The New Battlefield: Cybersecurity in an Era of Hybrid Warfare

Integrated Operational Domains in Contemporary Conflict

SPEAKER

Zari Uslu-Abdullayeva

DESIGNATION

Offensive Security Lead

Cyber as a Battlefield Domain

CONTINUOUS OPERATIONS
Cyber activities are run non-stop to disrupt systems and influence public perception outside traditional conflict windows.

DUAL-USE TARGETS
Tactics exploit interconnected civilian-military networks to maximize impact while clouding rapid attribution.

STRATEGIC DISRUPTION
Operations directly target institutional trust and data integrity to achieve long-term geopolitical objectives.

Cyber operations support broader strategic objectives beyond traditional front lines.

The Threat Mechanics: Jamming vs. Spoofing

JAMMING (SIGNAL DENIAL)

Broadcasting brute-force radio noise to completely block signal frequencies.

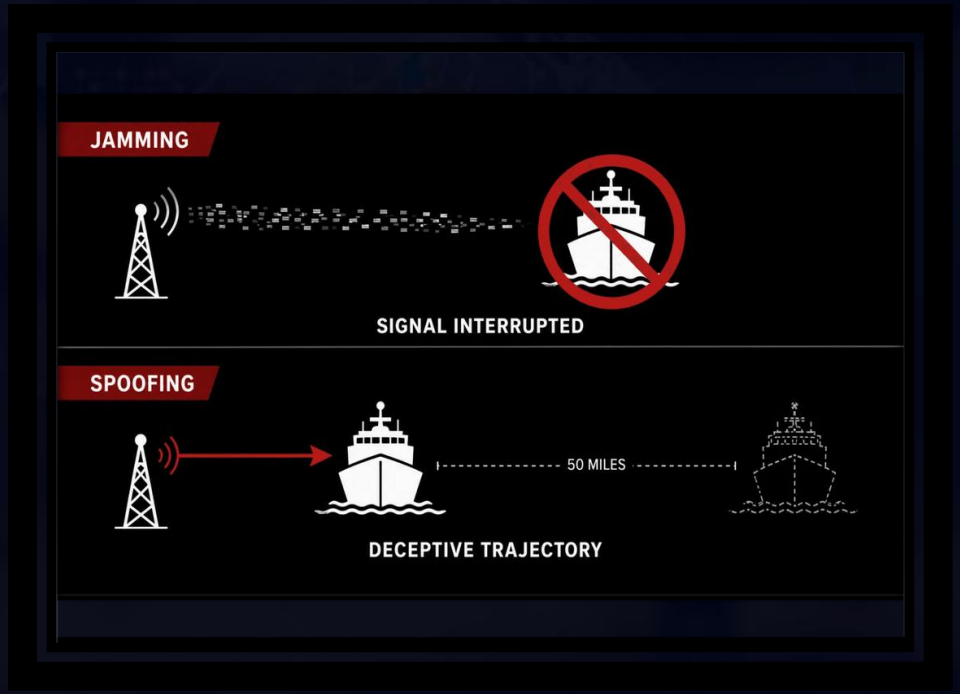
[RESULT: IMMEDIATE BLINDNESS]

SPOOFING (SIGNAL DECEPTION)

Injecting counterfeit location data to manipulate coordinates.
[RESULT: SILENT COMPROMISE]

THE CYBER-PHYSICAL RIFT

Adversaries exploit unauthenticated frequencies to manipulate physical operations without ever breaching an IT network firewall.



Geopolitical Spillover: The Electronic Warfare Reality

Case Study: Real-World Maritime Disruption

THE DRONE SHIELD
[On State-Level Defense]
Militaries are using heavy electronic interference to block drone paths.

1100+ SHIPS
[On Commercial Collateral Damage]
Over 1,100 commercial vessels experienced scrambled **navigation signals** within a single 24-hour window.

CHOKEPOINT DISRUPTION
[On Macro-Economic Impact]
Critical maritime traffic was completely paralyzed across the Strait of Hormuz, threatening 20% of global energy exports.

INFRASTRUCTURE COLLATERAL
[On Terrestrial Systems]
Civilian transport networks, regional emergency response tracking, and local automated logistics face immediate secondary blind spots from localized jamming.

Figure 1: Circular vessel tracks indicating sophisticated GPS spoofing in maritime corridors.

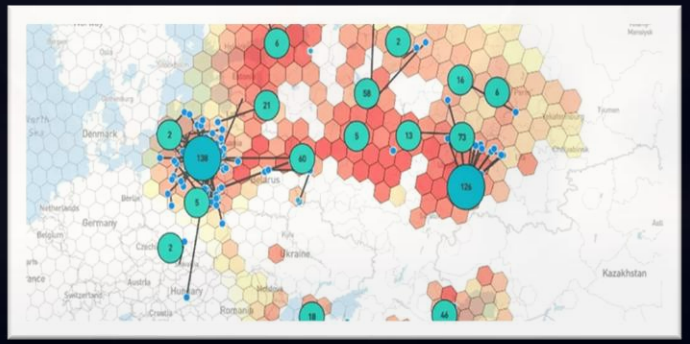


Figure 2: Regional heatmap of localized terrestrial signal interference.

The Path Forward: Building Resilience

DIVERSIFICATION

System Redundancy

Reduce dependence on single systems to eliminate critical points of failure across national infrastructure.

DETECTION

Real-time Monitoring

Implement advanced signal interference monitoring to improve detection and enable real-time response to technical disruptions.

RESILIENCE

Infrastructure Hardening

Strengthen the protection of critical military and national infrastructure infrastructure against hybrid threats.

COLLABORATION

Public-Private Synergy

Enhance coordination between government and private sectors sectors for a unified national defense posture.

> ***"Resilience is now as important as protection. We must prepare to operate even under disruption."***

SUMMARY & CLOSING

Modern conflict is *no longer limited by geography*.

Cyber operations now directly influence *infrastructure, transportation, economies, and national stability.*