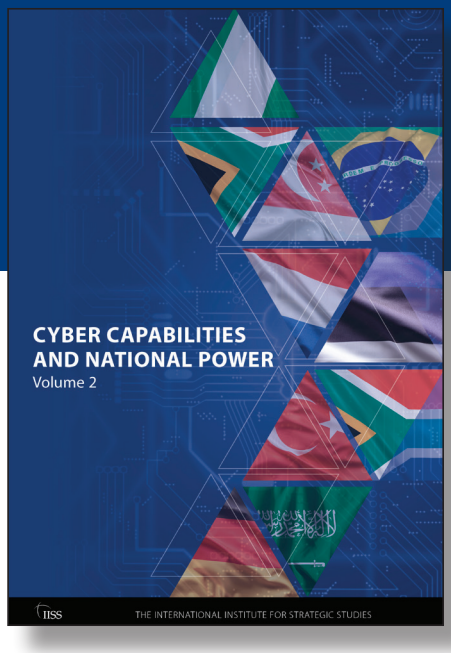
New IISS Research Paper

CYBER CAPABILITIES AND NATIONAL POWER
Volume 2



Executive Summary

This report is the second volume in a two-part series using the IISS methodology for assessing national cyber power. The first volume assessing 15 states was published in 2021. In this volume we assess Brazil, Estonia, Germany, the Netherlands, Nigeria, Saudi Arabia, Singapore, South Africa, Turkiye and the United Arab Emirates (UAE).

Our methodology differs from the index-based approaches developed by other organisations because it is broader and principally qualitative, analysing the cyber ecosystem of each state and how it intersects with international security, economic competition and military affairs. The states 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

THREE TIERS OF CYBER POWER

We have divided the states we analyse into three tiers of cyber power. The first tier is for states with world-leading strengths across all categories in the methodology. In Volume 1 we conclude that only the **United States** merits inclusion in that category. None of the ten states reviewed in Volume 2 match that.

Our second tier is for states that have world-leading strengths in some of the categories. In this second volume, **Germany** and **Netherlands** can be considered Tier-Two cyber powers because of their prominent presence in aspects of the global digital economy, their leadership in global cyberspace affairs and their strategic positioning amid an effective military alliance (NATO) and the collective cyberspace capabilities of the European Union. Germany and the Netherlands may be weaker in core cyber-intelligence capabilities and offensive cyber operations than other Tier-Two powers identified in Volume 1, such as France, Israel and the United Kingdom (see next page). But like these countries, Germany and the Netherlands can also make use of effective partnerships with other cyber-capable states, including the US.

Our third tier is for states that have strengths or potential strengths in some of the categories but significant weaknesses in others. We conclude that **Brazil**, **Estonia**, **Nigeria**, **Saudi Arabia**, **Singapore**, **South Africa**, **Turkiye** and the **UAE** are at that level.

Any attempt at a more granular ranking within the second and third tiers would depend on the degree of importance attributed to each category.

Singapore and Estonia are two important actors in cyberspace, but we assess them to be Tier-Three powers as they do not quite reach the level of world-leading strengths in three or more categories. Both are world leaders in cyberspace affairs and have implemented exemplary practices in cyber security and resilience.

Capabilities of the UAE and Saudi Arabia resemble in part the cyber-power credentials of Estonia, but the two Arab states have much greater wealth at their disposal to procure foreign cyber services and capabilities. Saudi Arabia and the UAE have demonstrated capabilities in use of cyber assets for intelligence, especially in cyber surveillance, but neither country has shown world-class strengths in the other six categories of cyber power.

Turkiye may well aspire to be a cyber power, but we assess it to be in Tier Three. Its robust interventions in Syria and its preparedness to stand up to Russia in that conflict, followed by the 2022 Russian invasion of Ukraine, have created the mindset in Ankara that it must and can do better in adoption of advanced technologies, especially in cyberspace, for

national security. For now, however, Turkiye is not a world leader in any of the seven categories of cyber power. Brazil, Nigeria and South Africa face the challenges of developing countries in building up their cyber capabilities. All three face low levels of consistency in the digitalisation of the economy and society, with the inevitable impact on cyber power.

Tiers of Cyber Power: A Qualitative Assessment

Categories of Analysis:

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

Tier One

1 2 3 4 5 6 7

World-Leading Strengths in All Categories:

VOL. 1: United States

VOL. 2: None

Tier Two

1 2 3 4 5 6 7

World-Leading Strengths in Some Categories:

VOL. 1: Australia, Canada, China, France, Israel, Russia, United Kingdom

VOL. 2: Germany, Netherlands

Tier Three

1 2 3 4 5 6 7

Strengths or Potential Strengths in Some Categories but Significant Weaknesses in Others:

VOL. 1: India, Indonesia, Iran, Japan, Malaysia, North Korea, Vietnam

VOL. 2: Brazil, Estonia, Nigeria, Saudi Arabia, Singapore, South Africa, Turkiye, UAE

IISS