The East Asian economic, military and geopolitical powerhouse of Japan is a highly-industrialized, highly-modern, and one of the world's premier urbanized nation-states in the world. The Japanese economy is presently the third-largest in the world, having registered Asia's second-highest Gross Domestic Product (GDP) of $5.95 trillion (although this has faced an over 20% reduction due to the Government of Japan's COVID19 stimulus packages), after the People's Republic of China (PRC). While the country's GDP may have been dealt a severe blow due to the ongoing COVID19 pandemic, the resilience of the Japanese leadership and its population of 126 million people will factor in, in post-pandemic scenarios.

While developed countries have embraced cyber security a long time ago, Japan has identified the domain of cyberspace as a priority for its overall national security only lately. The Japanese cyber domain was ravaged by an attack on the Japan Pension System (JPS) in June 2015 – a colossally-damaging compromise on the System which resulted in over 1.25 million records having been leaked to the public domain. The attack was the result of a virus received through an email on the JPS servers. Viruses, in the domain of cyber-security, are malicious codes that tend to have a multiplier effect on networked systems linked to the system of origin, when opened by an unsuspecting recipient.

The defense of Japan and cybersecurity: pointers from the defense document

The *Defense of Japan* is the Ministry of Defense, Government of Japan's official white paper. The *Defense* is a focal document that guides Japanese defense and strategic policies for a year, starting ideally from the month of August. As regards the cyber domain, Japan has accorded significant strategic priority to combating threats emerging from the domain. The domain figures alongside other non-traditional security domains such as outer space and the electromagnetic spectrum (EMS), and on par with the threats posed by countries such as Russia, the Democratic Peoples' Republic of China (DPRK), and most importantly, the Peoples' Republic of China. In addition, the country's steadfast security relationship with the United States factors considerably in its cooperation initiatives in the domain of cyber security and this has provided an added impetus to Japan's national security apparatus of which 'cyberspace' is a critical fragment.

The cyber domain, in a nutshell, is an area broadly related to information technology and information security, and one that has emerged to be of critical security concern to the information networks and the computer security architecture of most countries in the world. These concerns need to be allayed through robust hardware (whether manufactured indigenously, or imported from technologically-suave nation-states such as the United States of America and the United Kingdom), modern technologies and systems premised on quality, as well as high-end security software. Since the dawn of the internet in the early 1990s and a shift to increased digital reliance for a majority of the world's population (over 60% of the world's people own a smartphone) as a consequence of the promulgation of the internet as the 'world's country', miscreants and groups have resorted to all forms of 'cyber-terrorism' such as cyber espionage, data theft, cyber-crime, sabotage, propagation of computer and network malware, etc.

The domain has been on par with traditional domains of security such as air and naval forces in terms of accorded priority as far as Japan is concerned, and houses a country's vital national security secrets and archives, while ensuring seamless day-to-day communications through encrypted networks, firewalls, and other confidential protocols that enable the secure access of data. As is the apparent consequence of the adoption of modern technologies, the cyber domain is highly susceptible and vulnerable to hackers and thieves, if not secured. Mechanisms to address attacks, viruses, hijacks, etc. are also to be addressed by experts working in government and allied sectors. The cybersecurity domain is governed by several technical standards, the most pertinent ones being ISO 27001 and PCI-DSS, the latter to do with payment gateways.

As one of the world's premier countries (though the dent in Japan's Gross Domestic Product as a result of the novel Coronavirus pandemic will require a re-assessment of the world order as it stood before December 2019 – the month that marked the beginning of the spread of the virus into what has exploded into an all-consuming pandemic), Japan has identified, prioritised, and necessitated policies towards ensuring the comprehensive

security of this domain. The Tokyo 2020 Olympics (now re-scheduled to 2021 due to the ongoing COVID19 pandemic) have been at the centre of Japan's drive to secure its cyber domain, with the country fearing unauthorized attendances, hackings, monetary thefts, website attacks, etc. associated with the surge of international tourists into the country.

Japan's initiatives in the cyber domain

Drawing reference to the previously mentioned attack on Japan's Pension System, Japan had implemented a series of measures, churned out by its defense policymakers. Interestingly, the attack on the JPS was preceded by the enactment of legislation by Japan in the cyber domain. The November 2014 Basic Cybersecurity Act resulted in the establishment of the Cybersecurity Strategic Headquarters (CSH). The following year, the third iteration of Japan's National Defense Program Guidelines (NDPG) prioritized bilateral cooperation in the domain of cyberspace. Japan has, particularly emphasized the setting up of institutional frameworks with seamless coordination between national cyber 'agencies', and in retrospect, has devised a definitive strategy to deal with the cyber domain.

Japan's Ground Self-Defense Force personnel listen to a lecture on cyber defence/ Image: Nikkei

The National Center for Incident Readiness and Strategy for Cybersecurity (NISC) is the focal point for addressing cybersecurity issues in the country, and was established in 2015, after the setting up of the CSH. Cooperation is mandated between the NISC and the Japanese National Security Council (NSC) – the country's premier security policymaking body – and the IT Strategic Headquarters. A *Strategy Document* for the domain was released in July 2018.

A Cyber Defense Group (CDG) has been instated to respond to cyber attacks. The CDG was instituted in March of 2014, as part of the military forces of the country – the Self-Defense Forces (SDF). Individual units set up to deal with cyber attacks pertaining to the domains of land, sea, and air, too, have been institutionalised. The Government of Japan organises 'cybersecurity contests', to encourage budding talent and ethical hackers participate in these contests, annually. Early this year, before the eyes of the world were awakened to the Wuhan-originated COVID19 pandemic, documents related to the Ministry of Defense (MOD) were compromised via the NEC Corporation. Details for a submarine sonar of the Maritime Self-Defense Forces (MSDF) were leaked in what were a spate of attacks on Japanese national security assets.

Proactive diplomacy in the cyber domain has been a defining characteristic of Japan's approach to cybersecurity. A three-pronged strategy has been adopted by the Japanese Government that is, for the most part, focused on increasing cooperation with allies and friends. Results have been particularly evident in the partnership in the cyber domain with the United States. An annual US-Japanese Cyber Security Dialogue has been in place since 2012. Seven iterations have been held, since, with the latest one having been concluded in October 2019.

A report released in March 2020 by the British consumer technology services company *Comparitech*, before most nations of the world embraced stringent lockdowns while Japan opted for a national emergency, has ranked Japan as the fifth-most 'cyber-secure' country in the world, having been ranked first in the previous year's iteration of the report. This may be a key indicator of a drop in Japan's usually high-standard and carefully-thought pursuit towards plugging the holes in its national security architecture. Japan has also announced investments of ¥25.6 billion with a system based on Artificial Intelligence (AI) to combat threats emanating from this crucial domain.

To what extent the realm of cyberspace remains actively attributed to by Japanese leaders and decision-makers, with the implementation of judicious policies, high-end technologies,

robust infrastructure, seamless networking between the many cybersecurity centers to ensure the integration of their setups, as well as formalized cooperation with long-term allies such as the United States, remains to be seen for the nascent 'cyber power' that the country is – as of now.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team