability in South Asia and Africa: collaboration in joint programmes of remote sensing technical training, coordination of imagery systems or telecom bandwidths for distance

[34] Such as suggested by Narayan Prasad. See "Small Satellites for India's Security: A Techno-Entrepreneurial View", in *ORF Occasional Papers*, No. 81 (January 2016), http://www.orfonline.org/research/small-satellites-for-indias-security-a-techno-entrepreneurial-view.

learning or telemedicine, as India initially did for the country's first programmes of this kind, such as the Satellite Instructional Television Experiment (SITE);[35]

- migration:[36] control and localization by the Automatic Identification System (AIS) for digital radio.

Moreover, it is useful to raise the sensitive issue of technology transfer inherent to dual-use systems, an area in which Europe is largely bound to US decisions. This is an important discussion to be having and particular emphasis must be put on solutions with a multilateral approach rendered possible by the improvement of US-India relations and the continuity of the transatlantic dialogue on the European side.

In the same vein of sensitive issues, space surveillance programme known as Space Situational Awareness is not politically neutral. Europe is facing the reluctance of Member States to develop a collaborative satellite and space debris tracking system. Thus, we can envisage the creation of a space weather (SWE) monitoring system as a first step, which is a predominantly scientific project, and a near-Earth objects (NEO) monitoring system which deals with a global threat.

Indeed, if we consider the question of EU-India space cooperation from a broader perspective, an extensive review of the Joint Statement and the Agenda for Action shows that space opportunities tend to be overlooked in other strictly civilian domains whereas collaborative work is formally envisaged in pharmaceuticals and biotechnologies. Space opportunities – often referred to as a full-fledged element of the Agenda for Action – are reduced to Earth observation, without any mention of the Copernicus global monitoring programme for environment and security,[37] and the Galileo navigation system programme.

More broadly, it appears that the whole cooperation scheme, as conceptualized in the EU-India Dialogue, seems to ignore the wide range of opportunities that space technology can offer, not only in science and

[35] SITE was an experimental satellite communications project launched in India in 1975, designed jointly by NASA and ISRO.

[36] In the framework of the Common Agenda on Migration and Mobility (CAMM) between the EU and India.

[37] Initially called Global Monitoring for Environment and Security (GMES), Copernicus is a EU and ESA initiative.

technology, but also research and innovation. Indeed, this is a constant feature as space technology is 30 percent less present in the projects within the Framework Programme for Research and Technological Development (FP7) as shown by a study conducted by independent experts and published in 2012.[38] Considering that the EU and India have also agreed to intensify their cooperation on research and innovation, their statement highlights the extension of the India-EU Science and Technology Cooperation Agreement until 2020 and the setting up of mechanisms for jointly financing research and innovation projects.

For that reason, the political approach to space cooperation opportunities – on both the EU and the Indian side – should be re-evaluated.

5.5 Policy recommendations

It is fair to say that space is a topic of interest for both India and Europe but its contribution is underestimated in the EU-India Dialogue despite India's and the EU's programmes and ambitions. Similarly, it is not mentioned in policy documents such as the "Highlights of Cooperation Framework between the EU and India."[39]

This can be explained by various factors. First, space policies are key to the safeguarding of national interests and sovereignty. Second, the unique nature of space technologies and their symbolic dimension constitute a powerful tool for foreign policy goals. Third, outer space is increasingly an area of concern for international security.[40] But sovereignty, foreign policy and security policy are topical issues for which EU competencies are sometimes contested.

These weaknesses of the EU have played a well-identified role in disrupting the dialogue with India, and putting particular emphasis on trade agreements as consistent with EU priorities.[41] Moreover, India has

[38] Elisabetta Basile and Philippe Régnier, *Review of S&T Cooperation Agreement between the European Union and Government of the Republic of India 2007-2011*, Brussels, European Commission, 2012, http://dx.doi.org/10.2777/12336.

[39] European External Action Service, *Highlights of Trade and Economic Cooperation between the EU and India*, 17 October 2016, http://europa.eu/!DX93Dq.

[40] See *Space Security Index 2016*, November 2016, http://spacesecurityindex.org.

[41] Shazia Aziz Wülbers (ed.), *India-EU Relations. A Critique*, New Delhi, Academic Foun-

doubts over the EU's legitimacy to legislate on foreign and security policy issues given the political dissensions between Member States on various sensitive relevant topics for the EU-India Dialogue such as the recognition of India as a nuclear weapon State. The country prioritizes a bilateral approach to Member States and some few of them in particular, notably France in the space sector.

An additional difficulty is to be mentioned. Space cooperation generally takes place at the level of space agencies. But in Europe, the EU is a relatively recent and still marginal player in space policy compared to ESA and national agencies that have, in comparison, great technical know-how. As far as India is concerned, the role of ISRO is predominant in the policy-making process given its historical weight and its successful endeavours, even though political actors are more willing to get involved.

Negotiations on Galileo, the main EU-India space cooperation programme, have faced major difficulties.[42] They illustrate, on the whole, a rather severe judgement that can be traced in a 2015 report:

> The EU-India Strategic Partnership has lost momentum. Bilateral ties are not receiving sufficient priority from both sides. [...] On defence and security matters, India deals with EU Member States directly and has a good framework for cooperation with major European powers.[43]

The most recent bilateral EU-India summit aims to show that the Dialogue is entering a new phase with greater ambitions extending to 2020 as planned in the Agenda for Action. As far as space cooperation is concerned, especially when it comes to security, it is highly recommended that the EU and India make room for this specific area in the dialogues that have already been identified.[44]

---

dation in association with EuroIndia Centre, La Rochelle, 2008.

[42] Marika Vicziany, "EU-India Security Issues: Fundamental Incompatibilities", in Pascaline Winand, Marika Vicziany and Poonam Datar, *The European Union and India. Rhetoric or Meaningful Partnership?*, Cheltenham and Northampton, Edward Elgar, 2015, p. 275-315.

[43] Gulshan Sachdeva, *Evaluation of the EU-India Strategic Partnership and the Potential for its Revitalisation*, Brussels, European Parliament, June 2015, p. 1, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_STU(2015)534987.

[44] "New dialogues could be initiated on Afghanistan, maritime security, development cooperation, Africa and the Middle East." Ibid., p. 6.

Conclusion

The achievement of greater international stability is an objective shared by both the EU and India. The idea of global governance by a self-sufficient international institution is unlikely. Nonetheless, India[45] and Europe want to improve their political standing in international affairs. In this context, their space assets can help them both reach their goals. It has to be said that the principle of sovereignty and the difficulty of dealing with security and foreign issues in an institutional body like the EU, as compared to a single State, make the situation more difficult. On top of that, the issues of technology transfer and industrial cooperation complicate the whole situation. But it is crucial to bear in mind that space represents a real opportunity for broadening the dialogue for mutual benefit, and to recognize the value of deepening discussion, including a specific reflexion on a better integration of the competencies and experience of the national space agencies and ESA at the political level.

[45] Sunil Khilnani et al., *NonAlignment 2.0. A Foreign and Strategic Policy for India in the Twenty First Century*, New Delhi, Centre for Policy Research, February 2012, http://www.cprindia.org/node/3572.

6.

Potential and Challenges of India-EU Space Cooperation

Chaitanya Giri[*]

India is advancing its civilian space programme at a faster pace than ever before. This is evident in several such milestones as the actualisation of the Chandrayaan-1 (2008) and the Mars Orbiter-1 (2013) missions, the initial successes with the Reusable Launch Vehicle, the newly acquired heavy-lift capability with the GSLV Mark III (2014), the operationalisation of Navigation with Indian Constellation (NAVIC) (2016), and the ongoing commercial successes with the Polar Satellite Launch Vehicle.

New Delhi is a responsible space power that has grown from a modest colonial past. Since Independence, one of the foundational values of India's long diplomatic and cultural partnerships with most nations of the world has been the exchange of scientific knowledge. Such interactions make diplomatic relations more durable as compared to mere transactional and protocol-based exchanges.

Building on this value, India has cultivated strong bilateral and multilateral cooperation with several major space agencies – in the United States, Russia, France, Germany, Italy, Canada, and Japan. The country also provides satellite and rocket launch services to the developing world.

The coming together of India and EU's space programmes has immense civilian-strategic implications. However, space security, a crucial area of concern, has never been on the primary agenda between India and

[*] Dr. Chaitanya Giri is a ELSI Origins Network Scientist at the Earth-Life Science Institute, Tokyo Institute of Technology, Japan and Visiting Scientist, Solar System Exploration Division, NASA Goddard Space Flight Center. He previously worked at the Max Planck Institute for Solar System Research in Germany, where he was working on the European Space Agency's Rosetta mission to comet 67P/Churyumov-Gerasimenko.

the EU. As a geopolitically sensitive issue though, it demands greater and nuanced interaction.

The paper titled "EU-India Cooperation on Space Security" by Isabelle Sourbès-Verger for the Istituto Affari Internazionali, Rome, initiates a dialogue on this necessary interaction.

It raises several important points, as listed below, followed by this author's observations and commentaries.

6.1 INDIA AND EUROPE'S COOPERATION-DRIVEN SPACE PROGRAMME

The paper emphasises cooperation as the foundation for developing an intra-European framework of the national space programmes of the European Union (EU) member states, and for the evolution of the intergovernmental European Space Agency (ESA). It recommends this cooperative mechanism as a model for the India-EU space partnership in future.

Comment

The Indian scientific establishment of the 20th century was contemporaneous with the advanced countries of the world in its aspirations to pursue cutting-edge Earth and space exploration. Even during colonial rule, the country's scientists had already demonstrated exemplary proof-of-competence in this field. They collaborated internationally, operated a few, but top class, scientific institutions, won prestigious global accolades, and participated in or presided over international science coalitions.

At the same time, the establishment was aware that there was a wide technology gap between India and the then advanced nations of the world in crucial areas such as steel and metallurgy, mass manufacturing, automation, agriculture, health, transportation, precision instrumentation, communications, and power-generation. To rapidly minimise this gap, created by centuries of colonialism and arrested economic growth, India began to vigorously pursue science diplomacy.

India nurtured its science and technology partnerships with other nations through the International Geophysical Year (IGY, 1957-58). Con-

ceptualised in 1950, the IGY was the largest multilateral scientific engagement of its kind after World War II. India's scientific establishment, despite the varying tugs of alignment by the Soviet Union and the United States, was largely able to maintain its middle-ground and cooperate fairly and independently with all geopolitical and geoeconomic blocs.

At the present juncture, New Delhi perceives the EU as a remarkably cooperative region teeming with diverse member state-run space agencies, intergovernmental space agencies, and private space contractors all evolving synchronously. It has long-running space cooperation with many European Union member states, especially France and Germany.

India would be interested in forging space cooperation with the EU in areas of common interest.

6.2 India's cooperation on the Galileo programme

The paper points out the absence of progress on the (so-far) only potential space cooperation between India and EU – the Galileo navigation programme.

Comment

The EU, in Part I, Article 4 of the 2007 Treaty on the Functioning of the European Union, agreed to R&D of outer space as a shared competence between member states and the Union. Even so, the EU, in its Global Strategy for the European Union's Foreign and Security Policy (June 2016) has resolved to develop autonomy in space, security of its space-based services, and promotion of responsible space behaviour.

The executive wing of the EU, in partnership with private companies, is therefore reportedly creating nucleating centres for R&D in the space sector, such as the European Global Navigation Satellite Systems Agency (GSA) based in Prague, Czech Republic, and the EU Satellite Centre (EUSatCen) based in Torrejón de Ardoz, Spain. All this indicates the EU's intent to establish an autonomous network- and security-centric space programme.

The dual-purpose Galileo navigation programme is progressing at an intermittent pace and it will take a while to establish the entire satellite

constellation. Unlike civilian and commercial programmes, which often have a smooth progression, dual-purpose programmes are known to face geopolitical interference. If a non-nation sovereign unit like the EU intends to develop dual-purpose technological programmes like Galileo at a pace that serves its interests, it needs to follow two key aspects: indigenous competence and a limited number of confidantes.

So far though, India and the EU have not made any progress on their tentative cooperation on the Galileo programme. This is rooted in a context, as outlined below:

India is a peaceful democratic nation flanked by a volatile neighbourhood, including a state with nuclear weapons that promotes cross-border terrorism as a form of hybrid warfare. Additionally, India has a no-first-use policy. In this context, India faces specific vulnerabilities. It can be conjectured that as India increasingly began to suffer from external state-sponsored terrorism, since 1990s, its security forces must have plausibly felt the acute need for a vital satellite positioning/navigation data to keep a check on terrorist infrastructure. This external threat to national security and the compelling data deficiency brought to India's notice the stark necessity to develop indigenous competence in navigation/positioning systems.

In case of a war, India cannot afford to depend on any foreign positioning/navigation systems or be part of a delayed international navigation system project like Galileo. India therefore rapidly developed its NAVIC, which was operationalised in 2016 within a span of three years.[1] NAVIC serves India's security requirements, allowing it, when necessary, to neutralise conventional security threats; it helps the country to maintaining its national interests in a multipolar world.

6.3 On EU's diplomatic measures for addressing space security challenges

The paper discusses the EU's well-meaning attempt to promote its legally non-binding draft International Code of Conduct for Outer Space Activi-

[1] Indian Space Research Organisation (ISRO), *PSLV-C22 Successfully Launches IRNSS-1A, India's First Navigation Satellite*, 2 July 2013, http://www.isro.gov.in/node/384.

ties (ICoC), which is aimed at a global effort on space security. The author speaks of the possibility of the EU and India jointly writing a new ICoC-like proposal.

Comment

There will never be a lack of well-meaning diplomatic mechanisms for encouraging global peace and security, but there is always a dearth of the one mechanism that will completely realise this goal. True to this fact, in the past 16 years, several diplomatic mechanisms have been proposed. These include the EU-led ICoC, the Transparency and Confidence Building Mechanisms in Outer Space Activities by the United Nations Office of Disarmament Affairs, and the Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects jointly proposed by China and Russia.

The paper gives examples of geopolitical blocs opposing each other's diplomatic mechanisms. These oppositions establish three facts:

1. Those who draft space security agreements often deliberately overlook their own capability to inflict damage, and by doing so try to gain and maintain their own astrogeopolitical advantage.
2. They also often introduce clauses within agreements that are inimical to the interests of other nations.
3. Treaties and agreements are evolving much slower than the pace at which cutting-edge space capabilities (civilian, commercial, and military) are evolving.

Peace in space will prevail when the interests and abilities of all space-faring nations are in equilibrium. And this can only happen if crucial international bodies are democratised, especially considering the changing counters of geopolitical multipolarity.

If the revised version of the ICoC and its controls and checks were to apply globally, the ICoC will have to be apolitical, able to forecast futuristic threats, possess the most stringent and state-of-the-art control mechanisms, and ensure balanced participation by great powers, regional powers, and economically weaker states.

India's permanent membership in the United Nations Security Council (UNSC) would be a crucial factor in the success of any space security draft

it writes or co-writes. Therefore, democratising the UNSC is imperative if the stagnancy in outer space reforms movement is to be addressed.

6.4 Why India-EU space cooperation is nascent

The paper examines the reasons for the very limited India-EU space cooperation involving dual-purpose technologies and recommends possible areas for heightening the engagement.

Comment

Space cooperation between India and the EU space is still nascent when compared to the cooperation between India-France or India-Germany. This is largely due to the EU's limited autonomy over its tentative space programme. The EU is a large monetary contributor to the trans-governmental ESA. It runs its only two programmes with the ESA – Copernicus and Galileo. With such heavy dependency on the ESA, which is not an entirely EU agency, India views the EU as a promoter and facilitator of a tentative network- and security-centric dual-purpose space programme, rather than as a sovereign unit possessing a total autonomy over the programme.

The paper also refers to the EU's dependency on the U.S. for the transfer of dual-purpose technologies to India. At a time when India is interested in enhancing its indigenous capabilities, it will seek the transfer of only those dual-purpose technologies that it really lacks in and not those technologies that the provider itself is struggling to progress. All these factors have not helped EU-India cooperation.

It is evident from the roadmap charted in the EU-India Agenda for Action 2020 that the relations between the two sides are based on non-military common interests. In the same roadmap, space cooperation comes within the focus area of "research and innovation" and not under "security."

Therefore if a strong EU-India space partnership is to be forged, the path of space science research and space technology innovation will yield greater success than the path of military (dual-purpose technologies) partnerships. India-EU cooperation will be fruitful if it is not merely a vendor- purchaser exchange but a bilateral process between equal partners.

6.5 The scope of India-EU cooperation in monitoring space

The paper recognises that monitoring of space, also known as space situational awareness, is a crucial issue for all the major space powers of the world, including India and the EU. The authors view this surveillance as a technical as well as political issue.

Comment

Most space policy experts from across the world separate space security challenges into natural threats (space weather effects, meteorites) and anthropogenic threats (space-based weapons, surface-to-space weapons, runaway satellite debris scenarios). Most of these experts are in diplomacy-related think tanks, so they focus more on anthropogenic threats, which become the subject of perpetual diplomatic and political discussions. In this process, natural threats are underestimated. But this does not serve the comprehensive purpose of space security – or security from threats originating in space.

Celestial objects – the kilometre-sized asteroids, comets and their meter-sized fragments (meteorites, bolides) – that have the potential to cross the Earth's orbit and collide onto it – pose the highest form of hazard to life on Earth. Geological records testify that celestial objects were the cause of several life extinction events during the entire history of the Earth. Unfortunately, the world today does not have the necessary global infrastructure to mitigate this omnipresent but stealthy threat.

A recent sky survey done by the National Aeronautics and Space Administration suggests that more than 15,000 near-Earth objects (NEO) revolve close to the Earth, of which approximately 400 objects are deemed to be potentially hazardous.[2] The Earth annually receives an estimated 40,000 tons of non-hazardous microscopic extra-terrestrial material and an estimated 50 tons of meter-scale meteoritic material.[3] A considerable

[2] Jet Propulsion Laboratory (JPL), *Catalog of Known Near-Earth Asteroids Tops 15,000*, 27 October 2016, http://www.jpl.nasa.gov/news/news.php?feature=6664.

[3] S.G. Love and D.E. Brownlee, "A Direct Measurement of the Terrestrial Mass Accretion Rate of Cosmic Dust", in *Science*, Vol. 262, No. 5133 (22 October 1993), p. 550-553.

number of meter-scale objects enter the Earth's atmosphere and detonate with energies ranging up to a hundred mega tons of TNT.[4] Often such explosions occur over desolate swathes of land and oceans and hence go unnoticed.

But the meter-sized meteor that fell in 2013 over the city of Chelyabinsk in Russia exploded in the atmosphere with an intensity several orders of magnitude higher than the 1945 nuclear explosions.[5] The disaster damaged infrastructure worth billions of dollars and caused thousands of casualties.

Europe and the Indian subcontinent are both densely populated and have extensive rural and urban infrastructure. As a result, their geographical expanses are highly vulnerable to any falling celestial impactor. If a meter-sized meteor impact or an atmospheric meteor explosion were to occur over such densely populated regions of the world, it could cause terrible multi-dimensional and cascading consequences (mortalities, infrastructure, economic, social, and political).

Space situational awareness is already on the agendas of India and the EU. The Indian Space Research Organisation has expressed its intent to launch an asteroid exploration mission, possibly in the decade of 2020s.[6] The ESA and the American, German, and French space agencies have also received a proposal from a consortium of EU and American scientists for an Asteroid Impact and Deflection Assessment mission during the same time frame. Along the same lines, India and the EU can jointly develop ground-based NEO surveillance infrastructure within their territories. Sharing and pooling technical, scientific, human and monetary resources, will yield highly favourable results.

Michael Zolensky et al., "Flux of Extraterrestrial Materials", in Dante S. Lauretta and Harry Y. McSween Jr., eds., *Meteorites and the Early Solar System II*, Tucson, University of Arizona Press, 2006, p. 869-888, http://www.lpi.usra.edu/books/MESSII/9021.pdf.

[4] Jet Propulsion Laboratory (JPL), *New Map Shows Frequency of Small Asteroid Impacts, Provides Clues on Larger Asteroid Population*, 14 November 2014, http://www.jpl.nasa.gov/news/news.php?feature=4380.

[5] Olga P. Popova et al., "Chelyabinsk Airburst, Damage Assessment, Meteorite Recovery, and Characterization", in *Science*, Vol. 342, No. 6162 (29 November 2013), p. 1069-1073.

[6] Vijay Karthik, "ISRO Working on Launching Spacecraft to Venus, Asteroids: A.S. Kiran Kumar", in *Livemint*, 8 September 2016, http://www.livemint.com/Science/1Qn4uyqO0pe8iwIbqKX9AN/Isro-working-on-launching-spacecraft-to-Venus-asteroids-A.html.

The EU-India Agenda for Action-2020 has already listed "enhanced cooperation for joint scientific payloads" as one of the areas of cooperation.[7] Space missions like Rosetta and Chandrayaan-1 have demonstrated the enormous scientific discoveries that payloads are able to spin-off. (A space payload could be any scientifically valuable analytical instrument that carries out measurements of physical phenomena in space or transports passengers in space. In this context, a payload is an analytical precision instrument monitoring and analysing targeted local samples or scanning a physical matter remotely.) The agenda to co-develop scientific payloads for space exploration not only aids research and innovation but also precision manufacturing, trade, and skilled employment.

India and the EU's member states have a strong history of sharing scientific payloads, including the German-led SIR-2 and the Bulgarian RADOM instruments on the Indian Chandrayaan-1 mission (2008), the Indo-French Megha-Tropiques (2011) and SARAL-ALTIKA (2013) missions, and the French-contributed sodium vapour instrument to India's first-ever rocket launch at Thumba (1963). With robust rocket-launch infrastructures and technical expertise on both sides and a rich heritage of payload cooperation, India and the EU are favourably positioned to carry out joint NEO missions.

Concluding remarks

Astrogeopolitics is an inevitable successor to geopolitics. It therefore demands similar confidence-building measures as geopolitics – including regular bilateral and multi-lateral multi-track dialogues, joint-space gaming, techno-economic partnerships, and scientific cooperation.

Space security has several dimensions:

1. security of space-based assets from Earth-based anthropogenic threats;
2. security of space-based assets from another space-based anthropogenic threat;

[7] EU-India Agenda for Action 2020, 30 March 2016, http://www.mea.gov.in/Images/attach/EU_India_Agenda_for_Action_post_VC.pdf.

3. security of space-based assets from natural threats originating from outer space; and
4. security of Earth from natural threats originating from outer space.

The dialogue on space security should therefore not be constricted to merely anthropogenic threats but also include the more frequent and proven hazardous natural threats originating in space.

India-EU space cooperation, even for security issues, would be better served by the path of research and innovation and not through the geopolitically-sensitive dual-purpose technologies. Far greater value and attention must be given to space payloads in diplomatic interactions on space cooperation and space security.

7.

India-EU Defence Cooperation: The Role of Industry

Sameer Patil, Purvaja Modak, Kunal Kulkarni and Aditya Phatak[*]

Europe has for long been important in India's foreign policy priorities – more so as a continent that was able to emerge from the ravages of the two World Wars by overlooking its internal political differences and divisions to establish a supranational organisation. Despite the heavy losses and suffering inflicted on India by European colonial powers, after diplomatic relations were established between India and the then European Economic Community in 1963, the Indian policy establishment was eager to understand and leverage the benefits from Europe's regional integration process. The continent's advances in science and technology were especially alluring for India, which was looking to utilise technology for domestic development.

In 1993, the European Union was formed – but its member states had conflicting attitudes towards India. As a result, the relationship between the EU and India vacillated between distrust and misplaced expectations. It did not reach the next level of synergy and cooperation, despite India's explicit interest. Over time, it became much easier for India to develop closer ties with individual European countries.

---

[*] Sameer Patil is Fellow, National Security, Ethnic Conflict and Terrorism, at Gateway House. Purvaja Modak is Researcher and Assistant Manager, Research Office, Gateway House. Kunal Kulkarni is a former Senior Researcher at Gateway House. Aditya Phatak is Senior Researcher, Gateway House. Methodology followed for this paper is desk research and interviews with officials of the Government of India and officials of the EU delegation in India, serving and retired military officers, academicians, representatives of Indian defence companies and European defence companies operating in India.

7.1 Strategic partnership, little convergence

Both sides had shared beliefs in a stable international order, democracy, and the rule of law. Acting on these, in 2004, India and the EU formed a strategic partnership at The Hague Summit.[1] In 2006, India and the EU set up an annual Security Dialogue encompassing the Joint Working Groups (JWG) on counter-terrorism, cyber security, and counter-piracy.[2] And in 2013, a dialogue was established on non-proliferation and disarmament. While these mechanisms conveyed a sense of common understanding between India and the EU on the broader security dynamics, for most part the approaches of the two sides to key regional and international security issues have been quite different, and in some cases, even divergent.

For instance, many EU member states have been militarily engaged in Afghanistan for more than 10 years as part of the North Atlantic Treaty Organization (NATO)-led International Security Assistance Force. Yet, the EU has not made any substantive effort to consult with or include India in the process of political reconciliation with the Afghan Taliban, despite India's geographical location as a neighbour and an important contributor to Afghanistan's reconstruction.

Similarly, on terrorism there has been much common rhetoric, but very little cooperation between the two sides with regard to intelligence-sharing or countering terrorism financing. Another factor that has impacted India-EU interaction in the last five years is the Enrica Lexie case, in which two Italian marines were accused of the killing of two Indian fisherman off the coast of Kerala in February 2012.[3] Moreover, the protracted negotiations over the free trade agreement (FTA) between the two sides have also obstructed progress in other sectors of the relationship.

On some issues, India and the EU have clear disagreements, particularly on Pakistan and China – the main sources of security threats for In-

[1] Council of the European Union, *Fifth India-EU Summit* (14431/04 Presse 315), The Hague, 8 November 2004, http://europa.eu/rapid/press-release_PRES-04-315_en.htm.

[2] Embassy of India for Belgium, Luxembourg and the European Union, *India-EU Bilateral Brief*, 31 July 2016, http://www.indembassy.be/pdf/India-EU-Bilateral-Website-Brief-aug9-2016.pdf.

[3] Indian Directorate General of Shipping, *DG Shipping Press Release on Firing by Italian Ship on Indian Fishermen*, Mumbai, 16 February 2012, http://pibmumbai.gov.in/scripts/detail.asp?releaseId=E2012PR2301.

dia. Some Indian diplomats, who have served in the country's missions in Europe, have pointed out that the EU does not quite share or understand India's assessment of these threats. On other issues, India has objected to the activist stance of some Members of the European Parliament (MEPs). For instance, on the Kashmir issue, in the past, some MEPs – along with Pakistan's Inter Services Intelligence-backed organisations like the Kashmir Centre-European Union and Kashmir Centre-London – have highlighted, through lectures and events, India's alleged human rights violations in the Kashmir Valley. As a result, the Indian security establishment has questioned the EU's commitment to deepening ties with India.[4]

On the other hand, India's support to Russia and calls for a peaceful diplomatic resolution during the Ukraine crisis in 2013-14 drew critical reactions within the EU, which was keen to isolate Russia and impose sanctions.[5] Another factor which constrained cooperation was India's status of a non-signatory to the Nuclear Non-Proliferation Treaty (NPT). For long, the EU insisted that it can cooperate with India on defence and civilian nuclear issues only if India signed the NPT. This position seems to have softened after the 2008 India-U.S. civil nuclear cooperation agreement.

At another level, considering the EU's own struggle to evolve a common position on security and defence, and its standing as a major security actor in Europe in the context of NATO, many Indian officials and strategic analysts have questioned the practicality and relevance of engaging with the EU on security and defence issues.[6] The Global Strategy for the EU's Foreign and Security Policy document of June 2016, by the European External Action Service, also does not look at India as a security actor with whom ties can be enhanced to address regional and international security issues.[7] It primarily views India from the prism of economics – as

[4] US Department of Justice-Office of Public Affairs, *Two Charged with Conspiring to Act as Unregistered Agents of Pakistani Government*, 19 July 2011, https://www.justice.gov/opa/pr/two-charged-conspiring-act-unregistered-agents-pakistani-government; Praveen Swami, "Damaging Revelations Emerge from Fai Arrest", in *The Hindu*, 21 July 2011, http://www.thehindu.com/news/national/article2277658.ece.

[5] Neelam Deo and Karan Pradhan, "Ukraine", in Gauri Khandekar (ed.), *The EU-India Strategic Partnership. Facing the Foreign Policy Divide*, Delhi, Lenin Media, 2015, p. 113-125.

[6] Aditya Phatak, Aprameya Rao and Shefali Virkar, interviews with former Indian diplomats, Mumbai, August 2016.

[7] European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger*

an economic power, a part of the EU's economic diplomacy and a strategic partner in forging a free trade agreement. The only security area on which the two sides have converged, but with limited cooperation, is combating Somali piracy in the Indian Ocean.[8]

All these factors have contributed to the absence of a deeper defence cooperation between India and the EU. It remains a relationship that struggles to find its momentum.

7.2 Stronger relations between New Delhi and European capitals

The absence of a meaningful defence relationship with the EU collectively is in clear contrast to India's closer bilateral defence ties with individual European countries including France, the United Kingdom, and Germany. These ties have spanned defence and security dialogues, defence trade, and joint military exercises (see Table 1).

Table 1 – India's joint military exercises with European countries (2015-present)

Period	Type	Location	Name of exercise	Countries involved
April 2015	Naval	Off the coast of Goa	Varuna	France
June 2015	Army	Salisbury Plains, UK	Ajeya Warrior	UK
July 2015	Air	Lincolnshire, UK	Indradhanush	UK
September 2015	Naval	South Coast of UK	Konkan	UK
January 2016	Army	Jodhpur, Rajasthan	Shakti-2016	France
June-August 2016	Naval	Hawaii, US	RIMPAC 2016	26 countries in total hosted by the US. From the EU: Denmark, France, Germany, Italy, the Netherlands

Source: Gateway House Research, based on information from the Government of India's Ministry of Defence and the US Department of Defense.

Europe. A Global Strategy for the European Union's Foreign and Security Policy, 28 June 2016, p. 37-38, https://europa.eu/globalstrategy/en/language-versions.

[8] Sujay Mehdudia, "India, EU Join Hands for Anti-Piracy Military Operations", in *The Hindu*, 24 January 2012, http://www.thehindu.com/news/national/article2826395.ece.

For long, a major component of India's relationship with European countries was the purchase of defence equipment. Since Independence, India had made concerted but inadequate efforts to promote indigenous defence production.[9] As a result, and facing a hostile security environment in its neighbourhood, India had to rely on arms imports to augment its defence capabilities. Given their historical links, the UK was an inevitable initial source of defence equipment, before India turned to the Soviet Union for defence procurement in the 1960s. Some defence items were procured from France too in this decade, such as the Alize ASW aircraft and the Alouette helicopters.

The types of defence imports broadened by the early 1980s, when India began to acquire arms from West European countries, including Mirage aircraft from France, submarines from Germany, and the Anglo-French attack aircraft, SEPECAT Jaguar.[10]

While this trade was mostly with towards the Western Europe, Central and Eastern European countries such as Poland and the Czech Republic also got a share in India's defence market, primarily as a legacy of India's defence trade with the Soviet Union. Although the defence trade with Europe[11] may appear fragmented, it is consonant with India's foreign policy priorities and the need to diversify its military supplies. At present, European equipment provides some of the most critical capabilities for all the three wings of the Indian military (see Table 2, 3, and 4), some of which are also being upgraded. Broadly, Indian military personnel have found West European equipment to be technologically outstanding and reliable, but very expensive to procure and maintain.[12] However, many in the military have been doubtful about the quality of the spare parts coming in from Central and East Europe.[13]

---

[9] Sameer Patil, "The Business of Defence: Role of India's Private Sector", in *Gateway House Policy Perspectives*, No. 8 (12 May 2015), p. 2, http://bit.ly/1zXp5Bc.

[10] Stephen P. Cohen and Sunil Dasgupta, *Arming without Aiming. India's Military Modernization*, Washington, Brookings Institution Press, 2010, p. 77-78, 89.

[11] For the purpose of this paper, any reference to a EU or European company or companies will include: (a) a company registered as a European public limited-liability company (Societas Europea or SE) under the EU regulations on the Statute for a European company and allied laws, or (b) a company registered in an EU member state under the national laws of that particular state; (c) a company that is a subsidiary of a company registered outside the EU, and has a majority shareholding of non-EU persons, is excluded from this paper.

[12] Kunal Kulkarni and Aditya Phatak, interviews with retired and serving military officers, Mumbai, August 2016.

[13] Purvaja Modak, interview with retired Indian military official, Mumbai, August 2016.

Table 2 – European equipment in the Indian military

Service	Country	Vendor	Equipment
Indian Army	Germany	Diehl Remschied	Tracks and accessories for Arjun tank
	Poland	Polish Bumar	WZT-3 armoured vehicles
	Germany	EADS	Tactical Communications System
	Italy	Fincantieri	Two fleet tankers
	Spain	Nexter	Manufacturing of 1,400 155 mm towed cannons
	Czech R.	TatraTrucks	Tatra vehicles (in a JV with BEML Ltd)
Indian Air Force	France	Dassault Aviation	Mirage 2000 aircraft upgrade
		MBDA	Missile systems for Mirage 2000 upgrade
		Thales	Weapons system integrator for Mirage 2000 upgrade
	UK	BAE Systems	20 Hawk-132 jet trainers
		Cobham	5th generation air-to-air refuelling equipment
		Rolls Royce	AE 2100D3 engines on the C-130J Super Hercules fleet
	Germany	Dornier GMBH (license produced)	Dornier Do 228 turboprop utility aircraft
	UK & France	SEPECAT	SEPECAT Jaguar deep strike aircraft
Indian Navy	France	MBDA	Short-range surface-to-air missile
	UK	Vickers-Armstrongs Ltd	INS Viraat (originally commissioned as HMS Hermes) (to be decommissioned in late 2016)
	Germany	Atlas Elektronik	6 Active Towed Array Sonar systems
		Thyssen Krupp Marine Systems	Six HDW Class 214 submarines
		Dornier GMBH (license produced)	Dornier Do 228 turboprop utility aircraft
Mixed users	France	Aérospatiale (license produced)	Alouette III (Chetak) light utility helicopters

Source: Gateway House Research, based on the data obtained from the websites of the Indian Navy, Indian Air Force and Bharat Rakshak.

Table 3 – European defence companies operating in India

Company	Multinational ownership	Indian subsidiary	Projects/contracts/ proposals	Status	Contract type
Airbus (Netherlands)	France (10.9%), Germany (10.9%), Spain (4.1%)	Airbus India Operations (New Delhi)	Proposal to produce C-295 aircraft to replace the aging Avro aircraft of the Indian Air Force in partnership with Tata Advanced Systems Ltd (TASL)	No tangible progress yet; Awaiting trials for the C-295; process of evaluation and cost negotiation will begin after the trials	Commercial tender
Agusta Westland (subsidiary of Leonardo-Finmeccanica)	---	See Leonardo-Finmeccanica	12 AW101 helicopters	Deal was cancelled due to allegations of corruption and kickbacks	Commercial tender
Atlas Elektronik (Germany)	Krauss-MaffeiWegmann (51%), Airbus (49%)	Altas Elektronik India Pvt Ltd (New Delhi)	Manufacturing 6 Active Towed Array Sonar systems	Induction in progress	Commercial tender
BAE Systems (UK)	---	BAE Systems India Services Pvt Ltd (New Delhi)	Producing 20 BAE System Hawk-132 jet trainers	Being negotiated; agreement awaiting closure	Commercial tender
Cobham (UK)	---	Cobham India Pvt Ltd (New Delhi)	Cobham & TASL have agreed to manufacture Cobham's 5th generation air-toair refueling equipment as of July 2014	In production	Commercial tender
Dassault Aviation (France)	Dassault (55.55%), Airbus (23.36%)	Dassault Aircraft Services India Pvt. Ltd. (New Delhi)	36 French Dassault Rafale-B/C fighters in flyaway condition	Ongoing negotiations between India and France	G2G
DCNS (France)	Consortium with Navantia (Spain)	Scorpéne India Consortium	DCNS and Mazagaon Docks partnership for 6 Scorpéne class submarines	The first submarine began sea trials in October 2015; the next 5 submarines are expected to be delivered every 9 months, completing the project by 2020	Commercial tender
EADS (Germany)	See Airbus	EADS India Pvt Ltd (New Delhi)	Proposal for Indian Army's Tactical Communications System	Partnered with Tata in 2008 to secure bid	Commercial tender

Fincantieri (Italy)	Italian Co. Fintecna (72.5%)	Fincantieri India Pvt Ltd	Contract to supply two fleet tankers	Currently under investigation regarding the failure to meet specifications of steel as envisaged in the request for proposals	Commercial tender
Leonardo-Finmeccanica (Italy)	---	Selex ES India Pvt Ltd	Procurement of 98 heavy weight torpedoes for submarines	Request for proposal in this regard is withdrawn as of May 2016 due to controversy over allegations of improper procurement process	Commercial tender
MBDA (France)	Airbus (37.5%), BAE (37.5%), LF (25%)	Short-range surface-to-air missile for the Indian Navy	Talks with the DRDO and Bharat Dynamics Ltd	Commercial tender	MBDA (France)
Navantia (Spain)	Consortium with DCNS of France	Scorpene India Consortium	LPDs like INS Jalashwa for amphibious military operations	Existing memorandum of understanding (MoU) with Larsen & Toubro at Goa Shipyard	Commercial tender
Nexter (Spain)	---	Nexter Systems India Pvt Ltd	Manufacturing of 1,400 155 mm towed cannons	Final bid submitted for the tender	Commercial tender
Rolls Royce (UK)	---	Rolls-Royce India Pvt Ltd	AE 2100D3 engines on the C-130J Super Hercules fleet of six aircraft	Contract stipulated to be completed in 3 years	Commercial tender
Safran (France)	---	Safran India Pvt Ltd	Production of engine parts for Rafale aircraft	Project scaled back due to India's revised order	G2G
Thales (France)	---	Thales India Pvt Ltd	Upgrade of Mirage 2000 fleet, in partnership with Dassault	Upgrade progressing as scheduled; four upgraded jets have been already delivered till April 2016	Commercial tender
Thyssen Krupp Marine Systems (Germany)	Various German Corps (70%), Hellenic Shipyards (Greece) (25%)	Thyssen Krupp India Pvt Ltd	Proposal to participate in the submarine tender	Final tender not yet awarded	Commercial tender

Source: Gateway House Research, based on information from the websites of defence companies.

Table 4 – The European defence industry and its linkages to India

Country	Defence industry	Major enterprises	Cooperation with India	Bilateral treaties/ agreements with India
UK	- Large defence industry with heavy support from the government - Global share in arms exports is 5%	BAE Systems, Cobham	- Indian Navy operates BAE System's Sea Harrier aircraft - BAE's Hawk trainer jet is currently being produced under licence in India. - In-country assembly, integration and test facility for the M777 ultra lightweight Howitzer - TASL is manufacturing for Cobham's 5th generation air-to air refuelling equipment	2004, Strategic Partnership Agreement
Germany	- 5% share in global arms exports - Recently, the German government has sought to cut defence exports, particularly to West Asia - Some defence companies part of the major European companies such as Airbus	Krauss-Maffei Wegmann, Diehl Remscheid GMBH, Rheinmetall AG, Thyssen Krupp Marine Systems	- Ashok Leyland's JV with Krauss-Maffei Wegmann - Diehl Remscheid supplying tracks and accessories for the Arjun tank - Rheinmetall blacklisted by India on corruption charges - Navy operates a fleet of HDW diesel electric submarines	- 2006, Bilateral Defence Cooperation Agreement - 2001, Strategic Partnership Agreement
France	- 5% share in global arms exports - Heavily dependent on government spending for R&D investment	Dassault Aviation, MBDA, Thales, DCNS	- Extensive involvement in India - Many JVs with private defence companies	2006, Agreement on Defence Cooperation
Poland	- One of Eastern Europe's robust defence industries - Currently undergoing restructuring and consolidation - Major land equipment like tank, armoured vehicles, air systems - Many US companies source their components from Poland	Polish Bumar (Polish Defence Holding)	Bharat Earth Movers Limited has a contract with Polish Bumar for procuring armoured recovery and repair vehicles	- 2003, MoU on Defence Cooperation with 2011 addendum - 1996, Agreement Between India and Poland for the Promotion and Protection of Investments

Spain	- Major defence exporter in Europe - Government has encouraged domestic defence companies to partner with foreign companies - Companies including Airbus and General Dynamics have manufacturing facilities - The country has a 100% offsets policy	Indra Sistemas, Navantia, Instalaza SA	Navantia is part of the original contract awarded to the DCNS for the Scorpène submarines	- 2012, MoU on Defence Cooperation - 1972, Agreement on Trade and Economic Cooperation
Czech R.	- Defence industry underwent privatisation in early 1990s - Known for producing heavy equipment, radar technologies and jet trainer aircraft	TATRA trucks, OMNIPOL a. s., Gearspect Group a.s.	- Tatra trucks in partnership with Bharat Earth Movers Ltd. Has delivered 100 all-wheel drive vehicles - Omnipol is in collaboration with OFB, Heavy Vehicle Factory, Avadi and Heavy Engineering Corporation, Ranchi	2003, Agreement on Defence Cooperation
Bulgaria	- Large indigenous defence industry - Ranked as a "medium" small arms exporter	Arsenel AD, Kintex, TEREM, VMZ Sopot, Samel 90, Apolo GMBH, THOR Global Defense Group	- Arsenal AD supplied 67,500 AK-47 assault rifles to India's paramilitary forces, from 2010 to 2012, 9 of which proved defective in tests - The arms dropped over Purulia, West Bengal in 1995 were also allegedly procured from KAS Engineering Consortium, a stateowned Bulgarian agency[14]	1993, MoU on Defence Cooperation

Source: Gateway House Research, based on data obtained from the websites of Indian Ministry of External Affairs and Stockholm International Peace Research Institute (SIPRI).

[14] On 17 December 1995, a large consignment of arms including several AK-47 rifles and ammunition were illegally dropped from a Latvian aircraft in the Purulia district of West Bengal. The arms were intended for a spiritual organisation, Ananda Marga, to be used against the Communists in West Bengal. Six foreign nationals – one British and rest Latvian – were arrested and sentenced to life imprisonment. The alleged mastermind of the case, Niels Christian Nielsen, a Danish citizen remains at large. See Indian Central Bureau of Investigation, Judgment in the *Purulia Arms Dropping Case*, June 1997, http://cbi.nic.in/dop/judgements/padc.pdf.

7.3 India's military modernisation

At present, India is in the midst of a massive modernisation of its armed forces, given its persistent border disputes with Pakistan and China, and the Chinese Navy's growing profile in the Indian Ocean region. Estimates of India's military expenditure over the next decade, range from approximately 130 billion dollars (116.404 billion euros)[15] to approximately 223 billion dollars (Rs. 15 lakh crores/ 199,669 billion euros).[16] Most of these defence requirements (60 percent) have been met through the imported equipment.[17] This has made India the world's largest arms importer during the preceding five years, accounting for 14 percent of global arms imports.[18] More European equipment is proposed to be inducted (see Table 5) into the Indian military as part of this modernisation.

Table 5 – Proposed European equipment in the Indian military

Service	Country	Vendor	Equipment
Indian Air Force	France	Dassault	36 Rafale fighter planes
Indian Air Force	France	Airbus	C-295 twin turboprop planes
Indian Navy	UK	James Fisher Defence	Submarine rescue systems
Mixed users	Slovenia	Pipistrel Aircraft	194 microlight aircrafts

Source: Gateway House Research, based on information from the website of Indian Ministry of Defence and the websites of defence companies.

These imports have bridged the gaps in India's military capabilities from time to time, but this dependence on arms imports has also made the country susceptible to sanctions and technology denial regimes, which India witnessed after its 1974 and 1998 nuclear tests. Therefore, going

[15] Indian Ministry of Defence, *Make in India - Defence Sector*, 28 January 2015, http://pib.nic.in/newsite/mbErel.aspx?relid=114990.

[16] Sudhi Ranjan Sen, "On India's Shopping List, 500 Choppers, 220 Fighter Jets, 12 Submarines", in *NDTV*, 23 August 2016, http://www.ndtv.com/india-news/on-indias-shopping-list-500-choppers-220-fighterjets-12-submarines-1449315.

[17] See Make in India's website: *Defence Manufacturing*, http://www.makeinindia.com/sector/defence-manufacturing.

[18] Stockholm International Peace Research Institute (SIPRI), *Asia and the Middle East lead rise in arms imports; the United States and Russia remain largest arms exporters, says SIPRI*, 22 February 2016, https://www.sipri.org/node/1032.

forward, India is hoping to shed the tag of being the world's largest arms importer by achieving 70 percent defence indigenisation by the end of this decade.[19] A majority of the weapons procurement proposals cleared by the government in the last two years have been reserved for domestic production (see Table 6).

Table 6 – Weapons acquisitions cleared by India since 2014
(Reserve Bank of India rate as of 30 August 2016: 1 euro=75.1823 rupees)

Equipment	Vendor	Approximate cost
7 P17A stealth frigates	Mazagon Dock; Garden Reach Shipbuilders and Engineers	500 billion rupees (6,650.502 million euros)
6 P75I submarines	N.A.	600 billion rupees (7,980.602 million euros)
15 Chinook CH-47 heavy-lift transport helicopters	Boeing	70 billion rupees (931.07 million euros)
22 AH-64E Apache attack helicopters	Boeing	80 billion rupees (1,064.08 million euros)
Seahawk Multi-role S70-B helicopters	United Technologies	18 billion rupees (239.418 million euros)
4 Landing Platform Docks	Hindustan Shipyard Ltd and a private shipyard (contract pending)	250 billion rupees (3,325.251 million euros)
Avro aircraft replacement programme	Tata-Airbus (contract pending)	230 billion rupees (3,059.231 million euros)
Light utility helicopters	Rostec-Hindustan Aeronautics Ltd	60 billion rupees (798.06 million euros)

Source: Gateway House Research, based on information from the website of India's Ministry of Defence and news reports.

For this, India has launched the "Make in India" policy initiative, at the heart of which is the intent to create a domestic defence industrial base. Under this, the government has sought to tap the potential of private companies for defence production – the sector that is so far primarily dominated by state-owned enterprises.

Specifically for the defence sector, India has taken the following steps in the last two years:

[19] Indian Prime Minister's Office, *Text of PM's address at Aero India Show in Bengaluru*, 18 February 2015, http://www.pmindia.gov.in/?p=23700.

- Reviewing the country's direct foreign investment (FDI) policy and raising the cap for foreign investment to 49 percent from 26 percent,[20] and to beyond 49 percent through the government approval route in cases resulting in access to modern technology;[21]
- Allowing foreign investment in the manufacturing of small arms and ammunitions;[22]
- Updating the "Defence Products List" by de-licensing non-lethal and dual-use items;[23]
- Giving additional industrial licenses for defence production to a growing number of private companies, taking the total number to more than 150 companies[24] from 127 in 2010.[25]

In March 2016, India announced a new DPP, the policy under which military equipment is acquired. This policy aims to prioritise buying locally-developed military hardware for the three defence services through the introduction of a new category called Indigenously Designed, Developed and Manufactured.[26] Those Indian defence companies that can locally design and develop the required equipment will be preferred by the government of India's Ministry of Defence when it purchases new weapons for the military.

Even as it aims to increase the quantum of local defence production, India has also acknowledged that for the foreseeable future, high-technology arms import will continue to meet the current operational requirements of its military, as is evident in the proposed purchase of Rafale aircraft from France

---

[20] Indian Ministry of Defence, Answer to Lok Sabha Starred Question No. 198 [Domestic Manufacturing of Defence Equipment], 5 December 2014, http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=8674&lsno=16.

[21] Indian Prime Minister's Office, *Major Impetus to Job Creation and Infrastructure: Radical Changes in FDI Policy Regime…*, 20 June 2016, http://pib.nic.in/newsite/PrintRelease.aspx?relid=146338.

[22] Ibid.

[23] Indian Ministry of Defence, Answer to Lok Sabha Starred Question No. 198, cit.

[24] Indian Ministry of Defence, *Report of the Committee of Experts for Amendments to DPP 2013 including Formulation of Policy Framework*, July 2015, p. 29, http://www.mod.nic.in/forms/Sublink1.aspx?lid=2228.

[25] Indian Ministry of Defence, Answer to Lok Sabha Starred Question No. 256 [Private Sector in Defence Production], 15 March 2010, http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=84268&lsno=15.

[26] Indian Ministry of Defence, *Defence Procurement Procedure 2016*, March 2016, http://www.mod.nic.in/writereaddata/Background.pdf.

for the Indian Air Force. For imports, there is now an increasing preference within the Indian government to establish government to government (G2G) deals, rather than commercial deals, because of concerns over cost and corruption. Accordingly, the Rafale deal was moved from a commercial deal to the G2G sphere, where the Indian government has been negotiating with the French government, rather than with Dassault Aviation, for buying the planes. Similarly, in 2016, India scrapped a commercial tender for buying six aerial tankers from France's Airbus and is considering a G2G deal for the same.[27]

India has also initiated defence R&D and technology cooperation in the last 10 years with its top three arms supplier countries: the U.S. (Pathfinder projects, JWGs on aircraft carrier, and jet engine technologies),[28] Russia (BrahMos missile system, Fifth Generation Fighter Aircraft and the Multi-role Transport Aircraft), and Israel (Barak-8 missile system).

7.4 Opportunities in India's defence market

In view of the shrinking defence budgets in most European countries – notwithstanding the pledge by European NATO members to spend 2 percent of their GDP on defence by the end of the decade[29] – India, with its rising military expenditure, offers many opportunities for European companies. Earlier, a major area of contention for foreign companies, including European entities, about doing business in India was European ownership control over Indian joint ventures and the transfer of technology (ToT). With the relaxation of FDI norms in the defence sector, it is now possible for any foreign company willing to engage in ToT, to start a venture in India.[30] The new norms also allow them to tie up with Indian companies to cater to the domestic market and establish hubs for their global supply chains. Already, major Indian private sector companies such as

[27] "Government Scraps $2 Billion Mid-Air Tankers' Tender", in *The Asian Age*, 1 August 2016, http://www.asianage.com/india/government-scraps-2-billion-mid-air-tankers-tender-427.

[28] Sameer Patil, "Carter in India: A Foundational Visit", in *Gateway House Articles*, 14 April 2016, http://www.gatewayhouse.in/?p=93637.

[29] North Atlantic Treaty Organization, *Wales Summit Declaration*, 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[30] Aprameya Rao, interview with representative of Indian defence industry, Mumbai, August 2016.

the Tata Group and Mahindra Defence, through partnerships with foreign companies, have entered the global supply chain in the aerospace sector.[31]

European defence companies can substantially contribute to "Make in India" in land, air, naval, and electronic systems. India's major proposed acquisitions for the military are:

- Land systems: Infantry combat vehicles, specialised vehicles such as mine-protected vehicles, armoured vehicles and all-terrain combat vehicles, anti-tank and surface to air missiles, assault rifles;
- Air systems: Medium combat aircraft, land reconnaissance and maritime surveillance aircraft, unmanned aerial systems – surveillance and armed, medium and heavy-lift helicopters, light utility helicopters, VVIP transport helicopters, aerial tankers, amphibious aircraft;
- Naval systems: Aircraft carrier and associated systems, diesel-electric submarines with air-independent propulsion technology, Landing Platform Docks, guided missile frigates, interceptor boats.

There are also multiple opportunities in the sub-systems that form parts of the larger equipment. Other potential opportunities for European companies, especially through R&D and co-development, are in the defence electronics spanning systems, sub-systems, and systems of systems. At present, all three wings of the Indian military are in the process of integrating network-centric warfare capabilities, with the Indian Navy being the most advanced. By harnessing India's information technology sector as a hub, European companies can contribute to India's efforts to gain self-reliance in defence electronics.

Moreover, India has already made an effort to spell out the specific technologies required for its military. The Ministry of Defence, through the Technology Perspective and Capability Roadmap (TPCR), 2013, based on the Indian military's Long Term Integrated Perspective Plan 2012-27, has identified some high technologies related to sensors, propulsion, electronic communication, nano-materials, and other components (see Table 7), where foreign defence companies can significantly contribute.[32]

---

[31] G. Naga Sridhar, "Tata-Sikorsky JV Makes First Indigenous S-92 Helicopter Cabin", in *The Hindu*, 24 October 2013, http://www.thehindubusinessline.com/economy/logistics/article5267845.ece; "Make in India: Mahindra Group Bags Multi-Million Dollar Aerospace Deal with Airbus", in *The Economic Times*, 15 June 2015, http://ecoti.in/nswn6a.

[32] Indian Ministry of Defence, *Technology Perspective and Capability Roadmap (TPCR)*, April 2013, p. 5-28, http://www.mod.nic.in/forms/Sublink1.aspx?lid=2038.

Table 7 – Technological priorities identified by India

Category	Technologies
Communication/ electronic systems	- Information integration and analysis systems; battlefield information systems - C3I systems - Mobile satellite terminals with systems and applications supporting Software Defined Radios, including man-pack versions - Electrically controlled antennae - Pulse Power network technologies - Terahertz technologies
Space-based equipment	- Satellites producing sub-metric resolution images - Space-based radars and electronic warfare systems
Aerospace-related systems	- Long-range UAVs - Precision Air-Ground Weapons - Shared and Conformal Apertures - High performance turbo fan engines - Full Authority Digital Engine Control systems - Super Cavitations technology, - Super Cruise technology - Technologies for hypersonic flights (propulsion, aerodynamics, and structures)
Missiles	- BVR fire-and-forget air-to-air missiles - Surface-to-air missiles with electronic warfare capabilities - Anti-radiation missiles (air- and ground-launched varieties) - Stealth technology - Air-borne sensors and sensor fusion
Armament	- Electro-Magnetic Pulse weapons - Ammunition equipped with navigation and guidance systems - Electromagnetic Rail Gun technology - High-explosive squash head ammunition - Muzzle Reference System - Composite sabot manufacturing technology - Precision guided munitions - Advanced Recoil System - Gun barrel technologies
Nano-technology	- Nano-technology based sensors and displays
Others	- Artificial intelligence and robotics - Diesel-electric propulsion of ships and integrated electric propulsion generator - Fibre Lasers technology - Sensor technologies - CBRN protection suite, collective protection equipment, decontamination systems and equipment - Miniature SAR & ISAR technologies - High efficiency flexible Solar Cells technology - Molecularly Imprinted Polymers - Low Observable technologies - Technologies for generating High Power Lasers - Surface-Coated Double Base Propellant - Titanium casting, forging, fabrication, and machining - Under water systems including communication, sonar, stealth etc.

Source: Gateway House Research, based on data obtained from the websites of India's Ministry of Defence and the Defence Research and Development Organisation.

Separately, India's defence research agency, the Defence Research and Development Organisation (DRDO), regularly maintains a list for acquiring critical technologies such as those related to lasers and hypersonic flights.[33]

In addition to upgrading its military capabilities, India is also on its way to substantially upgrading the capabilities of its paramilitaries and police forces. This capability augmentation is especially important for India because even as it battles external security threats, a plethora of internal security challenges – insurgency in Jammu and Kashmir and the North East, left-wing extremism in central India, and porous borders – aggravate India's security situation. The need to augment the capabilities of the police forces became more urgent after the 2008 attacks in Mumbai exposed multiple vulnerabilities in India's security preparedness.

Under the Modernisation of State Police Forces Scheme, India is investing 123,790 million rupees (1,646.531 million euros) (2012-2017) including 4,329 million rupees (57.58 million euros) for Mega City Policing.[34] Capability addition for the police forces under this includes acquisition of armoured vehicles, weapons, and training equipment. In addition, some of the ongoing technology-based projects for potential deployment in the police force include ground-penetrating radar (for landmine and tunnel detection), explosive detectors, unmanned aerial vehicles, remotely operated robotic all-terrain vehicle, and thermal imaging.[35] There is an increased emphasis on installing closed-circuit television cameras for surveillance and controlling access to a location or area. Additionally, Indian paramilitaries such as the Border Security Force and the Sashastra Seema Bal are on a continuous lookout for technology-based solutions to plug gaps in border protection.

Many European companies have already sensed an opportunity with "Make in India" and have offered joint ventures and co-development projects (see Table 8).

---

[33] Defence Research Development Organisation (DRDO), *List of Critical Defence Technology Areas and Test Facilities for Acquisition by DRDO through Offsets*, May 2013, http://www.drdo.gov.in/drdo/English/List_of_Critical.pdf.

[34] See the Indian Ministry of Home Affairs' website: *Modernisation of State Police Forces (MPF) Scheme*, updated 29 March 2016, http://mha.nic.in/PMDivMPFScheme.

[35] See the website of the Indian Ministry of Home Affairs-Bureau of Police Research and Development: *Ongoing Projects*, updated 24 January 2017, http://www.bprd.nic.in/content/34_1_OngoingProjects.aspx.

Table 8 – Proposals from European defence companies since May 2014 under the "Make in India" initiative

Type of proposal	Indian company	European company	Nature of proposals
Co-development and technology	Larsen & Toubro Ltd (L&T) and Ashok Leyland Defence Systems	Nexter Systems (France)	A consortium agreement to collaborate for the Mounted Gun System artillery programme of the Indian Army
	TASL	Terma A/S (Denmark)	To jointly run the CMS Development Centre in New Delhi to work closely with the Indian Navy and support the modernisation process of Indian Navy, empanelment for the ongoing and future requirements of naval combat management system
	Hindustan Aeronautics Ltd (HAL)	Safran Helicopter engines (France)	Joint venture to establish a support centre in India for national and international rotorcraft customers
Systems	Mahindra Aerospace	Premium AEROTEC (Airbus) (Germany)	Large aero-components production contract
	TASL	Cobham (Wimborne, UK)	TASL will manufacture for Cobham's world-leading 5th generation air-to air refuelling equipment
	Reliance Defence and Engineering Ltd	Thales (France)	Sonar for surface ships and submarines, mine warfare and mine counter-measure equipment
	Larsen & Toubro Ltd (L&T)	Nexter Systems (France)	Nexter submitted, on 15 February 2016, its final bid in an Indian tender for a 1 billion euros (1.1 billion dollars) contract for 1,400 Caesar 155 mm towed cannons, and a pitch for its Trajan 155 mm/52 calibre gun
Sub-systems	Mahindra Aerospace and Defence	Airbus Helicopters (UK)	Airframe parts for the helicopter, AS565 MBe Panther
	Mahindra Aerospace and Defence	BAE Systems (UK)	In-country assembly, integration, and test facility for the M777 ultra lightweight howitzer (ULH)
Systems and subsystems	Kalyani Strategic Systems Ltd (KSSL)	Saab (Sweden)	Joint venture for the production and delivery of air defence systems

Source: Gateway House Research, based on information from the websites of defence companies.

However, most of these proposals are product-based, short-term partnerships. On the other hand, many Indian defence companies would also like to see a more long-term engagement from European companies in the form of commitment to set up defence R&D centres or transfer technology. This will enable the Indian companies to achieve economies of scale and secure contracts abroad.

Another pain point for Indian companies has been the Indian government's "No-Cost, No-Commitment" clause – the government will not bear the cost of the equipment trials nor is it committed to buy the equipment after the trials – in the procurement of defence equipment.[36] Since the trial of any defence equipment is a costly affair, many private companies are reluctant to participate in the bidding.[37] The foreign companies forming the JVs with their Indian partners should consider a burden-sharing model for this.

7.5 Potential minefields and challenges

As explained in the previous section, it is clear that multiple opportunities beckon European companies and they can play a niche role in meeting India's defence requirements. However, the potential minefields and challenges that can derail their prospects are:

a) *EU's dual-use regime*: The export control regime set up by the EU with regard to dual-use items presents a possible risk that could impinge on the defence cooperation between the two. The EU's dual-use control regime is extremely detailed, exhaustive, and restrictive.[38] Not only are there EU-level controls, but each member also has its own restrictions for brokering and transferring dual-use items. The complexity also suggests a high risk potential of disruption in

[36] Indian Ministry of Defence, *Defence Procurement Procedure 2016 - Capital Procurement*, 29 July 2016, p. 18, http://www.mod.nic.in/writereaddata/dppm.pdf.pdf.

[37] Mahendra Prasad, "'No-Cost, No-Commitment (NCNC)' Trials in Capital Procurements: Time for a Review", in *IDSA Comments*, 18 September 2012, http://www.idsa.in/node/10432.

[38] European Commission website: *Dual-use Export Controls*, updated 16 January 2017, http://europa.eu/!XQ46wc.

any future defence deal, especially in the supplies of hardware, given the large number of components that make up a weapons platform. For instance, under the October 2015 update of the EU "community regime," "fly-by-wire systems"[39] were added to the control list included under the Wassenaar Arrangement – which India is not a part of. More importantly, the EU is inclined to expanding its dual-use control regime despite its economic problems and political frictions.[40] A survey conducted by the EU in 2015 suggested that respondents favoured the development of the "catch-all" control process.[41] Under this, not only defence but any machine that could be remotely useful in any military programme deemed dangerous to the EU can be held back.

b) *EU's arms embargoes*: India has never been subject to an EU arms embargo. However, after India's 1998 nuclear tests, there were discussions within the EU about imposing EU-wide sanctions against India. The UK campaigned for these and for recalling all EU ambassadors from New Delhi, but was opposed by France, Germany, and Belgium.[42] As a result, there were no common EU sanctions, but some countries took national measures such as suspending development aid to India. Nearly all of the substantive sanctions were lifted three years later.[43] Indian policy makers are wary about a similar situation recurring, because despite the apparent compatibility in India's and EU's values in a stable international order, there are wide political differences between them on issues such as terrorism, human rights, and non-proliferation.

c) *Commercial rivalries among the European defence companies*: Bar-

[39] European Commission, Commission Delegated Regulation (EU) 2015/2420 of 12 October 2015 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items, October 2015, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32015R2420.

[40] European Commission, *EU Export Control Policy Review*, 23 November 2015, http://trade.ec.europa.eu/doclib/html/154003.htm.

[41] Ibid.

[42] Baldev Raj Nayar, *India and the Major Powers after Pokhran II*, New Delhi, Har-Anand, 2001, p. 112.

[43] Benjamin Kienzle, "Integrating without Quite Breaking the Rules: The EU and India's Acceptance within the Non-Proliferation Regime", in *Non-Proliferation Papers*, No. 43 (February 2015), p. 11, https://www.sipri.org/node/3217.

ring multinational European consortiums such as the Eurofighter Typhoon project, which lost out to Rafale in India's Medium Multi-Role Combat Aircraft competition, individual European companies generally compete with each other intensely for securing defence contracts abroad. This can sometimes lead to unethical business practices such as kickbacks, alleged corruption by rivals, and breaches of sensitive data. This is intended to damage the credibility of the rival companies, as evident in the recent data breach of the French company DCNS,[44] which is involved in India's Scorpène-class submarine project. In India's case, in the past too, some of these allegations involved European companies such as Tatra Trucks, AgustaWestland (now Finmeccanica), and BVT Poland. The combined effect of all this has been the cancellation of defence contracts, blacklisting of these companies, and prolonged investigations into the culpability of Indian middlemen and senior military personnel. This, in turn, has affected India's military modernisation plans. More importantly, it has reduced the scope and flexibility of enlarging cooperation with European companies.

d) *Impact of Brexit*: In terms of the strategic relationship, it is too early to assess how the UK's proposed exit from the EU will impact India-EU defence cooperation. But two potentially distinct scenarios can be expected. In the first scenario, the departure of a leading European military power can further weaken the EU's attempts to strengthen its military role in the continent and carve out an identity for itself that is distinct from NATO. This can impel India to further concentrate on bilateral channels to advance its defence cooperation with European countries. In the second scenario, Brexit may actually lead to better intra-EU defence cooperation as London had consistently blocked attempts at defence integration – it has resisted budget increases for the EDA and rejected proposals for the establishment of an EU headquarters for military operations, whereas other EU member states had pressed for integration (of

[44] Cameron Stewart, "Our French Submarine Builder in Massive Leak Scandal", in *The Australian*, 29 August 2016, http://www.theaustralian.com.au/national-affairs/defence/our-french-submarine-builder-inmassive-leak-scandal/news-story/3fe0d25b-7733873c44aaa0a4d42db39e.

defence forces to create a EU headquarters for military operations).[45] It is likely that a combination of factors – the situation at the EU's borders, falling national defence budgets, and that there could no longer be a British veto – will lead, over time, to deeper intra-Europe defence cooperation. This will make it easier for India to deal with the EU, even if it has less to offer. In any case, in terms of industrial cooperation, the UK is not a major contributor to European defence projects in India and its proposed departure from the EU should have no major impact.

7.6 Policy recommendations for deepening India-EU defence cooperation

As the European defence companies look for opportunities in India's military modernisation plans, a greater strategic convergence between New Delhi and Brussels will provide the necessary underpinning for a greater cooperation. At the last India-EU Summit held in Brussels in March 2016, both parties had agreed to enhance security cooperation, building on and strengthening the existing EU-India working groups on cyber, counter-terrorism, counter-piracy and non-proliferation, and disarmament.[46] To realise the true potential of the defence aspect of this strategic partnership and to strengthen the existing cooperation, the following measures are suggested in Table 9.

[45] Final Report of the Future of Europe Group of the Foreign Ministers of Austria, Belgium, Denmark, France, Italy, Germany, Luxembourg, the Netherlands, Poland, Portugal and Spain, 17 September 2012, p. 6-7, http://ec.europa.eu/dorie/cardPrint.do?locale=en&cardId=1275685.

[46] India-EU Joint Statement on the 13th India-EU Summit, Brussels, 31 March 2016, http://www.mea.gov.in/bilateral-documents.htm?dtl/26576.

Table 9 – Policy recommendations for deepening India-EU defence cooperation

Policy recommendation	Guiding principles
Strategic partnership	
Treating India as a strategic partner	The EU needs to build a strategic relationship with India, the way it has done with Israel and on the lines of what Israel has built with India – based on trust and technology-sharing. Cooperation between the EU and Israel has flourished despite the latter's status as non-signatory to the NPT. Given India's clean nonproliferation record, the EU should treat India in the same manner as Israel in building the strategic partnership.
Political interaction	
Annual summits	Despite an existing commitment to hold annual India-EU summits at the highest level, no summit was held between 2012 and 2016. Regular summits will help India and the EU to evolve a common understanding of foreign policy challenges facing both, such as the impact of Brexit.
Ministerial-level defence dialogue	While high-level visits such as the annual summits give the necessary visibility to the relationship, it is sustained engagement spread over multiple domains which will take the relationship forward. In this context, we propose a bi-annual Defence Dialogue between the Indian Ministry of Defence and the European Defence Agency (EDA) to develop and shape the India-EU strategic partnership and turn the existing bilateral defence ties between India and EU member-states into enhanced ties between India and the EU. The dialogue will also help EU officials to better appreciate India's sensitivities on issues such as Kashmir and iron out the known procurement hurdles.
Interaction with the Central and Eastern European countries	The focus within in the EU is mostly always on the West European countries. Therefore, this paper proposes that building on the involvement of Central and Eastern European countries in the Indian markets, India and the EU need to focus on engaging these countries in order to harness the opportunities for the "Make in India".
Security dialogues	
Strategic Intelligence Dialogue	A continued and increased interaction on intelligence and data-sharing between Indian and the EU security agencies to take forward the counter-terrorism cooperation. This engagement should preferably include sharing data on terrorist financing and money laundering activities. This interaction should also be used to reach a consensus on the UN Comprehensive Convention on International Terrorism, which India has been pushing for a long time.
Counter-terrorism cooperation	
Special forces interaction	Interactions such as the anti-terrorism exercises between the Special Forces from India and the EU will be a great catalyst for deepening the strategic engagement. Both sides have faced terrorist attacks of similar type and therefore have many lessons to share.

Homeland security collaboration	
Annual Homeland Security Dialogue	Unless the EU appreciates India's internal security and border protection challenges, it will be difficult for European companies to benefit from the opportunities that India's homeland security market has to offer.
Cooperation with other countries	
The EU, US and India business troika	Indian businesses are of the opinion that when it comes to doing business, American companies are more dependable than European companies, but Europe has an edge over the United States on many defence technologies. Hence, India can propose a trilateral dialogue with the EU and the US, looking at India's strategic national and defence interests as the priority.
Humanitarian Assistance and Disaster Relief (HADR) and Search and Rescue (SAR)	
India-EU joint military exercises	India already holds many joint military exercises individually with European countries. This can be taken to the next level to organise India-EU joint exercises for HADR or SAR operations. This will help them to develop interoperability.
Military engagement	
Continued senior command-level dialogue, exchanges, and exercises	As a matter of policy, even though the Indian Ministry of Defence and the Indian military does not deal with any blocs per se, the EU will need to find ways to increase its engagement with the Indian military. This engagement can also cover sharing notes on experiences from each other's participation in the UN peacekeeping operations.
Defence technology cooperation	
Defence Technology Dialogue	On India, the European countries need to shed their attitude of engaging in a transactional relationship. The G2G discussions focused on defence technology will bring more strategic content to the relationship and ensure unencumbered transfer of technology. The proposed dialogue will also help to understand the complexities and risks to India-EU defence relations from the latter's dual-use technology control regime. It can also help to identify technologies where India and the EU can collaborate, and to secure mutual assurances on non-addition of technologies that may figure in defence deals to the EU control list.
Business interaction and outreach	
India-EU Defence Trade meeting	It is necessary that there is a government-backed meeting of the defence companies from India and the EU to discuss possible collaborations, on the sidelines of an important event such as the Defexpo, the exhibition of weapons systems held biennially in India. This will help realistically evaluate the risks from the EU's dual-use technology regime. The discussions at these meetings could also include Intellectual Property Rights issues.
Setting up defence R&D hubs and Centres of Excellence	The European companies working in India can demonstrate their long-term commitment to India by establishing defence R&D centres and Centres of Excellence in India's academic institutions.

Conclusion

The India-EU defence partnership in the last decade has not realised its true potential, and this has further been affected by corruption and other issues. However, both sides should look at putting the past behind and focus on addressing critical challenges. India and the EU need to work on their common interest areas, forge collaborations, and expand the existing cooperation for mutual benefit. India's new policies, especially in the defence sector, encourage domestic production – EU members and companies can use these to their own advantage. With political dialogues and JWG meetings, the two sides can work towards solutions that facilitate growth of the strategic partnership. The increasing threat of terrorism and internal insurgencies necessitates that India and the EU must look at the larger picture and appreciate that a strong partnership between these two powers is the need of the hour.

Annexes

Table 10 – India-EU timeline of summits/important developments

Indian participants	EU participants
28 June 2000 (Lisbon) 1st India-EU Summit	
1. Prime Minister Atal Behari Vajpayee 2. External Affairs Minister Jaswant Singh 3. Finance Minister Yashwant Sinha 4. Commerce and Industry Minister Murasoli Maran 5. Information and Technology Minister Pramod Mahajan	1. European Commission President Romano Prodi 2. European Commissioner for External Relations Chris Patten 3. European Commissioner for Trade Pascal Lamy 4. European Commissioner for Research Philippe Busquin 5. High Representative for the EU's Foreign and Common Security Policy Javier Solana 6. Prime Minister of Portugal António Guterres (rotating Presidency European Council) 7. Portuguese Minister for Foreign Affairs Jaime Gama 8. Portuguese Minister for Science and Technology Mariano Gago 9. Portuguese deputy Minister for Economy Vitor Ramalho
23 November 2001 (New Delhi) 2nd India-EU Summit	
1. Prime Minister Atal Behari Vajpayee 2. External Affairs Minister Jaswant Singh 3. Human Resource Development, Ocean Development and Science & Technology Minister Murli Manohar Joshi 4. Commerce and Industry Minister Maran	1. European Commission President Prodi 2. European Commissioner for Trade Lamy 3. Prime Minister of Belgium Guy Verhofstadt (rotating Presidency European Council) 4. Belgian Foreign Affairs Minister Annemie Neyts-Uytterbroeck
10 October 2002 (Copenhagen) 3rd India-EU Summit	
1. Prime Minister Vajpayee 2. External Affairs Minister Sinha 3. Disinvestment Minister Arun Shourie	1. European Commission President Prodi 2. European Commissioner for External Relations Patten 3. High Representative for the EU's Foreign and Common Security Policy Javier Solana 4. Prime Minister of Denmark Anders Fogh Rasmussen (rotating Presidency European Council) 5. Danish Foreign Affairs Minister Per Stig Møller
29 November 2003 (New Delhi) 4th India-EU Summit	
1. Prime Minister Vajpayee 2. External Affairs Minister Sinha	1. European Commission President Prodi 2. European Commissioner for External Relations Patten 3. High Representative for the EU's Foreign and Common Security Policy Javier Solana 4. Italian External Affairs Minister Margherita Boniver (rotating Presidency European Council)
8 November 2004 (The Hague) 5th India-EU Summit	
1. Prime Minister Manmohan Singh 2. External Affairs Minister Natwar Singh 3. Minister for Commerce and Industry Kamal Nath	1. European Commission President Prodi 2. European Commissioner for Trade Lamy 3. High Representative for the EU's Foreign and Common Security Policy Javier Solana 4. Dutch Prime Minister Jan Peter Balkenende (rotating Presidency European Council) 5. Dutch Minister for Foreign Affairs Ben Bot

7 September 2005 (New Delhi) 6th India-EU Summit	
1. Prime Minister Manmohan Singh	1. European Commission President José Manuel Barroso 2. European Commissioner for Trade Peter Mandelson 3. UK Prime Minister Tony Blair (rotating Presidency European Council)
13 October 2006 (Helsinki) 7th India-EU Summit	
1. Prime Minister Manmohan Singh 2. External Affairs Minister Anand Sharma 3. Minister for Commerce and Industry Kamal Nath 4. National Security Adviser M. K. Narayanan	1. European Commission President José Manuel Barroso 2. European Commissioner for Trade Peter Mandelson 3. European Commissioner for External Relations Benita Ferrero-Walder 4. High Representative for the EU's Foreign and Common Security Policy Javier Solana 5. Finnish Prime Minister Matti Vanhanen (rotating Presidency European Council) 6. Finnish Foreign Minister Erkki Tuomioja 7. Finnish Minister for Foreign Trade and Development Paula Lehtomäki
30 November 2007 (New Delhi) 8th India-EU Summit	
1. Prime Minister Manmohan Singh 2. External Affairs Minister Pranab Mukherjee 3. Minister for Commerce and Industry Kamal Nath 4. National Security Adviser M. K. Narayanan	1. European Commission President José Manuel Barroso 2. European Commissioner for Trade Peter Mandelson 3. Portuguese Prime Minister José Socrates (rotating Presidency European Council) 4. Portuguese Minister of State for Foreign Affairs and Cooperation Joao Cravinho
29 September 2008 (Marseille) 9th India-EU Summit	
1. Prime Minister Manmohan Singh 2. Minister for Commerce and Industry Kamal Nath 3. National Security Adviser M. K. Narayanan	1. European Commission President José Manuel Barroso 2. High Representative for the EU's Common Foreign and Security Policy Javier Solana 3. European Commissioner for Trade Peter Mandelson 4. French President Nicolas Sarkozy (rotating Presidency European Council) 5. French Foreign Minister Bernard Kouchner 6. French Secretary of State for External Trade Anne-Marie Idrac
29 June 2009 (Prague) 20th Ministerial Meeting	
1. External Affairs Minister S.M. Krishna	1. EU Commissioner for External Relations Benita Ferrero-Walder 2. EU GAERC President, Czech Deputy Prime Minister and Foreign Affairs Minister Jan Kohout 3. Representative of EU High Representative for Common Foreign and Security Policy and the incoming Swedish Presidency Helga Schmid
6 November 2009 (New Delhi) 10th India-EU Summit	
1. Prime Minister Manmohan Singh	1. European Commission President José Manuel Barroso 2. European Commissioner for External Relations and Neighbourhood Policy Benita Ferrero-Walder 3. European Commissioner for Trade Catherine Ashton 4. Swedish Prime Minister Fredrik Reinfeldt (rotating Presidency European Council) 5. Swedish Foreign Minister Carl Bildt 6. Swedish Trade Minister Ewa Björling

22/25 June 2010 (New Delhi) 21st Ministerial Meeting	
1. External Affairs Minister S.M. Krishna	1. EU High Representative for Foreign Affairs Catherine Ashton
10 December 2010 (Brussels) 11th India-EU Summit	
1. Prime Minister Manmohan Singh	1. European Council President Herman Van Rompuy 2. European Commission President José Manuel Barroso
16/17 January 2012 (New Delhi) 22nd Ministerial Meeting	
1. External Affairs Minister S.M. Krishna	1. EU High Representative for Foreign Affairs Catherine Ashton
10 February 2012 (New Delhi) 12th India-EU Summit	
1. Prime Minister Manmohan Singh 2. External Affairs Minister S.M. Krishna 3. Trade Minister Anand Sharma 4. National Security Adviser Shiv Shankar Menon	1. European Council President Herman Van Rompuy 2. European Commission President José Manuel Barroso 3. EU Trade Commissioner Karel De Gucht
30 January 2013 (Brussels) 23rd Ministerial Meeting	
1. External Affairs Minister Salman Khurshid	1. EU High Representative for Foreign Affairs Catherine Ashton
30 March 2016 (Brussels) 13th India-EU Summit	
1. Prime Minister Narendra Modi 2. Minister of Commerce and Industry of India Nirmala Sithamaran	1. European Council President Donald Tusk 2. European Commission President Jean-Claude Juncker 3. EU High Representative for Foreign Affairs Federica Mogherini

Source: Gateway House Research, based on information from the websites of India's Ministry of External Affairs and the EU.

Table 11 – Joint ventures between Indian and European defence companies in India

Indian company	European company	Equipment offered
Ametek India	Enertec Management (Amertec Systems Pvt. Ltd.)	Electronic systems, simulators
Ashok Leyland Defence	Krauss-Maffei Wegmann	Artillery systems and armoured vehicles
Ashok Leyland Defence	Saab	Military vehicles
Axis Aerospace and Technologies	Thales	Aerospace equipment, flight simulators
Bharat Earth Movers India Ltd	Tatra Trucks	Military trucks
Bharat Electronics Ltd	Thales	Radar systems
Bharat Electronics Ltd	Terma	Naval radar systems
Hindustan Aeronautics Ltd (HAL)	Snecma	Aerospace equipment
Hindustan Aeronautics Ltd (HAL)	BAE Systems	Aerospace equipment
Hindustan Aeronautics Ltd (HAL)	Rolls Royce	Aerospace equipment
Hindustan Aeronautics Ltd (HAL)	Safran Helicopter Engines	Support centre for rotorcrafts (a rotary wing aircraft)
Indian Eye Security	Saab	Marketing tactical simulation systems
India Forge	DIEHL Remscheid (Track Systems India Private Ltd)	Tracks for armoured vehicles
Larsen & Tubro	EADS (including Cassidian)	Aerospace and electronic equipment
Larsen & Tubro	Nexter	Artillery systems
Larsen & Tubro	Thales	Avionics
Mahindra & Mahindra	Eurocopter	Helicopters and fixed wing aircraft
Mahindra & Mahindra	Saab	Air defence systems
Max Aerospace and Aviation	Snecma (Max Aero Engines Private Ltd)	Maintenance of military aircraft engines
Pipavav	Babcock	Aircraft carriers
Pipavav	DCNS	Shipbuilding
Precision Electronics	Raytheon	Communication systems
Samtel Avionics	General Dynamics	Digital displays
Samtel Avionics	Thales	To develop, customize, manufacture, sell and maintain Helmet Mounted Sight & Display (HMSD), Optronics and other Avionics systems for the Indian market

Tata Group	Airbus/EADS	Communication systems, proposal to produce C295 aircraft
Tata Group	AGT International	Homeland security solutions
Tata Group	Saab	Air defence systems
Tata Group	TCS-Rolls Royce	Engineering services
Tata Group	Thales	Optronic solutions
Tata Group	Agusta Westland	Assembling of AW119Kx helicopters (status unclear)

Source: Gateway House Research, based on information from the websites of defence companies and news reports.

8.

EU-India Defence Cooperation: A European Perspective

Stefania Benaglia and Alessandro R. Ungaro[*]

The ongoing turf war amongst EU Member States (MS) to position themselves at a comparative advantage results in a lose-lose situation that leaves European countries out of the real game: competing with global powers such as the US, Russia, China and soon to be India. The world powers of 2040 might well include India, but not likely any one single European country – unless the EU as a whole proves its value and becomes more integrated and capable of playing a credible global policy.

There is growing recognition by European industries of the need to better coordinate and consolidate the European Defence and Technological Industrial Base (EDTIB) in order to maintain its competitiveness on the global market. And since no European country can any longer afford, alone, new defence programmes and meet all of its own requirements from purely domestic sources, there is a clear need for greater consolidation on both the demand and supply sides.

As also highlighted in the EU Global Strategy (EUGS) by High Representative/Vice President (HR/VP) Federica Mogherini, EU institutions and Member States should facilitate this tendency and promote increased cooperation. Especially when looking at the EDTIB from India – where competition amongst major global defence players is fierce – there is a clear need for stepping up its coordination and integration. On the glob

[*] Stefania Benaglia is Associate Fellow in the Asia Programme at the Istituto Affari Internazionali (IAI). Alessandro R. Ungaro is Researcher in the Security and Defence Programme at IAI. This paper is the result of desk research activity and of a series of interviews with Italian institutions, European bilateral embassies in India and stakeholders from the European defence sector.

al scale, even the healthiest European company might face sustainability problems in the medium term.

There are a number of mechanisms that the EU can put in place to stimulate a fruitful competition amongst its EDTIB and prove the value of EDTIB as a whole, as competitive, innovative, high-tech and capability-driven. In addition, because the defence sector is closely interlinked with the political dimension – and given the Indian preference to purchase defence equipment through Government to Government (G2G) negotiations rather than through public procurement – the EU should also prove its value as interlocutor for discussions on defence, to partners such as India.

This paper provides recommendations on how industrial cooperation can be a driver to boost EU-India defence cooperation. Defence is indeed a major industrial European sector, directly employing about 400,000 people, up to another 960,000 indirect jobs, and generating a turnover of about 100 billion euros. In addition, India is a strategic partner of the EU, with whom it shares fundamental values, such as democracy – which is less and less valued throughout the world – and a certain view of foreign policy, without conflicting interests in the region.

8.1 An overview of the European defence market and industry

The European defence industry is one of the main European industrial sectors, fuelling innovation and growth to the wider EU economy. In 2013, the European Commission stated that with a turnover of 96 billion euros "in 2012 alone, it is a major industrial sector, generating innovation and centred on high-end engineering and technologies."[1]

As such, the defence industry has a pyramid structure with relatively few large companies at the top that act as system integrators/prime contractors. They put together complex platforms and systems by integrating different products, such as sensors and weapons, while in-

[1] European Commission, *Towards a More Competitive and Efficient European Defence and Security Sector* (COM/2013/542), 24 July 2013, p. 3, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52013DC0542.

teracting with Member States' defence procurement authorities, agencies and/or organizations such as the Organisation for Joint Armament Cooperation (Organisation Conjointe de Coopération en matière d'ARmement, OCCAR) and NATO. They are supported by lower-tiers companies on the supply chain, which produce specific components and subsystems.[2]

The European defence industry has three main subsectors: aeronautics, land and naval. Aeronautics is the main and most profitable sector with a turnover of 48.9 billion euros and approximately 180,000 people employed in 2014.[3] Considering its high level of technology and R&D costs, this sector has experienced collaborative projects between European countries with the objective of sharing the high and rising costs and to pool production orders.

In 2014, the land sector reached about 24.9 billion euros in turnover and employed around 130,000 people.[4] Compared to the aeronautics sector, it is less R&D intensive as demonstrated by the fact that roughly 80 percent of companies' sales are represented by defence-related and/or dual-use products whose application falls in the civilian domain (such as ammunition, sensor and security systems, and systems track/suspension components). After years of efforts in trying to consolidate this sector strongly affected by fragmentation and industrial duplication,[5] two of the leading European manufacturers of military land systems, the German Krauss-Maffei Wegmann (KMW) and the French Nexter Systems C, decided to merge, completing their association on December 2015. In effect, some experts argue that "only a number of functions will be pooled: co-

[2] These, in turn, are supported by their own suppliers and so on, involving a large number of small and medium enterprises (SMEs) which represent the basis of the pyramid.

[3] ASD/AeroSpace and Defence Industries Association of Europe, *Key Facts and Figures 2014*, November 2015, http://www.asd-europe.org/communication/publications/facts-figures.

[4] Ibid.

[5] Generally speaking, this limits the overall competitiveness of land sector when compared to US companies that are on average 1.5 larger than EU firms – and thus can benefit from significant economies of scale. For more information see, among others, IndustriAll, *Study on the Perspectives of the European Land Armament Sector*, 31 October 2012, http://www.industriall-europe.eu/Sectors/Defence/2012/INFF_E3779_Final%20Report_v02_clean.pdf.

operation in the supply chain, research and development, strategy definition, international marketing and sales, and communication" whereas "both trademarks still remain."[6]

Finally, the naval defence sector had a turnover of 22.5 billion euros in 2014 with about 80,000 employee.[7] These companies provide the full spectrum of services across the life cycle of a complex warship, from design and development to integration and logistic support. However, their relatively small market does not allow for significant economy of scale. A comparison with the US shows that the EU has 12 major warship companies versus two in the US, and that American firms are on average 3.4 times larger than in the EU.[8]

The presence of 28 national defence markets (soon to be 27, following the UK decision to leave the Union), each with its own regulations and bureaucracies, limits the development of the European defence industry by depressing competitiveness and preventing the exploitation of economies of scale. The lack of a fully integrated European defence market is therefore stifling the growth of the industry which underpins EU military capabilities and, ultimately, European defence policy itself.[9] Data show that Member States prefer to sustain national industry flagships and supply chains, and that they are adjusting to the financial crisis by relying on exports practices to third countries.[10]

---

[6] Hilmar Linnenkamp and Jean Pierre Maulny, "Krauss-Maffei Wegmann-Nexter: A Rapid Integration as the Key for a Real Marriage", in *ARES Group Comments*, June 2016, p. 3, http://www.iris-france.org/notes/krauss-maffei-wegmann-nexter-a-rapid-integration-as-the-key-for-a-real-marriage.

[7] ASD, *Key Facts and Figures 2014*, cit.

[8] European Commission, *Commission Staff Working Document on Defence* (SWD/2013/279), 24 July 2013, p. 4, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2013:0279:FIN.

[9] Valerio Briani, *The Costs of Non-Europe in the Defence Field*, Turin, Centro studi sul federalismo, April 2013, http://www.iai.it/en/node/793.

[10] The persistence of national rules and habits in the defence sector is indicated, for example, by the following data: in 2008-2010, more than 60 percent of the contracts in military equipment was awarded to domestic suppliers, 26 percent to providers from other EU MS and 5 percent to extra-EU suppliers. In addition, some data published by EDA show that in 2012 more than 80 percent of the contracts in the defence sector were still assigned nationally, especially in the area of defence procurement. EDA, *Defence Data 2012*, December 2013, https://www.eda.europa.eu/docs/default-source/eda-publications/defence-data-booklet-2012-web.

Overall, despite past and ongoing efforts to consolidate and integrate the European defence industry, this sector is still affected by fragmentation, overcapacities and duplications. The defence industrial production is mainly concentrated in six European countries, namely France, Germany, Italy, Spain, Sweden and the United Kingdom, with the defence industry in these countries accounting for 86 percent of the whole European defence production.

While bigger EU MS have the largest defence industries and account for the lion's share of all EU defence R&D and R&T expenditure, smaller countries mostly operate through SMEs or defence subsidiaries of civil-focused companies (which specialize in niche capabilities and/or form part of the supply chain for either European or American primes). Innovation takes place at all levels of the supply chain, from the prime system integrators through SMEs, and their relationship is indeed symbiotic: neither can expect to thrive without the other.[11] In this context, SMEs' role as subcontractors or suppliers of specialized components deserves particular attention as their contribution to the European defence industry is increasing, along with their role in the defence market. It is estimated that there are more than 1,320 defence-related SMEs, accounting for between 11 percent and 17 percent share of the EU's estimated sales of defence equipment.[12]

Because of domestic defence budgets cuts, including public expenditure in R&D and R&T, European defence companies are pushing their exports towards non-EU markets where competition is becoming ever more fierce – notably with the growing importance of Chinese production. Moreover, it should be kept in mind that the European defence market is not able to guarantee sustainable conditions for its defence industries; therefore, the level of European "dependence" on foreign markets is bound to increase.[13]

---

[11] The relationship between prime contractors and SMEs is mainly based on the so-called "risk-sharing partner" principle. According to this principle, the prime contractor assigns to the lower-tier companies the responsibility to design, develop and produce a new system. The development costs are thus distributed and shared between the prime contractor and its SME industrial partners.

[12] Europe Economics, *Study on the Competitiveness of European Small and Medium Sized Enterprises (SMEs) in the Defence Sector*, 5 November 2009, p. 43, http://ec.europa.eu/DocsRoom/documents/10486.

[13] The developing countries, driven by healthy balance sheets, trade surpluses and fi-

Against this backdrop, important initiatives have been taken by the EU and major European governments since the 1990s to strengthen the EDTIB and its competitiveness. Briefly, after the establishment of OCCAR in 1992 by four major European countries and the Letter of Intent (LoI) Framework Agreement signed by six major European countries in July 2000, an important step forward has been the creation of the European Defence Agency (EDA) in 2004 with the aim of contributing to the creation of a competitive European Defence Equipment Market (EDEM) and strengthening the EDTIB. Although defence remains mainly in the hands of EU MS, the European Commission has been playing an increasingly crucial and enabling role, starting with research, technological innovation and support for the competitiveness of the European defence industry. One of the most concrete examples of such involvement has been the so-called "Defence Package" (chiefly Directives 2009/43 and 2009/81) that forms the backbone of the EDEM and provides the Union with a legal instrument tailored to the specific nature of "sensitive" purchases in the defence and security sector.[14]

Most recently, after the release of the EU Global Strategy (EUGS) by HR/VP Federica Mogherini, there is a strong and renewed interest in the defence integration process. Outlining all the initiatives under discussion at the EU and intergovernmental level is beyond the scope of this paper.

---

nancial resources, are exploiting this unbalanced situation by requiring offset agreements to create their own Defence and Technological Industrial Base (DTIB). Indeed, these countries see offsets as a driver or stimulus for industrial development of the indigenous defence sector and capabilities, and are increasingly looking for medium- to long-term partnerships to cement relationships beyond the main purchase through the establishment of joint ventures, co-productions and licensed production. See, among others, Alessandro R. Ungaro, *Trends in the Defence Offsets Market*, paper presented at the SIPRI 17th Annual International Conference on Economics and Security (ICES), Stockholm, 14-15 June 2013, https://ssrn.com/abstract=2386528.

[14] Directive 2009/43/EC aims at simplifying terms and conditions of transfer of defence-related products within the EU. In fact, one of the obstacles affecting the market is that some Member States do not distinguish between exports to third countries (outside the EU) and transfers between Member States. This directive aims to address these obstacles by simplifying administrative procedures. Directive 2009/81/EC seeks to introduce a degree of competition in public procurement, while ensuring confidentiality of information and Security of Supply. However, it does not apply if a national government decides to rely on Article 346 of the Treaty on the Functioning of the European Union (TFEU), nor if contracts are settled on the basis of international agreements.

However, it is worth mentioning some proposals concerning the EDTIB. The aforementioned EUGS has underlined that "a sustainable, innovative and competitive European defence industry is essential for Europe's strategic autonomy and for a credible CSDP [Common Security and Defence Policy]."[15] For this reason and in line with the December 2013 European Council conclusions,[16] the European Commission proposed a European Defence Action Plan (EDAP) as a framework to promote the required EU policies and push for increased defence industrial cooperation.[17] The debate is currently open on three main levels of action: (1) EU-funded defence research, innovation and technology; (2) financial and tax incentives; and (3) internal market measures to support the competitiveness of the defence industry sector.

8.2 Most prominent areas of possible EDTIB cooperation with India

With a sustained GDP growth around 6 percent in the last 5 years,[18] the Indian defence budget is also in expansion. In 2015/2016, India's defence budget allocation was about 40 billion dollars, an increase of nearly 8 percent over the previous year, and it will likely continue to increase at a similar rate over the next five years.[19] However, although the expenditure is increasing rapidly, a detailed analysis seems to suggest that the relative allocation is imbalanced towards salaries and personnel. The share of funds for procurement, R&D and testing has decreased from 34 percent in 2005 to 25 percent in 2016.[20] That's why spending on defence acqui-

[15] European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, 28 June 2016, p. 46, http://europa.eu/globalstrategy/en/node/2.

[16] European Council, *Council Conclusions 19-20 December 2013*, http://data.consilium.europa.eu/doc/document/ST-217-2013-INIT/en/pdf.

[17] European Commission, *European Defence Action Plan* (COM/2016/950), 30 November 2016, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52016DC0950.

[18] World Bank, *India GDP Growth (Annual %)*, http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=IN.

[19] Deloitte, *2016 Global Aerospace and Defense Sector Outlook. Poised for a Rebound*, January 2016, p. 16, http://deloi.tt/2hsu8SH.

[20] Economist, "Opportunity Strikes", in *The Economist*, 16 April 2016, http://econ.

sition remains roughly flat in real terms and lower when compared to the 2013-14 peak, despite an increase in the overall budget.

Having said that, it is a matter of fact that India offers significant business opportunities for European defence companies. Such opportunities are also clear in consideration of the fierce competition occurring in the international defence market and especially in the Middle East, a region where the EU is entertaining strong interests in terms of foreign and security policy. According to the IHS Global Defence Trade Report released in June 2016,[21] Saudi Arabia and the UAE together imported 11.4 billion dollars (17.5 percent of the global total) in defence systems in 2015, up from 8.6 billion dollars in 2014, more than the imports of all Western Europe combined.[22] The biggest beneficiary of the strong Middle Eastern market remains the US while, surprisingly, the second tier of exporters to the Middle East is led by Canada, moving the UK to fourth place, just behind France. Germany and Russia each saw a 25 percent growth in exports to the region by a total amount of 1.4 and 1.3 billion dollars, respectively.[23]

India entertains a strong defence cooperation with Russia, the US, Israel and France; those countries provide the bulk of India's defence imports. India has imported over 10 billion dollars of American-made defence hardware since 2001, largely from Boeing,[24] while traditional exports from Russia are ships and transport helicopters.[25] It is no coincidence that during the recent India-Russia Summit in GOA, the two countries signed a deal to jointly produce 200 Kamov Ka-226T helicopters.[26] To be more specific, Moscow and New Delhi have agreed on establishing a joint venture which will part of the "Make in India" initiative. The agreement follows the inter-government agreement on "Cooperation in the Field of Helicopter Engineering" signed in Moscow during the De-

st/1qU3eHy.

[21] IHS, *Record-breaking $65 Billion Global Defence Trade in 2015 Fueled*, 13 June 2016, http://news.ihsmarkit.com/print/node/21318.

[22] Ibid.

[23] Ibid.

[24] See Amritt Ventures webpage: *Aerospace and Defence*, http://www.amritt.com/industries/aerospacedefense.

[25] IHS, *Record-breaking $65 Billion Global Defence Trade in 2015 Fueled*, cit.

[26] Shaurya Karanbir Gurung, "Explained: Kamov Helicopter Deal between India and Russia", in *The Economic Times*, 17 October 2016, http://ecoti.in/xe0OXZ.

cember visit of Indian Prime Minister Narendra Modi.[27] Apart from that, the major deal finalized after many years of negotiation has been the 8.8 billion dollar deal to purchase 36 Rafale.[28] According to *Defense News*: "France is expected to invest 30 percent of the total order cost in India's military aeronautics-related research programs and 20 percent into local production of Rafale components to fulfil the mandatory offsets under the deal." Of the total reported amount, 3.42 billion euros is for the cost of the platform; another 1.8 billion euros is for support and infrastructure supplies; 1.7 billion euros will be spent to meet India-specific changes on the aircraft; 710 million euros is the additional weapons package; and 353 million euros is the cost of performance-based logistics support.[29]

Generally speaking, the areas of possible defence industry cooperation between European defence companies and India include the entire spectrum of military domains: land, air, naval, space and cyber – ranging from the largest and most complex platforms to subsystems, components and advanced electronic systems. The opportunities in defence electronics, for example, have been recently pointed out in a report jointly produced by Roland Berger, the National Association of Software & Services Companies (NASSCOM), and India Electronics and Semiconductor Association (IESA). As outlined by the report: "The opportunity for electronics in India stems across both stand-alone systems as well as at a sub-system level for other systems." NASSCOM and Roland Berger estimate the total market opportunity for A&D electronics for India to ranges from 70-72 billion dollars in next 10-12 years. Of this almost 53-54 billion dollars emanates from electronics spend as part of platforms (i.e. at Tier 1 and Tier 2 levels). Another 17-18 billion dollars of demand emanates from projects which are traditionally called system-of-system projects like Indian Army's Project TCS, BMS, etc.[30]

---

[27] Ibid.

[28] Pierre Tran and Vivek Raghuvanshi, "India Inks Deal with France for 36 Rafale Fighter Jets", in *Defense News*, 23 September 2016, http://www.defensenews.com/articles/india-inks-deal-with-france-for-36-rafale-fighter-jets.

[29] Ibid.

[30] NASSCOM, IESA and Roland Berger, *Defence Electronics and System Design Policy. Executive Summary: Policy Recommendations*, July 2016, p. 2, http://www.nasscom.in/download/summary_file/fid/131927.

8.3 What could facilitate industrial cooperation?

The mantra of India's current government is "ease of doing business," but there's a long way to go – actually India ranks 130th in the World Bank's Ease of Doing Business.[31] Problems jeopardizing the current Indian economy – such as an unpredictable bureaucracy which often derails the process, corruption, unclear procurement strategy, and so on – need medium to long-term reforms. However, since 2001 India has opened its defence market to the private sector and is slowly adapting its procurement procedures, also in the effort of increasing the domestic manufacturing base. Contractors have often found themselves frustrated by opaque bureaucratic procurement processes, onerous domestic offset, work share requirements, and seemingly endless delays.[32] European companies that are active in the Indian market consider that the preference among stakeholders for a protectionist approach hinders cooperation. The win-win approach is not understood in its full potential, and therefore seldom applied. European industries, however, feel that some practical steps could ease cooperation, including:

Upgrading from offset policy to full chain production: Moving on from offset obligations by de-linking industrial cooperation to specific programmes can stimulate European and Indian companies to benefit from the real competitive advantage of India – such as its frugal engineering capacity and its competitive price. By so doing, India could manufacture truly competitive products for export. The Make in India initiative is promoting this approach, which could facilitate the establishment of a whole production chain. This could also result in moving the production chain of items of lower technological intensity that are currently produced in Europe, thereby making space in European venues for new technologically advanced products. The Make in India initiative could indeed improve the supply chain and enable SMEs to contribute to the creation of an ecosystem of companies – mirroring the European system – producing components that can feed into the final production line.

---

[31] World Bank, *The Ease of Doing Business in India 2017*, http://www.doingbusiness.org/data/exploreeconomies/india.

[32] Sebastian Sobolev and Aleksandar D. Jovovic, "The Evolving Landscape of Indian Defense Procurement", in *Defence Industry Daily*, 4 February 2016, http://www.defenseindustrydaily.com/?p=27154.

Protection of intellectual property rights: Technology transfer (ToT) is an especially sensitive issue, particularly now that European defence budgets are struggling to return to the pre-crisis levels. The necessity to protect Intellectual Property Rights (IPRs) goes hand-in-hand with the issue of Foreign Direct Investments (FDI). The decision to increase the FDI threshold to 49 percent did not change the business landscape, as demonstrated by the low level of FDI inflow in 2015 – only 0.08 million dollars for the defence sector.[33] That's why the Indian government has recently relaxed the FDI threshold in the defence sector, allowing up to 100 percent FDI in projects involving state-of-the-art technology. This could allow global defence companies to invest more strongly in India and be perceived as real partners. Having said that, even if this policy-change is particularly welcomed, the protection of IPRs relies also on a credible and effective regulatory "architecture" able to develop a friendly and safe business environment.

Market access and export opportunities: The Make in India initiative should be based on a win-win approach. Guaranteeing access to regional and/or national adjacent markets (such as security, police forces, etc.) is a first step in this direction.

8.4 How can an enhanced EU-India security dialogue facilitate European defence companies' investments in India?

There is a growing recognition from European industries of the necessity of better coordination and consolidation of the EDTIB to maintain its competitiveness on the global market. The EDTIB as a whole is competitive, innovative, high tech and capability-driven and its products are often perceived as being of better quality than those of its non-EU competitors. However, the lack of capacity for conducting effective G2G negotiations often results in losing the opportunity. The EU should therefore build on

[33] Thomas Mathew, "Road Map for a Robust Defence Industry", in *The Hindu*, 31 March 2016, http://www.thehindu.com/opinion/columns/road-map-for-a-robust-defence-industry/article8414445.ece.

the need expressed by EDTIB for stronger political support, and mature its foreign and, above all, security policy.

However, EU MS are still reluctant in approaching foreign policy through a European lens. This is also because they undervalue the potential of the EU as a multiplier of individual Member States' potential. However, there are a series of measures that the EU can undertake to boost credibility in EU MS and perform better in the global arena. In addition, the turf war amongst EU MS to position themselves at a comparative advantage puts India in a strong position where it can deflect competition to the EDTIB, to favour even further its leverage during negotiations. "Low hanging fruits" – such as those detailed below – can spin off positive EDTIB cooperation.

Moreover, there is a need for increased cooperation with India at the political level. The defence sector is indeed closely interlinked with the political dimension – and given India's preference to purchase defence equipment through G2G negotiations, rather than through public procurement, the EU should also prove its value as interlocutor for discussions on defence issues. This could also stimulate a greater buy-in on the part of EU MS into European defence cooperation programmes, as the political support would add long-term benefits – such as market opportunities in third countries – to the short-term benefits of the initial investments.

A multi-pronged approach should therefore be adopted, where practical cooperation facilitates the creation of political space, which in turn calls for more cooperation. The two dimensions, internal coordination and heightened political engagement, should develop at the same speed, as increased defence cooperation calls for increased political cooperation.

EU-India security dialogue can therefore be enhanced through boosting coordination amongst EU MS, and by enhancing EU political engagement with India.

8.4.1 Boosting coordination amongst EU Member States

To enhance its internal cooperation, the EU should better its coordinator role and prove to its MS the multiplying effect potential. Enhanced cooperation amongst European actors could facilitate an effective approach to the "un-ease" of doing business in India, and boost fruitful competition

amongst EDTIB. By tapping into its multiplying effect of the aggregated value of its MS, the EU could facilitate EDTIB to enter the Indian market. Below are some practical ideas for cooperation:

Create a normative framework for G2G relations: The Indian government buys military equipment via two major procurement procedures: either negotiations held at the governmental level (G2G) or selections through public tenders where private companies compete (public tender procurement). Whenever India engages in government relations, it prefers to deal directly with those EU MS with whom it has established a framework for cooperation, like the UK, Germany and (in particular) France.[34] However this unstructured relation does not guarantee a sustainable outcome in the medium term.

European countries do not have a standard framework regulating G2G negotiations, either nationally or at the European level. European companies are therefore in a weaker position in the negotiating game when compared to their American competitors – who enjoy strong G2G relations, thanks to enhanced political engagement but also thanks to the standard framework that the US imposes whenever entering into G2G negotiations with India. The EU could thus agree on a standard flexible contractual framework where general and shared principles are already agreed amongst its 28 MS and with India. In such a scenario, an EU MS entering into negotiations with India would benefit from speedier proceedings with the groundwork already laid, both on the EU level and bilaterally with India.

Enhancing an EDTIB coordinating and representative forum in India: There are currently a variety of fora dealing with European defence industries present in India, each of them with specific strengths and weaknesses. It would be more effective to limit this duplication and merge various organizations into a single forum, with stronger buy-in from the EDTIB and increased recognition by Indian authorities. Such a forum should effectively coordinate and represent EDTIB in India, act as interlocutor with Indian policy makers, identify areas of common interest and facilitate dialogue.

[34] Gulshan Sachdeva, *Evaluation of the EU-India Strategic Partnership and the Potential for Its Revitalisation*, Brussels, European Parliament, June 2015, p. 20, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_STU(2015)534987.

It could also advise Indian policy makers on the main trends affecting the EDTIB, for example in case of "blacklisting."[35]

Favouring defence cooperation through fiscal and tax incentives: The potential of European programmes such as Eurofighter, NH-90 and A400M has not yet been exploited fully. Since intra-EU competition hampers the European industrial and competitive footprint in the non-EU market, EU could develop new instruments and tools to increase immediate gain, such as fiscal and tax incentives, access to EU structural and regional funds as well as to European Investment Bank (EIB) financing, and/or a sort of European export credit agency – able to incentivize cooperation amongst defence companies and thereby benefitting from these initiatives. In addition, a body advising on technology transfer towards non-EU countries could be established, based on best practices and a win-win approach. Should then the EU mature its role in foreign policy, and provide political backing during G2G negotiations, long-term incentives – linked to export possibilities – would be added.

8.4.2 Enhanced EU political engagement with India

Defence cooperation embeds a high degree of political engagement: buying from a certain country also implies a degree of alignment in political matters, and a geostrategic deal. By purchasing defence equipment from Russia, for example, which is influencing the north of China, or the US – which is increasing its presence in the Indian Ocean – India nurtures a bilateral relation with relevant powers for its geostrategic approach. Un-

[35] About twenty years ago, defence industry structures were essentially nationally based but since the end of the Cold War industries have shifted from traditional single country production to transnational development and production. This trend started with international subcontracting, joint ventures and even cross-border Merger & Acquisition (M&A) processes. Moreover, the number and networks of subcontractors and suppliers have become even more transnational than before. Such "transnationality" of European defence companies has implications also from a legal perspective. Blacklisting one company with connections and ties with other transnational companies – established through consortia and/or JVs – could be detrimental because it denies the possibility for these companies (not affected by the process) to play their game in the international competition. Finally, the consolidation process within the EDTIB is expected to continue, making the blacklisting activity much more complex and with greater repercussions at the industry level.

derstandably, India prefers to cultivate its relations with whichever actor is able to guarantee a stronger political protection. As long as the EU continues to lack a truly common security and defence policy and its MS act independently and bilaterally, it cannot compete in the international arena. Therefore India prefers to deal with EU MS bilaterally, with the caveats that such relations entail.

However, should the EU be able to coordinate the action of its Member States in world politics and leverage its power accordingly, the position of its own industry would largely benefit. Currently, the EDTIB does not benefit from the political back-up and guidance of the EU. This penalizes the EU defence sector (and particularly European cooperation programmes, such as Eurofighter, currently "orphans" of a truly EU political support), which does not benefit from political back-up nor from a vigorous strategic partnership between the EU and India. As detailed above, such lack of political support plays a special role in the competition for the Indian defence market, because EDTIB competitors – which are mainly US, Russian and Israeli companies – benefit from the strong political support of their governments. Below are some recommendations on how to boost EU-India political engagement:

More frequent high-level exchanges and EU-India officers interactions: The EU should create a political space, deepen the political cooperation and enhance its capacity to leverage politically its dialogue with the Indian Government. To step up the partnership, the EU should create a "political space" with India, leading to a closer and more effective partnership. This can be done through more frequent high-level meetings and visits, including visits of the High Representative and Vice President of the European Commission.[36] The chairman of the EU Military Committee (EUMC) should also be regularly present at these high-level meetings. The immediately recognisable role and expertise of the EUMC would indeed facilitate India's defence counterpart in engaging and smoothing the security dialogue and cooperation.[37] The most recent EU-India Summit, held in Brussels on 30 March 2016, was one such opportunity to renew the commitment and revitalize interest in stepping up the partnership.

[36] Stefania Benaglia, "How to Boost EU-India Relations", in *CEPS Policy Briefs*, No. 341 (March 2016), p. 7, https://www.ceps.eu/node/11422.

[37] Ibid.

Greater interaction between EU and Indian officers, facilitated at the EU level, could also be considered with a view of promoting joint understanding of expectations and priorities in defence matters, as well as enabling a practical network of technical and procedural exchanges. Setting up joint exercises, collective maritime surveillance, common training as well as multinational research[38] between the EU and the Indian navies could be explored, especially for civilian crisis management or interoperability in anti-piracy missions.[39] In addition, India could be offered the opportunity to cooperate with EUROPOL.

EU to provide political weight during final negotiations of deals: Following the agreement of a standard framework for G2G negotiations with India, the EU should provide political support to its EDTIB during bilateral negotiations. When EU companies compete in a public procurement tender – like the French, Swedish and Eurofighter consortium did in 2011 for the procurement of Medium Multi-role Combat Aircraft for the Indian Air Force – the EU could assume the role of supranational neutral facilitator of commercial negotiations and provide political backing during the negotiating phase, whichever European defence company is selected. This way, the EU would multiply its political leverage, representing all the EDTIB and not just one national company. Such a role could be envisaged by the EDA.

Posting a permanent security advisor in the EU Delegation, and an EEAS (EU External Action Service) desk officer in charge of coordinating European defence actions in India: A security advisor should be permanently posted in the EU Delegation, charged with liaising with the Indian military and defence sector. The security advisor would help the EDTIB to navigate the Indian defence system and vice-versa. Indeed, without this link the entry-point officer and guidance are missing. Similarly to bilateral embassies – where often military attachés act also as a promoter of their domestic defence industry – the EU defence attaché would also provide guidance in understanding and dealing with the EDTIB – and possibly in liaising with the military attachés of individual EU Member States and with the EDA.

---

[38] Gulshan Sachdeva, *Evaluation of the EU-India Strategic Partnership and the Potential for Its Revitalisation*, cit., p. 25.

[39] Karine Lisbonne de Vergeron, "India and the EU: What Opportunities for Defence Cooperation?", in *EUISS Briefs*, No. 24 (July 2015), http://www.iss.europa.eu/publications/detail/article/india-and-the-eu-what-opportunities-for-defence-cooperation.

Conclusions

The EU struggles to pose as a security actor, and such lack of assertiveness leads to a decreased credibility and interest in cooperation. Increased EU defence cooperation needs to be fostered. As long as the EU does not engage in building a credible and reliable security and defence policy, it will not acquire a credible status as international security actor or partner.

India's growing defence needs offer many opportunities for defence cooperation that the EDTIB is well equipped to undertake. Should India undertake certain structural reforms (such as protection of IPRs, facilitating market access and export opportunities and upgrading from offsets policy to full chain production), cooperation would greatly benefit.

European defence companies' investments in India would benefit from an enhanced security dialogue. This can be accomplished by boosting coordination amongst EU MS, and by stepping up the EU's political engagement with India.

Enhanced EU MS coordination can be achieved by: agreeing on a standard normative framework for G2G relations with India; enhancing EDTIB coordination and representation; enhancing the EDA's international footprint and coordinating role for the EDTIB; and favouring defence cooperation through fiscal and tax incentives.

Enhanced EU political engagement with India can be achieved through more frequent high-level exchanges; through provision of political support during final negotiations of deals; and by posting a permanent Security Advisor in the EU Delegation as well as an EEAS desk officer in charge of coordinating European defence activities in India.

9.

EU-India: Starting a More Adventurous Conversation

Shada Islam [*]

Sometimes in foreign policy, the meeting really is the message. Such is certainly the case for the 13th EU-India Summit hosted in Brussels on 30 March 2016.[1]

Held after a break of four years, the meeting did not result in a much-needed breakthrough on negotiations on a Broad-Based Trade and Investment Agreement (BTIA). However, it has helped to revitalize other aspects of the increasingly multi-faceted relationship. By spotlighting a commitment by EU leaders and Indian Prime Minister Narendra Modi to work together on a range of old and new issues, the meeting provided a strong basis for reinvigoration of EU-India relations.

The hope is that both sides can now pave the way for a more ambitious, dynamic and adventurous EU-India relationship. It is time to move from speeches to policies and from words to action.

The good news is that the EU and India are taking a fresh look at each other, replacing tired misperceptions and clichés. There is a greater understanding of each other's strengths and weaknesses. Significantly, the summit in March endorsed a long list of new areas of cooperation which can give added "oomph" to the relationship while also anchoring it more firmly in the foreign policy agenda of each side.

---

[*] Shada Islam is Director of Europe & Geopolitics at Friends of Europe, Brussels.

[1] Council of the European Union, *EU-India Summit*, Brussels, 30 March 2016, http://europa.eu/!nc38bU.

9.1 The new conversation

If the long list of potential synergies articulated in the Agenda 2020[2] adopted at the summit is implemented by both sides, the EU-India strategic partnership will meet its avowed aim of deepening political dialogue and cooperation, bringing together people and cultures, enhancing economic policy dialogue and cooperation and developing trade and investment.

The partnership has the institutional architecture required to achieve these aims. The annual summits (starting in 2000) and ministerial meetings are the most visible feature of an ongoing political dialogue. Senior officials meet regularly to discuss broad foreign policy issues, and regular dialogues are held on issues of common concern such as security, counterterrorism, human rights, migration and mobility, trade and development, science and technology and environment and energy matters.

Political will to make the relationship more dynamic and vibrant has been lacking, however. The case of the Italian marines who allegedly killed two Indian fishermen off the coast of Kerala in 2012 became an obstacle in the two sides' efforts to reinvigorate the relationship, including attempts to organize a bilateral EU summit.

The broader relationship has also been impacted negatively by lack of progress in negotiating the BTIA. Negotiations on the deal opened in 2007 but talks quickly stalled as disagreements emerged over an array of issues including EU calls for lower tariff barriers, increased access to public procurement and stronger protection of intellectual property rights in India. Delhi, meanwhile, has said it wants greater temporary mobility for its skilled professionals in Europe and is urging the EU to grant its world-class IT companies "data security" status, thereby improving business prospects with and within Europe.

9.2 Going forward, three important drivers

Economics: Trade, investment and business will continue to be the backbone of the EU-India relationship. With growth rates of 7.5 percent, India now has

[2] EU-India Agenda for Action 2020, 30 March 2016, http://www.consilium.europa.eu/en/meetings/international-summit/2016/03/20160330-agenda-action-eu-india_pdf.

a more dynamic economy than China. The Indian government's demonetization drive in November 2016 will have an immediate negative impact on economic growth but economists predict that over the longer term, as more of the informal economy becomes formal and the Goods and Services Tax comes into effect, the move could help propel growth into double-digit levels. Another benefit could be a reduction of banks' non-performing assets, a critical constraint that is holding up the flow of bank credit for private sector investment in the country. The unexpected Indian move should not therefore impact India's strong long-term economic outlook or EU-India economic ties.

The EU, despite its current economic difficulties, will continue to have a strong interest in exporting and investing more in India. As noted by the Europe India Chamber of Commerce (EICC), "improving economic relations between the EU and India is essential for Indian and European companies, whose business links extend beyond import and export to include alliances and partnerships in supply chains, joint research projects and significant direct investments."[3] The EU has the technology India needs for its modernization drive, including in areas like energy, urbanization and preventing environmental degradation.

Creating jobs for India's young population demands an increase in foreign investments, including from Europe. The Indian government has taken steps to make India an easier place to do business, for example by widening the scope of FDI norms in defence, civil aviation, broadcasting services and pharmaceuticals. But other barriers to trade and investment, including lack of intellectual property protection and enforcement, continue to act as a deterrent for potential European investors.

India must work harder to modernize and reform economic governance and improve its ease of doing business, says the EICC, adding that action is needed to update the "intellectual property regime so that technology and innovations have adequate safeguards, ensur[e] transparency, predictability, and consistency in its corporate tax code, and provid[e] for an efficient system of adjudicating disputes."[4]

---

[3] Europe India Chamber of Commerce (EICC), *Europe and India – Anchors of Economic Stability in Today's Chaotic Times*, working paper for the Trade and Investment Partnership Summit (TIPS) 2016, Brussels, 8 November 2016, p. 2, http://eicc.be/wp-content/uploads/2016/10/TIPS2016WorkingPaper.pdf.

[4] Ibid., p. 7.

Modernization and development: India's new economic programme opens up fresh avenues for increased EU-India synergies that go beyond the two sides' traditional interaction. In the next decade, as India pursues its modernization drive and the "Make in India" initiative, the government hopes to see substantial investment flowing into energy (generation, distribution and transmission), mining, water, waste treatment and ports infrastructure. It also wants to attract FDI into advanced communication, visuals, automobiles, biotechnology and healthcare. The defence sector is also one of the 25 areas identified as part of the "Make in India" campaign.

Cooperation between the EU and India is therefore expected to expand to cover areas where both sides have a strong economic interest such as infrastructure investments, sustainable urbanization, renewable energy, innovation and synergies between "Digital India" and the EU's agenda for a Digital Single Market.

Although it is important to move beyond trade, there is no denying that negotiations on the BTIA need to speed up. Such an agreement would certainly help ease the concerns of some European companies as they seek out manufacturing venues and projects in India. So far, however, the talks have been like an unending obstacle race, with new problems emerging at every twist and turn. The EU wants a reduction in India's tariffs on cars, wine and spirits and a stronger regime for the protection of intellectual property. India is unhappy about EU restrictions on temporary movement of skilled professionals and wants data security status so that the thriving IT sector can do more business with European firms.

European investors are willing and eager to enter the Indian market, and India's new global companies are setting up shop across Europe. With two-way trade estimated at around 72.5 billion euros in 2014 while the EU's investment stock in India was 34.7 billion euros in 2013, there is certainly ample room for improvement. Agreement on the BTIA will require that both sides summon up the political will to look beyond the array of technical issues to the deeper strategic importance of their relations.

Security and geopolitics: Whether the context is violence and war in the Middle East, global terrorism or continuing instability in Afghanistan, the EU and India have a converging interest in working together in areas such as cybersecurity, counter-terrorism, maritime security, non-proliferation and disarmament. As such it is time for a more serious conversation on

refugees, peace and security in Asia, Africa and the Middle East as well as on wider questions such as the "Blue Economy."

While EU-India cooperation in the security sector is still in its infancy, there is a strong potential for increased synergies. The summit in March stressed the two sides' shared concerns and interests vis-à-vis a number of countries or regions, including Afghanistan, Pakistan, Nepal, North Korea, Iran and West Asia/the Middle East – in particular Syria.

In the maritime sector, the first EU military naval mission EUNAVFOR, also known as Operation Atalanta, has already cooperated on anti-piracy operations with Indian naval units in the Indian Ocean. The EU and India could now broaden that contact by establishing a regular high-level official dialogue on maritime security to build trust and explore avenues for further cooperation in areas such as search and rescue, humanitarian and disaster relief operations, tackling sea-borne crime such as smuggling or illegal fishing, and potentially joint maritime or evacuation exercises.

Significantly also, the EU-India Summit in March adopted a joint declaration on the fight against terrorism,[5] opening a potentially important and mutually beneficial dialogue on questions like terrorism financing, justice and police cooperation, designating groups as terrorists and efforts to increase the effectiveness of the UNSC sanctions regime against terrorist organizations. The declaration also calls for the EU and India to develop bilateral and multilateral cooperation in information and communication technology to tackle online radicalization.

9.3 The challenge ahead

Twelve years after they launched their strategic partnership, the EU and India appear ready to take their relationship into new and potentially more adventurous, exciting and mutually beneficial directions. The summit in March marked the beginning of a more mature and politically relevant dialogue between the EU and India. Agenda 2020 could therefore herald a new and more dynamic era in EU-India relations.

[5] India-EU Joint Declaration on the Fight against Terrorism, 30 March 2016, http://www.consilium.europa.eu/en/meetings/international-summit/2016/03/20160330-joint-declaration-terrorism_pdf.

Implementation of the different priorities set out at the March summit, however, will require time as well as energy and efforts to keep up the momentum.

In order to stay the course, both sides will have to avoid being *distracted* by other priorities and concerns. The fall-out from the Brexit referendum will continue to weigh heavily on the EU for several years to come. Tackling the refugee crisis and the challenge posed by the rise in populist parties will be other key concerns for the EU. For India, dealing with a troubled and troublesome neighbourhood and with myriad domestic challenges will remain a major concern. In addition, both the EU and India will also have to adjust and adapt their policies to the election of Donald Trump as the next US president.

In order to keep their relations vital and relevant, the EU and India must continue to *dialogue* on all important matters of bilateral, regional and global concern. Negotiations on the BTIA must continue but they should not be allowed to dominate the agenda. High-level summits should be held regularly – without an interval of four years as was the case this time – so that leaders can maintain contact and build better relations. New areas of cooperation, including in the security sector, must pick up pace and lead quickly to real action.

Given their different histories, identities and priorities, the EU and India will continue to disagree on many issues. But differences must not become an obstacle to relations. In a rapidly changing global environment, both sides should ditch old stereotypes and clichés and take a fresh look at each other. As such, unavoidable *differences* must be managed in a mature fashion.

Finally, having worked hard to establish the groundwork for a stronger and more diversified relationship, India and the EU must now demonstrate a *determination* to move forward and engage with each other over a sustained period. European member states have already recognized the importance of India, both as a regional actor and an influential global player. It is heartening that the EU institutions are also shedding their reservations and engaging with India as an increasingly powerful 21st century partner. Equally importantly, India is recognizing that while relations with national European governments are valuable, the EU also has much to offer. Both sides have much to gain from deepening their association so that the full potential of EU-India relations can be explored, tapped and realized.

Printed in May 2017
with technology *print on demand*
at the press centre Nuova Cultura Rome
p.le Aldo Moro n. 5, 00185 Rome
www.nuovacultura.it

for orders: ordini@nuovacultura.it

[Int_9788868128531_17x24bn+95-96col_LM01]