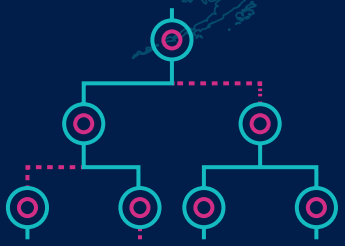
Threats, risks & vulnerabilities

Ransomware

A form of malware used by cyber criminals to prevent or limit users from accessing their systems or data – or threatening to leak it - until a ransom is paid

Commodity attacks

High-volume, low-sophistication attacks usually involving phishing and other scams often reaching citizens and small businesses



Proliferation

Increased commercial availability of high-end disruptive and offensive cyber capabilities and tools used by state and non-state actors

Supply chain

Attacks where perpetrators access an organisation's network or systems via third-party vendors or suppliers

Vulnerabilities

Weaknesses in an IT system that can be exploited by an attacker to deliver a successful attack

The threat from state actors

Russia

used cyber capabilities to maximise operational impact in Ukraine.
A seasoned cyber aggressor with a record of attacks against its neighbours and the UK, including attempts to steal Covid vaccine research in 2020

China

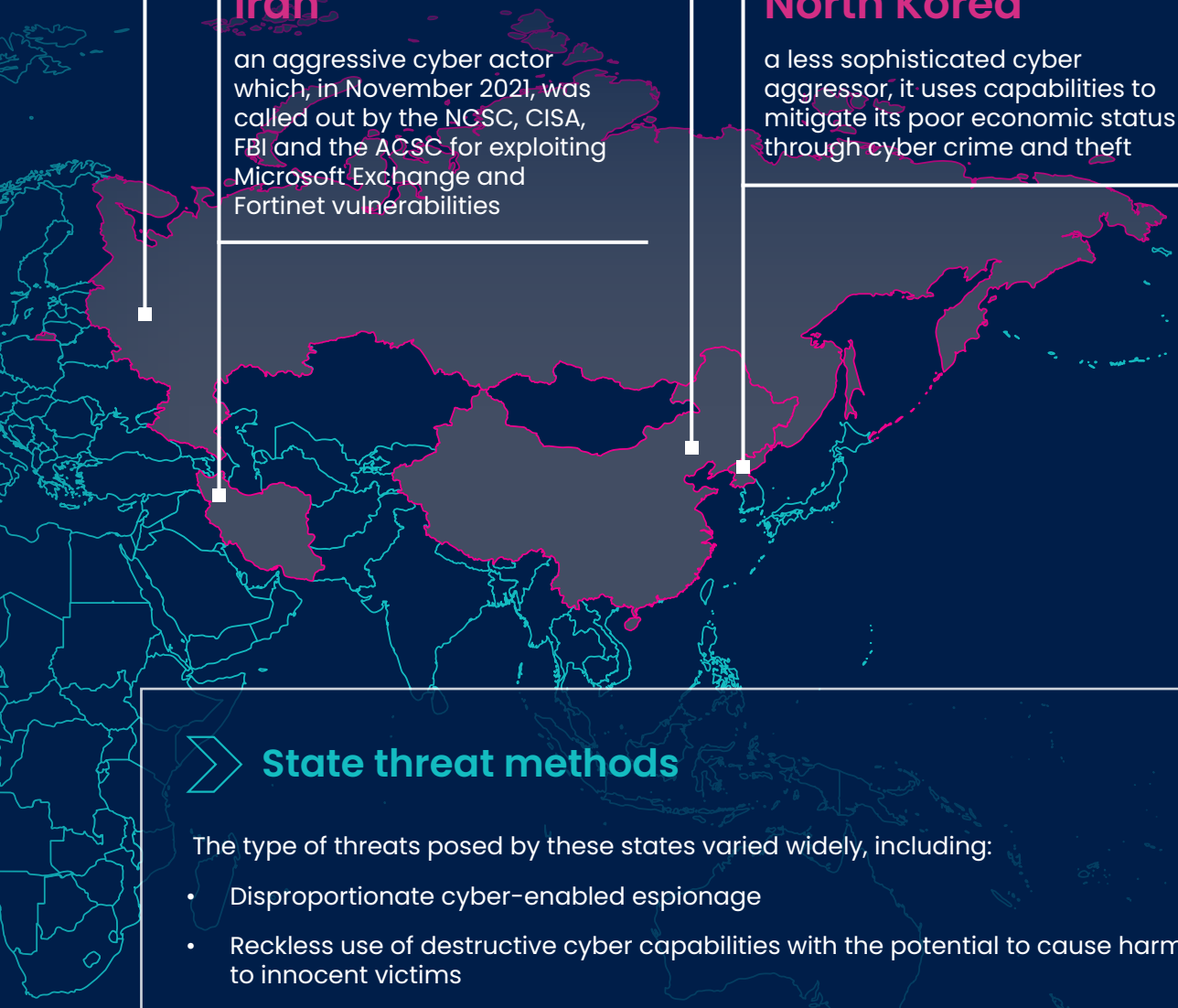
is becoming ever more sophisticated, increasingly targeting third-party technology, software and service supply chains

Iran

an aggressive cyber actor which, in November 2021, was called out by the NCSC, CISA, FBI and the ACSC for exploiting Microsoft Exchange and Fortinet vulnerabilities

North Korea

a less sophisticated cyber aggressor, it uses capabilities to mitigate its poor economic status through cyber crime and theft



State threat methods

The type of threats posed by these states varied widely, including:

- Disproportionate cyber-enabled espionage
- Reckless use of destructive cyber capabilities with the potential to cause harm to innocent victims
- Cyber-enabled theft of intellectual property or personal data of citizens for commercial advantage
- Undermining of legitimate democratic institutions including electoral processes