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

CYBER *Digest*

October 2021

- **AUKUS to focus on Cyber Capabilities, Artificial Intelligence**
- **Japan releases new cybersecurity strategy**
- **US crackdown on Cryptocurrency exchange to tackle ransomware**
- **Former U.S. intelligence operatives admit hacking networks for UAE**
- **QUAD Joint Statement on critical and emerging technologies**
- **U.S.-EU Trade and Tech Council meet**

AUKUS to focus also on Cyber Capabilities, Artificial Intelligence

In addition to the acquisition by Australia of nuclear-powered submarines, the new AUKUS trilateral security pact between Australia, the United Kingdom, and the United States, announced on September 15, will also focus on cyber capabilities, artificial intelligence, and quantum technologies as a means to enhancing undersea and military capabilities.[1]

AUKUS aims to promote deeper information and technology sharing, deeper integration of security, technology, and supply chains. The three nations involved in AUKUS are establishing "a new inner circle of strategic trust"[2] and cooperation in the Indo-Pacific region, to meet the challenges of the twenty-first century, in which cyber capabilities will play an important role. The US and UK defence forces would also benefit from Australian research on emerging technologies as part of mutual cooperation under the pact.

Japan releases new cybersecurity strategy

The Japanese government on September 27 adopted the draft of their new cybersecurity strategy for the next three years in a meeting of the Cybersecurity Strategic Headquarters at the Prime Minister's Office. The strategy for the first time has mentioned China, Russia and North Korea as potential cyberattack threats for Japan.[3] It would replace the current one adopted in 2018 once it is approved by the Cabinet.

The draft policy aims to strengthen Japan's cyber-defense capabilities. It mentions tough countermeasures to be taken that would include diplomatic responses and even criminal prosecutions against cyber-attackers. Japan will enhance cooperation in the cyber domain with its allies and partners in various multilateral frameworks like the QUAD, Association of Southeast Asian Nations, etc. in the Indo-Pacific region.

The strategy also aims to strengthen capabilities for defense and deterrence against attacks on critical infrastructure by enhancing the structure of the country's cyber units and creation of new safety standards for IT devices. Earlier, on September 1, the Digital Agency was launched for promoting digitalization in the country; the draft policy calls for expanding its remit towards the promotion of cybersecurity.

US crackdown on Cryptocurrency exchange to tackle ransomware

In order to tackle the growing threat from ransomware, the Biden administration on September 21 took steps to expand sanctions to digital payment systems involving cryptocurrencies.[4] Ransomware attacks have grown rapidly in the last year with most ransom payments being made through cryptocurrencies.

The first of these measures was reportedly imposed on a virtual currency exchange called Suex that had facilitated transactions in some of the latest ransomware attacks. According to the Treasury Department, more than 40 percent of Suex exchange's transactions had been linked to ransomware and cyberattacks, clearly making it an emergent threat to national security.[5]

The sanctions came three months after the meeting in Geneva between President Biden and President Vladimir Putin of Russia following the Colonial Pipeline hack, a major attack on US critical infrastructure. The sanctions involve blocking transactions and Suex's access to U.S. property. In 2020, ransomware payments were estimated around $400 million[6], a fourfold rise from the previous year as per the Treasury Department. Misuse of technologies like routers for anonymous communication and cryptocurrencies for payments have turned

out to be a tool kit for these ransomware attacks.

Former U.S. intelligence operatives admit hacking networks for UAE

Three former U.S. intelligence operatives on September 14 admitted to hacking into American networks illegally for gaining secret information and spying on networks before the US Federal Court.[7] The operatives were part of a secretive unit called Project Raven that helped the UAE spy on its enemies according to reports.

The operatives worked as cyber spies for the UAE and violated U.S. hacking laws by hacking into the accounts of various human rights activists, journalists, and government officials. As part of a deal with federal authorities in order to avoid prosecution, a sum of $1.69 million is to be paid by the operatives and they have been debarred from obtaining U.S. security clearance for jobs in US government agencies.

The court papers revealed that the operatives admitted that, under Project Raven, they had deployed a sophisticated cyber weapon named "Karma" that allowed the UAE to hack into iPhones even without the need to click on malicious links. It also allowed users to access millions of devices at a time. Karma qualified as an intelligence gathering system as per federal export control rules and no permission from the U.S. government was sought by the operatives to sell Karma to the UAE.

QUAD Joint Statement on critical and emerging technologies

The leaders of Australia, India, Japan, and the United States, in their joint statement at the conclusion of the Quad meeting on September 24, have recommitted to promoting the free, open, rules-based order, prosperity in the Indo-Pacific and beyond. As a part of cooperation on critical and emerging technologies, QUAD leaders have declared the way in which technology is designed, developed, governed, and used; will be shaped by shared values and respect for universal human rights.[8]

With respect to 5G, QUAD plans to advancing the deployment of secure, open, and transparent 5G and beyond-5G networks, and working in partnership with industry, to foster innovation and facilitate public-private cooperation. The supply chain of critical technologies and materials, including semiconductors, would be mapped to allow for government support measures through policies that are transparent and market oriented. The Quad Principles on Technology Design, Development, Governance, and Use was launched to guide the region and the world towards responsible and open, high-standards innovation.

On the cybersecurity front, the members pledged to foster new cooperation in cyber space and to work together to combat cyber threats, promote resilience, and secure critical infrastructure.

U.S.-EU Trade and Tech Council meet

The U.S.-EU Trade and Technology Council (TTC) meet took place in Pittsburgh on September 29.[9] The TTC is a new forum with ten working groups to discuss various issues, including sensitive technologies, boosting semiconductor production, addressing chip shortages and also the regulation of large technology firms.

The broad objectives of TTC were reaffirmed in the meet which included coordination in key global technology, economic, and trade issues with an approach to deepen transatlantic trade and shared democratic values. Cooperation between states to effectively address the misuse of technology and to protect societies from information manipulation were also discussed.

Among the various working groups, the working group on Technology Standards

was tasked with coordination and cooperation in critical and emerging technology standards including AI and other emerging technologies. Artificial intelligence (AI) technologies have the potential to bring significant benefits to citizens, societies and AI systems that are innovative and trustworthy and that respect universal human rights need to be encouraged.

The Information and Communications Technology and Services working group was tasked to continue to work towards ensuring security, diversity, interoperability, and resilience across the ICT supply chain, 5G and beyond, undersea cables, data security and cloud infrastructure. The Data Governance and Technology Platforms working group was given the task to exchange information on respective approaches to data governance and technology platform governance on common issues of concern like illegal and harmful content, algorithmic amplification, transparency, common approaches on the role of cloud infrastructure and services.

The Misuse of Technology to Threaten Security and Human Rights working group was tasked to combat arbitrary or unlawful surveillance also on social media platforms, working towards building an effective mechanism to respond to Internet shutdowns, working towards protection of human rights defenders online, addressing foreign information manipulation, disinformation, and interference with democratic processes, while upholding freedom of expression and privacy rights.

The TTC would ensure cooperation between regulators in both the U.S. and Europe trying to restrain tech giants such as Google, Facebook, Apple, and Amazon.com Inc. The US and Europe already have shared tech goals like curbing the use of AI for surveillance and repression, but the goal of TTC would be to help the U.S. and EU address the issues where they differ in principle, for instance: privacy rules, antitrust regulation, digital taxation, content moderation, etc.

---

[1] The White House, Joint Leaders Statement on AUKUS, at

https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/

[2] New AUKUS alliance will see Australian technological research assist US, UK defence forces at

https://www.abc.net.au/radio/programs/pm/alliance-will-see-australian-tech-assist-us-uk-defence-forces/13547368

[3] Draft of cybersecurity strategy names China, Russia and North Korea as a threat at

https://the-japan-news.com/news/article/0007815536

[4] Biden sanctions cryptocurrency exchange over ransomware attacks at

https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21/

[5] Ibid

[6] Ibid

[7] Ex-U.S. intel operatives admit hacking American networks for UAE at

https://www.reuters.com/world/us/american-hacker-mercenaries-face-us-charges-work-uae-2021-09-14/

[8] The White House, Joint Statement from Quad Leaders

https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/joint-statement-from-quad-leaders/

[9] The White House, U.S.-EU Trade and Technology Council Inaugural Joint Statement at

https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/