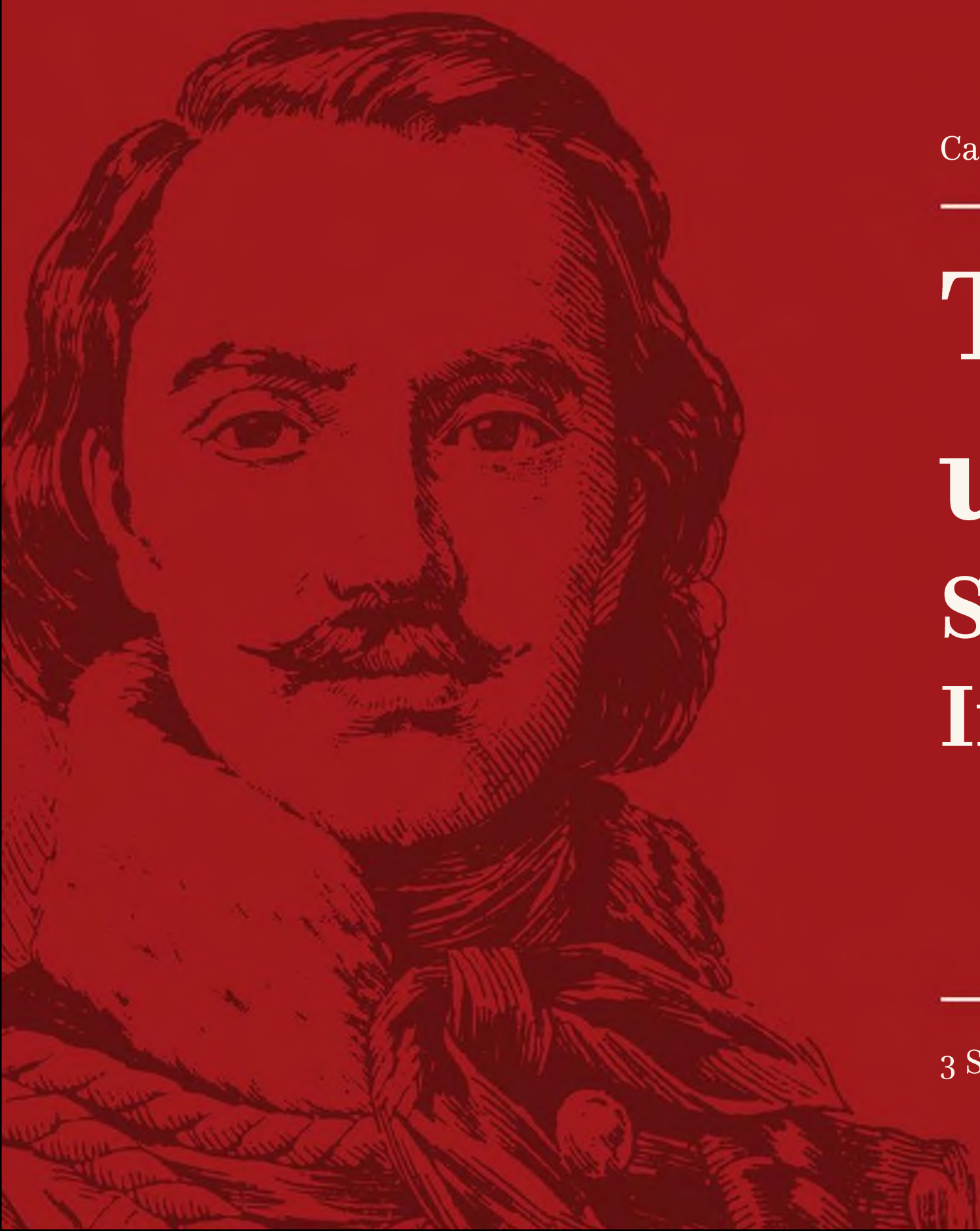




Casimir Pulaski Foundation

The costs of unpreparedness: Security of Energy Infrastructure in the Baltic Sea

3 September 2026, Warsaw

THE “CRITICAL SEA”

The Baltic is no longer a collection of national assets but one interconnected ENERGY-SECURITY SYSTEM

- Dense concentration of subsea power cables, telecom links, gas pipelines, ports and offshore wind assets
- The energy transition is adding new nodes, connections and dependencies faster than the security architecture around them
- Interconnection increases resilience, but also allows disruption to propagate across borders and sectors
- Many assets are dual-use, supporting civilian energy systems as well as defence, communications and situational awareness

A local physical incident can quickly spill over into a regional energy, economic and security event



RUSSIAN HYBRID CAMPAIGN AGAINST INFRASTRUCTURE IN THE BALTIC SEA

Russia-linked maritime activity has turned the Baltic, into a grey-zone battlespace where commercial vessels, undersea cables, pipelines, GPS interference are targeted below the threshold of war

- ~44 cable-damage incidents recorded globally/regionally between January 2024 - July 2025 (INSIKT Group, 2025); not all were deliberate.
- 7 Baltic subsea cable cuts between October 2023 - December 2024. (Bryjka, Dyner & Koziol, 2026)
- 2,313 Russia-affiliated vessels visited the Baltic Sea between February 2024 - February 2025; only 436 used the Russian flag (ACLED, 2026).
- Russia's shadow fleet is estimated at ~600–1,400 ships. (Reuters, 2025)
- NATO launched Baltic Sentry in Jan 2025, deploying frigates, maritime patrol aircraft, naval drones, and surveillance integration to protect undersea infrastructure. (NATO, 2025)



SABOTAGE INCIDENTS IN AUGUST 2026

- 4 Aug | **Germany – Leipzig/Halle Airport**
Explosive-laden drone found next to a Ukrainian Antonov cargo aircraft; Germany attributed the operation to Russia.
- 5–6 Aug | **Germany – Leverkusen**
Railway and fibre-optic cables deliberately cut; **suspected sabotage.**
- 8 Aug | **Bulgaria – Kardam**
Drone exploded near a compressor station on the Trans-Balkan / Vertical Gas Corridor; **deliberate targeting not established.**
- 10 Aug | **Bulgaria – Belitsa / Tryavna**
Fire and explosions at an EMCO ammunition storage facility; **cause under investigation.**
- 11 Aug | **Romania – Black Sea / Neptun Deep**
Two explosive-capable drones found near Romania’s largest offshore gas development; **intent unclear.**
- 13 Aug | **Italy – Colleferro**
Fire and explosion at KNDS Ammo Italy ammunition plant; **authorities currently favour an internal cause.**
- 14–15 Aug | **Estonia – Tallinn**
Deliberate arson at Milrem Robotics, producer of military unmanned vehicles supplied to Ukraine; **foreign-state angle investigated.**
- 20 Aug | **Romania – Black Sea / Neptun Deep**
Explosive unmanned surface vessel detected near strategic offshore gas infrastructure; **Russia publicly blamed by Romania.**
- 22 Aug | **Slovakia – Haniska / Prešov**
Planned arson attack disrupted at Skyeton, a Ukrainian military-drone manufacturer; **sponsor not publicly identified.**
- 23 Aug | **Germany – Backnang**
Railway and telecom cables deliberately cut, disrupting traffic and communications; **suspected sabotage.**
- 24–26 Aug | **Norway**
Major DDoS attack disrupted national digital public infrastructure; **claimed by a pro-Russian group.**
- 25 Aug | **Sweden**
Coordinated DDoS campaign targeted government and public-sector websites; **claimed by a pro-Russian group.**
- 30 Aug | **Poland – Lublin**
Major fire at JFG Composites, an aerospace/defence composites facility; **deliberate arson investigated.**
- 31 Aug | **Poland – Skarżysko-Kamienna**
Deliberate arson at WB Group, producer of military drone systems supplied to Ukraine; **foreign-intelligence investigation opened.**
- 1 Sep | **Germany – Brandenburg / Turnow-Preilack**
Deliberate attack on 50Hertz high-voltage transmission infrastructure; **sabotage confirmed.**
- 1 Sep | **Germany – Bergheim-Rheidt**
Intentional damage at an Amprion electricity substation caused grid faults; **investigation ongoing.**



THE COSTS OF UNPREPAREDNESS

The strategic variable is not only the cost of damage. It is TIME TO RECOVERY.

CRITICAL BOTTLENECKS

- specialised repair vessels and crews
- spare cables, components and equipment
- weather windows and port availability
- alternative capacity and rerouting
- cross-border contracting and emergency procedures

INFRASTRUCTURE	TYPICAL DISRUPTION / REPAIR	POTENTIAL LOSS
Telecom cable	7–24 days	€168–576m
HVDC interconnector	40–60 days	€480–720m
Offshore wind export cable	~60 days	€8.6–25.7m
Gas pipeline	5–9 months	€11.3–20.3bn

Illustrative estimates from sources already used in the draft: RAND, DNV, YLE/ICPC.

Repair capacity is becoming a critical capability in its own right

FROM ASSET PROTECTION TO SYSTEM RESILIENCE

We cannot physically protect every kilometre of cable, pipeline or offshore infrastructure.

OLD QUESTION

How do we prevent this asset
from being damaged?



NEW QUESTION

How does the system continue
operating
when an asset is lost?

REDUNDANCY

Alternative routes, spare
capacity, physical separation

RECOVERY

Repair vessels, crews,
spares, pre-agreed contracts

CONTINUITY

Alternative supply,
rerouting, emergency
operating modes

DESIGN

Security built into routing,
architecture and investment
decisions

The objective is not zero infrastructure damage. It is continuity of critical services despite damage

CASE STUDY: COUNTER-DRONE RESILIENCE

Deploying a C-UAS system does not solve the problem. The capability is organisational.

ASSESS

Threat and vulnerability
assessment

PREPARE

Clear response
procedures and
escalation paths

HARDEN

Passive protection and
physical safeguards

TRAIN

Prepared personnel who
know what to do

TEST

Realistic penetration
tests and repeated
exercises

TECHNOLOGY MATTERS.

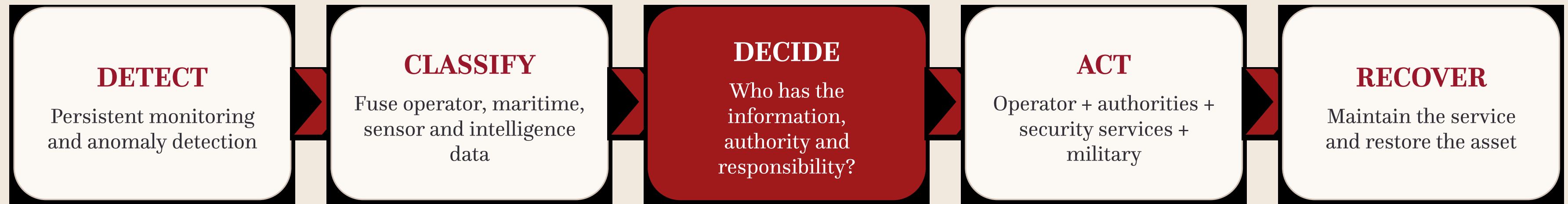
BUT PEOPLE, PROCEDURES AND REGULAR TESTING DETERMINE WHETHER IT WORKS UNDER
REAL-TIME PRESSURES IN AN EVOLVING ENVIRONMENT

Ergo: resilience is a capability, not a procurement item

THE BOTTLENECK IS MOVING FROM DETECTION TO DECISION

Technology can increasingly see anomalies

Resilience now depends on how quickly the system can interpret, decide and act



SOLUTIONS ARE IMPROVING FASTER THAN GOVERNANCE

The next resilience gap may not be seeing the threat but deciding who acts, on what information, and how quickly

THE BALTIC RESILIENCE GAP

CER • NIS2 • EU Cable Security Action Plan • Baltic Sentry • National measures

The problem is no longer awareness but OPERATIONALISATION

PRIVATE OPERATORS

assets • sensors • operational data

GOVERNMENTS / REGULATORS

rules • coordination • emergency
powers

SECURITY / MILITARY

threat intelligence • surveillance •
response

REGIONAL PARTNERS

interconnected assets •
neighbouring waters

NO SINGLE ACTOR OWNS THE WHOLE PROBLEM

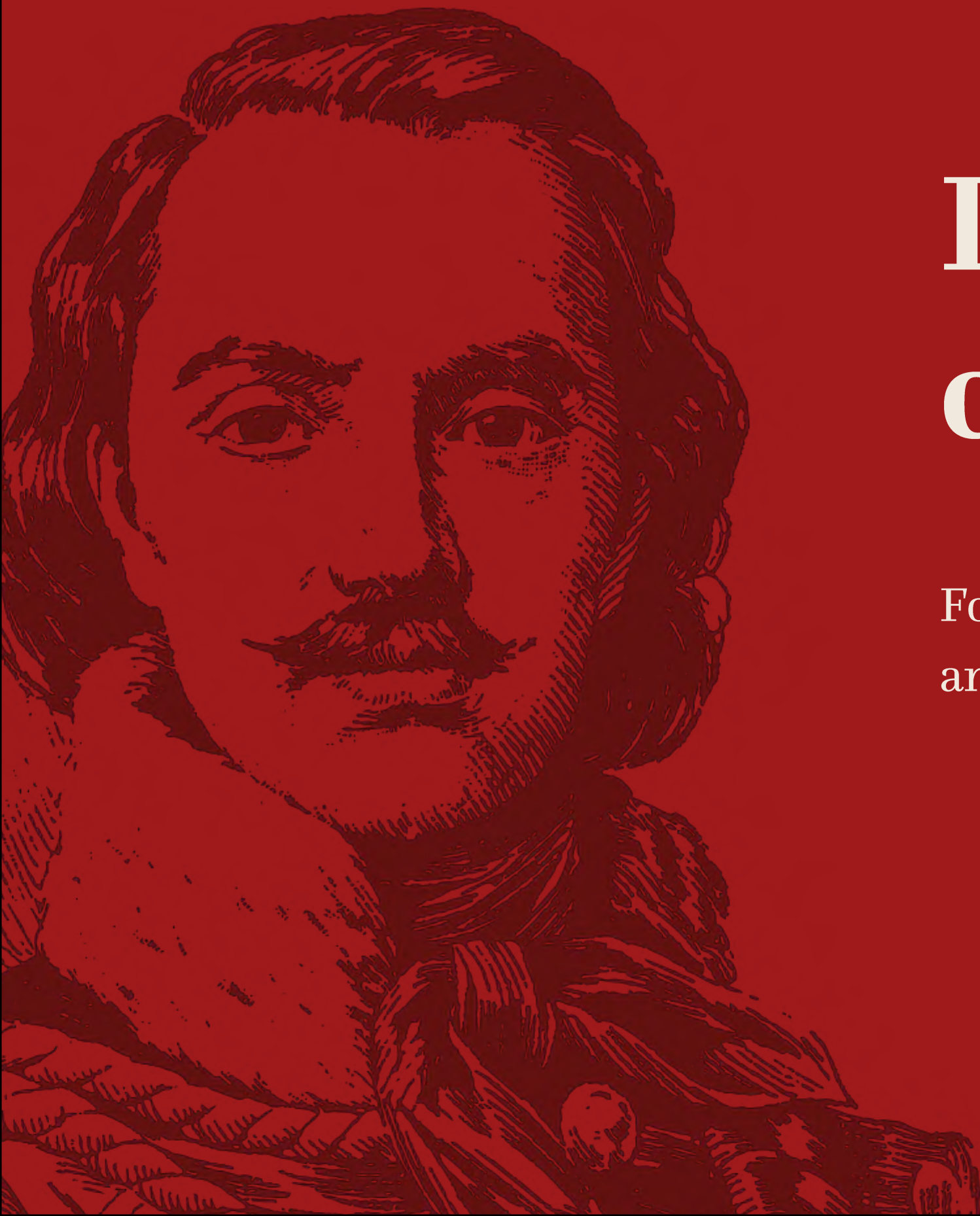
Our infrastructure is regional. Our threats are regional.
Yet ownership, information, authority and response remain fragmented

BALTIC RESILIENCE INITIATIVE

Turning fragmented capabilities into an operational resilience system: common risk planning • trusted information sharing • identification of interoperable procedures • pooling recommendations

BRI BALTIC
RESILIENCE
INITIATIVE





Let's stay connected

Follow us for news, insights,
and upcoming opportunities



Casimir Pulaski Foundation



@pulaskifoundation



@FundPulaskiego



@FundPulaskiego