

CONNEXUS

black sea tech forum

5 - 7 Октомври 2026
Варна



Под патронажа на президента на
Република България г-жа Илияна Йотова



ЧЕРНОМОРСКИ ТЕХНОЛОГИЧЕН ФОРУМ
Технологии от 7-мо поколение без граници

ARCFUND

Navigating the Perfect Storm

Cybersecurity Architecture as the Architecture
of Organisational Resilience



Dragomir Vatkov

Cyber Security Allrounder by Design



Navigating the Perfect Storm

Different seas. Same principles.
A stronger tomorrow.



Geopolitical
instability



Uncontrolled
AI adoption



New regulations
and compliance



Classical
threats



Insider / supply
chain risks



THE SHIP

A vessel built to withstand the storm.



Captain

Sets the course, makes decisive calls.



Crew

Executes, stays alert, adapts.



Navigation system

Provides direction and situational awareness.



Ship's hull

Built for strength, redundancy and resilience.



Cargo

Valuable assets that must be protected.



Destination

A safe and successful arrival.



THE ORGANISATION

A business built to thrive through uncertainty.



CEO / Leadership

Sets the strategy, makes decisive calls.



People / Teams

Execute, stay alert, adapt.



Cybersecurity architecture

Provides direction and situational awareness.



Organisational resilience

Built for strength, redundancy and adaptability.



Data, services, reputation

Valuable assets that must be protected.



Mission / Purpose

A resilient and successful future.

SAME
PRINCIPLES

The Perfect Storm: Five Forces Converging

Different forces. Same destination. One storm.



1. GEOPOLITICS The Weather

- Shifting global power dynamics
- Nation-state cyber operations
- Digital sovereignty & data jurisdiction
- Cyber + kinetic conflicts

“Weather does not ask whether you are ready. It arrives.”



2. ARTIFICIAL INTELLIGENCE The Waves

- AI for attackers and defenders
- Lower barrier for sophisticated attacks
- Faster iteration, no compliance
- Uncontrolled use in the organisation

“Waves do not stop because the ship is unprepared. They simply hit harder.”



3. REGULATION The Currents

- NIS2 – broader scope, personal liability
- DORA – financial sector resilience
- CRA – product lifecycle security
- EU AI Act – risk-based governance
- ISO 27001 – the baseline

“Regulation changes the route your ship must take. It does not make the sea any calmer. Compliance is not security. But non-compliance is an open hull.”



4. CLASSICAL THREATS The Pirates

- Ransomware-as-a-service
- Advanced phishing & social engineering
- Supply chain attacks
- Insider threats (malicious / negligent / manipulated)

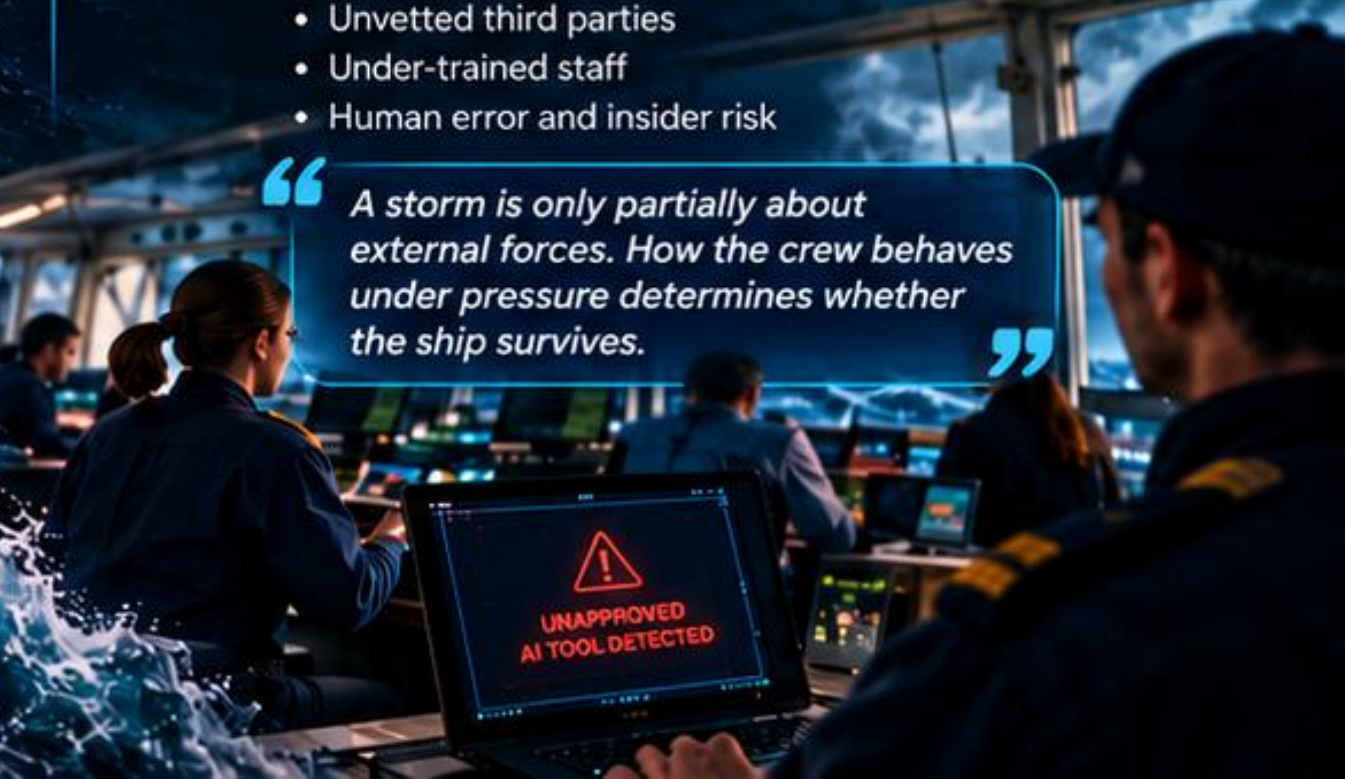
“Pirates do not retire because a ship gets larger. They adapt their tactics.”



5. SUPPLY CHAIN & HUMAN FACTORS The Crew Problem

- Shadow IT and unapproved tools
- Unvetted third parties
- Under-trained staff
- Human error and insider risk

“A storm is only partially about external forces. How the crew behaves under pressure determines whether the ship survives.”



Why Traditional Security is No Longer Sufficient

Point solutions patch the ship. Architecture keeps it seaworthy.

THE TOOL-BASED APPROACH

More tools. Same fragile ship.

Compliance tool

AI security product

Email security

Endpoint detection

Cloud security

Network security

Identity management

SIEM/SOAR

- ❌ Multiple point solutions
- ❌ Siloed technologies
- ❌ Complex and hard to manage
- ❌ Gaps between tools
- ❌ High operational overhead
- ❌ Still vulnerable to systemic failure

THE ARCHITECTURE APPROACH

A seaworthy ship designed for the storm.



TRAINED, PRACTISED CREW

People who know what to do



REDUNDANCY

Multiple systems for critical functions



CLEAR COMMAND STRUCTURE

Unambiguous decision authority



ROBUST HULL ARCHITECTURE

Distributes load and contains failures

“ A ship does not survive a perfect storm because it has a better anchor. ”
Anchors keep you stationary. Storms require movement, adaptation, and structural integrity.

Architecture as the Navigation System

Strategy sets the destination. Architecture gets you there — no matter what.

SAME DESTINATION.
GREATER RESILIENCE.

PEOPLE
PROCESSES
TECHNOLOGY
GOVERNANCE



1. BUSINESS FIRST

A business discipline, not an IT function.

- Business outcomes
- Critical assets
- Key relationships
- Follow strategy

"Know what must keep moving."



2. GOVERNANCE

The command structure.

- Clear ownership
- Decision rights
- Board alignment
- Regulatory focus

"In a storm, hesitation costs lives."



3. IDENTITY

Knowing who is on the ship.

- Verify people
- Verify devices
- Continuous verification
- Least privilege

"Trust nothing. Verify everything."



4. RESILIENCE

Prepare. Absorb. Recover. Continue.

- Rapid response
- Business continuity
- Test regularly
- Fund resilience

"It's not if. It's how quickly."



5. ZERO TRUST

An architectural principle.

- Assume breach
- Limit blast radius
- Verify continuously
- No single trust

"Check the hatches — now."



6. CONTINUOUS ADAPTATION

A living navigation system.

- Monitor threats
- Adapt controls
- Red team
- Learn and improve

"Drills today. Survival tomorrow."



7. RISK-DRIVEN DESIGN

Protect what matters most.

- Risk-based design
- Prioritise investment
- Compliance by design
- Deeper protection

"Reinforce the hull, not the deck chairs."



NAVIGATE. ADAPT. SURVIVE. **THRIVE.**

DIFFERENT
STORMS.
SAME
DESTINATION.

RESILIENCE
IS A JOURNEY
NOT A PROJECT.

You Cannot Calm the Sea. But You Can Build a Ship That Is Worthy of It.



You cannot stop geopolitical conflict.
The world will remain unpredictable.



No regulation will end the uncertainty.
The rules will keep changing.



No tool will eliminate human error.
People will always be people.



No AI system will make the unknown disappear.
New risks will always emerge.



You cannot calm the sea.
The storm is here to stay.



Cybersecurity is no longer a technology problem. It is the architecture of how your organisation survives, adapts, and continues to deliver its mission — regardless of what the sea throws at it.



The storm is already here.
What kind of ship are you building?

