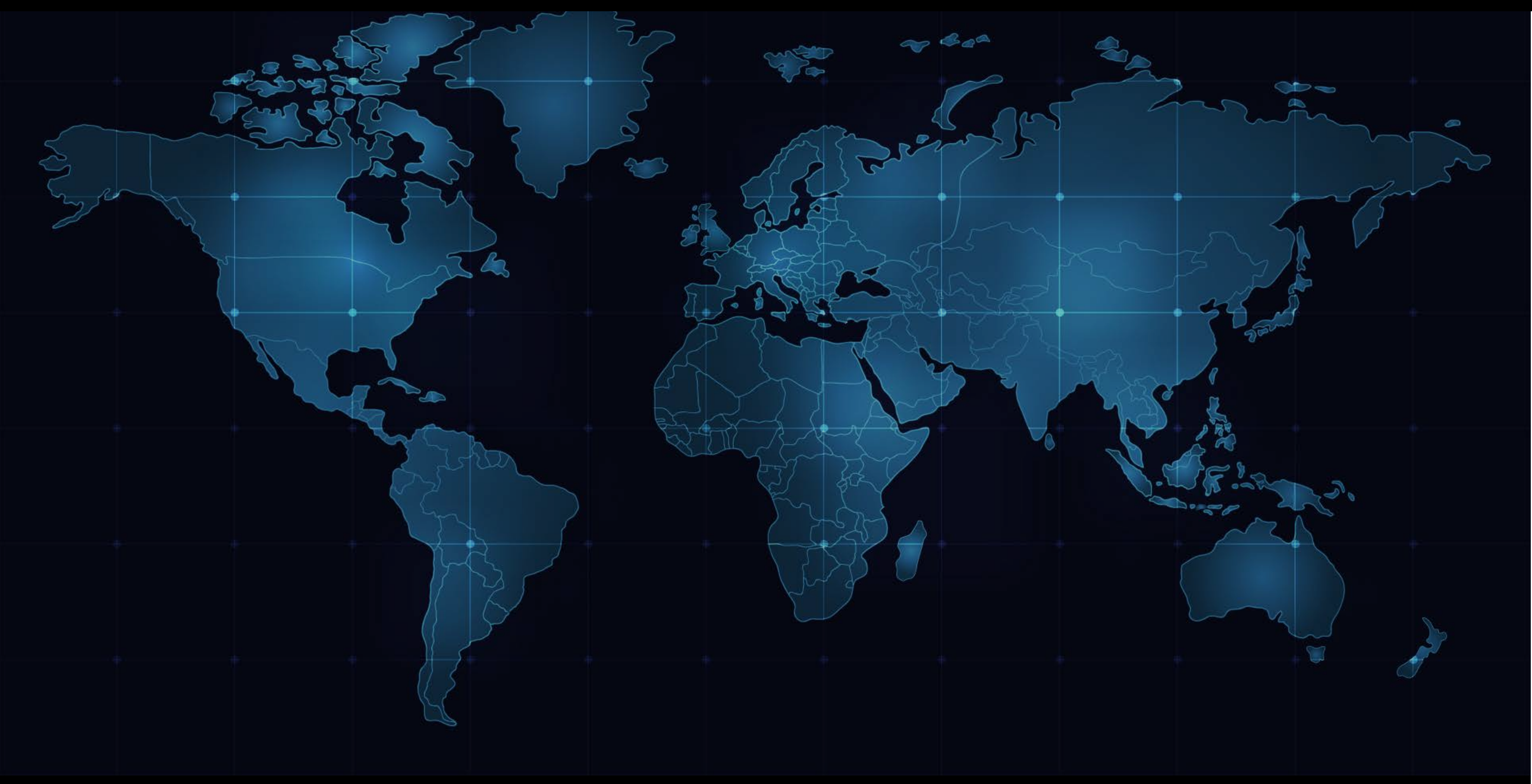
CYBER CONFLICT OBSERVATORY AND MARITIME CONFLICT THEATERS.

Last update: December 2025

TLP:CLEAR
PAP:CLEAR



CYBER CONFLICT OBSERVATORY AND MARITIME CONFLICT THEATERS.

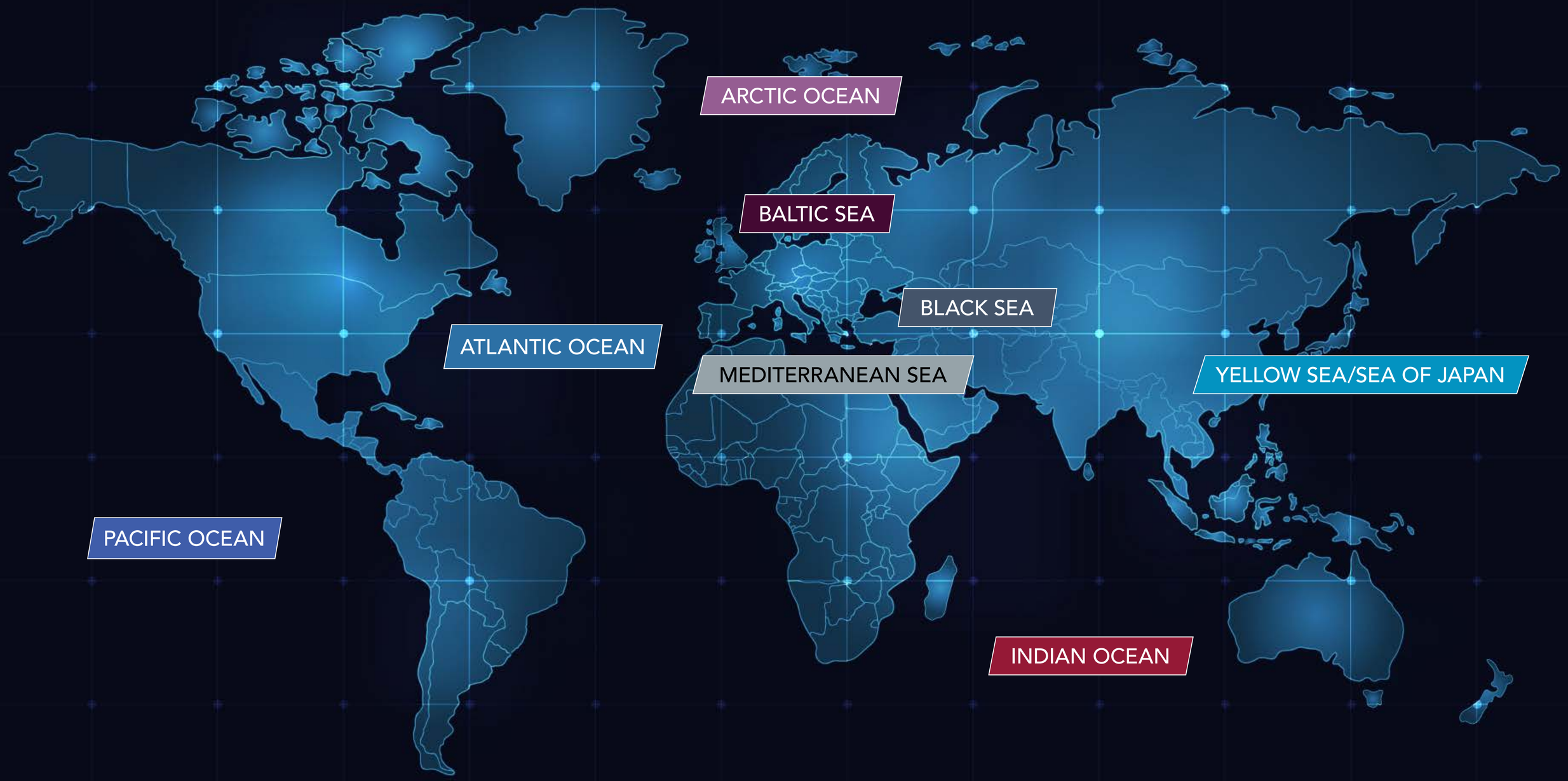
Maritime areas are simultaneously:
- theaters of operation and confrontation;
- strategic areas of influence;
- essential targets for the deployment of capabilities to build the industrial and technological base of naval defense;
- and positions occupied between two borders, often subject to claims.

The political, geopolitical, and military issues surrounding maritime areas are transposed into cyberspace in terms of hacktivist and state-sponsored activities. These take the form of attacks against public and private defense actors, and sometimes occur in traditional areas of conflict.

The cyber conflict observatory and maritime conflict theaters offers a different perspective on defense and cyber issues by bringing together intelligence on cyberattacks affecting the maritime sector in one place.

This document is produced by OWN analysts and is subject to regular updates.

CYBER CONFLICT OBSERVATORY AND MARITIME CONFLICT THEATERS



Baltic Sea

CYBER THREATS

- Espionage or disruption of Baltic undersea communication cables linking Scandinavia and mainland Europe.
- Ransomware or sabotage against key ports (Tallinn, Riga, Gdańsk, Stockholm) and logistics infrastructure supporting NATO supply routes.
- Potential manipulation of AIS (Automatic Identification System) data affecting maritime navigation and trade.

RELATED CONFLICTS

- Heightened tensions due to NATO enlargement (Finland, Sweden) and Russian opposition to Baltic Sea militarization.
- Hybrid warfare threats involving disinformation, cyberattacks, and energy infrastructure sabotage (Nord Stream incidents).

STATE ACTORS

- **APT28 «Fancy Bear» (Russia / GRU):** Focused on military, governmental, and strategic communication espionage.
- **Turla (Russia / FSB)** a long-running cyber-espionage group specializing in stealthy intrusions, satellite link compromise, and data exfiltration.
- **APT29 «Cozy Bear» (Russia / SVR):** Engaged in long-term espionage against European and NATO institutions, potentially targeting Baltic communications and government networks.
- **UNC1151 (Belarus / linked to Ghostwriter):** Conducts disinformation operations and cyber espionage in the Baltic states to undermine NATO cohesion and public trust.

Black Sea

CYBER THREATS

- Sabotage or espionage of undersea communication cables and energy pipelines connecting the Black Sea littoral states (Turkey, Romania, Bulgaria, Georgia, Ukraine).
- Ransomware or targeted disruption of major ports (Constanța, Varna, Odessa), logistics hubs that support regional military and commercial flows and regional energy infrastructure (offshore platforms, refineries, power grids)
- Disruption of naval communication networks or maritime traffic control systems.
- AIS manipulation and GNSS jamming/spoofing in congested straits and approaches

RELATED CONFLICTS

- Ongoing War in Ukraine: Russian cyber operations targeting Ukrainian and NATO-linked infrastructure in the region.
- Regional tensions between NATO and Russia over Black Sea military presence and intelligence-gathering operations.

STATE ACTORS

- **APT28 «Fancy Bear» (Russia / GRU):** Focused on military, governmental, and strategic communication espionage.
- **Turla (Russia / FSB):** a long-running cyber-espionage group specializing in stealthy intrusions, satellite link compromise, and data exfiltration.
- **Sandworm (Russia / GRU):** Known for offensive cyber operations in Ukraine and NATO member states; potential targeting of energy and maritime systems.

Pacific Ocean

CYBER THREATS

- Sabotage or espionage of undersea cables linking Asia to Americas/Europe
- Vulnerability of Asia-Americas trade routes, heavily reliant on digital infrastructure.
- Risks to major ports (Shanghai, Singapore, Los Angeles) and automated port systems: High strategic interest from major states for intelligence and disruption.
- Cybercrime targeting massive shipping lanes and container logistics.
- AIS/GNSS manipulation in busy straits and near archipelagos; supply-chain malware in maritime software vendors

RELATED CONFLICTS

- **China-Taiwan / United States tensions:** Risk of cyber sabotage of cables connecting Taiwan, attacks on port infrastructure, and GPS jamming.
- **South China Sea:** Increased militarization and risk of Chinese cyberattacks against foreign vessels.
- **US/Latin America:** Increased tensions in South America following US attacks

STATE ACTORS

- **Mustang Panda (China / MSS):** Targeting maritime and naval infrastructure, technological espionage.
- **APT41 (China / with known crossover between espionage and financially motivated operations):** Highly relevant wherever China has geopolitical, trade, or maritime interests — especially in Asia–Pacific, Indian Ocean, and infrastructure connected to Belt and Road (BRI).
- **SideWinder (India)** has been reported targeting maritime/port infrastructure in the region historically. (Arabian SEA, Gulf of Aden approaches)
- **APT28 «Fancy Bear» (Russia / GRU):** Focused on military, governmental, and strategic communication espionage.
- **Lazarus Group (North Korea):** Financial attacks, possible targeting of shipping for illicit funding.
- Regional APTs engaged in supply-chain targeting of maritime services.

Indian Ocean

CYBER THREATS

- Critical cables passing through the Red Sea and the Bab el-Mandeb Strait.
- Hybrid risks: piracy + manipulation of navigation systems.
- Oil and gas platforms are vulnerable to cyber intrusions.
- Attacks on offshore energy comms and satellite links used by vessels in long transits.

RELATED CONFLICTS

- **Conflict in Yemen (Houthis):** Physical attacks on navigation in the Red Sea, combined with attempts at electronic interference.
- Rivalries between **Iran and the United States / Saudi Arabia:** Risk of cyberattacks against energy flows.
- **War in Gaza and Israel–Iran tensions:** Threat of cyber operations on Mediterranean–Indian undersea cables.

STATE ACTORS

- SideWinder (India) has been reported targeting maritime/port infrastructure in the region historically. (Arabian SEA, Gulf of Aden approaches)
- Tortoiseshell (Iran/IRGC cyber unit): Targeting IT providers, defense contractors, telecoms, and occasionally logistics or maritime-linked firms.
- Mustang Panda (China / MSS): Targeting maritime and naval infrastructure, technological espionage.
- APT41 (China / with known crossover between espionage and financially motivated operations): Highly relevant wherever China has geopolitical, trade, or maritime interests — especially in Asia–Pacific, Indian Ocean, and infrastructure connected to Belt and Road (BRI).
- **APT34 «OilRig» (Iran):** Targeting energy, transport, and telecommunications in the Middle East.
- **Charming Kitten (Iran):** Cyber espionage and disinformation, potentially targeting maritime/logistics.
- Groups affiliated with the Houthis using cyber capabilities indirectly supported by Iran.

Arctic Ocean

CYBER THREATS

- Development of the **Northern Sea Route** with a new digital infrastructure, poorly secured.
- GPS/GNSS are vulnerable to spoofing and jamming.

RELATED CONFLICTS

- **War in Ukraine:** Militarization of the Arctic by Russia, with risks of cyberattacks to control routes and communications.
- Strategic competition as Arctic access and seabed resources attract state interest (militarization, surveillance, and contestation over shipping routes).
- Growing rivalry between **Russia and NATO:** Possible surveillance and sabotage of Arctic cables.
- Grey-zone activity using commercial vessels and research platforms as cover for undersea reconnaissance or interference.

STATE ACTORS

- **APT28 «Fancy Bear» (Russia / GRU):** Focused on military, governmental, and strategic communication espionage.
- **Turla (Russia / FSB):** a long-running cyber-espionage group specializing in stealthy intrusions, satellite link compromise, and data exfiltration.
- **Sandworm (Russia):** Already active in the maritime and energy space.

Mediterranean Sea

CYBER THREATS

- Sabotage or espionage of undersea communication cables: Very high density of cables connecting Europe, Africa, and the Middle East
- NATO/CCDCOE and allied reporting highlights rising state-linked cyber pressure on European Mediterranean ports and logistics hubs
- Strategic ports (Marseille, Piraeus, Tanger Med) vulnerable to ransomware and attacks on logistics.
- AIS data manipulation affecting ferry traffic and coastal trade routes

---

RELATED CONFLICTS

- **Israel-Hamas conflict:** Threat to Israeli maritime infrastructure and cables connecting Asia to Europe.
- **Instability in Libya:** Coastal areas vulnerable to trafficking + cyberattacks facilitating illicit flows.
- Tensions between **Turkey, Greece, and Cyprus** regarding gas deposits > cyber threats to offshore infrastructure.

STATE ACTORS

- **Turla (Russia / FSB):** a long-running cyber-espionage group specializing in stealthy intrusions, satellite link compromise, and data exfiltration.
- **SideWinder (India)** has been reported targeting maritime/port infrastructure in the region historically. (Arabian SEA, Gulf of Aden approaches)
- **APT41 (China / with known crossover between espionage and financially motivated operations):** Highly relevant wherever China has geopolitical, trade, or maritime interests — especially in Asia–Pacific, Indian Ocean, and infrastructure connected to Belt and Road (BRI).
- **Unit 8200 (Israel):** High-level cyber defense and cyber offense capabilities, capable of both protecting and conducting operations.
- **APT35/Charming Kitten (Iran/IRGC):** Already active against Israel and regional infrastructure.
- Turkish groups **pro-government** conducting DDoS campaigns and cyber espionage in the region.

Atlantic Ocean

CYBER THREATS

- Sabotage or espionage of transatlantic undersea cables (critical infrastructure connecting Europe and the Americas).
- Major ports (Rotterdam, Antwerp, New York) targeted by ransomware or supply chain attacks.
- AIS/ship-tracking manipulation on long oceanic legs to conceal or spoof movements of high-value cargo.

RELATED CONFLICTS

- **War in Ukraine:** Concern over Russian cyber operations against Europe–United States flows to disrupt military and logistical support.
- Increased espionage between **NATO – Russia/China** blocs.

STATE ACTORS

- **Sandworm (Russia / GRU):** Specializes in attacks against critical infrastructure (Ukraine, energy, telecommunications).
- **APT29 «Cozy Bear» (Russia / SVR):** Cyber espionage targeting governments and telecommunications, potentially impacting cables and data centers.
- **State-linked groups attributed to Russia and China:** intelligence collection and potential pre-positioning for crisis options against critical infrastructure.

Yellow Sea / Sea of Japan

CYBER THREATS

- Espionage or disruption of undersea communication cables and landing stations routing traffic between Korea, Japan and northeastern China (risk to regional comms and maritime domain awareness).
- Ransomware, DDoS or sabotage against key ports and logistics hubs (Incheon, Busan approaches, Dalian, Qingdao, Yokohama/Tokyo-area facilities) that support international trade and military logistics.
- Potential manipulation of AIS and GNSS (spoofing/jamming) affecting navigation, vessel tracking and safety in congested straits and approaches (increasing risk of misrouting, blind spots or concealed movements).

RELATED CONFLICTS

- Heightened regional tensions from Korea peninsula dynamics (DPRK provocations and military posture) and great-power competition in East Asia (maritime disputes, Taiwan Strait pressure) that increase the incentive to use cyber options alongside naval activity.
- Hybrid/grey-zone activity blending cyberattacks, DDoS and disinformation aimed at pressuring national authorities, disrupting logistics, or obscuring maritime operations (e.g., attacks timed with military/ political events).

STATE ACTORS

- **Mustang Panda (China / MSS):** Targeting maritime and naval infrastructure, technological espionage.
- **Lazarus Group (North Korea/DPRK):** financially motivated and state-directed intrusions historically targeting South Korean infrastructure, financial institutions and supply chains — plausible actor for maritime logistics/crewing/ supply-chain attacks.
- **Russian state-linked actors (various GRU/FSB-attributed groups):** capable of DDoS, disruption and influence operations against Japanese and regional maritime/logistics targets (observed in broader regional campaigns).
- **Organized cybercrime / ransomware gangs:** financially motivated actors opportunistically targeting port operators, terminals and third-party logistics providers across the region. Upcoming

OWN

PARIS • RENNES • TOULOUSE

Téléphone
+33 (0) 805 -690-234

contact@**own.security**

www.own.security