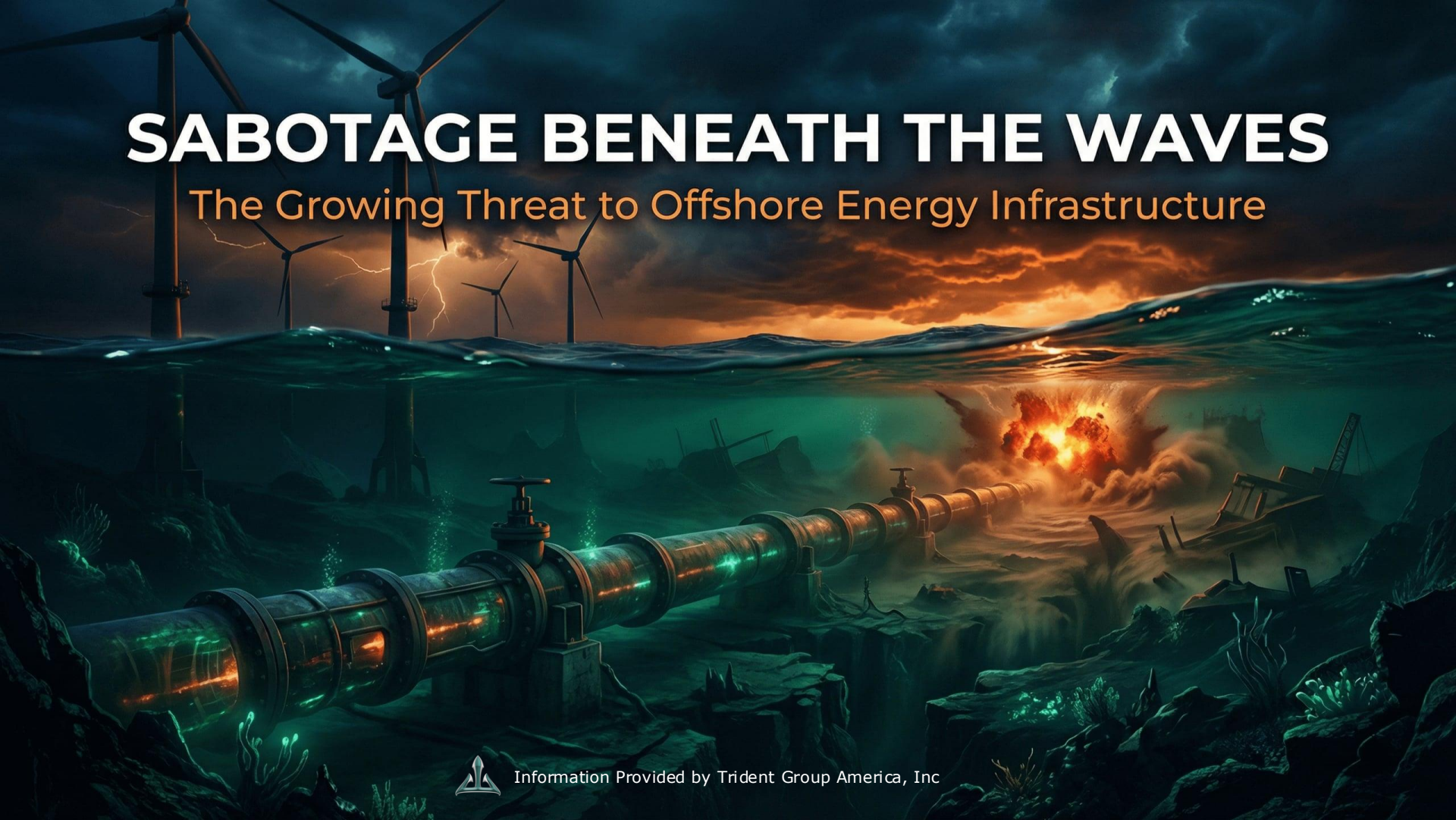

SABOTAGE BENEATH THE WAVES
The Growing Threat to Offshore Energy Infrastructure
Information Provided by Trident Group America, Inc

The Overlooked Dimension of a Familiar Threat

Fibre-Optic Cables Get the Headlines — But Offshore Energy Infrastructure Is More Consequential If Attacked

- ~20,000 miles of subsea pipelines move oil and gas across ocean floors
- Expanding fleets of LNG terminals, FSRUs, and export facilities
- Rapidly growing offshore wind farms and their interconnecting power cables
- Subsea substations and mooring systems tying it all together

Information Provided by Trident Group America, Inc

NORD STREAM: THE SINGLE MOST CONSEQUENTIAL ACT OF ENERGY INFRASTRUCTURE SABOTAGE IN MODERN HISTORY

THE SEPTEMBER 2022 NORD STREAM EXPLOSIONS PROVED THAT LARGE-SCALE PERMANENT DESTRUCTION IS ACHIEVABLE

- The single most consequential act of energy infrastructure sabotage in modern history.
- The pipelines remain out of operation more than three years later, permanently reshaping European energy flows.
- The attack demonstrated that subsea energy infrastructure can be destroyed permanently with a single operation.
- Attribution remains contested — a deliberate product of operational design to exploit jurisdictional gaps.

A Sustained Reconnaissance Campaign Is Already Underway

Russia Has Been Mapping North Sea and Baltic Energy Sites for Future Sabotage Since Before the Ukraine War

- **August 2024:** German authorities tracked long-range military-grade surveillance drones over ChemCoast Park in Brunsbüttel, adjacent to Germany's floating LNG facility.
- The same onshore pipeline had already been damaged in a separate sabotage action in 2023.
- **2023:** A joint investigation found Russia operating vessels disguised as fishing trawlers and research ships conducting underwater surveillance and mapping key North Sea sites.
- Adversaries are not merely capable of attacking — they are actively rehearsing operations.

OFFSHORE WIND: EUROPE IS BUILDING A CONTINENT-SCALE POWER SYSTEM WITHOUT SECURING IT

€1 Trillion in North Sea Wind Investment Is Creating a Vast, High-Value, Low-Protection Attack Surface

- Jan 2026: Hamburg Declaration pledges 100 GW of joint offshore wind by 2050, mobilising €1 trillion.
- EUROATLAS warns of a “continent-scale underwater power system without investing in a corresponding underwater security architecture.”
- Security professional James Bore assesses these assets as “attractive for sabotage by highly capable, motivated hostile actors.”

Information Provided by Trident Group America, Inc

THE U.S. PAUSED OFFSHORE WIND OVER CLASSIFIED NATIONAL SECURITY RISKS

The Pentagon Identified Classified Threats to U.S. East Coast Wind Farms — Including Chinese Kill Switch Scenarios

- Dec 2025: Trump administration paused leases of five large-scale offshore wind farms along the U.S. East Coast.
- Interior Secretary cited threats of undersea drone attacks and swarm drone strikes exploiting radar distortions.
- Heritage Foundation noted many turbine components are manufactured in China.
- NATO official warned of potential ‘kill switch’ scenarios embedded in Chinese-manufactured components.

THE CHINESE SUPPLY CHAIN IS EMBEDDED IN THE INFRASTRUCTURE BEING PROTECTED

HMN Technologies Controls Cable Manufacturing and Repair — and Supplies Components for Energy Interconnection Systems

- HMN Technologies dominates global submarine cable manufacturing and repair, and supplies components for offshore energy interconnection systems.
- FCC voted unanimously in 2024 to propose rules barring Chinese technology from undersea cables connecting to the U.S.
- FCC Chair stated the agency is guarding submarine cables against foreign adversary ownership and access.
- Control Risks documented that adversaries may not need to physically damage assets if they can compromise software and communications systems remotely.
- The convergence of physical sabotage risk and embedded digital vulnerability creates a layered threat.

Information Provided by Trident Group America, Inc

LNG TERMINALS ARE PROVEN MILITARY TARGETS

Iranian Drones Struck Qatar's Ras Laffan Gas Facilities in 2026 — Demonstrating That Energy Terminals Can Be Neutralised With Commercial Weapons

- Europe's pivot from Russian pipeline gas to LNG imports has made its FSRUs and onshore terminals a concentrated high-value target set.
- During the 2026 Iran war, Iranian drones struck Qatar's gas facilities at Ras Laffan Industrial City, forcing QatarEnergy to declare force majeure.
- This demonstrated that offshore energy terminals are legitimate military targets in active conflict and can be neutralised with commercially available weapons systems.
- Cable damage in the Strait of Hormuz represents a "credible threat" that could cause "service blackouts".

ATTRIBUTION IS ENGINEERED TO FAIL

Subsea Attacks Are Deliberately Designed to Be Ambiguous, Deniable, and Legally Inconclusive

- “A minority of incidents have thus far been positively attributed” — disinformation actively muddies waters.
- This is not an intelligence failure — it is deliberate operational design.
- Attacks exploit jurisdictional gaps and forensic limitations.
- Political thresholds for invoking NATO Article 4 remain too high despite sustained campaigns.
- Statements of intent to protect infrastructure do not equal operational capability.

The Repair Gap: Nord Stream Has Been Down for Over Three Years

Subsea Energy Infrastructure Takes Months or Years to Repair — and the Capacity to Do So Is Dangerously Limited

- Average repair time for a subsea cable: ~40 days under normal conditions.
- For subsea pipelines and offshore energy export infrastructure, restoration can take months or years.
- The Nord Stream pipelines remain out of operation more than three years after the 2022 attacks.
- The U.S. licensing process for subsea infrastructure projects averages two years in duration.

Information Provided by Trident Group America, Inc

THE 2026 ESCALATION RISK: CRACKING DOWN ON THE SHADOW FLEET COULD TRIGGER ENERGY INFRASTRUCTURE ATTACKS

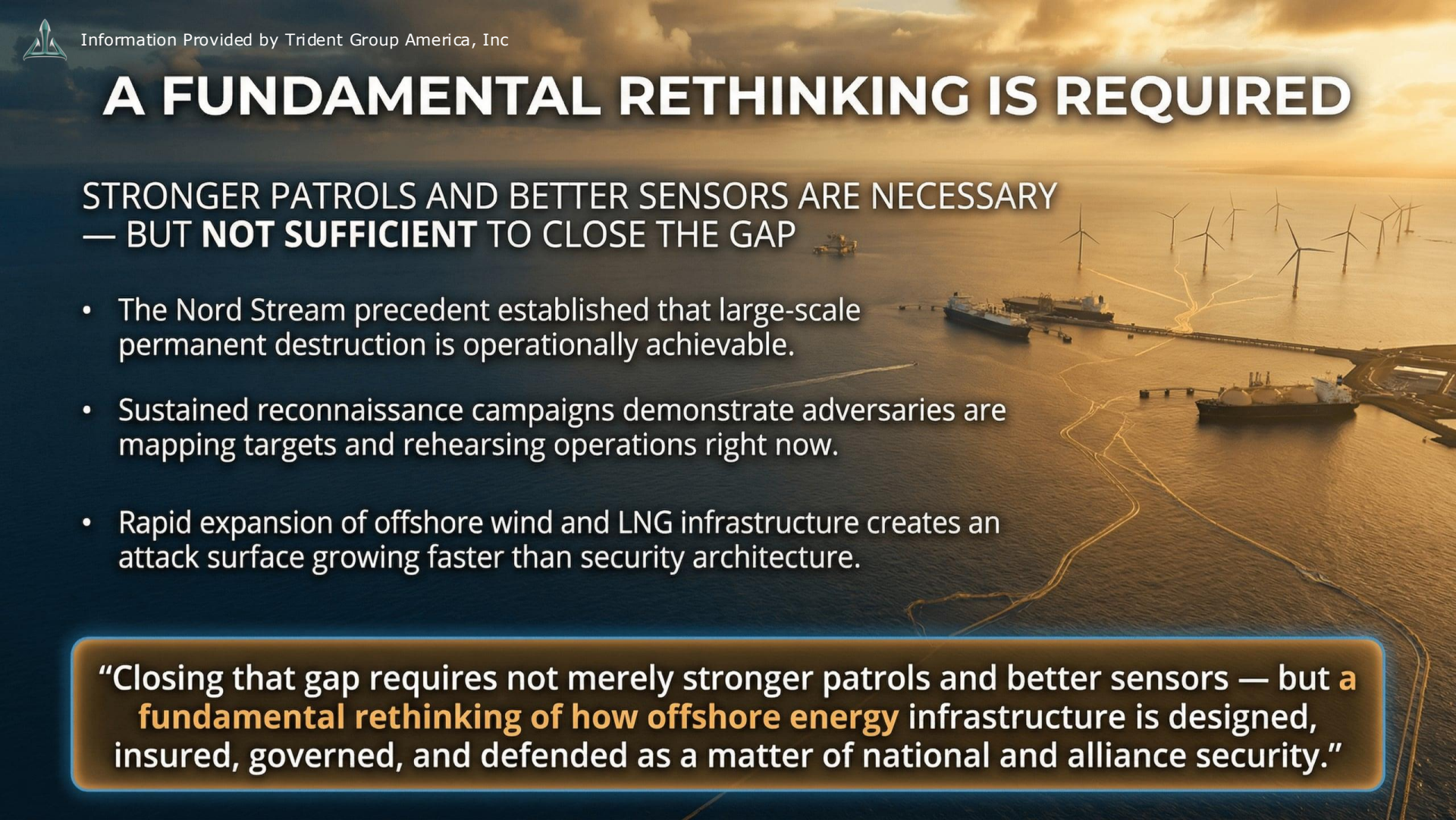
Every Escalation Against Russia's Shadow Fleet Carries a Corresponding Risk of Retaliation Against European Energy Infrastructure

- Herminius senior adviser predicted Russia may respond to European enforcement actions by targeting subsea energy infrastructure.
- Consistent with Russia's broader campaign as a 'shadow war' (skyggekrigen).
- Designed to impose cumulative costs on NATO states below the threshold of armed response.
- Creating political pressure to ease sanctions and reduce support for Ukraine without triggering Article 5.

A FUNDAMENTAL RETHINKING IS REQUIRED

STRONGER PATROLS AND BETTER SENSORS ARE NECESSARY — BUT **NOT SUFFICIENT** TO CLOSE THE GAP

- The Nord Stream precedent established that large-scale permanent destruction is operationally achievable.
- Sustained reconnaissance campaigns demonstrate adversaries are mapping targets and rehearsing operations right now.
- Rapid expansion of offshore wind and LNG infrastructure creates an attack surface growing faster than security architecture.



"Closing that gap requires not merely stronger patrols and better sensors — but **a fundamental rethinking of how offshore energy** infrastructure is designed, insured, governed, and defended as a matter of national and alliance security."