Report on cyber capability by International Institute for Strategic Studies

June 29, 2021

In news

Report on cyber capability has been released by the International Institute for Strategic Studies (IISS) recently.

About the IISS report

In February 2019 the International Institute for Strategic Studies (IISS) announced in a Survival article its intention to develop a methodology for assessing the cyber capabilities of states and how they contribute to national power.

This report is intended to assist national decision-making, for example by indicating the cyber capabilities that make the greatest difference to national power. S

Countries covered under the report

IISS has studied the cyber forces of 15 countries and then prepared the report. The countries covered in this report are:

- The US, the United Kingdom, Canada and Australia (four of the Five Eyes intelligence allies)
- France and Israel (the two most cyber-capable partners of the Five Eyes states)
- Japan (also an ally of the Five Eyes states, but less capable in the security dimensions of cyberspace, despite its formidable economic power)
- China, Russia, Iran and North Korea (the principal states posing a cyber threat to Western interests).
- **India,** Indonesia, Malaysia and Vietnam (**four countries at earlier stages in their cyberpower development).**

Criteria assessed by the report

The report assess each country's capabilities 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

Three tiers of Cyberpower

The report has divided the 15 states into three tiers of cyber power.

- **The first tier** is for states with **world-leading strengths across all the categories** in the methodology. It concludes that only the United States merits inclusion.
- **The second tier** is for states that have **world-leading strengths in some of the categories.** The states it places at that level are, in alphabetical order, Australia, Canada, China, France, Israel, Russia and the United Kingdom.
- **The third tier** is for states that have s**trengths or potential strengths in some of the categories but significant weaknesses in others.** It concludes that India, Indonesia, Iran, Japan, Malaysia, North Korea and Vietnam are at that level.

Key findings

- This report provides confirmation of the likely durability of US digital-industrial superiority, including through international alliances, for at least the next ten years.

- There are two strands to this judgement.
    1. The first is that in advanced cyber technologies and their exploitation for economic and military power, the US is still ahead of China.
    2. The second is Cyber Capabilities and National Power: A Net Assessment that since 2018 the US and several of its leading allies have agreed to restrict, with differing degrees of severity, 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.
- How robustly the US continues this strategy, and how China responds, will dictate the future balance of cyber power.

Status of India

- The report has revealed that India's offensive cyber **capabilities are Pakistan-focused, 'regionally effective', and not directed towards China.**
- The report found that **India has made only modest progress in developing its policy and doctrine for cyberspace security despite the geostrategic instability** of its region and a keen awareness of the cyber threat it faces.
- It said that India's intelligence priorities are deeply shaped by internal and external terrorist threats, internal political violence and the ongoing conflict with Pakistan over Kashmir
- However, India's cyber-intelligence reach appears weak: it tends to rely on partnerships such as those with the U.S., the U.K. and France for a higher level of cyber situational awareness and to help it develop a greater reach of its own in future.
- It has found that as a nuclear power with large

conventional forces, a burgeoning digital economy and a determination to increase its geopolitical influence, India is the target of cyber espionage by a wide range of states.

- It said that India knows its defensive capabilities are relatively weak, that as a result, the country pursues diplomatic efforts to bring the governance of cyberspace within the rules-based international order.
- 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.
- It said that the strengths of the Indian digital economy include a vibrant start-up culture and a very large talent pool.
- According to the report, the **private sector has moved more quickly than the government in promoting national cyber security.**
- Overall, 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.

International Institute for Strategic Studies(IISS)

- IISS is a British research institute in the area of international affairs.
- Since 1997 its headquarters have been Arundel House in London, England.
- The IISS produces independent, policy-relevant data about conflict, however caused, that may have an important military dimension.
- The Military Balance Plus digital database allows users to produce bespoke graphics and employ advanced analytic tools to understand defence trends.
- The IISS identifies crucial questions and publishes

clear, precise and timely analysis on strategic issues.