HWG Sababa

DEFENCE, SPACE & CTI

We secure strategic assets across defence, space, and critical infrastructure through intelligence-driven cyber operations.

"Defence assets are only as strong as their weakest supplier."

Cyber Sovereignty & Strategic Resilience

Geopolitical instability, economic fragmentation, and rising regulatory pressure are redefining cybersecurity as a matter of sovereignty. Across Europe, over 80% of digital infrastructure still relies on non-European providers, exposing critical systems to dependencies that are increasingly misaligned with national security and compliance requirements.

At the same time, the threat landscape is evolving. State-sponsored actors, proxy groups, and coordinated influence operations are targeting not only IT systems but entire strategic ecosystems – from defence supply chains to space assets and critical infrastructure.

This shift is accelerating investment and reshaping priorities. According to Gartner®[1]: «The $45 billion sovereign cloud IaaS market is forecast to grow at a five-year CAGR of 38% to reach $224 billion in 2029», while countries increasingly adopt region-specific platforms to retain control over data, operations, and intelligence.

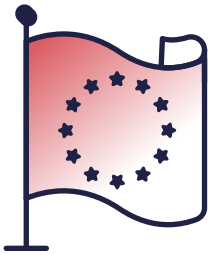
In this context, cybersecurity is no longer just protection. It is about ensuring operational continuity, strategic autonomy, and control over mission-critical assets.

HWG Sababa supports defence and institutional organizations in navigating this transformation – combining intelligence, operational capabilities, and advanced security operations to secure what matters most.

HWG Sababa is an Italian cybersecurity group delivering managed services, advanced solutions, and strategic advisory to protect critical infrastructures and high-value organizations. Founded in 2008, the Group today employs over 300 professionals and operates internationally across Europe, the Middle East, and Central Asia, supporting more than 500 organizations in defence, energy, finance, telecommunications, transportation, and other regulated sectors.

Its **Defence, Space & CTI Business Unit** focuses on securing high-value and mission-critical environments. Operating at the intersection of cyber defence and cybersecurity, it combines advanced technical protection with predictive intelligence to anticipate and mitigate threats from state-sponsored actors (APTs), proxy groups, and ideologically driven campaigns.
Each engagement is tailored to the partner's specific needs across all phases – from planning and execution to lessons learned – leveraging highly specialized, multidisciplinary teams.

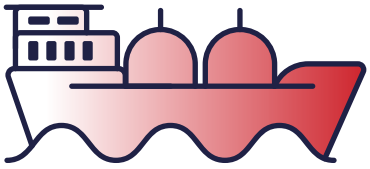
What we secure



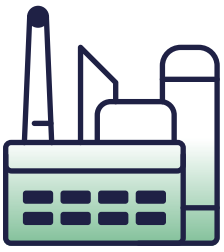
DEFENCE SYSTEMS AND NATIONAL INFRASTRUCTURES



SPACE AND SATELLITE ECOSYSTEMS



CRITICAL SUPPLY CHAINS



INDUSTRIAL AND OPERATIONAL ENVIRONMENTS

[1]Gartner®, Forecast Analysis: Sovereign Cloud IaaS, Worldwide, by Rene Buest, Fernando Pereiro, Gregor Petri, Hardeep Singh 11 December 2025. GARTNER is a trademark of Gartner, Inc. and/or its affiliates.

Defence

Protecting national and military assets against advanced and state-level threats.

Strategic Intelligence
Forward-looking analysis of the geopolitical landscape to anticipate emerging threats and risks.

Operational / Tactical Intelligence
Monitoring of the web, social media, dark web, and closed forums to identify imminent threats targeting specific assets or the broader national ecosystem.

Technical Intelligence (IoCs)
Identification and analysis of Indicators of Compromise related to malware used in cyber espionage and sabotage activities.

National Security Compliance
Advisory services to support compliance with NIS2 requirements and national critical infrastructure protection frameworks.

Training
Cyber warfare scenario simulations designed to train personnel in protecting critical infrastructures and adopting proactive defence strategies.

Government Network Hardening
Strengthening classified networks to prevent data exfiltration and unauthorized access to sensitive information.

Dual-Use Service Security
Protection of satellite systems used for both civilian (e.g. weather, environmental monitoring) and military (e.g. surveillance) purposes, ensuring data integrity and operational resilience.

Geopolitical & Disinformation Threat Monitoring

Monitoring and countering hybrid and influence-based threats.

Geopolitical Threat Landscape
Periodic reports analyzing how international tensions (e.g. conflicts in strategic regions) may translate into cyber threats targeting national infrastructures.

Early Detection of Disinformation Campaigns
Monitoring of bot networks and social media channels to identify influence operations aimed at destabilizing public opinion or undermining defence institutions.

Hacktivist Group Analysis
Continuous monitoring of hacktivist collectives targeting government portals for ideological reasons (e.g. DDoS attacks during international summits).

Space & Aerospace

Securing orbital and ground-based assets across the full mission lifecycle.

Supply Chain Security
Cyber risk assessment for hardware and software suppliers across the aerospace and space ecosystem.

Satellite Asset Protection
Threat monitoring across ground segments and strengthening the cybersecurity posture of both terrestrial and space-based assets.

Tailored Red Teaming
Adversary emulation (APT-style) targeting specific aerospace assets, space systems, and/or orbital control infrastructures.

Satellite Ground Segment Security
Protection of ground stations managing satellite command and control (C2), including data-in-transit encryption and defense against signal hijacking attempts.

Mission Assurance Support
Cybersecurity advisory across the full lifecycle of space missions – from design to de-orbiting – ensuring continuous control and integrity of the asset.

GNSS Protection
Services to detect and mitigate jamming and spoofing attacks targeting GPS/Galileo signals, which are critical for transportation and defence operations.

Supply Chain Security & Third-Party Risk Management

Reducing systemic risk across defence ecosystems.

Software Bill of Materials (SBOM) Analysis
Security validation of all software components – including open-source – embedded in products delivered to the defence sector.

Supplier Auditing & Scoring
Assessment of the cybersecurity posture of subcontractors through external scanning and technical audits, ensuring the protection of data and flows across the supply chain.

Hardware Integrity Verification
Testing of hardware components (e.g. microchips, sensors) to detect potential backdoors or malicious code introduced during manufacturing in third-party countries.

Industries

Strengthening resilience across industrial and mission-critical environments.

Awareness
Targeted training on secure social media usage for personnel.

OSINT
Open-source intelligence monitoring services to protect the reputation of senior executives and institutions.

OT Systems Security
Protection of automated production lines used to manufacture satellites or defence systems. Disruptions in these environments can result in significant operational and financial impact.

Crisis Management Exercises
Tabletop simulations for senior leadership (e.g. ministries, executive teams) to prepare response strategies to scenarios such as ransomware attacks affecting critical services.

Tailored Technical Training Platforms
Hands-on training environments for Blue Teams, enabling them to practice defending networks under attack in a controlled and secure setting.

Technical Vetting of Personnel
Support in assessing the cybersecurity skills of new hires and third-party providers.

Internal Assets Security Checks
OSINT, SOCMINT, and ASINT analysis on partner personnel to identify potential risk profiles.

Secure SAT–OT Integration
Securing gateways that connect satellite communications with industrial control systems (SCADA), preventing attackers from pivoting from satellite signals into physical operations.

Anti-Jamming & Spoofing Detection
Signal monitoring to detect jamming or spoofing attempts targeting remote sensors. For example, if a wind farm stops transmitting data via satellite, the OT SOC can determine whether it is a technical failure or a coordinated attack.

Encrypted Telemetry as a Service
Delivery of end-to-end encryption protocols optimized for satellite bandwidth constraints, ensuring that telemetry data from critical sites cannot be intercepted.

Resilient Emergency Communications (in partnership)
Design of hardened backup satellite communication systems to be activated in case of large-scale cyberattacks impacting terrestrial networks.

HWG Sababa

Why HWG Sababa

HWG Sababa delivers cybersecurity as an integrated operational capability – combining intelligence, protection, and response to secure strategic assets across defence, space, and critical infrastructures.

Anticipate.
We provide forward-looking intelligence to identify emerging threats, monitor hybrid and influence operations, and understand adversarial ecosystems.

Protect & Validate.
We secure complex environments – from supply chains to satellite and OT systems – and validate real exposure through adversary emulation and attack-driven testing.

Respond & Strengthen.
We prepare organizations to withstand real-world scenarios through crisis simulations, technical training, network hardening, and mission assurance across the full lifecycle.

Contact us

www.hwgsababa.com
contacts@hwgsababa.com