MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

Strategic Digest

Vol. 2 | No. 23 | 30 December 2020

No. 1, Development Enclave, Rao Tula Ram Marg, Delhi Cantt., New Delhi-110 010
Tel: Phone: +91-11-2671 7983, Fax: +91-11-2615 4191, E-mail: contact.idsa@nic.in

EU's Cybersecurity Strategy for the Digital Decade

The European Union (EU) issued a new Cybersecurity Strategy for the Digital Decade on December 16. It is a key component of the EU's mission to shape the continent's "Digital Future" and of its Security Union Strategy 2020-2025. The EU is quadrupling previous levels of investment over the next seven years.

The new Cybersecurity Strategy's goal is to ensure a global and open Internet, which, at the same time, protects the fundamental rights and freedoms of people, businesses and institutions from cyber threats. It contains proposals for employing regulatory, investment and policy instruments to address three areas of EU action: 1) ensuring resilience, technological sovereignty and leadership; 2) building operational capacity to prevent, deter and respond; and 3) advancing a global and open cyberspace.

The strategy aims to build a European Cyber Shield with a network of Artificial Intelligence (AI)-enabled Security Operations Centres across the EU as well as an ultra-secure communication infrastructure by harnessing quantum technologies to shield against cyberattacks. In addition, it would promote the widespread adoption of cybersecurity technologies through dedicated support to small and medium enterprises.

The EU is expected to determine the process, milestones and timeline for establishing a Joint Cyber Unit, continue implementation of the cybercrime agenda under the Security Union Strategy, and advance the Union's cyber deterrence posture.

On the global front, the strategy calls for advancing responsible state behaviour in cyberspace, fostering cooperation with partners as well as the private sector, academia and civil society, promoting human rights and fundamental freedoms in cyberspace, and strengthening the Budapest Convention on Cybercrime. It also proposes the formation of an informal EU Cyber Diplomacy Network to expand the Union's cyber dialogue with third countries and regional and international organisations.

The concerted implementation of the new strategy is expected to contribute to a cyber-secure digital decade for the EU, the achievement of a Security Union, and the strengthening of the EU's global position.

US National Space Policy Directive, December 2020

On December 9, President Donald Trump issued a National Space Policy directive that provides direction for all US space activities. This policy directive replaces the previous one issued in 2010.

The new policy sets out the US commitment to remain a global leader and ensure the responsible and constructive use of the domain of space. An integral part of this effort would be the promotion of a strong US commercial space industry that retains leadership in the space sector and remains in sync with the national interest.

The United States is keen to ensure its leadership in future space exploration missions. The new policy directive identifies the aims of establishing a permanent human presence on the Moon and undertaking a manned mission to Mars. These ventures would be undertaken in cooperation with private industry as well as with international partners. Another major project would be the development and use of space nuclear power and propulsion (SNPP) systems.

Highlighting the imperative of defending US and allied interests in space, the 2020 space policy directive identifies the importance of protecting the electromagnetic spectrum, securing cyberspace, elevating space as a priority intelligence and military operational domain, and ensuring freedom of navigation and secure lines of communication.

Israel Conducts Multi-layered Missile Defence Intercept Tests

The Israel Missile Defence Organisation (IMDO) announced on December 15 that it had successfully conducted a series of live-fire intercept tests involving the Iron Dome, David's Sling, and Arrow missile defence systems. The US Missile Defense Agency (MDA) was also involved in the conduct of these tests, which simulated a diverse and simultaneous threat environment involving cruise missiles, ballistic missiles and unmanned aerial vehicles (UAVs).

The Israel Navy (IN) and the Israel Air Force (IAF) participated in the tests, which were led by Rafael Advanced Systems, the prime contractor for the David's Sling system, along with the US Raytheon. The Israel Aircraft Industries' (IAI) Elta Division developed the multi-mission radar (MMR) while Elbit Systems developed the Golden Almond Battle Management Center (BMC).

David's Sling being launched from offshore ship.
Source: Israel Defence Ministry via Haaretz.com

IMDO stated that the tests demonstrated the inter-operability of the multi-layered air defence system. While all three systems have been deployed under the operational control of the Israeli Air Force, the latest tests employed an advanced version of the David's Sling system that is currently under development.

David's Sling, first operationally used on the Syrian border in July 2018, is meant to counter medium-range missiles and rockets. The Iron Dome system, deployed since March 2011, counters short-range rockets. And the Arrow system, deployed since 2000, is designed to counter longer-range ballistic missiles. The Arrow system was used operationally for the first time in March 2017 to shoot down a Syrian surface-to-air missile.

It has been reported that the September 2019 Abqaiq attack on Saudi refineries, allegedly perpetrated by Iran using UAVs and cruise missiles, was what motivated the IMDO to embark on the multi-layered intercept tests. During these tests, the Iron Dome system was specifically used to intercept cruise missiles – a new capability for the system which has until now been used primarily to counter unguided rockets.

CAATSA Sanctions on Turkey

On December 14, the US State Department imposed sanctions on Turkey's Presidency of Defence Industries (SSB) under Section 231 of the Countering America's Adversaries through Sanctions Act (CAATSA) for acquiring and activating the Russian S-400 surface-to-air missile defence system. The sanctions entail a ban on the issue of export licences for goods and transfers to the SSB as well as visa restrictions and assets freeze of four of its senior officials. This is the first instance of a CAATSA provision being used against a NATO ally.

Though the sanctions are limited in scope, it is estimated to affect nearly 40 per cent of Turkey's defence imports from the United States – done through the SSB, which is Turkey's primary defence project and planning entity. The SSB functions under the President's office and is responsible for the modernisation of the Turkish defence industry as well as reduction of reliance on external

Source: Tass.com

procurement. SSB holds shares in numerous Turkish defence manufacturers, including Turkish Aerospace Industries Inc. (TAI), which produces fuselage parts for the F-35 fighter jet. Nearly 600 projects – ranging from the development of engine parts to the production of ammunition – which the SSB is associated with are likely to be affected by the sanctions, thus undermining Turkey's efforts to develop an indigenous defence industry as well as impeding existing defence cooperation between US and Turkish defence companies.

The issue of US sanctions on Turkey over the procurement of the S-400 missile defence system has been lingering since 2017. Turkey was prompted to acquire the S-400 system after the failure of protracted efforts to obtain the US Patriot missile defence system. When Russia delivered the S-400 system to Turkey in July 2019, the US suspended Turkey from the F-35 joint strike fighter programme. President Trump, however, resisted Congressional pressure to impose wider sanctions, and instead chose to demand that the S-400 system not be activated. When Turkey finally test-fired the S-400 in October 2020, the Trump administration had no choice but to impose sanctions.

Turkey's reaction to the US sanctions has been predictable. President Erdogan termed the move a "grave mistake" and "hostile attack" on Turkish defence industry. Ankara has ruled out rolling back the S-400 procurement, with the Foreign Minister observing that "If there was to be a step back, it would have happened by now."

Turkey-US relations have witnessed a steady decline in recent years over a variety of bilateral and regional issues. These include Turkey's military intervention in Syria, its maritime activities in the Eastern Mediterranean and consequent tensions with fellow NATO member Greece, support for Azerbaijan's military action against Armenia, strained relations with Israel, and above all the decision to buy the S-400 missile defence system from Russia.