Cyber Capabilities and National Power Report: IISS

drishtiias.com/printpdf/cyber-capabilities-and-national-power-report-iiss

Why in News

According to a report by **International Institute for Strategic Studies (IISS),** an influential think tank, **India's offensive cyber capability** is **"Pakistan-focused"** and **"regionally effective",** and not tuned towards China.

Key Points

- **Countries Under Observation:**
    - The report has done a qualitative assessment of cyber power in **15 countries.**
    - **Four members** of the **Five Eyes intelligence alliance** – the United States, the United Kingdom, Canada and Australia.
    - Three cyber-capable **allies of the Five Eyes states –** France, Israel and Japan.
    - **Four countries** viewed by the Five Eyes and their allies as **cyber threats –** China, Russia, Iran and North Korea.
    - Four states at **earlier stages in their cyber power** development – India, Indonesia, Malaysia and Vietnam.
- **Assessment Criteria:**

    The methodology analyses the cyber ecosystem of each state and how it intersects with international security, economic competition and military affairs. The countries are assessed in **seven categories:**

    - Strategy and doctrine
    - Governance, command and control
    - Core cyber-intelligence capability
    - Cyber empowerment and dependence
    - Cyber security and resilience
    - Global leadership in cyberspace affairs
    - Offensive cyber capability

- **Key Observations:**
    - The report has **divided the 15 states into three tiers of cyber power:**
        - **First Tier:** States with **world-leading strengths across all the categories** in the methodology. The **United States of America** is the only country in this tier.
        - **Second Tier:** States that have **world-leading strengths in some of the categories.** Australia, Canada, China, France, Israel, Russia and the United Kingdom are in this tier.
        - **Third Tier:** States that have strengths or **potential strengths in some of the categories but significant weaknesses in others. India,** Indonesia, Iran, Japan, Malaysia, North Korea and Vietnam are in this tier.
    - This report provides confirmation of the **likely durability of US digital-industrial superiority** for at least the next ten years. There can be **two reasons** for this.
        - In advanced cyber technologies and their exploitation for economic and military power, the **US is still ahead of China.**
        - Since 2018, the US and several of its leading allies have agreed to **restrict China's access to some Western technologies.**

            By doing so, these countries have endorsed a partial decoupling of the West and China that could potentially impede the latter's ability to develop its own advanced technology.

- **India Specific Observations:**
    - Despite the **geo-strategic instability of its region** and a keen awareness of the cyber threat it faces, India has made only **“modest progress” in developing its policy and doctrine** for cyberspace security.
    - India has **some cyber-intelligence and offensive cyber capabilities** but they are **regionally focused, principally on Pakistan.**

        However, the **military confrontation with China** in the disputed Ladakh border area in June 2020, followed by a sharp increase in Chinese activity against Indian networks, has heightened Indian concerns about cyber security, not least in systems supplied by China.
    - India is currently aiming to compensate for its weaknesses by building **new capability with the help of key international partners –** including the US, the UK and France – and by looking to concerted international action to develop norms of restraint.
    - India’s approach towards **institutional reform of cyber governance** has been **“slow and incremental”,** with key coordinating authorities for cyber security in the civil and military domains established only as late as 2018 and 2019 respectively.

        The key authorities work closely with the main cyber-intelligence agency, the **National Technical Research Organisation.**
    - The strengths of the Indian digital economy include a **vibrant start-up culture and a very large talent pool.**

        The private sector has moved more quickly than the government in promoting national cyber security.
    - The country is **active and visible in cyber diplomacy** but **has not been among the leaders on global norms,** preferring instead to make productive practical arrangements with key states.

National Technical Research Organisation

- National Technical Research Organisation (NTRO), established in 2004, is under the **National Security Advisor** in the Prime Minister’s Office and focuses on intelligence gathering.
- The agency specializes in **multiple disciplines,** which include remote sensing, data gathering and processing, cyber security, geospatial information gathering, cryptology, strategic hardware and software development and strategic monitoring.
- The **National Critical information Infrastructure Protection Centre (NCIIPC),** an agency under the control of **National Technical Research Organisation,** aims to monitor, intercept and assess threats to critical infrastructure and other vital installations from intelligence gathered using sensors and platforms which include satellites, underwater buoys, drones, VSAT-terminal locators and fiber-optic cable nodal tap points.

- NTRO has the same **“norms of conduct” as the Intelligence Bureau (IB)** and the **Research and Analysis Wing (R&AW).**

Way Forward

- According to the report, India is a third-tier cyber power whose best chance of progressing to the second tier is by **harnessing its great digital-industrial potential** and **adopting a whole-of-society approach** to improving its cyber security.
- Also, the key is **“political will” and “how India organises its intelligence agencies.”** One of the **“leapfrog opportunities”** for governments to be more effective in cyberpower is “how they align themselves with other governments”.

Source: IE