Shielding the Sky: NATO SATCOM Survival Against Russia & China's EW Onslaught

Prepared for the thinktank ICRD. Author: R. K. D. Kho Date: 17 October 2025

1. Executive Summary

NATO's satellite-communications (SATCOM) and broader C4ISR architecture are being pressured from two divergent but equally destabilising directions:

- Russia – employs a "denial-by-overwhelm" doctrine that relies on high-power, broadband jamming, rapid adaptive-jamming cycles, and GNSS spoofing. Its tactics have matured on the Ukrainian battlefield, where a three-month "radio life-cycle" has become the norm for counter-acting NATO-supplied precision weapons.
- China – pursues a systemic "information-dominance" strategy under the Strategic Support Force (SSF). It integrates photonic-core spoofing, high-power-microwave (HPM) weapons, and on-orbit counter-space operations to manipulate, degrade, or permanently disable NATO's high-end radar, SATCOM, and command-and-control (C2) nodes.

Both adversaries exploit NATO's historic reliance on centralised, high-value SATCOM nodes and high-end radar platforms. NATO's response is shifting from pure electronic protection (EP) to a multi-domain command-and-control (MD-C2) paradigm that couples AI-enhanced counter-spoofing, distributed SATCOM constellations, hardened electromagnetic-pulse (EMP) shielding, and integrated electromagnetic-picture software. Recent contracts for radar-target generators, EW simulators, and a NATO-wide EW-planning suite illustrate the acceleration of this pivot.

2. Introduction

The electromagnetic spectrum (EMS) is now recognised as a fifth warfighting domain that underpins Multi-Domain Operations (MDO). NATO's ability to command, control, communicate, compute, and conduct intelligence, surveillance, and reconnaissance (C4ISR) hinges on satellite communications (SATCOM), high-frequency (HF) and X-band links, and advanced radar.

Two distinct threat models have emerged:

Threat Model	Primary Actor	Core Characteristics
Acute, localized denial	Russian Federation	High-power jamming, rapid adaptive-jamming cycles, GNSS spoofing, focused on tactical links and precision-guided munitions (PGMs).
Systemic, long-term manipulation	People's Republic of China	Photonic/6 GHz spoofing, HPM non-kinetic weapons, integrated cyber-space-EW operations, on-orbit counter-space (RPO) activities.

Understanding the evolution of these capabilities, their operational impact, and NATO's emerging counter-measures is essential for preserving alliance-wide electromagnetic superiority.

3. Technical Comparison: NATO vs. Russian and Chinese EW

Feature	NATO (primarily US & major allies)	Russia (Russian Armed Forces)	China (People's Liberation Army – PLA)
Doctrinal priority	Electronic Protection (EP), SEAD, cyber/info integration; increasingly decentralised under JADC2.	Integrated EW as an intrinsic part of all operations (information dominance).	"Informationized warfare" – SSF-coordinated space-cyber-EW synergy.
Key capability focus	Airborne EW platforms (EA-18G Growler), resilient SATCOM (M-Code GPS, protected satcom), digital RF memories (DRFMs).	Ground-mobile high-power jammers (Krasukha-4, R-330Zh Zhitel), long-range HF (Murmansk-BN), adaptive GPS/PGM jamming cycles.	Photonic/6 GHz EW system (≥ 3 600 false radar targets), HPM weapons, co-orbital EW satellites, Y-9LG ELINT/jammer, Sharp-Sword UCAV.
SATCOM/C4ISR targeting	Primarily defensive (EP). Offensive EW is highly classified.	Proven ability to degrade encrypted GPS (M-Code) and tactical data links; widespread GNSS interference.	Targeting X-band radars, high-band SATCOM, L-band navigation, space-based ISR; HPM attacks on commercial LEO constellations.
System integration	Historically siloed; moving toward joint all-domain C2 (JADC2).	EW tightly integrated across strategic, operational, tactical levels;	Unified under SSF; space-EW-cyber triad delivers coordinated effects.

Feature	NATO (primarily US & major allies)	Russia (Russian Armed Forces)	China (People's Liberation Army – PLA)
		automated linkage to fires.	

Sources: Russian adaptive-jamming cycles ; Chinese photonic/6 GHz EW ; NATO EW policy ; Collins Aerospace EWPBM contract ; Keysight radar-target generator contract .

4. NATO's Current Vulnerabilities

- Centralised SATCOM Nodes – Dependence on a limited set of Ku/Ka-band satellites makes the network vulnerable to concentrated jamming or HPM strikes.
- High-End Radar Dependence – Platforms such as AN/TPY-2 and F-35 AESA radars lack built-in full-duplex spoof-resilience, exposing them to photonic false-target generation.
- Legacy EP Suites – Existing electronic-protection tools (e.g., DRFM-based jammers) are tuned for Russian-style broadband noise, not for adaptive, AI-driven deception.
- Supply-Chain Exposure – 5G/6G equipment from high-risk vendors can be leveraged for cyber-EW convergence, a concern highlighted in NATO's supply-chain security policies .

5. NATO's Emerging Resilience Architecture

Initiative	Objective	Implementation Highlights
AI-Enhanced Counter-Spoofing	Detect and nullify photonic/6 GHz spoofing in real time.	Machine-learning classifiers ingest raw RF signatures; auto-generate inverse waveforms for on-the-fly cancellation.
Distributed SATCOM Constellations	Reduce single-point failure risk.	Rapid-deploy LEO "responsive-space" clusters with anti-jamming antennas; cross-linked via optical inter-satellite links.
HPM/EMP Hardening	Shield critical electronics from non-kinetic system-kill.	EMP-rated enclosures, surge-suppression filters, hardened ASICs on ground stations and airborne platforms.
Electromagnetic Picture (EWPBM) Software	Provide a recognised electromagnetic operating picture (REMP).	Collins Aerospace's EWPBM aggregates sensor, intelligence, and jammer data into a unified dashboard .
EW Simulation & Training	Validate tactics against realistic threat sets.	Keysight radar-target generators and EW simulators enable high-fidelity lab and field exercises .
Maritime EW Working	Align naval EW capability	New capability-target documents

Initiative	Objective	Implementation Highlights
Group	targets with alliance goals.	(summer 2025 rollout) focus on distributed, non-US-centric solutions .

6. Expanded Timeline of Russian and Chinese Threats to NATO (2022 – 2025)

Year	Actor & Threat	Detailed Development & Impact
2022 (Q1-Q4)	Russia – Adaptive Jamming Cycle	After the invasion of Ukraine, Russian EW units repeatedly retuned frequency, power, and waveform to defeat NATO-supplied GPS-guided munitions (e.g., Excalibur 155 mm shells). Within six weeks the hit-rate fell from ~70 % to < 6 %, illustrating a rapid "radio life-cycle" of roughly three months before a software/hardware refresh was required .
2022 (Q3-Q4)	Russia – GNSS & Satellite Jamming	Deployments of high-power R-330Zh Zhitel and Murmansk-BN systems created continent-wide GPS denial zones over Eastern Europe, degrading both military navigation and civilian aviation .
2023 (Jan-Dec)	NATO – Strategic-Concept Update	NATO's 2023 Strategic Concept formally declared cyberspace "contested at all times" and mandated an integrated response to Russian and Chinese hybrid/EW threats, laying doctrinal groundwork for later capability programmes .
2023 (Q2-Q4)	Russia & China – Hybrid-War Escalation	Recorded-Future's 2025 NATO-Summit threat assessment documents a sharp rise in Russian sabotage, cyber intrusions, and disinformation, alongside parallel Chinese cyber-espionage and influence operations that began intensifying in 2023 .
2024 (Q1)	China – First Operational 6 GHz Photonic EW System	Open-source reporting (Global Tenders) describes a Chinese photonic-core EW platform operating above 6 GHz that can generate > 3 600 false radar targets in real time, specifically engineered to overload NATO X-band radars such as those on the F-35 .
2024 (Q2)	Russia – Large-Scale GPS/GLONASS Spoofing	Ukrainian field reports confirm coordinated spoofing bursts that mislead UAV navigation, causing loss of control of dozens of drones in a single day .
2024 (Q3)	NATO – Electronic-Warfare	Collins Aerospace (RTX) wins a NATO Communications & Information Agency (NCIA)

Year	Actor & Threat	Detailed Development & Impact
	Planning & Battle-Management (EWPBM) Contract	contract to deliver a software suite that fuses sensor, intelligence, and jammer data into a "Recognised Electromagnetic Picture," enabling alliance-wide situational awareness of EW activity .
2024 (Q4)	NATO – Radar-Target Generator & EW Simulator Procurement	Keysight Technologies is awarded a NATO contract to supply high-fidelity radar-target generators and EW simulators for laboratory and field training, allowing realistic testing against Russian jamming cycles and Chinese photonic spoofing .
2024 Nov	China – Counter-Space & High-Power Microwave (HPM) Tests	DefenseScoop reports Chinese experimental satellites conducting rendez-vous-and-proximity operations (RPO) and field-testing HPM weapons capable of delivering non-kinetic "system-kill" pulses to NATO SATCOM and ISR payloads .
2025 (Jan-Feb)	Russia – Surge in Hybrid Sabotage	Recorded-Future notes a tripling of Russian-directed sabotage attacks in Europe (12 → 34 incidents) between 2023-2024, targeting power grids, railways, and communication hubs—a clear escalation of the "shadow war" against NATO infrastructure .
2025 (May)	NATO – Maritime EW Working Group Capability Targets	NATO's maritime EW working group publishes new capability-target documents (summer 2025 rollout) focusing on distributed, non-US-centric EW solutions to counter Russian sea-domain jamming and Chinese "Kill-Web" concepts .
2025 (Jun-Jul)	China – Space-Based EW "Dog-Fighting"	DefenseScoop confirms Chinese satellites practising on-orbit "dog-fighting" manoeuvres designed to approach, inspect, and potentially disrupt NATO communication satellites, raising the risk of sustained space-EW confrontation .
2025 (Oct)	NATO – Pre-Summit Threat Briefing	Recorded-Future's pre-summit analysis warns that both Russia and China will likely employ coordinated cyber-EW campaigns, HPM attacks, and large-scale misinformation operations during the NATO summit, prompting accelerated activation of the newly-procured EW tools .
2025 (Throughout)	NATO – Ongoing Dependency on Allied SATCOM	Chatham House analysis (2019) reiterates that NATO does not own its own SATCOM satellites; it relies on allied and commercial assets (e.g., UK, France, Italy, commercial LEO constellations). This structural dependency is a focal point for both Russian jamming

Year	Actor & Threat	Detailed Development & Impact
		and Chinese space-EW strategies .
2025 (Throughout)	MilSatCom Evolution	Armadainternational (2024) highlights how military SATCOM (MilSatCom) has become a decisive factor in modern warfare, stressing the need for NATO to secure its satellite links against both Russian jamming and Chinese photonic/EW attacks .

Observations

- Speed of adaptation – Russian EW moved from tactical jamming in 2022 to a systematic hybrid-war campaign that blends sabotage, cyber intrusion, and disinformation by 2025.
- Chinese technological leap – Photonic-core EW, HPM weapons, and on-orbit counter-space tactics constitute a long-term, systemic threat that targets NATO's SATCOM, radar, and C2 nodes.
- Alliance response – Since 2023 NATO has institutionalised EW as a continuously contested domain, procured advanced simulation and planning tools (Keysight, Collins Aerospace), and begun restructuring its maritime and space-EW capabilities to counter both Russian and Chinese threats.

7. Policy Recommendations

- Adopt a Distributed SATCOM Blueprint – Formalise a NATO-wide "Responsive-Space Architecture" that mandates a minimum of three independent LEO layers for all mission-critical links, with anti-jamming antennas and optical inter-satellite links.
- Accelerate AI-Driven EW Counter-Measures – Allocate dedicated funding within the Defence Innovation Accelerator for NATO (DIANA) to transition prototype AI-counter-spoofing modules into operational payloads across air, land, and maritime platforms.
- Standardise EMP/HPM Hardening – Issue a NATO-wide technical standard (akin to MIL-STD-188-125) for EMP/HPM resilience, covering both legacy and next-gen platforms (ground stations, airborne receivers, ship-board radars).
- Integrate EW Simulation into Joint Exercises – Institutionalise the use of Keysight's radar-target generators and EW simulators in NATO's annual "Cold Response" and "Trident Juncture" drills to stress-test multi-domain interoperability against realistic Russian and Chinese EW scenarios.

- Strengthen Supply-Chain Vetting for 5G/6G Components – Enforce the German Marshall Fund-styled "5G Toolbox" across all member procurements to eliminate high-risk vendors (e.g., Huawei, ZTE) from core NATO communications and SATCOM subsystems .
- Expand Maritime EW Working Group Mandate – Broaden the group's charter to incorporate HPM-resistant shipboard architectures, distributed maritime C2 nodes, and cooperative engagement with Indo-Pacific partners (Japan, Australia, South Korea).
- Enhance Intelligence Sharing on Photonic & HPM Developments – Create a NATO-level "Emerging EW Threats" cell tasked with continuous monitoring of Chinese photonic-core prototypes, HPM weapon tests, and space-EW activities, feeding directly into capability-development roadmaps.

8. Conclusion

The dual-track threat—Russia's high-power, adaptive jamming and China's photonic-core, HPM-enabled information-dominance strategy—forces NATO to abandon a purely defensive electronic-protection posture. The Alliance must pivot to an active, full-spectrum manipulation and resilience architecture that blends AI-driven counter-spoofing, distributed SATCOM, hardened hardware, and integrated electromagnetic-picture tools.

By institutionalising these capabilities, investing in rapid-deployment responsive-space constellations, and tightening supply-chain security, NATO can preserve electromagnetic superiority, protect its C4ISR backbone, and retain the strategic freedom necessary for Multi-Domain Operations in the face of an increasingly contested spectrum.

9. References

NY Times (2024). Some U.S. Weapons Stymied by Russian Jamming in Ukraine. https://www.nytimes.com/2024/05/25/world/europe/us-weapons-russia-jamming-ukraine.html

Business Insider (2024). Russia's jamming of American weapons in Ukraine shows the U.S. what it needs to be ready for in a future fight. https://www.businessinsider.com/russian-electronic-warfare-shows-us-needs-for-future-wars-2024-5

Recorded Future (2025). Threats to the 2025 NATO Summit: Cyber, Influence, and Hybrid Risks. https://www.recordedfuture.com/research/threats-2025-nato-summit

Collins Aerospace (2025). Electronic Warfare Planning and Battle Management (EWPBM) Solution – NATO contract. https://www.rtx.com/news/news-center/2025/09/16/rtxs-collins-aerospace-awarded-nato-contract-for-electromagnetic-warfare-command

Keysight Technologies (2025). Radar Target Generators & EW Simulators Delivered to NATO. https://thedefensepost.com/2025/04/29/keysight-radar-electronic-warfare-nato/

DefenseScoop (2025). China practicing on-orbit “dogfighting” tactics with space-EW assets. https://www.defensescoop.com/2025/03/18/china-practicing-on-orbit-dogfighting-tactics

Global Tenders (2025). China develops first 6 G electronic warfare system to disrupt radar of US F-35. https://www.globaltenders.com/2025/06

For further information or an interview, you can get in touch via **remy.kho@crd-hk.com** or **remykho@pm.me**.

Remy Kho works as a journalist and researcher at the leading international thinktank ICRD that focuses on societal, economic, and security issues. With a background in technology, he combines analytical sharpness with practice-oriented analyses of the dynamics surrounding public policy, technological innovation, and security.