Cyber security: the potential for Japan-India cooperation

Japan is pushing to standardise cyber defence policy at the international level so that states can share rules and best practices, and thus isolate countries that do not commit to international norms. For all these reasons, Japan shares common ground with India. The two countries have built a special relationship over the last decade that represents one of the most important recent geopolitical developments, and cybersecurity is one aspect of this blossoming relationship writes ***Anne-Léonore Dardenne****.*

More than ever, cybersecurity figures prominently on leaders' agenda around the world. Global economy and military technologies are deeply dependent on cyberspace, therefore cyber protection units are set up at different levels of government. Interestingly, Japan has been lagging behind other states despite its heavy reliance on information and communications technology. This article will briefly examine Japan's cybersecurity strategy as part of Prime Minister Abe's Grand Strategy and the potential for India-Japan cooperation.

A Vulnerable Country

Deloitte ranked Japan the fourth most vulnerable country to cyber threats, estimating that it is nine times more vulnerable than other Asian countries like South Korea, Australia, New Zealand and Singapore. Indeed, the country has witnessed an increase in the number of cyber-attacks in recent years, and the National Centre of Incident Readiness and Strategy for Cybersecurity reported that government networks and related agencies faced over seven thousand cyber-attacks in 2016. Japan has been the target of large-scale cyber-attacks since 2010, including the well-publicised 2011 attack on Mitsubishi Heavy Industries (Japan's largest defence contractor), the attack on the Monju nuclear power plant of 2014, and the leaking of at least two million sets of personal data in 2015. These incidents opened Japan's eyes to the seriousness of the issue, and the government released its first real Cybersecurity Strategy in 2013 officially recognising cyber-attacks as a national security threat. The Cybersecurity Strategy introduced several measures, such as the establishment of a Cyber Defence Unit within the Self-Defence Forces (SDF) to respond to cyber-attacks perpetrated by foreign governments. However, the SDF has not acquired offensive cyberware capabilities as it would violate Japan's pacifist constitution.

Boosting Cyber Defence Capabilities

Since he came to power in 2012, Prime Minister Abe has been pursuing incremental changes to step up defence capabilities and strengthen cooperation with the United States and other like-minded partners to tackle a range of traditional and non-traditional security threats. In 2014, the Abe Administration passed the Cybersecurity Basic Act, which aims to strengthen the legal background for Japanese cybersecurity strategy and designates the Cybersecurity Strategic Headquarters as the command and control body of national cybersecurity. The second Cybersecurity Strategy released in September 2015 stresses the importance of building more comprehensive cyber defence capabilities and recommends that, given the nature of the challenges, stakeholders like businesses, civil society, critical infrastructure operators should contribute to secure the cyberspace.

Mindful of the risks around the 2020 Tokyo Summer Olympic Games, Japan is gradually enhancing its national network monitoring and protection system while governmental bodies develop internal capacities to facilitate a more rapid and effective response to cyber threats. For instance, the Ministry of Foreign Affairs established a Cyber Security Policy Division in 2016 and both the Ministry of Economy, Trade and Industry and the Japanese Ministry of Internal Affairs and Communications launched cybersecurity training centres in 2017. The government also plans to create a cybersecurity response centre in late 2018 to facilitate information-sharing between the various public and private stakeholders, and to oversee the protection of crucial infrastructure during the Tokyo Olympics and Paralympics. The Ministry of Defence is considering increasing the number of cyber warriors to around 1000 from the current 110 by the end of 2023 and is to set up a new team to study cyber-attack techniques as a tool to build an appropriate defence posture. In comparison, China boosted its cyberforces in 2016, increasing it from 30,000 to 50,000 people, as well as reportedly having a separate cyber militia comprising more than 100,000 hackers.

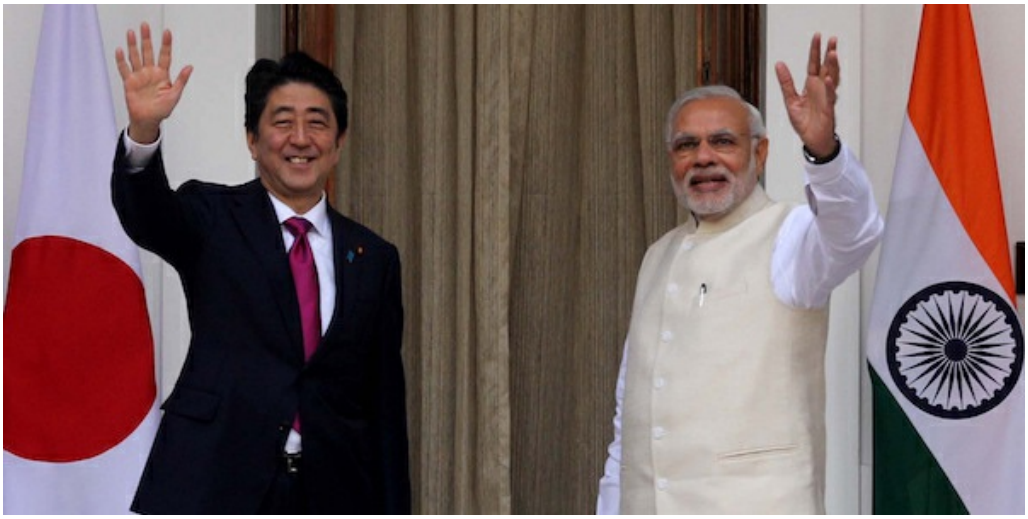
Geopolitics Counts

Date originally posted: 2018-06-12

Permalink: http://blogs.lse.ac.uk/southasia/2018/06/12/cyber-security-the-potential-for-japan-india-cooperation/

Blog homepage: http://blogs.lse.ac.uk/southasia/

In the face of cyberthreats, geopolitics is as relevant as ever. Many experts hold that many cyber-attacks are state-sponsored. Japan has uneasy relations with its neighbours, including the three top countries for cybercrimes: China, Russia and North Korea. 40 percent of the attacks against Japan were traceable back to China in 2014, and the Ministry of Defence notes in its white paper that Chinese cyber-attacks aim to obtain sensitive information concerning critical infrastructure, national security decision-making, and military tactics of other countries. The recent allegation about Chinese government-backed hackers targeting Japanese defence companies, possibly to get information on Japan's policy towards North Korea, seems to confirm such suspicions. Cyberspace is international by nature and calls for multilateral cooperation. For that reason, cyber-diplomacy is one of the most important elements of Japan's cybersecurity strategy.



Japanese Prime Minister Shinzo Abe and Indian PM Narendra Modi. Image Credit: Indian Ministry of External Affairs/Flickr.

Cyberspace interlinked with Japan's Grand Strategy

In the pursuit of its grand strategy to shape a more favourable external environment for peace and prosperity, Japan has been deepening ties with like-minded countries such as Australia, India, the United States, as well as regional bodies like ASEAN. Japan's Free, Fair, and Secure Cyberspace strategy resonates with its Free and Open Indo-Pacific strategy, and Tokyo has been working with the United States and other international partners to implement three main pillars. These are the promotion of the rule of law in cyberspace, development of confidence-building measures, and cooperation on capacity building. To this end, Japan is holding cyber dialogues with fourteen countries and regions, and is also involved in capacity- building, especially in ASEAN countries where it is notably providing cybersecurity devices, equipment and training through Official Development Assistance.

At a multilateral level, the Japan-ASEAN Cybersecurity centre will be launched in June 2018 in Thailand and is expected to reduce cybercrimes in the region and to train at least 700 cybersecurity personnel. In terms of legislation, Japan is pushing to standardise cyber defence policy at the international level so that states can share rules and best practices, and thus isolate countries that do not commit to international norms. For all these reasons, Japan shares common ground with India. The two countries have built a special relationship over the last decade that represents one of the most important recent geopolitical developments, and cybersecurity is one aspect of this blossoming relationship. As the Indian Electronics and IT Minister Ravi Shankar Prasad puts it, "there is a great convergence between the two countries."

Japan-India Cybersecurity Cooperation

Date originally posted: 2018-06-12

Permalink: http://blogs.lse.ac.uk/southasia/2018/06/12/cyber-security-the-potential-for-japan-india-cooperation/

Blog homepage: http://blogs.lse.ac.uk/southasia/

The First and Second Cyber Dialogues were held respectively in November 2012 and August 2017. The two governments affirmed their shared vision of a free and secure cyberspace and their commitment to international law. They also discussed further bilateral and multilateral cooperation, alluding to the ASEAN Inter-Sessional Meeting on Security and the use of Information and Communication Technologies as a possible platform to address the range of issues and to strengthen confidence-building measures. The next cyber dialogue is to be held in 2018, barely a year after the second one, showing both countries' strong will to further enhance cyber cooperation. In October 2013, the Japan-India ICT Comprehensive Cooperation Framework was launched to enhance business ties, boost investments, cyber security cooperation and use of ICT for addressing societal and economic challenges. Six new projects such as cyber defence exercises or telecom network security testing were adopted during the 4th session that took place in July 2017. India's major strength lies in its large pool of IT professionals, where Japan is facing a shortage of trained cybersecurity experts. For Japan, its strength lies in its public-private partnership – which is essential to maximise the country's cyberdefences – but is actually one of India's weaknesses. Indo-Japanese relations took another step by agreeing in May 2018 to bolster cooperation in the field of cyber security and exchange IT professionals.

Despite Japan's efforts under Prime Minister Abe, there is still some way to go before the country becomes a cyberpower. Japan's military cyber capabilities are still in their early stage, yet the establishment of a legal framework and a comprehensive national cybersecurity strategy is a big step forward. Finally, strengthening coordination with other allies and specifically with India – poised to become the World's third largest economy and an indispensable partner for Japan's overall national security – is a critical condition.

This article originally appeared on the IAPS blog and has been republished with permission. The original article can be accessed here.

Cover image:Computer keyboard in operation, Ministry of Defence, Wikimedia Commons, OGL 1.0.

This article gives the views of the authors, and not the position of the South Asia @ LSE blog, nor of the London School of Economics. Please read our comments policy before posting.

About the Author

Anne-Léonore Dardenne is a research student at Lyon Law School and International Institute of Humanitarian Law. Her research interests lie in International Relations and International Humanitarian Law, with a particular focus on Strategic and Security Issues in the Indo-Pacific and India-Japan-China Relations. She tweets @aldardenne.

Date originally posted: 2018-06-12

Permalink: http://blogs.lse.ac.uk/southasia/2018/06/12/cyber-security-the-potential-for-japan-india-cooperation/

Blog homepage: http://blogs.lse.ac.uk/southasia/