IAI
Istituto Affari Internazionali

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

by Patryk Pawlak

GATEWAY HOUSE
INDIAN COUNCIL ON GLOBAL RELATIONS
भारतीय वैश्विक सम्बंध परिषद्

DAI

EU Public Diplomacy and Outreach in India and in the SAARC

Project funded by the European Union

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.

European Union | India | Cyber security

keywords

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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

by Patryk Pawlak*

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 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

* 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.

· Paper presented at the conference "Moving Forward the EU-India Security Dialogue: Traditional and Emerging Issues" held in Rome on 21 November 2016 within the framework of the project bearing the same name and 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.

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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 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.

[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/node/2.

[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.

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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.

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 particular 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.

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

[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.

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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 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 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,

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

[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.

ISSN 2280-4331 | ISBN 978-88-9368-016-5

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.

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.

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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.

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

[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.

[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-

ISSN 2280-4331 | ISBN 978-88-9368-016-5

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."

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 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. 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."

en.pdf.

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

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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

[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.

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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.

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 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."

[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.

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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 exercises 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.

Updated 21 November 2016

[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.

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

References

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

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

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

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

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

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, http://europa.eu/globalstrategy/en/node/2

Freedom House, *Freedom on the Net 2016*, November 2016, https://freedomhouse.org/report/freedom-net/freedom-net-2016

Human Rights Watch, *World Report 2016*, January 2016, https://www.hrw.org/world-report/2016

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

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

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. 129-153, https://ccdcoe.org/node/956.html

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

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

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

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

Anuj Srivas, "India No Haven for Net Freedom But It Did Not Oppose UN Move on Internet Rights", in *The Wire*, 6 July 2016, http://thewire.in/49131

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

UN Department of Economic and Social Affairs (UNDESA), *World Population Prospects. The 2015 Revision*, July 2015, https://esa.un.org/unpd/wpp

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

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

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

IAI WORKING PAPERS 16 | 36 - DECEMBER 2016 ISSN 2280-4331 | ISBN 978-88-9368-016-5

Istituto Affari Internazionali (IAI)
Founded by Altiero Spinelli in 1965, does research in the fields of foreign policy, political economy and international security. A non-profit organisation, the IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations. The IAI publishes an English-language quarterly (The International Spectator), an online webzine (AffarInternazionali), two series of research papers (Quaderni IAI and IAI Research Papers) and other papers' series related to IAI research projects.

Via Angelo Brunetti, 9 - I-00186 Rome, Italy
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Latest IAI WORKING PAPERS

16 | 36 Patryk Pawlak, *EU-India Cooperation on Cyber Issues: Towards Pragmatic Idealism?*

16 | 35 Stefania Benaglia and Alessandro R. Ungaro, *EU-India Defence Cooperation: A European Perspective*

16 | 34 Aldo Liga, *Israel and Iraqi Kurds in a Transforming Middle East*

16 | 33 Anja Palm, *Did 2016 Mark a New Start for EU External Migration Policy, or Was It Business as Usual?*

16 | 32 Janiki Cingoli, *The New Energy Resources in the Centre-East Mediterranean: Potential Current and Future Geo-Strategic Consequences*

16 | 31 Eleonora Poli, *Mapping Member States' Stances in a Post-Brexit European Union*

16 | 30 Mohammed Alsaftawi, *Who Needs Whom? Turkey and Israel Agree on Normalization Deal*

16 | 29 Bernardo Venturi, *The EU's Struggle with Normative Leadership in Sub-Saharan Africa*

16 | 28 Ismaeel Dawood, *Moats, Walls, and the Future of Iraqi National Identity*

16 | 27 Nicolò Sartori, Lorenzo Colantoni and Irma Paceviciute, *Energy Resources and Regional Cooperation in the East Mediterranean*