

Morocco and Cyberspace

Anticipating a cybersecure world

Version control

Version	By	Description	Date	Event
1.0	#016	Initial version	September 2026	

Table of Contents

Part I. The basis	8
Introduction.....	8
Principal findings	8
Executive Summary	9
Working methodology	10
Part II. Strategic and political foundations	13
Introduction.....	13
Politics and geopolitics	14
The Makhzen.....	17
Strategic priorities	18
Part III. The security and intelligence architecture	22
The intelligence community.....	22
DGED 23	
DGST 26	
Relevant DGSN intelligence functions	29
Law enforcement and internal security	31
DGSN 32	
BCIJ 33	
Royal Gendarmerie	35
Auxiliary forces.....	37
Armed Forces and military intelligence.....	39
FAR command architecture	40
2nd and 5th Bureaux	42
Royal Guard	43
Military regions and Western Sahara posture	44
Other relevant actors	45
Private companies	46
Universities.....	48
Crime 49	
Coordination and oversight.....	51
Part IV. The Moroccan cyber ecosystem.....	55
The Moroccan Cyberspace.....	55
Law and regulation.....	55
Defensive cybersecurity and incident response	58
Intelligence collection and surveillance	60
Military cyber, electronic warfare and C4ISR	62
Cybercrime and digital forensics	63
LEA in cyberspace	63
Cybercrime	64
Hacktivism and information confrontation	65
Other actors	68
Private vendors.....	68
Foreign vendors.....	69

The academia.....	71
APT groups	71
Key dependencies	72
Part V. Assessment	77
Capability model	77
Constraints and vulnerabilities.....	78
Conclusions.....	80
References.....	81
Acronyms	94

List of Tables

Table 1. The Strait of Gibraltar: three converging strategic pressures on Morocco's Spain policy.	16
Table 2. Morocco's six strategic-priority theatres, ranked, with lead evidentiary basis and assessed confidence.	18
Table 3. Ceuta and Melilla migration-crossing episodes, 2021-2026: distinct events, overlapping figures.	20
Table 4. Morocco's civilian intelligence and police agencies at a glance.	22
Table 5. DGED, DGST and DGSN leadership succession.	22
Table 6. Competing attribution questions in Morocco's Pegasus and Jabaroot record.	27
Table 7. Morocco's four internal-security forces at a glance.	31
Table 8. Four structurally distinctive Armed Forces bodies compared.	39
Table 9. Three foreign surveillance-technology vendor relationships identified for Morocco.	48
Table 10. Documented 2025-2026 law-enforcement and security operations, by date.	50
Table 11. Morocco's principal formal security-coordination and oversight bodies.	53
Table 12. Morocco's cyberspace and data-protection legal and regulatory instruments.	57
Table 13. Notable financially-motivated cybercrime cases and cooperative operations.	65
Table 14. Competing attribution theories for the Jabaroot/JabaROOT DZ campaign.	66
Table 15. Morocco-registered CERT/CSIRT teams listed in FIRST's member directory.	69
Table 16. Foreign commercial vendors named in this collection, confirmed and checked-and-absent.	70
Table 17. Submarine cable systems serving Morocco, and the 2Africa non-landing contrast.	72
Table 18. Ownership structure of Morocco's three licensed mobile network operators.	74
Table 19. International hyperscale cloud and CDN presence relevant to Morocco.	75
Table 20. Morocco's principal cyber-domain constraints and vulnerabilities, with assessed confidence.	80

List of Figures

Figure 1. The Makhzen's constitutional and economic channels, simplified (both run from the King rather than from elected government).....	18
Figure 2. Simplified reporting lines of Morocco's civilian intelligence and police architecture (King Mohammed VI sits above both branches as Supreme Commander).	23
Figure 3. The DGSN emblem, traced from the service's own 2021 annual report.	33
Figure 4. The emblem associated with the Gendarmerie Royale in open sources (provenance caveat below).	37
Figure 5. The Auxiliary Forces emblem, sourced to an official Inspection Générale des Forces Auxiliaires recruitment announcement.	38
Figure 6. FAR command architecture, so far as open sources allow it to be stated with confidence (the Royal Guard's reporting line is contested, not resolved, in this diagram).	41
Figure 7. The FAR insignia, in continuous use across Wikipedia's FAR articles since 2008.	42
Figure 8. The Royal Guard emblem, sourced to an official Garde Royale recruitment announcement.	43
Figure 9. The Moroccan Wall/Berm: reported construction sectors and enclosed towns (figures single-sourced and flagged as uncorroborated -- see text).	44
Figure 10. Morocco's security-coordination apparatus, consolidated (personal fusion links and undocumented convening frequency are marked explicitly rather than smoothed over).	54
Figure 11. DGSSI's institutional structure: departments, and its regulatory relationship to vital-infrastructure entities and qualified Cloud providers.	59
Figure 12. The DGSSI institutional logo, retrieved directly from the agency's own official website....	59
Figure 13. Morocco's hacktivism landscape: three functionally distinct clusters rather than a single two-sided rivalry.	68
Figure 14. Morocco's submarine-cable topology: landings clustered on the northern coast against the Strait of Gibraltar chokepoint, with 2Africa shown as a non-connecting reference system.	73
Figure 15. Ownership structure of Morocco's three mobile network operators.	75
Figure 16. Morocco's three-track cyber capability model: offensive/collection, defensive, and influence/information-operations, each annotated by its dominant foreign-dependency vector and evidentiary confidence.	78

Part I. The basis

Introduction

This report analyses Morocco's security, intelligence and defence ecosystem, with a particular view on cyberspace -- that is, on the country's cybersecurity, cyber-intelligence and cyber-defence ecosystems. It examines the Kingdom's political and historical baseline, the Makhzen as the country's central governance concept, Morocco's strategic priorities across the theatres that matter most to it, the structure and conduct of its intelligence, law-enforcement and military communities, the wider ecosystem of private, academic and criminal actors around them, Morocco's activity in cyberspace specifically -- from its legal framework through to the intelligence services', military's, law-enforcement's and civilian actors' respective roles there -- and, finally, the digital dependencies and capability model that together determine how much of this activity Morocco can sustain.

This is a full, ground-up rebuild of the report rather than an update of a prior edition: every section below rests on a fresh open-source collection and analysis pass conducted for this edition alone, covering Moroccan, Spanish and Algerian sources across all domains the skeleton below requires, rather than on material carried forward from an earlier report. Spain-relevant findings are integrated directly into the section that already covers the relevant ground -- migration and border leverage under Strategic priorities, hybrid-pressure practice under the intelligence-community chapter, and espionage and surveillance activity under Intelligence collection and surveillance -- rather than isolated in a separate chapter, since Morocco's conduct toward Spain is better understood as one thread running through each domain than as a self-contained topic. A synopsis of the report's principal findings follows immediately below, for a reader who wants the core picture before the supporting analysis.

Principal findings

Morocco's security governance model is Palace-centred rather than institutionally distributed, and this single fact organises almost everything else in this report. The Makhzen -- examined below not as a metaphor but as a nameable set of institutions, from the Royal Cabinet and its advisers to the wali corps, the royal holding company Al Mada, and state enterprises such as Maroc Telecom -- coordinates security, economic and information levers around the Palace's own priorities, with parliamentary and judicial oversight that this report finds, on the best independent evidence available, to be consultative at most and in several respects entirely absent. It is almost certainly the case that this arrangement persists through the 23 September 2026 legislative elections regardless of their outcome (confidence: high), since day-to-day authority over intelligence, defence procurement, Western Sahara policy and much of cyber policy runs through Palace-adjacent institutions rather than through the elected government.

Within that model, function is distributed rather than duplicated across the bodies this report profiles in detail: the DGED handles external intelligence and Sahel security diplomacy; the DGST handles domestic counter-espionage and, on the evidence assessed under Intelligence collection and surveillance, Morocco's commercially sourced cyber-surveillance capability; the DGSN is the national civil police, fused with the DGST at the top since 2015 through the single person of Abdellatif Hammouchi, a structural fact with no direct European equivalent examined in this report; the FAR provides conventional defence and commands the Western Sahara theatre; and DGSSI, sitting within the defence establishment rather than a civilian ministry, is the national cybersecurity authority, with maCERT nested inside it as the incident-response function. It is

highly likely that this distribution, and the Palace's position above all of it, remains the organising logic of Moroccan security governance through the remainder of this decade (confidence: moderate).

On cyber capability specifically, this report's observed model is procurement-led rather than development-led: no Moroccan state-attributed offensive cyber actor was identified in any tracked threat-intelligence catalogue, but a well-evidenced sequence of commercial-vendor relationships -- Hacking Team from 2009, NSO Group's Pegasus from at least 2017 -- gave the DGST a forensically confirmed surveillance capability used against domestic journalists and activists and, on the balance of the evidence, against senior Spanish officials. Defensively, DGSSI and maCERT have built a legally structured framework -- Law 05-20, the IIV critical-infrastructure designation regime, and CNDP's data-protection enforcement under Law 09-08 -- whose practical, day-to-day effectiveness this report was substantially less able to verify independently, given a persistent lack of published performance data comparable to what better-resourced national CERTs routinely release.

The authorship of the 2026 Jabaroot/JabaROOT hack-and-leak campaign against Moroccan institutions remains genuinely contested across this report's sources, among at minimum an Algerian-hacktivist theory, an Algerian-state-directed theory, a lone-operative theory, and a theory naming a specific former DGED official as a source -- and this report treats none of them as established, carrying all forward with their respective sourcing rather than converging on one for narrative convenience.

The Western Sahara dispute and the rivalry with Algeria it sustains are this report's two organising strategic drivers, running through nearly every chapter: they explain Morocco's military posture along the Moroccan Wall, the bulk of its hacktivist and information-operations exposure, and a foreign policy that has increasingly traded recognition of Moroccan sovereignty over the territory -- from the United States, Israel, and a strengthening degree of endorsement at the UN Security Council -- for normalisation and defence-industrial deepening with Washington and Tel Aviv.

Spain occupies a genuinely multi-sided position in this picture: a security partner with real, valuable liaison relationships across counter-terrorism and counter-narcotics; a demonstrated target, most starkly through the forensically confirmed 2021 Pegasus infections of Spain's own senior officials and a live 2026 Audiencia Nacional judicial process reaching into DGST/DGED personnel; a structural dependency, through the submarine electricity and communications infrastructure crossing the Strait of Gibraltar and examined in full under Key dependencies; and an object of calibrated migratory and diplomatic leverage during successive Ceuta crises. Holding these roles in view simultaneously, rather than collapsing them into either an alarmist or an uncritical frame, is this report's central methodological contribution to how Spain-Morocco relations should be read, and each is developed with its full evidentiary chain, WEP tags and confidence levels in the chapters that follow.

Executive Summary

Morocco enters the second half of this decade governed, in practice, from the Palace rather than from any of its elected institutions. This report's account of the Makhzen -- the network of royal advisers, territorial governors, and Palace-linked business and media holdings that surrounds the monarchy -- is not a metaphor but a description of how appointments, resources and strategic direction actually move through the Moroccan state, with parliamentary and judicial oversight that this report finds thin at best and, in the security and intelligence domain specifically, largely absent. The 23 September 2026 legislative elections, and the socio-economic grievances the 2025 Gen Z 212 protest movement gave voice to, are the most consequential near-term test of this

arrangement's durability, but nothing in the evidence assessed here suggests the underlying structure of power is itself on the ballot.

Within that structure, Morocco's security and intelligence apparatus divides cleanly by function rather than by rivalry: external intelligence and Sahel diplomacy sit with the DGED, domestic counter-espionage and, on this report's evidence, offensive cyber-surveillance sit with the DGST, and ordinary policing sits with the DGSN -- the last two fused at the top since 2015 in the person of Abdellatif Hammouchi, a concentration of authority with no direct parallel among this report's comparators. The most consequential single finding in this architecture is forensic rather than testimonial: independent technical laboratories have confirmed NSO Group's Pegasus spyware was used against journalists, activists and, on the balance of the evidence, Spain's own Prime Minister and Defence Minister, a capability this report characterises as bought rather than built, since no Moroccan state-attributed offensive cyber-development programme was identified anywhere in the material reviewed. A separate, still-unresolved thread running through 2026 is the Jabaroot hack-and-leak campaign against Moroccan institutions, whose authorship this report was unable to establish among several competing and mutually inconsistent claims, and which it therefore reports as contested rather than resolved.

Two external relationships shape almost everything else in this picture. Algeria and the Western Sahara dispute are the organising strategic rivalry behind Morocco's military posture, its diplomatic courtship of Washington, Tel Aviv and a strengthening bloc at the UN Security Council, and the bulk of the hacktivist and information-operations activity documented in this report's cyberspace chapters. Spain, meanwhile, is impossible to describe in a single register: a genuine security partner on counter-terrorism and counter-narcotics; a demonstrated surveillance target at the highest level of its own government; a structurally dependent neighbour through the submarine cables and power interconnectors crossing the Strait of Gibraltar; and, during successive Ceuta migration crises, an object of calibrated Moroccan leverage. This report's central argument about the Spain-Morocco relationship is that all four of these are simultaneously true, and that reading the relationship through only one of them -- partnership or threat -- misses how Rabat actually uses the tools available to it.

Defensively, Morocco has built a legally comprehensive cybersecurity framework under DGSSI and its national CERT, maCERT, spanning data protection, critical-infrastructure designation and incident-response cooperation with international partners; this report was substantially better able to verify the existence of that legal architecture than its day-to-day operational effectiveness, for want of the published performance data that better-resourced national CERTs routinely release. That asymmetry -- strong on paper, thinly evidenced in practice -- recurs across this report's assessment of Morocco's institutions generally, and readers should weigh every judgment that follows against the confidence level attached to it rather than against the confidence of the underlying institution's own public messaging.

Working methodology

This report was produced through a structured intelligence cycle implemented as a chain of specialised skills, each responsible for one stage and each auditable independently of the others. Acquisition collects raw open-source material -- Moroccan, Spanish and Algerian press, official government and regulatory sites, think-tank output, technical forensic reporting and, where publicly accessible, court records -- logging every item to a per-reference archive with its source URL, author, institution, date of publication and date of acquisition, and an explicit six-tier reliability grading (from primary legal/official documents down to partisan or tertiary sources), without analysis or interpretation at that stage. Processing translates and normalises non-English

material into a common working language while preserving named entities, transliterations and quote fidelity, so that translation choices remain visible and auditable rather than silently absorbed into later analysis.

A set of domain research passes -- covering Morocco's political and Makhzen framework, its strategic priorities, its intelligence community, its law-enforcement and military institutions, coordination and oversight mechanisms, its cyberspace legal and defensive framework, its cybercrime and hacktivism landscape, and its key digital dependencies and capability model -- each produced a working paper for its domain, applying Words of Estimative Probability and NATO/Admiralty source grading consistently so that the final product speaks with one analytic voice regardless of which pass authored which section. Production then assembled those working papers into the structured, referenced document the reader now holds, carrying forward every WEP tag, confidence level and citation exactly as the research stage recorded it rather than re-analysing the underlying material, while adding the figures and tables needed to present relationship structures and enumerations clearly.

This edition is a complete, ground-up rebuild rather than a refresh: every domain was re-researched from scratch for this edition, rather than carrying forward analysis from an earlier report, so that a reader can treat every citation in the chapters that follow as belonging to this collection run specifically. This report is built exclusively on open sources: official Moroccan, Spanish, US, EU and UN publications; Moroccan, Spanish, French and international press; academic and think-tank output; and technical reporting from threat-intelligence vendors and forensic laboratories. Collection ran through 8-9 September 2026, with the substantive reporting window running from 2020 to that date and earlier material used only to establish institutional lineage.

Analytic judgments are expressed using the Words of Estimative Probability (WEP) convention derived from ICD 203 -- almost certainly (95-99%), highly likely (80-95%), likely/probable (55-80%), roughly even chance (45-55%), unlikely (20-45%), highly unlikely (5-20%), remote chance (1-5%) -- each paired with an explicit confidence level (high/moderate/low) that is independent of the probability band; facts that are directly documented carry no WEP band, and every citation additionally carries a NATO/Admiralty grade (A-F for source reliability, 1-6 for information credibility), reproduced from the collection record and never altered during drafting. Where a state actor has a documented incentive to deny or deceive on a topic -- Pegasus attribution and intelligence-service activity above all -- official denials are treated as data about the state's declared position, not as disconfirming evidence, and the same discipline applies to hacktivist and advocacy claims advanced for propaganda effect.

Several collection passes for this edition operated for part of their run under a constrained search-tool budget, and in those cases fell back to direct retrieval against known canonical sources (official government sites, established encyclopaedic references, and previously identified vendor and press domains) rather than broad search; every source obtained this way is graded and flagged accordingly rather than presented with an inflated confidence it does not merit, and several sections state explicitly, at the point the gap arises, where this constrained a particular sub-topic's evidentiary depth.

The report's principal uncertainties, each flagged explicitly at the point it arises rather than smoothed over, are: the precise chain of command behind Morocco's operation of Pegasus and other commercial intrusion tools, which rests substantially on testimonial and forensic-device evidence rather than documentary proof of institutional ownership; the true authorship of the 2026 Jabaroot/JabaROOT leaks, contested among at least four distinct theories; the near-total opacity of the FAR's 2nd and 5th Bureaux and of several of the Makhzen's own informal decision-making channels, which open sources illuminate only at the margins; and the practical, day-to-day cyber-collection role, if any, of the DGSN's own General Intelligence directorate, on which almost no independent reporting exists. Each is addressed the same way throughout this report: by stating

the gap explicitly, by keeping a WEP band and confidence level attached to any judgment that bridges it, and by declining to convert a single-source or testimonial claim into an established fact merely because it fits an otherwise plausible narrative.

Part II. Strategic and political foundations

Introduction

Morocco's modern statehood rests on the Alaouite dynasty, which has ruled continuously since the seventeenth century and which the country's post-independence and current constitutional order both treat as the central organising institution of the state rather than merely its ceremonial head. France and Spain established separate protectorates over Moroccan territory in 1912, administered respectively from Rabat and from a smaller northern and Saharan zone centred on Tetouan, and Morocco recovered full independence in 1956 under Sultan Mohammed V, who then assumed the title of King. This colonial partition is itself the background fact that explains why Spain retains Ceuta, Melilla and several smaller enclaves on the Moroccan coast to this day, a legacy examined throughout the chapters that follow; it is stated here as established historical background rather than as a WEP-tagged judgment.

Morocco's population reached 36,828,330 at the 2024 general census, with life expectancy at birth of 77.2 years and a 2050 population projection of roughly 43.6 million against a rising old-age dependency ratio of 69.7% [1]. The 2011 Constitution describes national identity as forged by the convergence of the country's Arab-Islamist, Berber (Amazigh) and Saharan-Hassanic components, nourished by African, Andalusian, Hebraic and Mediterranean influences, and declares Islam the religion of the State while guaranteeing the free exercise of beliefs to all [2]. Arabic and Tamazight are both constitutionally official languages, the latter elevated from merely recognised to fully official status by the 2011 reform; French remains the de facto language of business, higher education and much administration, and Spanish retains a residual regional presence in the former northern protectorate zone, though current bilingualism or language-use percentages were not independently verified in the material available and are recorded here as an explicit gap rather than an assumed figure [2].

Morocco is constitutionally a parliamentary, democratic and social Monarchy in which sovereignty is formally vested in the Nation, but the King retains decisive reserved powers that sit outside ordinary parliamentary control: as Amir al-Mouminine (Commander of the Faithful) he exercises exclusive religious prerogatives by dahir; as Head of State he is Supreme Arbiter between the institutions and guarantor of the Kingdom's independence and territorial integrity; he appoints the Head of Government from the leading party in the Chamber of Representatives and appoints ministers on that Head of Government's proposal; and he presides personally over the Council of Ministers, which under Article 49 approves the appointment, nominally on Head-of-Government proposal, of the Bank Al-Maghrib governor, ambassadors, walis and governors, and the leadership of both internal-security administrations and public strategic establishments and enterprises [2]. It is almost certainly the case that this constitutional architecture gives the Palace a durable, legally grounded channel of control over the state's territorial-administration, security and state-enterprise leadership, independent of which party wins a parliamentary election (confidence: high), a judgment that follows directly from the plain text of Articles 41, 47, 49, 53 and 54 rather than from any contested interpretation.

Morocco enters a politically consequential window, with legislative elections scheduled for 23 September 2026 that current Moroccan academic commentary analyses less as a contest over which party governs than as a test of whether the incoming government can address a longstanding centre-periphery divide, since place of birth and place of residence continue to strongly influence individual trajectories in education, healthcare, employment and access to services across Morocco's regions [3]. That commentary recommends differentiated territorial financing, measurable State-Region performance contracts, prioritised rural digital infrastructure and a shift

from symbolic to institutionally implemented Tamazight-language policy in schools and administration [3]. On the ballot itself, the Justice and Development Party (PJD) -- reduced from 125 to 12 seats in its 2021 collapse -- has re-entered the race with an economic-populist platform proposing a top corporate-tax bracket for dominant fuel, telecommunications and cement firms and an overhaul of Morocco's subsidy system on the grounds that poorer households receive little direct benefit from the existing arrangement [4]. It is likely that this reflects a deliberate strategic pivot away from the religious and identity framing of PJD's earlier electoral cycles toward anti-monopoly economic populism, in an attempt to rebuild a coalition after 2021 (confidence: moderate), a judgment drawn from the platform's own content rather than from any statement of strategic intent by the party itself.

Morocco's most significant recent internal-security event, the Gen Z 212 protest wave, began in late September 2025 as a leaderless, Discord-organised youth movement demanding better public healthcare and education, crystallising around the contrast between multibillion-dollar 2030 World Cup infrastructure spending and underfunded hospitals [5, 6]. Security forces killed three protesters in Leqliaa, near Agadir, an episode the Interior Ministry attributed to an attempted seizure of police weapons, a claim two independent outlets note no witnesses corroborated; over 1,000 people were reportedly arrested, roughly 70% of demonstrators were minors by the Interior Ministry's own estimate, and protests spread across 23 of Morocco's provinces before Prime Minister Aziz Akhannouch's sole public response, an offer of dialogue without specifying concrete reforms, while some crowds called for his resignation and others chanted for King Mohammed VI himself to intervene against the government [5, 6]. It is highly likely that Gen Z 212 represents the most significant leaderless, extra-institutional challenge to the Moroccan government's authority of the current decade (confidence: high), given the multiply-sourced scale and casualty toll independently corroborated by two separate outlets.

Politics and geopolitics

Morocco's most consequential external alignment in the current period is with the United States, anchored in Washington's December 2020 recognition of Moroccan sovereignty over Western Sahara -- the first Western government to do so -- and reinforced by US sponsorship of a UN Security Council resolution in October 2025 backing Morocco's autonomy proposal for the territory [7]. That alignment carries visible commercial and symbolic expression: a September 2026 US Foreign Military Sales award of up to \$42.1 million to CAE Inc. for F-16 Block 72 training simulators at Sidi Slimane Air Base follows the State Department's 2019 approval of a potential \$3.79 billion sale of 25 new F-16C/D aircraft plus a \$985 million upgrade of Morocco's existing fleet [8], while a viral, unverified claim that Morocco named a new Western Sahara highway after President Trump -- never confirmed or denied by Rabat -- illustrates, whether or not literally true, how closely Moroccan diplomacy is perceived to track US recognition of its core territorial claim [7]. It is highly likely that Morocco continues to treat the US relationship as its single most valuable external validation of the Western Sahara position through the remainder of this decade (confidence: high).

France remains Morocco's deepest and most institutionally dense European partnership, illustrated concretely by the fifteenth Morocco-France High-Level Meeting in Rabat in July 2026, at which the two governments signed over a dozen cooperation agreements spanning high-speed rail financing between Kenitra and Marrakech, water-sector partnership, feminist-foreign-policy cooperation, civil aviation, postal services, cultural exchange and joint scientific research simultaneously [9]. It is highly likely that this breadth of simultaneous institutional agreement reflects a deliberately deepened, multi-sector bilateral relationship rather than a one-off diplomatic

gesture (confidence: high), given the number and functional diversity of the instruments signed at a single meeting. This institutional depth is notable for coexisting with, rather than being visibly disrupted by, DGED's own alleged 2021 Pegasus targeting of seven French government ministers, examined further under *DGED* below [10]; this report's research located no France-specific friction indicator -- a visa dispute or a ministerial-level protest, for instance -- in the current collection to weigh against the July 2026 cooperation evidence, and accordingly treats the France relationship as actively deepening at the technical and ministerial level in the present period rather than as currently strained, revising an assumption of strain that earlier framings of this relationship might otherwise carry forward unexamined.

Spain's relationship with Morocco is, by contrast, Morocco's most volatile major European tie, alternating between normalisation and acute crisis on a roughly annual cycle: Prime Minister Pedro Sánchez's 2022 declaration that Morocco's autonomy plan was the most serious, credible and realistic solution for Western Sahara ended a rupture triggered by Spain's 2021 admission of Polisario leader Brahim Ghali for medical treatment, yet on 30-31 July 2026 a mass border-crossing episode into Ceuta -- Spanish-press reporting cited more than 49,000 entrants within 24 hours while Moroccan-press reporting of Spanish official figures cited over 70,000, two unreconciled counts for what this report's sourcing treats as the same window rather than two separate episodes, both distinct from the earlier roughly 10,000-person 2021 surge -- reopened tension within days of Sánchez travelling to Algiers to repair ties with Rabat's principal regional rival [11, 12]. Humanitarian organisations subsequently reported approximately 141 deaths across the July-August crossing attempts, a toll neither government has confirmed [13]. It is a roughly even chance that Morocco deliberately calibrates the volume of irregular migration crossings into Ceuta and Melilla as a diplomatic-pressure instrument timed to Spanish political developments, as opposed to the surges reflecting migration dynamics genuinely outside Rabat's control (confidence: low), since Sánchez himself told Congress that Spain currently lacks solid evidence tying the Moroccan government directly to organising the influx, even as the same reporting explicitly treats the question of Moroccan border-control passivity as deliberately left unclarified by official explanations [11, 12].

This report's own weighing of that unresolved question sets three competing explanations against each other rather than adopting the first plausible one. A top-down facilitation hypothesis -- the Palace or DGST leadership deliberately easing border controls as coercive signalling timed to Sánchez's 20 July 2026 Algiers visit -- draws some support from that timing coincidence and from a Spanish national-police characterisation, relayed to Audiencia Nacional judge María Tardón, of the crossing as a predefined process with objectives different from migratory ones requiring a high capacity of influence in networks and persons linked to Morocco's security forces, but the only claims naming a specific architect come from the hacktivist actor Jabaroot, whose own stated aim of maximising the crisis's political cost to Rabat is precisely the kind of source-incentive-to-deceive this report discounts rather than accepts at face value [14, 15]. A pure loss-of-control hypothesis, consistent with Madrid's own people-trafficking-mafia framing and with Sánchez's statement to Congress, struggles against the sheer logistical difficulty of covertly staging a surge of this scale and against Morocco's own subsequent multi-agency mobilisation -- DGSN, Royal Gendarmerie and Auxiliary Forces jointly deployed -- to block a smaller 15 August crossing attempt near Castillejos, behaviour difficult to reconcile with an ongoing deliberate-facilitation policy. A third, intermediate hypothesis -- localised or mid-level tolerance by security elements short of any documented top-down order, consistent with Morocco's security architecture being a set of separately tasked institutions (DGST, DGED, the Auxiliary Forces and the Royal Gendarmerie were all separately active in the period) rather than a single frictionlessly coordinated command -- best accommodates the evidence without requiring either a unified conspiracy or a pure accident. It is a roughly even chance that some form of security-apparatus tolerance or

facilitation occurred at some level, with the mid-level-tolerance hypothesis favoured over top-down orchestration specifically (confidence: low), a judgment this report reaches on its own evidentiary record but which converges with the same three-hypothesis structure and conclusion independently returned by this edition's diplomatic and geopolitical research passes; it should be revisited if a documented change in border-guard standing orders, forensic linkage between DGST/DGED communications and the crossing's timing, or a judicial finding naming a specific Moroccan agency emerges.

Algeria is Morocco's principal regional adversary, a rupture dating to August 2021 and sustained since by a genuine bilateral arms race: the two countries together accounted for 88% of North Africa's measurable 2025 military spending, some \$33 billion combined, with Algeria's \$25.5 billion far outweighing Morocco's \$7.51 billion, though Algeria's 2026 budget is projected to fall roughly 10% in real terms while Morocco's rises to a record \$7.87 billion, a divergence the IISS attributes to Algeria's hydrocarbon-dependent public finances against Morocco's more diversified economy [16]. The same source describes Algeria leaning on Russian and increasingly Chinese equipment, with reported Su-57 fifth-generation fighters, against Morocco's preference for US and Western systems alongside developing cooperation with Israel and its own domestic defence industry -- a rare direct sourced indication of a Morocco-Israel defence-industrial dimension, though no source located in this collection elaborates its specific content. It is likely that the two states' parallel modernisation drives will continue to reinforce, rather than ease, what the IISS itself terms a security dilemma through the 2026-2027 horizon (confidence: moderate), a judgment the source's own analysis supports directly.

The Strait of Gibraltar's strategic significance to Morocco's foreign policy is best understood as the convergence point of three distinct pressures rather than as a single well-documented chokepoint file in its own right. It is the migration corridor whose surges have repeatedly reopened and closed the Spain-Morocco relationship, discussed above [11, 12]; it is the terminus toward which Morocco's prospective Nigeria-Morocco gas pipeline -- approved by ECOWAS in July 2026 as a \$25 billion, roughly 6,000-kilometre project intended eventually to connect to the existing Maghreb-Europe Pipeline into Spain -- would deliver an estimated 15 of 30 billion cubic metres of annual gas onward to Europe [17]; and it is, per one Spain-based outlet citing an unverified defence-analysis group, the notional line across which Moroccan missile and drone systems are now assessed to be able to reach mainland Andalucía, prompting a serving Spanish general's public assertion that Spain retains the capability to shut off Morocco in 24 hours [18]. This collection located no dedicated primary or technical source -- a port-authority traffic statistic or a NATO or Instituto Español de Estudios Estratégicos assessment, for instance -- addressing the Strait's shipping-chokepoint role directly, a gap noted explicitly here rather than papered over with an unsupported figure; the table below sets out the three pressures side by side.

Table 1. The Strait of Gibraltar: three converging strategic pressures on Morocco's Spain policy.

Pressure	Mechanism	Key evidence
Migration corridor	Irregular crossings into Ceuta/Melilla repeatedly reopen and close the bilateral relationship	2021 Ghali-crisis surge (~10,000); July 2026 mass crossing (over 70,000 reported; a separate figure of more than 49,000 in 24 hours)
Energy/infrastructure terminus	Nigeria-Morocco gas pipeline routed toward the Maghreb-Europe Pipeline into Spain	USD 25bn, ~6,000 km, ECOWAS-approved (Jul 2026); ~15 of 30 bcm/year assessed onward to Europe; construction from 2028, deliveries from 2031

Military-capability perception

Assessed missile/drone reach toward mainland Andalucía

Unverified defence-analysis-group assessment; a serving Spanish general's public assertion that Spain could "shut off Morocco in 24 hours"

The Makhzen

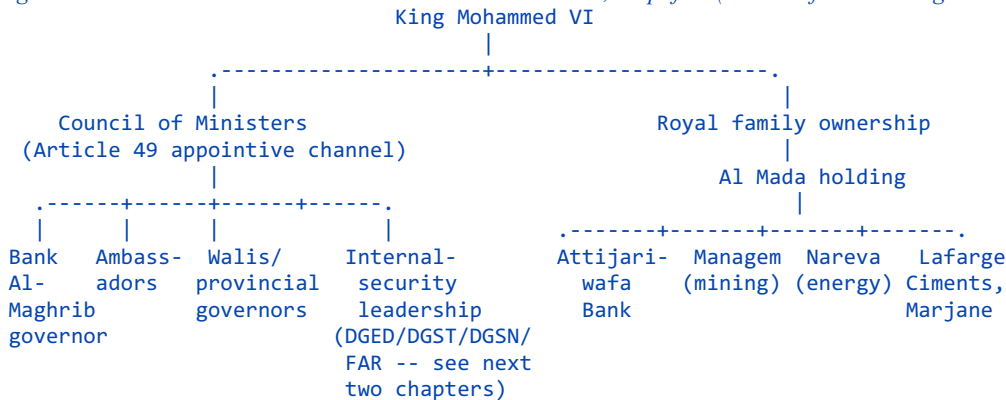
Makhzen functions in current open-source material as a genuinely contested term rather than a settled analytic category. An establishment-aligned Moroccan commentator, writing in mainstream Moroccan English-language press, defines it benignly as the network of traditional authority centred around the monarchy -- tribal leaders, dignitaries, religious scholars and local notables -- crediting it with having proven highly adaptive and with ensuring Morocco's institutional continuity through colonialism, independence, modernisation and the present regional turmoil [19]. Algeria's official state news agency deploys the identical term as an instrument of delegitimisation, describing Morocco as cementing its position as a safe haven for criminals fleeing European justice and positioning the Makhzen at the centre of fostering an environment that allows transnational organised crime to regenerate itself, an unverified, single-source claim advanced by a state actor in active diplomatic rupture with Rabat and with no independent corroboration located anywhere in this collection [20]. It is highly likely that neither framing should be read as a neutral definition of the term (confidence: high), and no independent Western-academic or think-tank definition was located in the material reviewed, a gap stated explicitly rather than papered over.

The concrete institutional mechanism by which informal Palace authority is exercised over the formal state is, notwithstanding that definitional gap, directly documented in the Constitution's own text rather than left to contested characterisation. Article 49 routes the appointment of the Bank Al-Maghrib governor, all ambassadors, the entire corps of walis and provincial governors, and the leadership of both internal-security administrations and public strategic establishments and enterprises through the King-chaired Council of Ministers, nominally on the Head of Government's proposal but decided in a body the King himself presides over; Article 53 makes the King Supreme Head of the Royal Armed Forces with the power to appoint to military offices, and Article 54 establishes a King-presided Superior Council of Security coordinating both internal and external security strategy [2]. It is almost certainly the case that these three articles, read together, provide the legal chassis through which whatever informal network of advisers, notables and security officials constitutes the Makhzen in practice actually reaches into territorial administration, the security services and state-enterprise leadership simultaneously (confidence: high), since this is a direct reading of the constitutional text rather than an inference requiring additional evidence.

On the network's economic dimension, Al Mada -- Morocco's largest private holding conglomerate, renamed in 2018 from the Société Nationale d'Investissement founded in 1966 -- is primarily owned by the royal family and holds significant stakes simultaneously in Attijariwafa Bank, Managem, Nareva, Lafarge Ciments and Marjane, with expanding investment activity across Cameroon, Ivory Coast, Rwanda and Gabon [21]. It is highly likely that this single conglomerate structure gives the monarchy a direct commercial stake, not merely a regulatory or appointive one, in outcomes across banking, extractive industry, energy, construction and consumer retail simultaneously (confidence: high), a judgment drawn directly from the sectoral breadth this source confirms; a comparable royal or Makhzen-network ownership stake in

Morocco's telecommunications or media sectors was not independently verified within this material and is recorded here as an explicit gap rather than asserted on background knowledge alone.

Figure 1. The Makhzen's constitutional and economic channels, simplified (both run from the King rather than from elected government).



Whether this fusion of appointive, security and economic authority under a single informal network functions chiefly to distribute state resources efficiently or chiefly to insulate decision-making from meaningful legislative or judicial oversight cannot be resolved on the evidence reviewed, and the two readings are presented here as a live tension rather than adjudicated. The Gen Z 212 protests' central demand -- redirecting public spending from World Cup infrastructure toward hospitals and schools, discussed under *Introduction* above -- is itself evidence that a substantial share of the Moroccan public perceives current resource allocation as poorly aligned with popular priority, a perception echoed in PJD's own stated rationale for its 2026 subsidy-reform proposal that poorer households receive little direct benefit from the existing system [4, 5]. It is likely that the constitutional concentration of appointive authority documented above reduces the practical accountability of walis, governors, security-service leadership and state-enterprise heads to elected institutions relative to a system where such appointments required parliamentary confirmation (confidence: moderate), a judgment following from the plain constitutional allocation of that appointive power rather than from a source asserting oversight failure directly; no dedicated audit or oversight-specific source was located, and this gap is stated accordingly.

Strategic priorities

Morocco's strategic priorities are best read as an ordered hierarchy in which internal regime security outranks every external file, since no foreign-policy outcome is worth pursuing at the cost of domestic stability that the monarchy itself does not survive to enjoy. The table below sets out the six theatres in ranked order together with their lead evidentiary basis and assessed confidence, before each is developed in turn.

Table 2. Morocco's six strategic-priority theatres, ranked, with lead evidentiary basis and assessed confidence.

Rank	Theatre	Lead evidentiary basis	Assessed confidence
1	Internal regime security	Gen Z 212 protest wave (Sep-Oct 2025); Sept 2026 elections; PJD's populist re-entry	Moderate
2	Western Sahara	Dec 2020 US recognition; Oct 2025 UNSC resolution; UN Security Council Resolution 2797 (2026)	Moderate

3	Algeria rivalry	88% of North Africa's 2025 military spending; IISS arms-race analysis	Moderate
4	Sahel and Atlantic strategy	Nigeria-Morocco gas pipeline (2026 ECOWAS approval); Tiznit-Dakhla highway; Atlantic Initiative	Moderate
5	Spain, France and the EU	15th Morocco-France High-Level Meeting (Jul 2026); Ceuta/Melilla rhetoric and crossings	Moderate
6	US, Israel and the Gulf states	Sept 2026 F-16 FMS training-simulator award; single unelaborated Israel-cooperation reference	Low

The Gen Z 212 protest wave and the September 2026 elections are the two live indicators of internal regime security's current stress level: PJD's populist re-entry, the Palace's own preoccupation with territorial-inequality policy commentary, and a protest movement whose core demand -- health and education spending over World Cup prestige projects -- directly challenges the government's declared spending priorities together indicate that internal legitimacy management, not any external rivalry, remains the first-order concern of Moroccan governance in the current period [3, 4, 5]. It is likely that the September 2026 elections will be read by the Palace primarily as a referendum on this internal-legitimacy question rather than as a genuine transfer of policy authority to whichever coalition governs (confidence: moderate), consistent with the constitutional concentration of appointive power in the Palace documented under *The Makhzen* above, regardless of the election's outcome.

Western Sahara ranks second, as the one issue on which Morocco has secured its most significant recent external validation and continues to invest disproportionate diplomatic capital. The core sequence -- US recognition of Moroccan sovereignty in December 2020, a US-sponsored UN Security Council resolution favouring Morocco's autonomy proposal in October 2025, and the adoption of a further UN Security Council Resolution 2797 referenced independently by both a Moroccan think tank and Greece's foreign minister by September 2026 -- indicates an accumulating, rather than static, diplomatic momentum behind Rabat's position [7, 22, 23]. This collection did not independently retrieve Resolution 2797's own text, a gap flagged consistently across three separate sources, and downstream assessment should not characterise the resolution's contents beyond adopted and referenced as endorsing UN-mediated negotiation on the basis of Morocco's autonomy proposal, pending direct verification [22, 23].

A separate, Moroccan-press-sourced claim holds that Algeria's own rhetoric on the dispute is softening under US diplomatic pressure, but this claim was advanced entirely by named analysts and a pro-Moroccan-position advocacy figure, with no Algerian-side or official Algerian corroboration located [24]. It is unlikely that this represents a confirmed genuine shift in Algiers' position rather than a Rabat-aligned interpretive narrative (confidence: low), given the complete absence of independent corroboration.

Algeria ranks third as Morocco's most active and materially consequential regional rivalry, distinct from the Western Sahara file even though the two are closely linked; Algiers' own state media's

use of the term *Makhzen* as a term of criticism, discussed under *The Makhzen* above, is itself a data point in this rivalry's current temperature, since state-to-state rhetorical attacks of this kind are not typical between states with normalised relations [20]. Layered atop that rhetorical hostility is the arms-race dynamic detailed under *Politics and geopolitics* above, to which this section defers rather than repeating the underlying figures; it is likely that this rivalry continues to shape Moroccan defence procurement and diplomatic alignment -- toward the US, Israel and its own domestic defence industry, away from any Algeria-aligned bloc -- as a near-permanent structural feature of Moroccan strategic planning through the remainder of this decade (confidence: moderate), a judgment consistent with the trajectory the IISS's own data describes [16].

Sahel and Atlantic strategy ranks fourth, anchored in the \$25 billion, ECOWAS-approved Nigeria-Morocco gas pipeline -- a roughly 6,000-kilometre project crossing thirteen countries plus Western Sahara, intended to carry Nigerian gas to Morocco and onward to Europe via the existing Maghreb-Europe Pipeline, with construction scheduled to begin in 2028 and first deliveries in 2031 [17]. This project sits alongside Morocco's completed Tiznit-Dakhla highway, fully operational since January 2026 at roughly 1,055 kilometres and \$1 billion, linking southern Morocco to the Dakhla peninsula, where Morocco is developing a major Atlantic port explicitly tied to its Atlantic Initiative for connecting landlocked Sahel states to Atlantic trade via Moroccan territory [7]. It is likely that Morocco intends this Atlantic-facing infrastructure buildout to position itself as an alternative export corridor to Europe that structurally bypasses Algeria, whose own rival trans-Saharan gas project is a direct competitor for the same function (confidence: moderate), a judgment consistent with, though not conclusively proven by, the pipeline's own geography and timing relative to the Algeria rupture [17].

Spain, France and the wider European Union rank fifth, and the evidence shows an approach that varies significantly by partner rather than a single uniform European strategy: France receives the deepest institutional engagement, already detailed under *Politics and geopolitics* above, while Spain receives a more volatile mix of normalisation and crisis cycling on the migration and Ceuta/Melilla files, illustrated starkly by Justice Minister Abdellatif Ouahbi's public reference to the two cities as our lands and Religious Affairs Minister Ahmed Toufiq's reference to their liberation, made at an event attended by King Mohammed VI, which together prompted a categorical Spanish rejection of any discussion of Spain's territorial integrity from Foreign Minister José Manuel Albares [12]. The table below places the successive Ceuta and Melilla migration-crossing episodes side by side, since Spanish and Moroccan reporting have repeatedly cited overlapping but distinct figures for what are, on close reading, separate events.

Table 3. *Ceuta and Melilla migration-crossing episodes, 2021-2026: distinct events, overlapping figures.*

Date	Reported scale	Context
Apr-May 2021	~10,000 crossings	Triggered by Spain's admission of Polisario leader Brahim Ghali for medical treatment
7 Apr 2022	n/a	Sánchez declaration endorsing Morocco's autonomy plan; formal end of the 2021 rupture
30-31 Jul 2026	Over 70,000 reported; a separate figure of more than 49,000 in 24 hours	Mass crossing into Ceuta days after Sánchez's Algiers visit to Rabat's regional rival

Smaller EU states, meanwhile, are aligning incrementally toward the US and Israeli position on Western Sahara: Greece's foreign minister publicly welcomed Morocco's autonomy proposal and UN Security Council Resolution 2797 in September 2026 [23], while Denmark's foreign minister, in the same month, called Morocco our ally on the southern flank and indicated Denmark could

adjust its position to move closer to the United States' position on Western Sahara ahead of a planned December 2026 strategic-partnership agreement [25]. It is likely that this pattern of incremental smaller-EU-state alignment continues to isolate Spain's more contested and politically constrained domestic position on Western Sahara from the broader EU trend (confidence: moderate), a judgment drawn from the accumulating count of EU states now audibly endorsing the autonomy framework relative to Madrid's more cautious public posture.

The United States, Israel and the Gulf states rank sixth as a group, not because the relationships are unimportant but because the evidence available on them is comparatively thin relative to the other five theatres and concentrated almost entirely on the Western Sahara file already discussed above. The clearest concrete evidence is the September 2026 US Foreign Military Sales award for F-16 training infrastructure, following the 2019-approved \$3.79 billion F-16 sale framework [8], alongside the single, unelaborated reference to Morocco developing cooperation with Israel found in the IISS-sourced defence-comparison reporting [16]; no dedicated source on Gulf-state investment, ownership or security relationships with Morocco was located in the material reviewed for this section, a gap explicitly flagged here rather than filled by reference to material developed elsewhere in this report. It is a roughly even chance, on this comparatively thin evidentiary base, that US, Israeli or Gulf relations see a materially new development within the near term, as against a continuation of the current steady-state pattern (confidence: low), a judgment offered at low confidence precisely because this theatre is the least densely evidenced of the six.

Part III. The security and intelligence architecture

The intelligence community

Morocco's civilian intelligence and police architecture traces to a single royal dahir of 12 January 1973, issued in the wake of the failed 1971 and 1972 military coups against King Hassan II, which dissolved the earlier CAB-1 political-police structure and created two successor services on the same day: the DGED for external intelligence and the DGST for domestic security and counter-espionage [26, 27]. That shared origin helps explain why the two services' mandates still overlap in practice, particularly in foreign-facing technical collection, even though the DGED is administratively attached to the Administration de la Défense Nationale while the DGST answers to the Ministry of Interior [26, 27]. The DGSN, Morocco's national civilian police force, has a distinct and older lineage, having been established on 16 May 1956 under Dahir n° 1-56-115 to replace the colonial-era Police Chérifienne, and its relevance to this chapter rests on one constituent directorate rather than the force as a whole, examined in full below [28].

Since 15 May 2015, a single official, Abdellatif Hammouchi, has directed both the DGST and the DGSN concurrently, a dual-hatting the open-source record consistently describes as unprecedented in the post-1999 Moroccan security apparatus and one that fuses domestic counter-espionage and national policing authority without a direct European equivalent [27, 29]. It is almost certainly the case that this concentration of authority in a single official gives Hammouchi a degree of institutional control over Morocco's internal-security architecture that no comparable arrangement among Morocco's principal European partners approaches (confidence: high), since no source reviewed identifies any equivalent single-official fusion of a counter-espionage service and a national police force elsewhere in the region this report examines. The table below gives a comparative snapshot of the three bodies before their individual profiles, and the figure that follows sets out their reporting lines in simplified form.

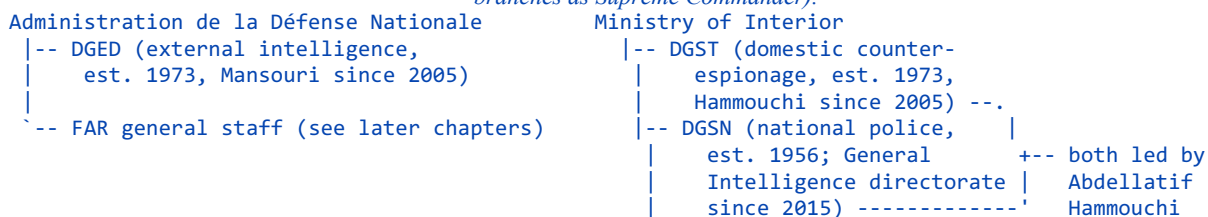
Table 4. Morocco's civilian intelligence and police agencies at a glance.

Agency	Founded	Reports to	Director (since)	Core mandate
DGED	1973 (dahir, 12 Jan)	Administration de la Défense Nationale	Mohammed Yassine Mansouri (2005)	External intelligence, counter-espionage, Sahel security diplomacy
DGST	1973 (dahir, 12 Jan)	Ministry of Interior	Abdellatif Hammouchi (2005)	Domestic counter-espionage, counter-terrorism, signals intelligence (PCR), judicial police (BCIJ)
DGSN	1956 (dahir, 16 May)	Ministry of Interior	Abdellatif Hammouchi (2015)	National civil police: public order, judicial police, General Intelligence

Table 5. DGED, DGST and DGSN leadership succession.

Agency	Director	Tenure	Notable prior role
DGED	Ahmed Dlimi	1973-1983	Former head of CAB-1
DGED	Abdelhak El Kadiri	1983-2001	—
DGED	Ahmed El Harchi	2001-2005	—
DGED	Mohammed Yassine Mansouri	2005-present	Former director, Maghreb Arabe Presse; first civilian director
DGST	Ahmed Dlimi	1973-1983	Concurrently DGED's first director
DGST	Driss Basri	1983-1999	Concurrently Interior Minister
DGST	Hamidou Laanigri	1999-2003	—
DGST	Ahmed Harari	2003-2005	—
DGST	Abdellatif Hammouchi	2005-present	Joined DGST 1993; also DGSN director from 2015
DGSN	Abdellatif Hammouchi	2015-present (dual-hatted with DGST)	Concurrently DGST director since 2005

Figure 2. Simplified reporting lines of Morocco's civilian intelligence and police architecture (King Mohammed VI sits above both branches as Supreme Commander).



The three profiles that follow -- DGED, DGST and the intelligence-relevant slice of DGSN -- account for essentially all of the open-source record on Moroccan civilian intelligence activity, and two of the three have documented operational histories in Europe that touch Spain directly. Each profile addresses the same evidentiary weak point from a different angle: the precise division of labour between DGED and DGST on Morocco's use of commercial spyware, an attribution question this report resolves only at low-to-moderate confidence and addresses consistently across all three profiles rather than settling once and treating as closed.

DGED

The Direction Générale des Études et de la Documentation (DGED), Morocco's foreign-intelligence and counter-espionage service, was established by Royal Dahir 1-73-8 on 12 January 1973 as part of the same post-coup restructuring that produced the DGST, and is headquartered in Rabat, administratively attached to the Administration de la Défense Nationale rather than to the Ministry of Interior -- an arrangement that keeps it, at least on paper, outside the domestic-security ministerial chain that governs the DGST and DGSN examined below [26]. Its stated mandate covers external intelligence collection, counter-espionage and protection of national institutions' security, and this founding attachment to the defence administration rather than Interior places it, structurally, in the same chain that ultimately answers to the King as Supreme Commander rather than to any minister accountable to parliament [26].

Leadership has passed through four directors: Ahmed Dlimi (1973-1983), who had previously headed CAB-1; Abdelhak El Kadiri (1983-2001); Ahmed El Harchi (2001-2005); and Mohammed Yassine Mansouri, in post since 14 February 2005 [26]. Mansouri is the first civilian to hold the

post, a former classmate of King Mohammed VI at the Royal College who previously directed the state news agency Maghreb Arabe Presse, and open-source profiles consistently frame him as a discreet royal confidant [26]. It is likely that Mansouri's appointment reflected a deliberate Palace preference for a trusted, non-military director over the service's earlier tradition of military leadership (confidence: moderate), given that no comparable civilian appointment had occurred in the service's first three decades and no source located offers a competing explanation for the change.

It is highly likely that command and control over the DGED runs directly to the Royal Palace with only nominal intermediation through the defence administration (confidence: moderate), a judgment resting on Mansouri's personal-confidant profile, the pattern of direct royal appointment to the directorship, and the absence, in any source reviewed, of a named minister exercising real oversight of DGED operations. Staffing and budget figures available in open sources are dated and should be read as indicative rather than current: approximately 4,000 personnel as of a 2003 estimate, roughly 60% drawn from the Royal Armed Forces and the remainder civilian, with an estimated 250 to 300 officers deployed abroad and an annual budget cited at MAD 1.08 billion as of 2015 [26]; no source located updates any of these figures past the mid-2010s, and this is recorded as an explicit gap rather than an assumption of continuity.

DGED's collection disciplines, as documented in open sources, centre on human intelligence built through foreign liaison relationships rather than domestic technical collection, which is more consistently the DGST's documented remit; the clearest evidence of this orientation is the service's Sahel mediation portfolio since 2020, credited with securing the 2022 release of German hostage Jörg Lange in Niger, the 2023 release of Romanian citizen Iulian Ghergut in Burkina Faso, involvement in 2024 negotiations concerning detained former Niger president Mohamed Bazoum, the 2024 release of four French DGSE officers held in Burkina Faso, and assistance reported in 2025 to Niger in tracking Boko Haram figure Bakura Doro [26]. It is likely that this mediation role reflects a deliberate Moroccan strategy of filling a security-diplomacy gap left by receding French influence in the Sahel (confidence: moderate), since the timing and consistency of these episodes across three separate countries and four years is difficult to explain as coincidental liaison work.

Domestic counter-terrorism casework is a secondary, earlier-documented DGED mission set: the service is credited with a role in the investigation following the May 2003 Casablanca bombings, which led to convictions of several Justice and Development Party figures and an Al-Manar correspondent for alleged complicity [26]. This casework is itself controversial given the political-party status of some of those convicted, and it is a roughly even chance (confidence: low) that it reflects genuine counter-terrorism necessity rather than a politically convenient use of security powers against an Islamist party then rising electorally, since no source located resolves that question either way.

The DGED's cyber and technical-collection role is the single most consequential open question addressed in this profile, and the evidence must be read in layers rather than as one settled fact. Network-level evidence from Citizen Lab's 2018 survey identified a suspected Pegasus operator, internally codenamed ATLAS, geolocated via DNS-cache probing to Moroccan telecom networks from August 2017 onward -- infrastructure-level evidence of a Morocco-nexus Pegasus presence, explicitly not device forensics [30]. Device-level forensic confirmation followed independently: Amnesty's Security Lab documented network-injection Pegasus attacks on journalist Omar Radi's phone across four dates in 2019-2020, attributing responsibility to Moroccan authorities generically without naming a specific agency [31], and a second, cross-lab-corroborated case confirmed Pegasus traces on Sahrawi activist Aminatou Haidar's phone in 2018 and again in 2021, with Citizen Lab independently reproducing the 2021 findings from Amnesty-supplied records [32]. It is almost certainly true that Moroccan state services have operated Pegasus against

domestic civil-society targets since at least 2019 (confidence: high), given this cross-lab, device-level corroboration.

Whether DGED specifically, as opposed to DGST, holds any operational role in this Pegasus programme is far less settled. The July 2026 Forbidden Stories consortium investigation, built on leaked DGST documents and insider testimony, attributes primary operational control to the DGST rather than DGED [33, 34], and a separate consortium article on French-minister targeting appears to reference DGSE as the implicated Moroccan agency -- almost certainly a transcription error for DGED, since Morocco has no agency called DGSE and DGSE is France's own external service, though this could not be verified against the primary text and should not be silently corrected [10]. A related Gabon case, in which Forbidden Stories attributes to the DGST the targeting of Gabonese presidential-entourage and opposition figures via roughly twenty Moroccan personnel rotating through Gabon on six-month postings since the Hassan II era, reads structurally as DGED's typical foreign-liaison remit rather than DGST's domestic counter-espionage one, a cross-service attribution question the consortium's own reporting does not resolve [35]. It is a roughly even chance (confidence: low) that DGED holds a facilitation or foreign-liaison role in Pegasus acquisition or targeting distinct from DGST's device-operation role, given that DGED's documented foreign-liaison function is functionally the kind of role a foreign-facing acquisition broker would occupy, even though no source located states this directly.

The DGED's European footprint since 2014 has generated a string of controversies that, taken together, point to a foreign-influence and liaison-disruption mission set beyond classic human intelligence collection: the 2014 MarocLeaks episode, in which correspondence between DGED and Moroccan consulates was published and Rabat blamed pro-Polisario and Algerian actors; a 2017 case in which a French border-police officer was arrested for allegedly passing DGED contacts security-watchlist files on roughly 200 individuals; a 2021 allegation of DGED infiltration of the French Council of the Muslim Faith; and a 2022 scandal involving alleged DGED-linked infiltration of the European Parliament, contemporaneous with the broader Qatargate affair [26]. It is unlikely (confidence: low) that these were all centrally directed DGED operations rather than looser networks of Morocco-aligned actors, since the underlying sourcing for this cluster is a single tertiary compilation that does not itself distinguish the two possibilities.

A further, distinct gap concerns Morocco's Mohammed VI-A and Mohammed VI-B optical reconnaissance satellites, launched in 2017 and 2018 respectively at a combined cost of roughly EUR 500-600 million and described in French press reporting at the time as serving a strong military purpose; no source located anywhere in this report's research identifies which Moroccan body -- DGED, the FAR general staff, or another agency entirely -- actually tasks the satellites or receives their imagery [36, 37]. Given DGED's own foreign-liaison and human-intelligence orientation, this report neither assumes DGED holds a tasking role merely because the capability is intelligence-relevant, nor rules one out; it records the absence of any documented link between DGED and the satellite programme as an explicit gap that widens, rather than narrows, the uncertainty already attached to DGED's technical-collection profile.

The most significant new development bearing on DGED is the emergence, in September 2026 Spanish press reporting, of Mehdi Hijaouy as a named person of interest: described as a former DGED deputy chief and head of a covert-operations unit the reporting calls Service Action, Hijaouy is reported to have fled Morocco roughly two years ago, been detained in Spain in September 2024 on an international warrant, and subsequently disappeared from judicial supervision while allegedly retaining access to Pegasus-derived material from the phones of Spain's Prime Minister and two ministers, with a further claim that a Moroccan contact offered a Spanish police collaborator two to three million euros to locate him [38, 39]. This is a single-outlet exclusive resting on unnamed security sources, and the Service Action unit name is not corroborated elsewhere in this collection; it should be treated as a serious lead rather than an

established fact, but if substantiated it would be the first named DGED defector directly tied to the Pegasus evidentiary chain, examined further under *DGST* below.

DGED's principal strength, on the open-source record, is its demonstrated capacity for discreet, Palace-backed security diplomacy in a region where conventional Western state influence has weakened, giving Morocco a mediation niche that generates diplomatic credit without requiring public acknowledgment of intelligence-service involvement; its principal constraints are the accumulating reputational cost of the European infiltration controversies and the Pegasus attribution controversy, both of which complicate DGED's relationships with the same European partners its Sahel mediation role is presumably meant to help cultivate, and the newly reported Hijaouy defection, which, if the allegations hold up, would represent a significant internal-security failure. Confidence in this profile is mixed rather than uniform: the founding history and leadership succession rest on consistent, if tertiary, sourcing and merit moderate-to-high confidence; current staffing and budget detail are a decade or more out of date and constitute an explicit gap; and the DGED-versus-DGST attribution for Pegasus specifically is the weakest-sourced, highest-stakes judgment in this profile, resting on a single investigative consortium's testimony that has not been independently replicated.

DGST

The Direction Générale de la Surveillance du Territoire (DGST) is Morocco's domestic counter-espionage and internal-security service, established by the same 12 January 1973 royal dahir that created the DGED, and renamed from its earlier DST designation in 2005 [27]. Unlike DGED, the DGST operates under Ministry of Interior supervision, with headquarters at Témara and a subordinate law-enforcement branch, the Bureau Central d'Investigations Judiciaires (BCIJ), based at Salé; its founding mandate covers counter-espionage, counter-terrorism and protection of economic and scientific assets, framed in its original dahir as preventing, through intelligence collection, activities inspired, undertaken or supported by subversive or terrorist movements [27]. Leadership succession runs from Ahmed Dlimi (1973-1983) through Driss Basri (1983-1999, who held the post concurrently with his long tenure as Interior Minister), Hamidou Laanigri (1999-2003) and Ahmed Harari (2003-2005), to Abdellatif Hammouchi, director since December 2005 [27, 29]. Hammouchi joined the service in 1993 at age 27, specialising early in analysis of Islamist and jihadist networks, and headed its counter-terrorism service after the 2003 Casablanca bombings before his 2005 promotion to the top post [29]. Since 15 May 2015 he has also directed the DGSN, Morocco's national police, a dual-hatting the open-source record consistently describes as unprecedented in the post-1999 Moroccan security apparatus [27, 29]. It is almost certainly the case that this concentration of domestic-intelligence and law-enforcement authority in a single official gives Hammouchi a degree of institutional control over Morocco's internal-security architecture with no direct European parallel (confidence: high), as already established under *The intelligence community* above.

A subordinate but institutionally significant structure beneath the director is the BCIJ, created in 2015 following legislation passed after the 2011 Marrakesh café bombing that granted DGST officers formal judicial-police status for the first time; the BCIJ functions as the DGST's law-enforcement arm while operating under Public Prosecutor's Office supervision for casework, a dual-reporting design that gives the DGST prosecutorial reach it did not previously possess [27]. Its first chief was Abdelhak Khiame, and by 2021 the BCIJ was credited with dismantling 86 terrorist cells and making 1,386 arrests since its 2015 inception, against a longer-run total of 213 cells dismantled since 2002, figures not updated in the material reviewed past that year [27].

The DGST's collection disciplines span signals intelligence, human intelligence and, since 2017 per contested but converging reporting, offensive technical collection via commercial spyware. Its signals-intelligence arm, the Police des Communications Radioélectriques (PCR), dates to the

1960s under Hassan II and reportedly intercepts thousands of daily communications, with technical capability as of a 2010 reference point including keyword search, speech-recognition and handwriting-recognition analysis, while a Groupe d'Intervention Rapide provides a special-operations raid capability [27]. The July 2026 Forbidden Stories consortium investigation adds a human-intelligence and insider-testimony layer largely absent from the tertiary compilations: a former DGST agent using the pseudonym Safir described distributing pre-infected Samsung Galaxy S6 Edge phones through phone shops in the Rif region and infiltrating internet cafés to target activists, under an internal programme the consortium's leaked documents label Op S6_Edge, dated 2017 [33].

The DGST's cyber role is the service most directly implicated, across the material reviewed, in Morocco's Pegasus programme, though the strength of that implication varies sharply by source and claim. The Forbidden Stories consortium names specific DGST personnel allegedly involved in spyware operations -- Abdeljalil Taki as department head, chief IT specialist Amine Labbardi, director Abdelaziz Brachmi, and Mohammed Raji, nicknamed the king's Mr Eavesdrop -- and dates the operational shift from Hacking Team's earlier Remote Control System software to Pegasus to September 2017, when Taki and Labbardi reportedly tested Pegasus on their own personal phones [33]. The same consortium's reporting on that original acquisition adds a further, distinct layer: under the internal codename Morgan, the licence was reportedly brokered through FSSYS Morocco, described as a subsidiary of the UAE-based Al Fahad/Edge-Etimad group, with NSO Group co-founder and then-chief executive Shalev Hulio said to have travelled to Morocco on an Israeli diplomatic passport in connection with the deal; the consortium itself flags the UAE-financing element as unclear and unconfirmed, and this report carries that qualification forward rather than treating the acquisition channel as established [40]. This is meaningfully more specific than either Citizen Lab's infrastructure-level ATLAS finding or Amnesty's device-forensic confirmations, neither of which names any Moroccan agency or individual [30, 31, 32], and it is likely (confidence: moderate) that operational control of the domestic Pegasus programme sits specifically with DGST rather than DGED, since that division rests on a single investigative consortium's sourcing that is detailed and internally consistent, but not yet independently replicated by a second outlet or confirmed by any forensic lab or judicial finding.

Table 6. Competing attribution questions in Morocco's Pegasus and Jabaroot record.

Attribution question	Competing positions	Best-sourced answer	Assessed confidence
Which service operationally controls the domestic Pegasus programme?	DGST (named personnel, Op S6_Edge) vs DGED (foreign-liaison/acquisition role)	DGST, per Forbidden Stories insider testimony and leaked documents	Moderate (single-consortium sourcing, not independently replicated)
Who is behind the Jabaroot/JabaROOT leak?	Algerian actor (self-description) vs an ex-Moroccan intelligence officer based in Germany vs five former DGST members in European exile (per Le Monde)	Not resolved; three mutually exclusive claims stand unadjudicated	Low (each claim single-sourced or unconfirmed)
How strong is the evidentiary basis for Moroccan Pegasus use overall?	Amnesty/Citizen Lab device- and infrastructure-level forensic findings (no agency named) vs	Forensic confirmation of Pegasus use is high-confidence; agency-level	High for use; low for agency attribution

Forbidden Stories
insider-testimony
agency and personnel
attribution

attribution rests on
testimony alone

DGST's foreign-facing Pegasus targeting, as distinct from its domestic use against journalists and activists, has directly damaged one of the service's own most important European liaison relationships: Forbidden Stories reports that a Pegasus account its sources link to the DGST targeted Colonel Alberto Aguilera -- Spain's Interior Attaché in Rabat from 2012 to 2017 and the Guardia Civil officer responsible for DGST counter-terrorism training curricula -- five times beginning 8 March 2019, with the Spanish-language edition of the same investigation naming DGST as the primary operating service while DGED appears only in a coordination role [34, 41]. It is likely (confidence: moderate) that this reflects a genuine DGST operation against a training partner, given the specificity of leaked documents and named sourcing including a former DGST officer, though the claim has not been independently corroborated by a second investigative outlet or confirmed by either government.

The same reporting places DGST at the centre of the 2021 targeting of Spanish Prime Minister Pedro Sánchez and members of his cabinet, alongside earlier French-minister targeting whose agency attribution is separately clouded by the likely DGSE/DGED transcription error noted under *DGED* above [10, 41]. Spain's Audiencia Nacional opened a judicial investigation into these infections in May 2022, archived it in July 2023 citing Israel's non-cooperation, reopened it in April 2024 following a French European Investigation Order, and archived it a second time on 22 January 2026, again for insufficient evidence, with the court's chief prosecutor reportedly rejecting the underlying evidence on the grounds that it did not concern Morocco; no Spanish court has ever formally attributed the intrusions to Morocco or any specific Moroccan agency, and Morocco has denied involvement throughout [42, 43]. September 2026 Spanish reporting on Hijaouy's alleged possession of the underlying Pegasus material suggests this evidentiary question remains genuinely live rather than closed, though every specific claim in that thread remains single-outlet and unverified [38, 39].

DGST's foreign liaison record extends well beyond the Guardia Civil training relationship, and includes credited 2015 warnings to French counterparts regarding Abdelhamid Abaaoud ahead of the November 2015 Paris attacks [27]. It is highly likely (confidence: moderate) that this liaison-warning function remains an active, valued channel for European partners despite the parallel Pegasus controversy, since European governments have continued security cooperation and even honoured Hammouchi personally -- Spain's Interior Minister presented him the Grand Cross of the Civil Guard's Order of Merit in November 2025 -- even after the 2021 Pegasus revelations were already public, a juxtaposition that itself signals how European partners have chosen to compartmentalise counter-terrorism-liaison value from spyware-abuse concerns rather than let the latter override the former [44].

Torture and rendition allegations connected to the Témara facility constitute the DGST's most persistent human-rights controversy: French judicial authorities attempted to summon Hammouchi personally in 2014 over torture complaints, including those of Sahrawi activist Naama Asfari and French-Moroccan citizen Adil Lamtalsi, and diplomatic immunity prevented his testimony, prompting Morocco to suspend judicial cooperation with France before resuming it in January 2015, after which France nonetheless promoted Hammouchi to Officer of the Légion d'Honneur the following month, a sequencing open sources do not explain [29, 44]. It is likely (confidence: moderate) that Rabat's willingness to suspend judicial cooperation over this episode reflects a broader pattern of using diplomatic leverage to shield senior security leadership from foreign legal

process, consistent with DGED's own French border-police and infiltration controversies discussed above.

The most recent and least resolved DGST-relevant controversy is the August 2026 Jabaroot leak of an alleged dataset covering more than 70,000 Moroccan security personnel, which the DGSN and DGST jointly and publicly denied represents any breach of their own systems, attributing it instead to older third-party insurance and social-coverage data [45]. Jabaroot's own identity is subject to three mutually exclusive attribution theories examined in the table above, none of which this analysis attempts to adjudicate; what can be said with higher confidence is that Jabaroot's leaked material has been used, in September 2026 Spanish reporting citing a Spanish national-police report submitted to Audiencia Nacional judge María Tardón, to implicate Hammouchi personally in facilitating a Ceuta border-crossing event, alongside a police assessment describing the crossing as requiring a high capacity of influence in networks and persons linked to Morocco's security forces without itself naming an agency or individual [14, 15]. It is roughly an even chance (confidence: low) that this reflects deliberate DGST-level tasking around the Ceuta crossing rather than incidental facilitation by lower-level contacts, and it should be treated as an unverified allegation pending corroboration.

DGST's principal strength is the integrated security-intelligence-law-enforcement continuum Hammouchi's tenure has built: a counter-espionage service with a formal judicial-police arm and, since 2015, direct top-level fusion with the national police, giving Morocco's internal-security apparatus a coordination depth that most peer services achieve only through inter-agency liaison rather than unified command. Its principal constraints are the accumulating reputational costs of the Témara torture allegations, the Pegasus programme's demonstrated capacity to damage even the DGST's closest European training partnership, and the unresolved Jabaroot leak, which, whatever its true origin, signals either a genuine personnel-data security failure or a sophisticated information operation against the service. Confidence in this profile should be read claim by claim: founding history, Interior Ministry subordination, the BCIJ's creation and Hammouchi's leadership timeline rest on consistent sourcing and merit moderate-to-high confidence; PCR technical-capability detail and BCIJ cell-dismantlement statistics are dated; and the named-personnel detail behind the domestic Pegasus programme rests entirely on one investigative consortium's insider-testimony sourcing, the single largest evidentiary gap given how much analytic weight the DGST-versus-DGED attribution question carries.

Relevant DGSN intelligence functions

The DGSN is, first and foremost, Morocco's national civilian police force, established on 16 May 1956 under Dahir n° 1-56-115 to replace the colonial-era Police Chérifienne, and its relevance to this chapter rests specifically on one of its seven constituent directorates -- Judicial Police, Public Security, Information Systems and Communication, General Intelligence (Renseignements Généraux), Human Resources, Equipment and Budget, and Royal Palace Security -- namely the Direction des Renseignements Généraux, which gives the DGSN its own domestic information-collection function [28]. That function runs alongside, and since May 2015 is coordinated at the top with, the DGST's counter-espionage mandate through the person of Abdellatif Hammouchi, director of both services simultaneously [28, 29]. It is almost certainly the case that this fusion removes an institutional separation between ordinary police intelligence-gathering and counter-espionage or domestic-security intelligence that exists, at least nominally, in most European systems, including Spain's own division between the CNI and the Policía Nacional and Guardia Civil (confidence: high), since no source located identifies any comparable single-official fusion among Morocco's principal partners.

Staffing and budget figures for the DGSN as a whole -- approximately 78,146 personnel as of 2021 and an annual budget of roughly MAD 13 billion as of 2022 -- are considerably more recent than

the comparable DGED and DGST figures set out above, but open sources provide no breakdown specific to the General Intelligence directorate's own staffing, budget or leadership [28]. This is an explicit and analytically significant gap: the directorate whose fusion with DGST does the most to concentrate Moroccan domestic intelligence authority is also the one about which open sources say the least regarding its internal organisation or output.

The clearest documented point of operational fusion between DGSN and DGST beyond the leadership level is that the BCIJ's organised-crime unit operates under joint supervision with the DGSN's own National Judicial Police Brigade, alongside a separate counter-terrorism unit under direct DGST direction [27]. It is likely (confidence: moderate) that this dual-unit design reflects a deliberate effort to route counter-terrorism casework through the more intelligence-oriented DGST chain while keeping conventional organised-crime casework under DGSN's ordinary judicial-police structure, since the split tracks the two services' respective core mandates rather than appearing arbitrary.

DGSN's most visible recent cyber-adjacent initiative is the E-blagh digital citizen-reporting platform, launched in October 2024, which allows the public to report online content assessed as criminal or violent, scoped explicitly to terrorism incitement, threats to minors and data-protection violations, and credited with processing 7,083 notifications as of that month [28]. This is a content-moderation and citizen-reporting tool, not evidence of an offensive or technical cyber-investigation capability, and no source located describes any DGSN technical cyber-investigative unit comparable to the DGST's PCR signals-intelligence directorate. It is likely (confidence: moderate) that this reflects a genuine division of labour in which offensive and technical cyber-collection sits with DGST, and defensive cybersecurity with the civilian DGSSI/maCERT authority, rather than with DGSN, since reporting on Moroccan cyber capability collected across this project consistently concentrates on those other bodies rather than on DGSN.

The most consequential recent development touching DGSN's intelligence-relevant leadership is the September 2026 allegation, examined in full under *DGST* above, that Hammouchi -- in his capacity spanning both DGSN and DGST -- played a personal role in facilitating the Ceuta border-crossing event; the underlying Spanish police assessment is worded in capability terms, describing the crossing as requiring a predefined process with objectives different from migratory ones, without itself naming Hammouchi, DGSN or DGST specifically, and the personal attribution in Spanish press coverage derives from combining that language with Jabaroot's own separate and independently unverified claim [14]. It is roughly an even chance (confidence: low) that this reflects genuine personal direction by Hammouchi rather than lower-level facilitation that press reporting has attached to Morocco's most visible security official by association, and this should be treated as a serious but unproven allegation.

DGSN's principal strength, for the intelligence functions relevant to this profile, is scale: a personnel base an order of magnitude larger than either DGED or DGST gives its General Intelligence directorate a domestic collection reach that neither of the two dedicated intelligence services can match on numbers alone. Its principal constraint is opacity: unlike DGST and DGED, which each generate periodic press-visible controversies that at least partially illuminate their activity, the General Intelligence directorate specifically has generated almost no independent open-source reporting on its methods, output or current leadership, leaving its actual contribution to Morocco's domestic intelligence picture essentially unassessable from the material reviewed. Confidence in this section should therefore be read as high for the institutional and structural facts -- founding, staffing scale, the Hammouchi dual-hat fusion, the E-blagh platform's narrow scope - - and explicitly low to unassessable for anything concerning the General Intelligence directorate's actual operational activity, which constitutes the clearest single gap in this profile.

Law enforcement and internal security

Beyond the DGST/DGSN intelligence fusion profiled in the previous chapter, Morocco's internal-security apparatus rests on four distinct forces with overlapping but formally separate mandates: the DGSN as national civil police, the BCIJ as the DGST's judicial-police arm for counter-terrorism, the Royal Gendarmerie as a militarised rural and highway police force, and the Auxiliary Forces as a general-purpose reserve for public order, disaster relief and support to the other three [46, 47, 48, 49]. The clearest recent evidence that these bodies function as parallel rather than hierarchically linked institutions is operational rather than doctrinal: at the 15 August 2026 mass migrant-crossing attempt at the Ceuta border fence, DGSN, Royal Gendarmerie and Auxiliary Forces personnel operated side by side using helicopters, ground units and containment tactics, the single clearest documented instance of all three domestic security institutions deploying jointly at one event [13, 50].

No primary source describing the operational-coordination protocol linking these institutions' own prefectural chains to the walis and governors who formally head each wilaya's civil administration was identified in this research, and that absence is recorded as an explicit structural gap rather than inferred from the administrative hierarchy alone [51]. The table below gives a comparative institutional snapshot before the individual profiles, which give particular attention to how each force relates to the FAR, the Ministry of Interior and the DGST/DGSN fusion, since it is precisely at those seams that Moroccan internal security is least documented in open sources.

Table 7. Morocco's four internal-security forces at a glance.

Agency	Founded	Reports to	Current leadership	Personnel / budget	Primary mandate
DGSN	16 May 1956 (Dahir n° 1-56-115)	Ministry of Interior	Abdellatif Hammouchi (since 2015; also DGST director)	~79,830 personnel (2023); MAD 13bn budget (2022)	Civil policing, judicial police, border control, General Intelligence
BCIJ	2015 (post-Marrakesh-bombing law)	DGST (judicial-police arm); Public Prosecutor's Office for casework	Cherkaoui Habboub / Haboub Cherkaoui (since ~2021; low-confidence continuity to 2026)	Not identified in open sources (no current headcount located)	Counter-terrorism and organised-crime judicial-police investigation
Royal Gendarmerie	29 April 1957 (Dahir n° 1-57-079)	FAR (military status); Justice (judicial police); Interior (administrative police)	Min.-Delegate Abdellatif Loudiyi (admin.); General Haramou (field commander) - appointment	Sources disagree: ~75,000 (one source) vs. ~25,000 (another) -- unresolved threefold gap	Rural/highway policing, maritime interdiction, border and coastal security

			dates not identified		
Auxiliary Forces	Reorganised 2018 (Dahir n° 1.17.71); older lineage undocumented	Ministry of Interior	Col.-Maj. Mustapha Hdioud (South, since Oct. 2020); Gen. Khaled Jabrane (North, since Oct. 2020)	Not identified in open sources (no personnel or budget figure located)	Public-order support, disaster relief, no judicial-police function

DGSN

The Direction Générale de la Sûreté Nationale, Morocco's national civilian police, was established on 16 May 1956 following independence under King Mohammed V and remains headquartered in Rabat under Ministry of Interior authority [46]. Leadership has passed through a documented, unbroken sequence of directors-general — Hamidou Laanigri (2003-2006), Charki Draiss (2006-2012), Bouchaib Rmail (2012-2015) and Abdellatif Hammouchi, who has held the post since 2015 and continues to direct the DGST concurrently, the personal fusion this report's *intelligence community* chapter treats as Morocco's clearest coordination fact [46, 52]. Beneath this national leadership sits at least one named sub-national post, director of public security, held until August 2026 by El Hail Zitouni across a four-decade career that included commanding a 2024 Marrakech operation involving 1,200 officers, 2,956 arrests and 415 vehicle seizures; Zitouni's death left the post vacant, and no successor had been identified in open sources as of this collection, a structural gap this report records explicitly rather than assumes resolved [53].

DGSN's own tertiary-sourced organisational description asserts three specialist divisions — a Border Police, a Mobile Intervention Corps and a National Brigade handling serious-crime investigation including terrorism and white-collar offences — though no single primary citation for this exact structure was located, so it is held at moderate rather than high confidence (confidence: moderate) [46]. A more granular layer is independently corroborated at regional level: the Agadir Security Directorate's August 2026 launch of an eighth regional explosives-disposal brigade, following equivalents at Rabat, Casablanca, Fez, Tangier, Oujda, Marrakech and Laâyoune, confirms that specialist units report through regional security prefectures rather than directly to national headquarters, and that this rollout extends into Western Sahara via the Laâyoune unit [54]. Personnel strength was reported at approximately 79,830 in 2023, up from roughly 46,000 in 2007 and 70,000 in 2017, on an annual budget of MAD 13 billion for 2022 [46, 52]. It is likely that DGSN is pursuing a genuine, resourced technology-modernisation programme rather than a purely rhetorical one, given the July 2026 Casablanca deployment of AI-equipped Amane and Madar patrol vehicles carrying automatic number-plate recognition and facial recognition (confidence: moderate, since the cited performance figures are DGSN/vendor-supplied and were not independently tested) [55].

DGSN's cyber role remains thin in the open-source record: the only concretely documented function is E-blagh, a citizen-facing digital platform for reporting criminal or violent online content, with no detail located on a dedicated internal cybercrime investigative brigade, its staffing or its caseload, an absence read as a stated collection gap rather than evidence that no such capability exists, particularly since dgsn.gov.ma itself was unreachable on repeated attempts across this and the prior collection round [52]. Foreign partnerships are better documented: Morocco's INTERPOL National Central Bureau in Rabat has operated since 17 June 1957, the oldest and

broadest multilateral channel identified across this collection, and an October 2025 joint operation with the Spanish National Police, triggered by a DGSN-originated tip-off, seized over 22 tonnes of hashish concealed in refrigerated produce trucks across Cádiz and Granada provinces [56, 57]. A further set of 2024-2026 partnership claims with France, the United Kingdom, the French insurer ARGOS and the FBI rests on a single tertiary source not cross-checked against any French, British or US primary release, and is treated as likely accurate in broad outline but unconfirmed in detail (confidence: low) [52].

DGSN's principal documented strengths are a sustained personnel and budget growth trajectory, an active technology-modernisation programme, and a specialist-unit rollout that now extends into Western Sahara, indicating the institution's administrative reach matches Morocco's full claimed territorial extent. Its most concrete constraint is the leadership gap at the sub-national director-of-public-security level following Zitouni's death, alongside a broader pattern in which several structural claims rest on single tertiary sources rather than primary DGSN documentation, itself unreachable throughout this collection. It is highly likely that DGSN's core civilian-policing and judicial-police functions are accurately described in outline by the sources reviewed (confidence: high, given convergent independent press and encyclopaedic accounts), but its precise divisional structure, cyber capability and the durability of its newest foreign partnerships should all be treated as low-to-moderate confidence pending primary-source access this research could not obtain.



Figure 3. The DGSN emblem, traced from the service's own 2021 annual report.

The emblem is a police-badge-shaped shield surmounted by a royal crown, itself topped by a small five-pointed star, echoing the Moroccan royal crown used across state institutional insignia to denote the monarchy's authority over the security services; the main red field bears a large green five-pointed star, the same Seal-of-Solomon-style pentagram found on the national flag, with a stylised Arabic letter beneath it, and the shield's green border carries a white laurel motif on each side [58]. No official DGSN text explaining the specific heraldic meaning of these elements was located in the sources reviewed; the description above is a factual visual inventory rather than a sourced symbolic gloss, and the letter beneath the star is recorded as an unconfirmed abbreviation rather than a stated one.

BCIJ

The Bureau Central d'Investigations Judiciaires was founded in 2015 pursuant to a law passed in the wake of the 28 April 2011 Marrakesh (Djemaa el-Fna/Argana café) bombing, granting DGST officers judicial-police standing for the first time, and is headquartered at Salé [47]. Structurally the bureau sits subordinate to the DGST — Morocco's domestic intelligence service — while operating under Public Prosecutor's Office supervision for judicial-investigation purposes; the same tertiary source describes an internal split between an elite counter-terrorism division

overseen directly by the DGST and an organised-crime unit supervised instead by DGSN's own National Judicial Police Brigade, a cross-institutional linkage carried here at moderate rather than high confidence given its single sourcing [47]. This places the BCIJ's legal and administrative position squarely within the domestic-intelligence chain rather than the ordinary police hierarchy, and no operational or command relationship between the BCIJ and the FAR was identified in any source reviewed, consistent with its explicitly civilian, judicial-police character.

Leadership has passed through at least two, and very likely three, named individuals since 2015. Founding chief Abdelhak Khiame led the bureau from its creation until his death in August 2022 [47]. An October 2021 interview names Haboub Cherkaoui as the sitting head of the BCIJ at that date — meaning he had already succeeded Khiame before Khiame's death — and a French Wikipedia snapshot last edited 15 April 2026 names Cherkaoui Habboub, the same name reordered, as the article's current director [59, 60]. It is likely that Cherkaoui/Habboub remained BCIJ chief through the first half of 2026 (confidence: low), since this rests on a single tertiary source with no independent press confirmation of continuity, and the name-order variation across the two sources is flagged rather than silently resolved.

On statistics, the bureau's own reporting credited it with 91 dismantled cells and over 1,400 people referred to justice since 2015 as of March 2023, roughly 85% ISIS-affiliated, against the DGST's own longer-run total of 213 cells dismantled since 2002; neither figure has been updated in the sources reviewed past that date [47, 60]. A directly dated April 2026 operation nonetheless demonstrates continued tempo: a six-member cell was dismantled across Kenitra, Casablanca, Dar El Gueddari and Sidi Taibi, framed by BCIJ/DGST statements as engaging in theft, burglary and money laundering under an ideological legitimisation-of-loot justification, targeting rural livestock farms for resale through local markets [61]. It is likely that the BCIJ continues to fold ordinary organised-crime predicate offences into terrorism-labelled casework whenever an ideological veneer is alleged (confidence: moderate, based on this single but detailed 2026 case), a pattern blurring the line between its counter-terrorism and organised-crime mandates even where its internal unit structure formally separates them.

Foreign partnerships are comparatively well documented for the BCIJ. A November 2024 joint operation with Spain's *Comisaría General de Información* (CNP) arrested nine suspects across Tetouan, Fnideq, Madrid, Ibiza and Ceuta, described in Moroccan press as part of long-standing exceptional security collaboration and building on prior June and July 2024 joint actions [62]. A separate tertiary compilation additionally cites DGST contact with Germany's BND regarding Anis Amri before the December 2016 Berlin attack, DGST information-sharing with French authorities on Abdelhamid Abaaoud's whereabouts before the November 2015 Paris attacks, a 2022 Qatar-Morocco security declaration tied to the FIFA World Cup, and an October 2022 Morocco-Germany agreement covering organised crime, terrorism, human trafficking, cybercrime and fraud [47]. No confirmed formal BCIJ-Europol or BCIJ-CNI(Spain) instrument was identified, and the Amri/Abaaoud episodes are attributed in the source itself to the DGST at the intelligence level rather than to the BCIJ as executing judicial-police body, a distinction this report preserves rather than collapses.

One BCIJ leadership statement in this record carries a specific denial/deception flag: in an October 2021 interview at BCIJ headquarters, Cherkaoui stated that the Polisario Front is an important supplier of jihadists, alongside claims about a thwarted Tangier plot and Sahel-region ISIS expansion [59]. This is a single-source, politically charged assertion from an official whose institution has an evident interest in delegitimising Morocco's principal Western Sahara adversary, and it should be read as a stated official narrative rather than an independently corroborated fact; no other source in this collection corroborates or contests it. No dedicated internal BCIJ cyber capability was identified beyond a passing reference to cybercrime within the broader October

2022 Germany cooperation agreement, an absence recorded as an explicit gap rather than assumed non-existence [47].

The BCIJ's principal documented strength is a decade-long, incrementally growing record of cell dismantlement corroborated across independent compilations and at least one directly dated 2026 operational case, together with the most concretely evidenced multi-country liaison network — Spain, Germany, Qatar — of any institution profiled in this chapter. Its principal constraints are an unconfirmed current leadership identity resting on a single low-confidence source, an evident susceptibility to politicised public framing, and no reachable primary web presence or officially published statistics beyond the March 2023 figure. It is highly likely that the BCIJ remains DGST's operationally active judicial-police arm for counter-terrorism through 2026 (confidence: high, given the dated April 2026 operation), but confidence in its precise leadership, internal unit strength and cyber capability remains low. On emblem: no distinct, officially published BCIJ emblem was identified; the only logo circulating online is a self-published Wikimedia Commons graphic credited to an anonymous editor with no citation to any BCIJ or DGSN publication, consistent with the BCIJ operating as an emanation of the DGST/DGSN structure rather than maintaining a separately branded identity [63].

Royal Gendarmerie

The Gendarmerie Royale was founded on 29 April 1957 under King Mohammed V (Dahir n° 1-57-079), with a follow-on operational-framework Dahir n° 1-57-280 of 14 January 1958 setting out its detailed organisation; an attempt to retrieve this founding dahir's full primary text via refworld.org returned an HTTP 403 error in this research, leaving the text itself unverified and its provisions known only through a tertiary summary [48, 64]. That summary describes the Gendarmerie as explicitly a military force in structure, administration and command, subordinate to the FAR and staffed by commissioned officers and NCOs, while its mandate divides into judicial-police functions under Ministry of Justice supervision and administrative-police functions — border security, traffic control, port and airport protection, illegal-fishing enforcement — under Ministry of Interior oversight, layered atop its FAR chain through the Secretary-General for the Defence Administration [48, 64]. This dual civil/military legal character distinguishes it sharply from both DGSN's purely civilian policing and the Auxiliary Forces' purely Interior Ministry status.

Its territorial structure comprises a General Headquarters overseeing 22 Regional Gendarmeries, 64 Companies and 322 posts, supplemented by Mobile, Air and Maritime Gendarmerie divisions and a special-intervention unit, the GSIGR; these specific figures are asserted without a clearly dated primary citation and are held at moderate rather than high confidence pending direct verification against a Bulletin Officiel or Gendarmerie-issued document, which this research did not obtain [48]. Personnel figures carry a genuine, unresolved discrepancy that this report flags rather than resolves: one source gives roughly 75,000 personnel, while a separate tertiary compilation gives only about 25,000 for what should be the same institution, a threefold gap neither source's own sourcing allows this report to adjudicate [48, 65]. Current named leadership comprises Minister-Delegate Abdellatif Loudiyi, responsible for National Defence administration matters touching the Gendarmerie, and a General Haramou as field commander; no appointment date, tenure length or predecessor for either post was identified in this research, and this absence is recorded as a gap rather than filled by inference [48].

No subordination between the Gendarmerie and the DGSN or DGST was identified in this research, consistent with the three bodies operating as parallel rather than hierarchically linked institutions; the clearest documented instance of inter-institutional coordination is again the 15 August 2026 Ceuta border operation, where Royal Gendarmerie helicopter surveillance and ground units operated alongside DGSN and Auxiliary Forces personnel at the same event [13, 50].

A named maritime sub-unit with a defined area of responsibility, the Royal Maritime Gendarmerie of M'diq, separately intercepted an inflatable boat carrying thirteen Bangladeshi migrants in October 2025, evidencing operational-level command granularity below the regional-command layer [66]. A July 2026 interdiction off Tarfaya, in the Laâyoune-Sakia El Hamra region, seized over three tonnes of cocaine transferred at sea from an offshore vessel to inflatable boats before landfall — the clearest 2026 evidence that the Gendarmerie's maritime counter-narcotics role now extends to Atlantic-transiting cocaine near Western Sahara, not solely the cannabis/hashish trade more commonly associated with Morocco [67]. This suggests, with moderate confidence, that the Gendarmerie functions as Morocco's lead institution for at-sea narcotics interdiction specifically, complementing DGSN's more land-based, cross-border cooperation role on hashish.

Two independently reported judicial cases document narco-corruption as a recurring, rather than isolated, institutional vulnerability within Gendarmerie ranks. In Beni Mellal, 37 gendarmerie officers faced trial for accepting bribes to protect a drug trafficker's operations, with the trafficker admitting to payments both directly and through intermediaries, though no verdict had been reported as of the article's March 2025 publication or located elsewhere in this collection [68]. Separately, in the El Borouj/Beni Meskine district, seven gendarmes were ordered detained in January 2025 on charges of concealing a drug baron's criminal activity prior to a murder the baron allegedly committed against a former associate [69]. It is likely that narco-corruption represents a recurring rather than one-off institutional constraint on the Gendarmerie (confidence: moderate), given these two independently reported, geographically distinct prosecutions within roughly a two-year span, though both rest solely on press reporting of unresolved judicial proceedings rather than a final adjudicated record.

A further documented constraint is the Gendarmerie's exposure to domestic unrest at the level of individual rural posts: in October 2025, a Royal Gendarmerie post at Lqliaa, near Agadir, was attacked during Gen Z 212-linked protests by a crowd reported at over 200, including armed minors, resulting in three deaths and eight injured gendarmes, with Public Prosecutor Abderrazak Fattah attributing the gendarmes' use of service weapons to self-defence after warning shots [70]. No independent, non-official corroboration of the self-defence framing or the precise casualty figures was located, so this incident is carried forward as single-sourced to the prosecutorial account rather than as an independently verified fact. On technical and human resources, foreign partnerships and cyber role, this research is genuinely thin: no dedicated cyber capability was located for the Gendarmerie specifically, and the only documented multilateral affiliation is membership in FIEP, the international association of gendarmeries and police forces with military status, since 1999 [48]. These are recorded as explicit gaps rather than assumed to mirror DGSN's or the BCIJ's more developed partnership records.

Overall, the Gendarmerie's core documented strength is a broad, multi-domain territorial and maritime footprint evidenced by concrete 2025-2026 operations spanning cocaine interdiction, migrant-smuggling interception and rural public-order response, while its most concrete constraints are recurring narco-corruption allegations and demonstrated vulnerability of static posts to crowd violence — both judgments held at moderate confidence given reliance on press reporting of still-unresolved proceedings. The unresolved personnel-count discrepancy compounds this uncertainty, leaving any assessment of the force's true capacity and density genuinely open.



Figure 4. The emblem associated with the Gendarmerie Royale in open sources (provenance caveat below).

The image depicts a hexagonal shield topped by a royal crown, flanked by two stylised serpents or cords wrapped around the shield's frame, with Arabic script fragments around the border reading in part royal and the king, and a green five-pointed star with a red centre at its heart, surrounded by radiating gold lines [71]. Unlike the DGSN, Royal Guard and Auxiliary Forces emblems in this report, this file's own Wikimedia Commons record does not cite an official government or recruitment source, so its authenticity as a precise reproduction of the Gendarmerie's real insignia cannot be independently confirmed from the source record alone; it is presented here as the image long used for this purpose on Wikipedia rather than as a verified official file, and no official explanation of its heraldic elements was located.

Auxiliary forces

The Forces Auxiliaires are described in open secondary sources as an old corps within Morocco's security apparatus, operating under Ministry of Interior authority, though no founding date or pre-2018 institutional lineage was corroborated by any primary or reliably-graded source located in this research, and this report records that absence explicitly rather than supplying an unsourced founding narrative [49]. What is well documented is a 2018 legal reorganisation: King Mohammed VI, acting as supreme commander and chief of staff of the FAR, approved a restructuring plan at a 22 January 2018 Council of Ministers meeting, later given legal form as Dahir n° 1.17.71 of 15 February 2018, replacing earlier 1973 and 1976 texts [49, 72]. Two implementing décrets dated 6 March 2018 were independently confirmed at Morocco's official mmsp.gov.ma legal-texts portal — Décret n° 2.17.827, reorganising the force's officer/cadre training school, and Décret n° 2.17.825, governing the organisation of its central and regional administrative services — the clearest primary-source corroboration obtained anywhere in this chapter [73].

Command is structurally bifurcated rather than singular: two General Inspectorates, a Northern Zone based at Rabat and a Southern Zone based at Agadir, sit above three functional components — territorial units providing local administrative and security presence, mobile intervention units for public-order and border-security response, and support units for logistics [49]. Both inspector-general posts changed hands on 22 October 2020: Colonel-Major Mustapha Hdioud took the Southern Zone, replacing the retiring General Lahcen Imejane, while General Khaled Jabrane took the Northern Zone, replacing General Mostafa Mestour, with both incoming officers drawn directly from FAR command postings rather than an Interior Ministry-internal career track [74]. A tertiary snapshot last edited 18 August 2026 still names the same two officers as zone commanders, suggesting, with moderate confidence, roughly six years of continuity in this leadership pairing, and no single national commander-general above the two co-equal zone inspectors was identified in any source reviewed [49].

The force's mandate centres on public-order maintenance in support of territorial administrators, administrative support functions and disaster-relief assistance, with no judicial-police or investigative function of its own [49]. Its legal position places it under the Ministry of Interior rather than the FAR chain, notwithstanding that both current zone commanders are FAR-origin general officers, and command and control specifically vis-à-vis the walis and governors it is mandated to support was not detailed by any source reviewed beyond the general statement of that supporting role — a gap compounding the identical wali-coordination silence already noted for DGSN [49, 51]. The only directly dated 2026 operational evidence for the Auxiliary Forces specifically is their participation, alongside DGSN and the Royal Gendarmerie, in the response to the 15 August 2026 mass migrant-crossing attempt at the Ceuta border, the clearest documented instance of all three domestic security institutions operating jointly at one event [13]; no independent operation distinct from this joint deployment was located, which is itself consistent with, though does not prove, the force's characterisation as a support rather than an independently initiating institution.

Technical and human resources, cyber role and foreign partnerships are the three checklist items on which this research is most clearly thin for the Auxiliary Forces specifically: no personnel-strength total, budget figure or equipment inventory was located, no cyber capability of any kind was identified, and no named foreign liaison partnership was identified, in clear contrast to DGSN's INTERPOL and Spain-facing record and the BCIJ's Spain/Germany/Qatar record [73]. This asymmetry is treated as a genuine structural feature — a domestic public-order support force would not obviously require such partnerships — rather than as an artefact of incomplete search, though it cannot be fully distinguished from the latter on the evidence available. The force's principal documented strength is a clearly dated, King-directed 2018 modernisation with corroborated primary legal texts and stable, continuous zone-command leadership since October 2020; its principal constraint is the near-total absence of open-source detail on its size, budget, technical capacity and external partnerships, which limits any assessment of its operational weight relative to DGSN and the Gendarmerie beyond the single documented joint deployment.

It is likely that the Auxiliary Forces functions as intended — a Ministry of Interior-controlled, FAR-officered public-order support corps operating under territorial civil administrators — rather than as an independent security actor with its own investigative or foreign-liaison profile (confidence: moderate, based on the consistent absence of contrary evidence), though this judgment rests substantially on an absence of evidence rather than a strong positive record, and is recorded as such.



Figure 5. The Auxiliary Forces emblem, sourced to an official Inspection Générale des Forces Auxiliaires recruitment announcement.

The badge is a shield surmounted by a royal crown, with two crossed spears or tridents behind it; the shield's red field bears a green five-pointed star in the same Seal-of-Solomon style seen on the national flag and other security-service emblems, and a scroll beneath reads God, Homeland, King, Morocco's official national motto [75]. No official Forces Auxiliaires document explaining the

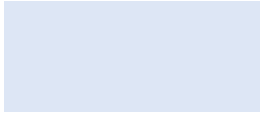
specific heraldic meaning of the crossed spears was located in the sources reviewed; the crown, star and national motto are consistent with widely used Moroccan state-security iconography, but the spears' specific significance is not documented and is not speculated on here.

Armed Forces and military intelligence

The Forces Armées Royales (FAR) are Morocco's unified national military, and King Mohammed VI holds the constitutional title of Supreme Commander and Chief of the General Staff, a role the Palace treats as substantive rather than ceremonial [65, 76]. Day-to-day administration runs through a Minister Delegate for the Administration of National Defence — Abdellatif Loudiyi has held this post continuously since December 2010 — since Morocco maintains no conventional Ministry of Defence, an arrangement that keeps the institution answering upward to the Palace rather than to any elected government [65]. It is highly likely that this dual structure — a royal command apex over a civilian-administered but Palace-loyal defence bureaucracy — remains the single most important fact for understanding how FAR is actually run, more so than any branch-level order of battle (confidence: high), since every other structural claim collected is consistent with it and none contradicts it. The table below gives a comparative snapshot of FAR's most structurally distinctive bodies before the individual profiles that follow.

Table 8. Four structurally distinctive Armed Forces bodies compared.

Body	Command relationship	Personnel (reported)	Key leadership	Primary role
FAR command architecture	Under the King as Supreme Commander; Minister-Delegate Loudiyi (administration)	Army ~175,000-250,000; Air Force ~13,000-16,000; Navy ~7,800-12,000 (sources diverge)	Lt. Gen. Mohamed Berrid, Inspector General since 22 April 2023	Conventional national defence and force employment
2nd and 5th Bureaux	Numbered bureaux attached to the FAR General Staff (unconfirmed reporting line)	Not identified in open sources	Not identified in open sources (no confirmed current chief for either bureau)	Military intelligence (2nd Bureau, asserted); internal counter-intelligence (5th Bureau, asserted)
Royal Guard	Contested: nominally an FAR branch; one source cites direct Royal Household control; another describes an autonomous FAR-internal corps	~6,000 (1999-era figure; not updated since)	Not identified in open sources (current commander unconfirmed; one source's named commander itself carries a citation-needed flag)	Personal protection of the King and royal family; ceremonial escort duties
Military regions / Western Sahara posture	Zone Sud (Southern Zone) territorial command; no current full zone structure identified	Up to ~100,000 troops in the Western Sahara theatre (indicative figure)	Historically Ahmed Dlimi as "Commandant de la Zone Sud" (1975-76, 1980-83); no current	Western Sahara territorial defence; garrison of the Moroccan Wall/Berm



successor
designation
identified

Collected figures on FAR's size, budget and supplier mix diverge sharply across not two but three distinct source streams, and this divergence is itself analytically significant rather than a nuisance to smooth over. English-language sourcing gives 196,000 active personnel and a 2026 defence budget of USD 15.7 billion (8.5% of GDP), while French-language sourcing gives 235,000 personnel across five branches and a 2025 budget of USD 13.3 billion (4.28% of GDP) [65, 77]. A third, materially larger personnel figure appears in a Spain-focused defence-assessment relay of an analysis referred to in that reporting only as GEOPOL 21: roughly 400,000 active personnel plus 250,000 reservists, more than double the English-language active count, set against a reported Spanish strength of approximately 120,000 active and 15,000 reserve; the same relay carries a set of UAV, loitering-munition and precision-strike range claims (Bayraktar Akıncı, TB2, Wing Loong, Harop/Harpy, EXTRA-family rockets and ATACMS) that its own authors flag as partly unconfirmed and that read as maximum advertised rather than demonstrated employment ranges [18]. On budget specifically, a separate IISS-attributed figure relayed via a lower-tier aggregator gives Morocco's defence spending at USD 7.51 billion in 2025 rising to a reported record USD 7.87 billion in 2026, with GDP share around 4% — essentially half the English-language \$15.7bn/8.5% figure and, for the same 2025 year, also well below the French-language \$13.3bn figure [16]. It is likely that the true current personnel and budget figures sit somewhere within this now three-way rather than two-way spread, and that all three streams draw on outdated, partial or methodologically distinct estimates rather than a Moroccan government primary disclosure (confidence: low), since Morocco does not publish a fully itemised defence-budget breakdown in any source reviewed; any single-sourced FAR personnel or budget figure — English-language, French-language or Spain-focused — should be treated as indicative only until corroborated against an authoritative order-of-battle source such as IISS's own Military Balance, which this research could not directly access despite an IISS attribution surfacing at second hand in one of the three streams. This three-way conflict is flagged here rather than resolved, consistent with this report's general practice of stating discrepancies explicitly instead of silently picking a preferred figure.

On suppliers, French-language sourcing specifies a 2025 split of United States 60%, Israel 24% and France 10%, broadly consistent with reported recent acquisitions: Apache AH-64E attack helicopters from the United States (24 ordered, 6 delivered March 2025), Tata WhAP 8x8 armoured vehicles, and Chinese HQ-9 air-defence systems as a secondary-supplier diversification [65]. It is highly likely that Morocco continues to prioritise a US-France-Israel core supplier base while adding limited Chinese systems for air defence (confidence: moderate), a judgment resting on a single tertiary source's supplier percentages that could not be cross-checked against an independent arms-transfer database in this research — a concrete follow-up item for any future collection pass on this topic.

FAR command architecture

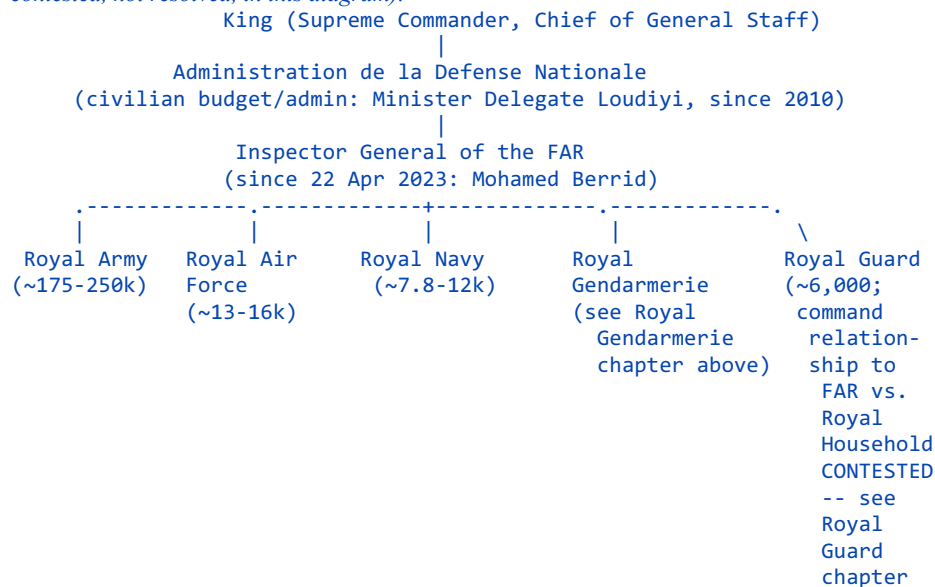
FAR comprises five branches under the King as Supreme Commander: the Royal Army, Royal Air Force, Royal Navy, Royal Gendarmerie and Royal Guard, with a Lieutenant General serving as Inspector General — Mohamed Berrid has held this post since 22 April 2023 — acting as the senior uniformed officer beneath the King [65, 77]. FAR headquarters sits on Rue Farhat Hachad in Rabat [65]. Branch-level personnel estimates diverge between the two tertiary sources collected — Army 175,000-250,000; Air Force 13,000-16,000; Navy 7,800-12,000 — and it is roughly an even chance that the higher French-language figures reflect nominal or paper strength including

reservists while the English-language figures reflect active-only strength (confidence: low), a plausible but unconfirmed reconciliation that a more authoritative order-of-battle source would need to settle.

The Royal Gendarmerie, profiled above, holds full military status within this architecture, established by Dahir n° 1-57-079 of 29 April 1957 with a follow-on operational-framework Dahir n° 1-57-280 of 14 January 1958 that reportedly remains its founding legal basis, and it uniquely answers to civilian ministries for specific mission sets — judicial-police functions to the Ministry of Justice, administrative-police duties to the Ministry of Interior — even while remaining military in status and subordinate to the FAR chain through the Secretary-General for the Defence Administration [64]. On formal military-region organisation more broadly, this research located no current list of FAR's régions militaires from any source reviewed. The only concrete historical anchor identified is Ahmed Dlimi's title Commandant de la Zone Sud (Commander of the Southern Zone), which he held twice — November 1975-May 1976 and March 1980-January 1983 — while directing FAR operations against the Polisario Front after the 1975 Green March [78].

It is unlikely that Zone Sud survives today as the operative designation for Morocco's Western-Sahara-facing command given the intervening decades of reorganisation (confidence: low), but no current successor designation was identified in this research, and this is logged as an explicit structural gap rather than resolved by inference. The figure below sets out FAR's command architecture in the form that can be stated with confidence, leaving the Royal Guard's precise reporting line marked as contested rather than forcing a resolution the sources do not support; that contradiction is examined in full under *Royal Guard* below.

Figure 6. FAR command architecture, so far as open sources allow it to be stated with confidence (the Royal Guard's reporting line is contested, not resolved, in this diagram).



FAR's principal documented strength, on this architecture, is a clear and consistent command apex — the King as Supreme Commander, an Inspector General as senior uniformed officer, and a civilian Minister Delegate handling administration without an elected minister of defence — corroborated across every source reviewed. Its principal constraint is the same one already flagged for personnel and budget figures: the near-total absence of a current, authoritative FAR order-of-battle or territorial-command document, which leaves military-region structure, Zone Sud's current institutional survival, and the precise branch-strength figures all resting on tertiary sources with materially different numbers. The clearest confidence and intelligence gap in this section is the current territorial-command structure itself, on which this research found nothing more recent than Dlimi's 1970s-80s Zone Sud title. A separate, independently conducted review of Morocco's naval posture, Strait-of-Gibraltar presence and NATO Mediterranean Dialogue engagement, carried out

on 10 September 2026, corroborates rather than closes this same gap: it likewise located no hull-by-hull naval order of battle, no patrol-pattern detail and no bilateral or NATO-channel exercise activity for the reporting window, beyond a bare mention of FREMM frigates as a modernisation line. This convergence across two independent research passes raises confidence (confidence: high) that the absence of open-source naval-domain and NATO-cooperation detail is a genuine structural visibility gap rather than an artefact of any single collection round.



Figure 7. The FAR insignia, in continuous use across Wikipedia's FAR articles since 2008.

The badge is a small oval shield topped by a royal crown, containing a five-pointed star inside a circular field bordered with radiating lines, flanked by short Arabic text fragments [79]. The file has been in continuous use across many language editions of Wikipedia's FAR articles for close to two decades, which supports, without an explicit primary citation in the file record, that it is a stable and widely recognised reproduction of the real FAR insignia rather than a one-off invention; it is nonetheless a Wikipedia-hosted reproduction rather than a file published directly by Morocco's Administration de la Défense Nationale. No official FAR document explaining the badge's specific heraldic elements was located in the sources reviewed; the crown and star are consistent with the general Moroccan state/royal insignia vocabulary noted for the Auxiliary Forces and Royal Guard emblems elsewhere in this report [79].

2nd and 5th Bureaux

This research found no source, at any reliability tier, that names, describes the mandate of, or profiles the current leadership of a Moroccan military Deuxième Bureau (2nd Bureau) or Cinquième Bureau (5th Bureau). This absence was tested deliberately rather than assumed: the most detailed available profiles of Morocco's two civilian successor intelligence services — the DGST, examined in an earlier chapter, and the DGED — were checked specifically for whether either traces its lineage to a named military bureau, and neither does so in the material retrieved [80, 81]. The DGED's own founding narrative states only that it was created in 1973, in the context of the reorganisation of Moroccan security services following the early-1970s coup attempts, succeeding unnamed prior structures of foreign intelligence, with Ahmed Dlimi as its first director from 1973 to 1983 [81]. It is highly likely that this silence reflects a genuine, structural low-visibility characteristic of these bureaux in the open-source record generally, rather than merely a limitation of this particular research pass (confidence: moderate), since two independently authored tertiary compilations focused on the two most plausible successor institutions both omit the topic entirely rather than disagreeing about it.

What can be stated is adjacent and circumstantial rather than direct: Dlimi served under Mohamed Oufkir in Moroccan security services before his 1975 Western Sahara command, and both men are well documented in general historical literature as central figures in Hassan II-era military-

linked repression and intelligence work, without this research locating a source that ties either man explicitly to a bureau bearing the 2nd or 5th designation [78]. Analysts relying on this report should treat any claim about the 2nd/5th Bureau's current mandate, staffing or relationship to the DGST/DGED as effectively unsourceable from open material collected to date, and should flag this explicitly rather than filling the gap with inference dressed as fact. This is one of the starkest illustrations, anywhere in this report, of a stated rather than inferred gap: it is highly likely that the gap itself is real, independent of any judgment about the bureaux's actual current existence or function, which this report cannot assess (confidence: high that the silence is genuine; no confidence is offered on the bureaux's substantive current activity, which remains entirely unassessable from the sources reviewed).

Royal Guard

The Royal Guard's core mission is protecting the King and the royal palaces, supplemented by a ceremonial role in which cavalry units escort the King and appear at state occasions and during visits by foreign heads of state [82]. Its lineage is traced by one source to the Garde Noire, a corps of Sub-Saharan-origin soldiers formed in the late eighteenth century under Sultan Moulay Ismaïl, reorganised into its present form at independence in 1956 and opened since then to Moroccans of all ethnic origins [82]. Reported personnel strength is approximately 6,000, referenced to a 1999-era press citation embedded in the tertiary source rather than a current count; it is roughly an even chance this figure remains accurate today given the twenty-five-plus-year gap (confidence: low), and no more recent figure was located in this research.

The Royal Guard's exact command relationship to FAR is a genuine open question rather than a settled fact, and this report deliberately does not pick a single version to state as true. Three sources collected give three different framings: one lists the Royal Guard simply as one of FAR's five branches with no further qualification [77]; a second states the Guard remains under the direct control of the Ministry of the Royal Household despite formal integration within the Army [65]; and a third describes it as a *corps autonome des Forces armées royales* — autonomous within FAR, rather than under either a straightforward FAR branch command or an external ministry [82]. It is likely that some version of the third framing is closest to reality — an FAR-internal but functionally separate command reporting in practice more directly to the Palace than to the ordinary FAR General Staff chain — given the pattern in Moroccan security-sector design of keeping palace-proximate forces under direct royal rather than institutional control (confidence: low), but this is inference from structural pattern rather than a source that resolves the contradiction directly, and the named current commander given in one source itself carries that source's own citation-needed flag, meaning current Royal Guard leadership should be treated as unconfirmed [82].



Figure 8. The Royal Guard emblem, sourced to an official Garde Royale recruitment announcement.

The gold badge features a royal crown at its centre flanked by two red pennants each bearing a green six-pointed star, distinct from the five-pointed star used by the other services profiled in this report; behind the crown is a sunburst motif topped by a small five-pointed star, with the lower portion bordered by wheat-sheaf or laurel-style fronds and a banner reading The Royal Guard at the base [83]. No official Royal Guard document explaining the specific heraldic meaning of the crown, hexagram flags, sunburst or fronds was located in the sources reviewed; the description above is a factual visual inventory rather than a sourced symbolic explanation.

Military regions and Western Sahara posture

Morocco's military position in Western Sahara rests physically on the Moroccan Wall (the Berm), a six-phase sand-and-stone fortification system built between August 1980 and April 1987 with reported assistance from French, Israeli, South African and Portuguese advisers, whose main line runs roughly 2,500 km from Guerguerat north through the territory, flanked by what is described as the world's longest continuous minefield [84]. It is highly likely that the Berm remains the structural anchor of Morocco's Western Sahara military posture essentially unchanged in concept since 1987 (confidence: moderate), since every source describing current MINURSO or Moroccan activity in the territory continues to reference the Berm as the operative dividing line, though the specific troop-density and radar-range figures reported — observation posts roughly every 5 km with 35-40 troops each, overlapping radar coverage at 60-80 km — come from a single tertiary source and were not independently corroborated in this research [84].

Figure 9. The Moroccan Wall/Berm: reported construction sectors and enclosed towns (figures single-sourced and flagged as uncorroborated -- see text).

MOROCCAN-ADMINISTERED (west)	THE BERM / MOROCCAN WALL	BUFFER ZONE / EAST
El Aaiun, Smara, Bou Craa phosphate deposits	~2,500 km main line; built in six phases, Aug 1980 - Apr 1987	Tindouf-camp-administered territory

Reported enclosed/flanking towns, north to south (single tertiary source, uncorroborated -- treat as indicative only):

El Aaiun / Smara / Bou Craa -- Amgala -- Jdiriya / Haouza --
Mahbes / Farciya -- Guelta Zemmur / Bir Anzarane / Dakhla --
Auserd / Tichla / Bir Ganduz

Observation posts ~every 5 km (35-40 troops each); radar coverage reported
60-80 km beyond the wall (single source, unconfirmed)

Guerguerat crossing (far south) -- ceasefire functionally broken since Nov 2020

Politically, the underlying dispute remains formally live and unresolved on the negotiating track that frames FAR's deployment. UN Security Council Resolution 2797, adopted 31 October 2025 by a vote of 11 in favour with three abstentions (China, Pakistan, Russia) and Algeria not voting as a then-Council member, extended the MINURSO mandate to 31 October 2026 and endorsed Morocco's autonomy proposal as the basis for negotiations while also reaffirming the Sahrawi people's right to self-determination — holding both elements in tension rather than resolving in favour of either side [85]. Morocco's UN ambassador in Geneva has since told the Human Rights Council's 63rd session that 40 countries back Moroccan-sovereignty autonomy under this resolution, a claim that fits the broadly corroborated resolution itself but was reported through only a single Moroccan outlet in this research [86]. It is likely that Rabat will continue building on Resolution 2797 as diplomatic leverage through 2026 (confidence: moderate), given the pattern of the September 2026 Geneva statement building directly on the October 2025 resolution text.

MINURSO itself continues to function as the monitoring and mine-action mechanism along this line, with Major General Jawwad Ahmed of Pakistan having taken over as Force Commander from General Fakhrul Ahsen in late July 2026, against a backdrop the mission's own site frames around hostilities that resumed in November 2020 — that is, MINURSO's own framing treats the original 1991 ceasefire as functionally broken since that date even as the mission persists [76]. Separately, an Algerian independent daily reported that the UN General Assembly adopted a Correct the Map

resolution on 4 September 2026 by 164 votes to one, replacing the Mercator projection with an Equal Earth projection depicting Western Sahara as a distinct 266,000 km² entity with Laâyoune as capital, and claimed Morocco itself voted in favour without reservation [87, 88]. This is a single-sourced, unverified claim from an editorially pro-Sahrawi outlet not corroborated against any UN primary record or Moroccan-press account in this research, and it should not be treated as confirmed — if accurate, however, it would be a notable and almost certainly under-analysed development meriting priority follow-up (confidence: low pending corroboration).

On the ground, a Moroccan outlet reported on 8 September 2026 that a FAR drone struck two vehicles carrying suspected Tindouf-camp gold miners who had crossed into the buffer zone, attributing casualty and damage details to unnamed Mauritanian sources, with Mauritanian authorities said to have repeatedly warned citizens against entering the zone [89]. It is likely that this reflects a genuine, recurring enforcement pattern rather than an isolated incident, given the source's own framing of prior similar events (confidence: low), since the report rests on a single Moroccan outlet's relay of unnamed foreign-government sourcing with no independent Mauritanian, Polisario or Algerian corroboration located — but it is a concrete, dated data point demonstrating FAR's current use of armed drones to enforce the buffer zone, a capability not evidenced in the older material on the Berm's original 1980s design.

Other relevant actors

Around the four institutions profiled above sits a wider Ministry of Interior apparatus and a small set of adjacent bodies that shape Moroccan internal-security practice without being law-enforcement or intelligence services in their own right. The Ministry, headed by Abdelouafi Laftit since 2017, houses a General Secretariat; the DGSN and the General Inspectorate of the Auxiliary Forces, both profiled above; a General Inspectorate of Territorial Administration supervising the wali/governor system; a General Directorate of Territorial Collectivities; a General Directorate of Civil Protection; and specialised directorates for human resources, legal affairs, rural affairs and natural-risk management [90]. A narrower, disaster- and emergency-focused coordination body sits inside this same ministry: the Centre de Veille et de Coordination (CVC), established in 2008 by King Mohammed VI's directive to coordinate disaster response across the DGSN, Civil Protection and the Royal Gendarmerie [90]. No source located states whether the CVC's remit extends to routine security-intelligence coordination as opposed to disaster management specifically; it is likely (confidence: low) that the CVC is functionally distinct from, and narrower than, the constitutional Conseil Supérieur de Sécurité examined under *Coordination and oversight* below, though this is inferred from the CVC's stated founding purpose rather than a directly documented exclusion.

The DGST, profiled in an earlier chapter as parent institution to the BCIJ, carries a pre-BCIJ legal-authority history directly relevant background here: a 2004 Human Rights Watch report — used strictly as a pre-2015 historical baseline, not as evidence of current practice — documented that the DST/DGST was not authorised by law to arrest, detain or interrogate persons, and recorded systematic post-2003-bombing detention abuses including arrests without judicial warrants and prolonged incommunicado detention [91]. It is likely that the BCIJ's 2015 creation was intended, at least in part, to place DGST-fed counter-terrorism investigation on a more defensible judicial-police footing than the DGST's own pre-2015 legal standing allowed (confidence: moderate), given the direct temporal and legal linkage between the 2011 post-Marrakesh law and the bureau's founding documented above [47].

Walis and governors — Interior Ministry officials appointed directly by the King to head each wilaya — recur as the nominal civil-administrative counterpart to which both DGSN's regional

structure and the Auxiliary Forces' mandate are formally oriented, yet no source in this research documents the specific operational protocol by which walis task or coordinate with DGSN prefectural directors, Gendarmerie regional commands or Auxiliary Forces zone inspectorates [51]. This is one of this report's most consequential structural gaps, since it means the practical mechanics of Morocco's territorial security-coordination system, as opposed to its formal administrative hierarchy, remain unverified.

The Public Prosecutor's Office (*parquet*) appears repeatedly across this research as the judicial-supervision authority for both BCIJ counter-terrorism casework and Royal Gendarmerie criminal investigations, including the Lqliaa post-attack inquiry and the Beni Mellal and El Borouj corruption cases, indicating that prosecutorial oversight, rather than any dedicated security-sector oversight body, is the most consistently documented check on operational conduct across the institutions profiled in this chapter [68, 69, 70].

On the foreign side, Spain's National Police and its *Comisaría General de Información* (CNP), and Germany's BND, are the two most concretely named foreign counterpart services identified, engaging respectively with DGSN on organised-crime interdiction and with the DGST/BCIJ chain on counter-terrorism liaison [47, 57, 62], while INTERPOL's Rabat-based National Central Bureau remains the one multilateral channel spanning the whole system since 1957 [56].

The Institut Royal des Études Stratégiques (IRES), a Rabat-based body created by royal dahir with a direct reporting relationship to the monarchy, rounds out this section as a Palace-adjacent strategic-analysis actor rather than an operational security body: its stated mission is to contribute to illuminating strategic decision-making through analyses referred by the King and ongoing strategic monitoring of nationally and internationally critical domains, spanning geopolitics, defence and public policy [92]. IRES is not degree-granting and is treated here as an actor adjacent to, rather than a component of, Morocco's formal security-coordination architecture.

Private companies

Three distinct, chronologically overlapping foreign surveillance-technology vendor relationships emerge from this research, the strongest-evidenced being NSO Group's Pegasus spyware. Press reporting attributes principal Moroccan Pegasus use to the DGST, and specifically its internet and operations department, from 2017 onward, independently corroborated by Amnesty International's Security Lab, which documented Pegasus infection or targeting of two named Moroccan civil-society figures — activist Maati Monjib (November 2017-July 2019) and journalist Omar Radi (February 2019-January 2020) — through device forensics rather than mere assertion [93, 94]. Given this convergence of named-outlet attribution and independent forensic confirmation, it is highly likely that the DGST has operated Pegasus against domestic civil-society targets since at least 2017 (confidence: high), a judgment this report's *intelligence community* chapter examines further alongside the DGED-versus-DGST attribution question for Pegasus's foreign-facing use. An earlier Citizen Lab technical finding bears directly on which private-sector networks carried this activity: the same 2018 *Hide and Seek* report that first catalogued Pegasus's global footprint geolocated a suspected Moroccan Pegasus operator, internally labelled ATLAS, to infrastructure on the Maroc Telecom and Orange Maroc networks via DNS-cache probing and TLS fingerprinting from August 2017, a method the report's own authors describe as a guide for further investigation rather than ironclad evidence [30]. Since Maroc Telecom is itself majority foreign-owned (Etisalat by e&, 53%, with the Moroccan state holding roughly 22%) and Orange Maroc is close to majority-owned by France's Orange S.A. (49%) [95, 96], this finding indicates the suspected DGST operator infrastructure sat on privately and partly foreign-owned telecommunications networks rather than on dedicated state infrastructure, a distinct locus from both the BCIJ/Forces-Auxiliaires-linked Circles infrastructure and any DGST-operated system

proper (confidence: low on the ATLAS-DGST link specifically, since the report itself treats this as investigative lead rather than confirmed attribution).

A second, technically distinct vendor relationship involves Circles, an Israeli/Cypriot company affiliated with NSO Group through shared ownership history but selling SS7/signalling-system exploitation for phone geolocation and call/SMS interception rather than NSO's on-device exploit chain. Citizen Lab's December 2020 Running in Circles report, based on internet-wide scanning for a distinctive firewall signature, places Morocco's Circles deployment infrastructure in the same subnet as several BCIJ websites and the same subnet as the Forces Auxiliaires website — both entities sitting under the Ministry of Interior — with activity documented from March 2018 through the report's December 2020 publication [97]. Because this finding rests on disclosed technical methodology rather than an unverified claim, it is likely that the Ministry of Interior, via BCIJ/Auxiliary Forces-linked infrastructure, hosts or operates Morocco's Circles deployment (confidence: moderate) — a materially different institutional locus than the DGST-centred Pegasus finding above, suggesting Morocco's foreign-vendor surveillance capability is not concentrated in a single agency.

A third, older and non-Israeli vendor relationship is documented only at a low reliability tier: the 2015 Hacking Team email leak, as synthesised by a tertiary source rather than verified against the primary leak archive, lists a Moroccan client coded CSDN, sector Intelligence, with a first contract dated 2009, annual maintenance fees of €140,000, and total identified contract revenue of €1,936,050 [98]. This would make Morocco one of Hacking Team's longer-standing Middle East/Africa clients, predating both the NSO and Circles relationships, but confidence in the specific figures is low given the single tertiary sourcing; the underlying pattern — that Morocco's intelligence services have used at least three distinct foreign intrusion/surveillance vendors across three national origins since 2009 — is nonetheless assessed as likely (confidence: moderate), since each vendor claim rests on a separately sourced finding rather than a single repeated citation. This research specifically searched for, and did not find, any documented Moroccan client relationship with QuaDREAM, Candiru, Intellexa/Cytrox, Verint, Nexa Technologies/Amesys or Rayzone Group; this is recorded as a stated negative finding for this pass, not as evidence that no such relationship exists, since commercial-surveillance vendor relationships are by design difficult to detect absent a leak or forensic infection event.

Separately, Morocco's own cybersecurity law creates a distinct, domestically regulated private-sector layer: Law 05-20 requires any critical-infrastructure operator that outsources cybersecurity services to use a DGSSI-qualified provider, and DGSSI's qualification regime requires Moroccan incorporation for all qualified providers and majority-Moroccan capital and nationality among proposed specialists for the most sensitive systems [99]. The implementing text for cloud providers specifically, Décret n° 2-24-921 of 22 October 2024, sets out two qualification levels: Level 1, covering the hosting, management or operation of sensitive information systems, carries no ownership restriction, while Level 2, covering the processing, operation or storage of sensitive data itself, requires majority-Moroccan ownership, exclusively national-territory processing and management, and Moroccan-national operating staff, with qualifications valid up to five years, DGSSI audit authority throughout, and a 24-month compliance transition for incumbent providers that expires on or about 22 October 2026 [100]. Since no major foreign hyperscaler (Microsoft Azure, Google Cloud and Cloudflare each confirm no Moroccan regional presence) currently operates Moroccan in-territory infrastructure, it is highly likely that Level 2 qualification will in practice be met, if at all, through Moroccan-incorporated joint ventures or domestic providers rather than direct foreign-hyperscaler subsidiaries by that deadline (confidence: moderate, since the decree text and the infrastructure baseline are both well evidenced but the practical market response to the approaching deadline has not yet been observed). This creates a bifurcated private-sector picture: unregulated or covertly used foreign offensive-surveillance vendors on one hand,

and a nationality-restricted, state-licensed domestic cybersecurity- and cloud-services industry on the other. The table below sets the three identified surveillance-technology vendors side by side, since a reader should be able to see at a glance that the three findings rest on three different evidentiary bases rather than uniform certainty.

Table 9. Three foreign surveillance-technology vendor relationships identified for Morocco.

Vendor	Country of origin	Product / technique	Identified Moroccan client / infrastructure	Activity window	Evidentiary basis
NSO Group (Pegasus)	Israel	On-device exploit chain (spyware)	DGST, specifically its internet and operations department	2017-2021 (device-forensic confirmation)	Named-outlet press attribution plus independent forensic confirmation (Amnesty International)
Circles	Israel / Cyprus	SS7/signalling-system exploitation (geolocation, call/SMS interception)	Ministry of Interior infrastructure (same subnet as BCIJ and Forces Auxiliaires websites)	March 2018-December 2020	Citizen Lab internet-wide technical scanning (disclosed methodology)
Hacking Team	Italy	Remote Control System intrusion software	Client coded "CSDN", sector "Intelligence"	2009-2015 (leak date)	Tertiary synthesis of the 2015 leaked emails, not independently re-verified against the primary archive

Universities

Of the Moroccan academic institutions examined in this research, only one offers a clearly degree-granting, security-specific curriculum: the École Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS), a public engineering grande école founded in 1992 and formally attached to Université Mohammed V de Rabat, which runs a dedicated Sécurité des Systèmes d'Information specialisation track and an associated Master Recherche en Sécurité des Systèmes et Services research master's [101]. This is the most directly responsive finding to the requirement for a Moroccan academic institution relevant to security and cyber studies, though no institutional partnership between ENSIAS and DGSSI or another state cybersecurity agency was documented in the source retrieved, which is logged as an evidentiary gap rather than a confirmed absence.

Two other prominent Moroccan universities were checked specifically for a security/intelligence/cyber linkage and yielded negative findings. The University Mohammed VI Polytechnic (UM6P), a private, OCP Foundation-funded research university with strong artificial-

intelligence and computing programmes and a notable campus presence in Laâyoune, Western Sahara, showed no documented cybersecurity-specific institute or government defence/security-agency partnership in the source examined [102]. The International University of Rabat (UIR), Morocco's first public-private-partnership university, offers aerospace- and automotive-engineering double degrees with international partners but likewise showed no documented cybersecurity programme or defence-agency partnership [103]. Both negative findings are plausible candidates for a genuine linkage — UM6P given its AI/computing strength and state-linked funding, UIR given its aerospace programme's proximity to Morocco's growing drone/defence-industrial base — but neither is substantiated in this research, and it is unlikely, though not ruled out, that either institution has an undisclosed security-agency partnership invisible to open-source review (confidence: low).

The Institut Royal des Études Stratégiques, profiled above as a Palace-adjacent strategic-studies actor, is explicitly not a university in the degree-granting sense and is excluded from this section's core finding for that reason [92]. DGSSI's own site references a Master spécialisé en cybersécurité with a sixth enrolment cycle opened in March 2013, implying a training relationship dating to at least the mid-2000s, but the retrieved content does not name the delivering university partner [104]; two attempts to identify a Moroccan military academy or staff/war college with a documented security- or intelligence-studies curriculum returned no retrievable page, an open, unresolved gap for future research rather than a negative finding, since such an institution is a plausible candidate this research could not confirm or rule out.

Crime

Morocco's organised-crime landscape, as evidenced in this research, centres on two geographically and institutionally distinct trafficking corridors: an established hashish route moving north toward Spain concealed within agricultural export trucks, and an emergent Atlantic maritime cocaine route running through the Western Sahara-adjacent coast. The hashish route is evidenced by an October 2025 joint DGSN-Spanish National Police operation seizing over 22 tonnes concealed in refrigerated pepper-truck convoys between Morocco and Spain, triggered by Moroccan-originated intelligence [57], while the cocaine route is evidenced by the Royal Gendarmerie's July 2026 interdiction of over three tonnes transferred ship-to-shore off Tarfaya [67]. It is likely that these two commodities now run through substantially different institutional and geographic channels — DGSN-Spain land/agricultural-export cooperation for hashish, Gendarmerie-led maritime interdiction for cocaine — rather than through a single undifferentiated trafficking network (confidence: moderate, based on the consistent institutional and geographic separation across the specific 2025-2026 cases reviewed).

Migrant smuggling recurs across this research as both a standalone crime type and one that overlaps directly with narcotics trafficking on the same vessels and networks. A single Sidi Ifni interdiction charged the same boat and crew with both international drug trafficking and organised maritime migration, evidencing network overlap between hashish logistics and migrant-smuggling infrastructure on the Atlantic coast, even though the specific quantity reported for that seizure is flagged as almost certainly an extraction error and should not be relied upon [105]. Separately, the Royal Maritime Gendarmerie's interception of Bangladeshi migrants off M'diq demonstrates that Morocco's Mediterranean-coast smuggling clientele is not limited to regional, sub-Saharan African nationals, indicating a broader, more international smuggling-facilitation market operating through Moroccan territory than a purely regional migration frame would suggest [66]. The August 2026 Ceuta border crisis further illustrates how Moroccan authorities distinguish migrants from facilitators for prosecutorial purposes: alongside roughly 300 detained migrants, 61 additional people were separately charged with inciting illegal migration, a distinct smuggling/organising offence [50].

Institutional corruption is a documented, recurring vulnerability that organised-crime networks appear able to exploit at the law-enforcement level itself: the two independent Royal Gendarmerie narco-corruption cases in Beni Mellal and El Borouj, discussed above under *Royal Gendarmerie*, indicate that trafficking networks have, on at least two separately prosecuted occasions, successfully cultivated protection from within Gendarmerie ranks rather than relying solely on evasion [68, 69]. Finally, the April 2026 BCIJ case shows a distinct pattern at the terrorism-organised-crime boundary: an ISIS-affiliated cell engaged in ordinary theft, burglary and money laundering under an ideological legitimisation-of-loot justification, indicating that at least some ideologically motivated networks in Morocco fund themselves through conventional organised-crime predicate offences rather than external terrorist financing [61]. It is likely that this ideological/ordinary-crime blending is an intentional recruitment and self-financing strategy rather than an isolated framing choice by prosecutors (confidence: low, given this rests on a single detailed case in this research). A broader, politically charged claim about the Makhzen's relationship to organised crime recurs in this collection and is recorded here strictly as a contested framing rather than an evidenced finding: Algerian state media (Algérie Presse Service) has characterised Morocco's Makhzen as fostering an environment that allows transnational organised crime to regenerate and as sheltering fugitives wanted by European justice on drug-trafficking and money-laundering charges, a claim carried on a single, only partially accessible state-wire item from a rival government with an evident interest in delegitimising Rabat [20]. An establishment-aligned Moroccan commentator, by contrast, defines the Makhzen as the traditional monarchy-centred authority network credited with historical continuity rather than any criminal-facilitation role [19]. Neither framing is independently verified against the concrete 2025-2026 hashish, cocaine and migrant-smuggling casework detailed above, and it is unlikely, though not ruled out, that the APS characterisation reflects a documented institutional pattern rather than rhetorical delegitimation of a rival state (confidence: low, given the single, biased and only partially accessible sourcing on this specific claim). The table below sets out the documented 2025-2026 operations across all the institutions profiled in this chapter side by side, since it is a natural enumeration rather than a prose narrative.

Table 10. Documented 2025-2026 law-enforcement and security operations, by date.

Date	Institution(s)	Operation / incident	Outcome
January 2025	Royal Gendarmerie	El Borouj/Beni Meskine drug-baron cover-up case	Seven gendarmes ordered detained
March 2025	Royal Gendarmerie	Beni Mellal narco-corruption trial	37 officers on trial; verdict not reported in sources reviewed
August 2025	DGSN	Sidi Ifni maritime interdiction	Hashish and irregular-migration boat intercepted (seizure quantity flagged as an extraction error)
October 2025	DGSN; Spanish National Police	Cádiz/Granada hashish interdiction	Over 22 tonnes seized, concealed in refrigerated pepper-truck convoys
October 2025	Royal Gendarmerie (M'diq)	Bangladeshi migrant-smuggling interception	Inflatable boat intercepted; 13 migrants

October 2025	Royal Gendarmerie	Lqliaa post attack (Gen Z 212-linked unrest)	Three deaths, eight gendarmes injured
April 2026	BCIJ / DGST	ISIS-affiliated cell (Kenitra, Casablanca, Dar El Gueddari, Sidi Taibi)	Six-member cell dismantled; "legitimisation of loot" self-financing pattern
July 2026	Royal Gendarmerie	Tarfaya Atlantic cocaine interdiction	Over three tonnes seized, ship-to-shore transfer
August 2026	DGSN; Royal Gendarmerie; Auxiliary Forces	Ceuta mass border-crossing (15 August)	~300 migrants detained; 61 additionally charged with inciting illegal migration
August 2026	DGSN	Agadir eighth regional explosives-disposal brigade launch	Regional specialist-unit rollout completed, extending into Western Sahara via Laâyoune

Coordination and oversight

Formal coordination of Morocco's security and intelligence apparatus rests constitutionally with the King rather than with any interagency civilian structure. Article 53 of the 2011 Constitution makes the King Supreme Head of the Royal Armed Forces with the power to appoint to military office, and Article 54 creates the Conseil Supérieur de Sécurité (CSS) as the country's constitutionally designated coordination body for internal and external security strategy, crisis management and the promotion of good-governance standards in the security domain [106, 107]. The King chairs the CSS but may delegate the chair to the Head of Government for a specific agenda, and the Council's membership spans the Head of Government, the presidents of both parliamentary chambers, a representative of the judicial authority, the ministers of Interior, Foreign Affairs, Justice and National Defence, and senior security and military officials — a composition that formally embeds inter-branch coordination at the apex of the security system, whatever the Council's practical operating rhythm turns out to be.

That constitutional text is conspicuously silent on any dedicated parliamentary security or defence oversight committee comparable to Western intelligence-oversight structures: the only defence-adjacent parliamentary role specified is Article 99's requirement that a declaration of war, decided in the Council of Ministers, be communicated by the King to Parliament, and Article 49's reservation of war-declaration and military-domain bills to Council of Ministers deliberation [106]. It is highly likely that Morocco's constitutional order does not provide Parliament with a standing, security-cleared oversight mechanism over intelligence and security agencies as a matter of institutional design, rather than as an unwritten but functioning convention (confidence: moderate), based on the absence of any such provision across two independently retrieved constitutional-text sources. Privacy International's synthesis of Morocco's surveillance-oversight legal architecture converges with that constitutional silence: it states plainly that little is known about the laws and regulations that would govern the CSS's authority, and separately documents that Act 85-13, which empowers parliamentary commissions of inquiry, carves out documents of a secret nature or falling under national defence from those commissions' reach [108]. It is highly

likely that Morocco's Parliament possesses no operative mechanism for reviewing classified intelligence or security-agency activity (confidence: moderate-high), a judgment resting on the convergence of constitutional silence and this specific statutory carve-out.

Judicial rather than parliamentary oversight nominally governs communications interception: the Code de Procédure Pénale's Articles 108-116 require a written warrant from the First President of the Appeals Court, addressed to an investigating judge or the Crown Prosecutor, capped at four months and renewable once, with a 24-hour judicial-ratification exception for cases of extreme emergency [108]. This safeguard's practical weight is doubtful on two independent grounds documented in the same source: Privacy International cites the judiciary's lack of independence as a standing concern among Moroccan judges' professional associations and civil-society organisations, and separately notes that a 2011 statute (Act 35-11) granting DST/DGST agents *Officier de Police Judiciaire* status applies only narrowly to the specific offences the agency is empowered to investigate, functioning as a criminal-procedure status grant rather than a general oversight mechanism over the agency's broader intelligence activity [108]. It is likely that the CPP 108-116 warrant regime constrains ordinary criminal-procedure interception more than it constrains intelligence-service surveillance activity proper (confidence: moderate), given this status-scope distinction.

The clearest single coordination fact in Morocco's entire security architecture is Abdellatif Hammouchi's simultaneous directorship of the DGST, which he has led since December 2005, and the DGSN, which he has led concurrently since May 2015, an arrangement multiple independently named outlets treat as a *de facto* fusion point between Morocco's law-enforcement and counter-espionage apparatus [46, 93]. This dual-hatting is reinforced institutionally by the BCIJ's placement under DGST authority as its judicial arm, meaning intelligence product, judicial-police casework and national police command converge under a single office-holder [109]. The constitutional mechanism enabling this concentration is itself identifiable rather than merely inferred: Article 49 places the appointment of heads of internal-security administrations and strategic public establishments in the King-presided Council of Ministers, on the Head of Government's proposal, giving Hammouchi's continued dual appointment and retention a direct textual constitutional basis rather than resting on administrative practice alone [106, 107]. It is almost certainly the single most consequential coordination mechanism documented in this research (confidence: high), given the convergence of independent press attribution, the structural BCIJ finding and this constitutional appointment power, though no source located documents any formal check on this fusion beyond ordinary ministerial reporting to the Minister of Interior.

The Amnesty International forensic finding on Pegasus targeting of Maati Monjib and Omar Radi, discussed above under *Private companies*, is directly relevant here because neither target was a criminal suspect under active investigation at the time of targeting, meaning their surveillance cannot be explained as an application of the CPP 108-116 judicial-warrant framework [94]. It is highly likely that this and comparable Pegasus operations against Moroccan civil-society figures were conducted as intelligence-service activity entirely outside Morocco's documented judicial-authorisation framework for communications interception (confidence: high), since no warrant process, investigating-judge referral or comparable judicial artefact is documented for either target in the retrieved forensic report or in any other source reviewed. This illustrates concretely what the constitutional and statutory silences discussed above mean in operational practice.

By contrast, Morocco's cybersecurity-specific governance architecture is comparatively well codified in primary legal text, even though it remains DGSSI-dominated in practice. Law 05-20 designates critical infrastructure through what is, on the statute's own terms, a two-key mechanism set out at Article 16: each vital-activity sector's own coordinating governmental authority makes the designation decision, but only after the mandatory advisory opinion of DGSSI, with the resulting list kept secret and updated at intervals of no more than two years [99]. The same law

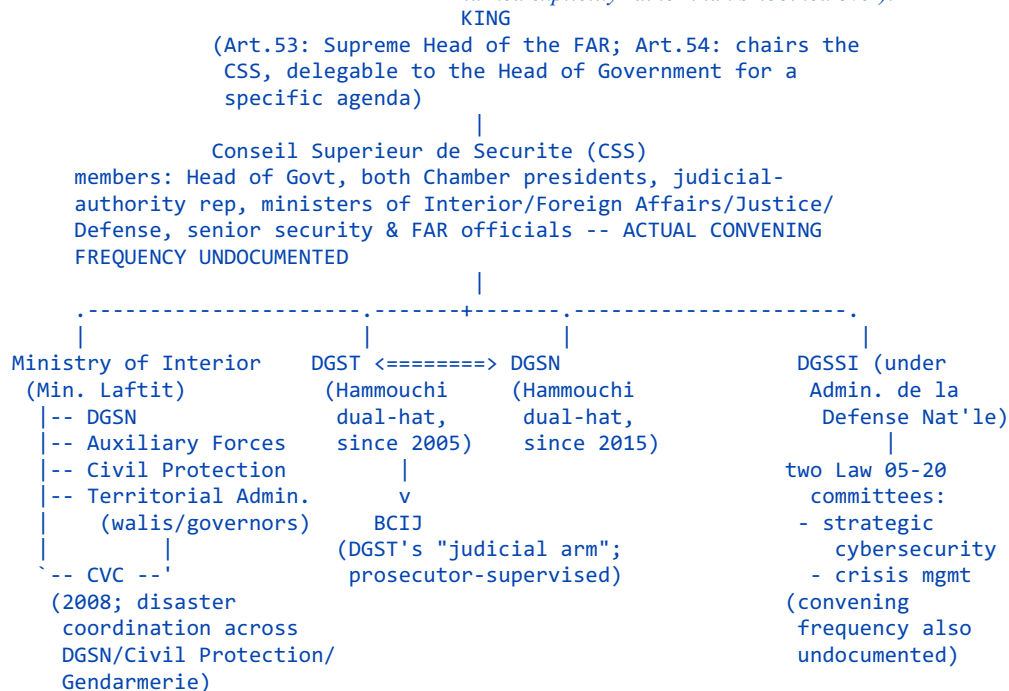
establishes two standing governance committees — a comité stratégique de la cybersécurité setting national strategic direction and evaluating DGSSI's own annual activity report, and a subordinate comité de gestion des crises et événements cybernétiques majeurs for crisis coordination, empowered to compel telecommunications operators and service providers to furnish technical assistance during a declared major cyber crisis [99]. It is highly likely (confidence: high, given this rests on primary legislative text) that Morocco's cyber-domain coordination architecture is materially more procedurally documented than its human-intelligence and signals-intelligence coordination architecture, even though both nominally answer to the same apex security structure. This asymmetry should not be read as evidence that DGSSI's governance committees function as intended in practice: no source documents how frequently either cybersecurity committee has actually convened, mirroring the identical and already-noted gap around the CSS's own convening history. Taken together with the CVC's narrower disaster-coordination role documented above under *Other relevant actors*, Morocco's coordination landscape is better characterised as a set of parallel, topically bounded bodies — the CSS for general security strategy, the CVC for emergency management, DGSSI's two committees for cybersecurity — rather than as a single integrated command structure, and it is roughly an even chance, on current open-source evidence, that this fragmentation reflects deliberate compartmentalisation rather than simple administrative accretion over time (confidence: low). The table and figure below draw this apparatus together: the table enumerates each body's mandate and reporting line, and the diagram distinguishes constitutional and statutory links from the Hammouchi dual-hatting fusion, which is personal rather than structural.

Table 11. Morocco's principal formal security-coordination and oversight bodies.

Body	Founding instrument / date	Stated mandate	Chair / reporting line	Documented oversight mechanism
Conseil Supérieur de Sécurité (CSS)	Article 54, 2011 Constitution	Coordination of internal and external security strategy, crisis management, good-governance promotion	King (delegable to the Head of Government for a specific agenda)	None documented; actual convening history unconfirmed
Centre de Veille et de Coordination (CVC)	2008, royal directive	Disaster and emergency-response coordination across DGSN, Civil Protection and the Royal Gendarmerie	Ministry of Interior	None documented beyond its stated founding purpose
Comité stratégique de la cybersécurité	Law 05-20 (2020)	Sets national cybersecurity strategic direction; evaluates DGSSI's own annual activity report	DGSSI	Convening frequency undocumented

Comité de gestion des crises et événements cybérnetiques majeurs	Law 05-20 (2020)	Crisis coordination; can compel telecom operators and service providers to give technical assistance	DGSSI	Convening frequency undocumented
BCIJ (as a coordination point)	2015, post-Marrakesh-bombing law	Functions as the DGST's "judicial arm", converting intelligence into judicial-police casework	DGST, via Public Prosecutor's Office supervision of casework	Prosecutorial supervision of casework; no parliamentary oversight mechanism identified

Figure 10. Morocco's security-coordination apparatus, consolidated (personal fusion links and undocumented convening frequency are marked explicitly rather than smoothed over).



Judicial oversight of interception: CPP Arts. 108-116 (warrant from First President of the Appeals Court) -- practical weight doubtful (judiciary-independence concerns; Act 35-11 OPJ status is narrow, not general oversight)

This research closes by stating explicitly, rather than silently omitting, the gaps that remain: the CSS's actual meeting frequency and practical output are undocumented in any source located here; no source names the specific authority that technically executes a judicially authorised communications intercept once issued; no legislative body with security clearance to review classified material was identified anywhere in Moroccan statute or reporting; and the university partner delivering DGSSI's own cybersecurity master's programme remains unnamed. Morocco's security-coordination and oversight architecture is, on the evidence assembled here, a genuinely low-transparency domain, and these gaps should be read as such rather than resolved by inference.

Part IV. The Moroccan cyber ecosystem

The Moroccan Cyberspace

Morocco's internet and mobile markets are close to saturation by subscription count rather than by unique-user reach. By the end of 2025 the Kingdom carried more than 41 million internet subscriptions against a population of roughly 38 million -- a headline penetration rate above 110% that reflects multi-device and multi-SIM use rather than universal household connectivity -- alongside more than 58 million mobile subscriptions [110]. It is almost certainly best read as evidence of a mature, competitive mobile market rather than of uniform household access (confidence: high, since ANRT's own Q1 2026 sector-observatory report, a primary regulatory source, independently corroborates the same order of magnitude directly: a 111.54% internet-penetration rate and 3.22 million 5G users served by 8,400 5G sites as of that report [111], upgrading the earlier tertiary-sourced figure above from a standing sourcing caveat to a directly confirmed data point, though ANRT's own page did not break out operator-level market share). Three licensed operators structure the market -- Maroc Telecom, the historic incumbent majority-owned by the UAE's e& since 2013, examined for its ownership dimension under *Key dependencies* below; Orange Maroc, reported slightly ahead of Maroc Telecom in mobile subscriptions as of mid-2025; and Inwi -- each offering mobile, fixed-line and broadband service [110]. ANRT, the sector regulator, launched 5G commercially on 7 November 2025, reaching an estimated 38% population coverage by end-2025, alongside more than 1.4 million fixed fibre connections and roughly 30% of fixed infrastructure deployed through operator infrastructure-sharing arrangements [110].

The clearest evidence located of the digital economy's growing legal salience is indirect rather than statistical: the CNDP's need, ahead of the 23 September 2026 legislative elections, to impose a specific labelling obligation on AI-generated political content [112], examined in full under *Law and regulation* below, is a requirement that would not exist absent a digital-economy context in which generative-AI tools are already in political-communication use. Beyond this single indicator, no primary Moroccan statistical source on e-commerce scale, digital-services GDP contribution or platform-economy size was located for this chapter; this is stated as an explicit scope gap rather than papered over with an inferred figure, and remains a natural target for dedicated economic-domain research rather than the cyber-focused material this chapter draws on. This connectivity base, and the legal and institutional architecture Morocco has built to govern and defend it, are examined in turn below: *Law and regulation* sets out the legislative framework; *Defensive cybersecurity and incident response* profiles DGSSI and maCERT; *Intelligence collection and surveillance* addresses the DGST/DGED surveillance question in full; and *Military cyber, electronic warfare and C4ISR* closes this first cluster of chapters by examining -- and, in large part, documenting the absence of open-source reporting on -- a dedicated Moroccan military-cyber capability.

Law and regulation

Morocco's cybersecurity statute, Law 05-20, was promulgated by dahir n°1-20-69 of 4 hja 1441 (25 July 2020), as confirmed directly in the preamble of its own implementing decree [100]. That decree, n°2-24-921 of 22 October 2024, operationalises Law 05-20's article 25 by requiring vital-infrastructure (IIV) entities to use only a DGSSI-qualified Cloud provider for sensitive systems and data, under a two-tier qualification scheme: a Level 1 tier, open to any suitably resourced

Moroccan-registered company, covering the hosting or operation of sensitive information systems; and a materially stricter Level 2 tier, covering the processing or storage of sensitive data itself, which additionally requires Moroccan-majority ownership, exclusive national-territory data processing and service management, and Moroccan-national operating staff [100]. Qualification decisions run up to five years and are published in the Bulletin Officiel, and DGSSI itself audits qualified providers under Law 05-20's article 38 [100]; the decree's own article 18 further grants IIV entities already using cloud services when it entered into force a 24-month compliance transition, placing that transition's close at approximately 22 October 2026, roughly six weeks after this chapter's own reporting period, and its article 16 conditions any Level 2 provider's exit from the market on data-recovery and certified-deletion guarantees to the departing IIV client [100]. It is highly likely that Level 2 qualification is attainable only by domestic Moroccan providers rather than by any global hyperscaler, examined for its own absence from Morocco under *Key dependencies* below (confidence: moderate), since the nationality and exclusive-territoriality requirements in the decree's own text amount to a categorical exclusion of foreign-controlled entities from that tier rather than merely a stringent compliance bar; it is correspondingly highly likely (WEP 80-95%) that Level 2 qualification will in practice be met, where it is met at all, through domestic or joint-venture providers rather than a direct foreign-hyperscaler subsidiary (confidence: moderate, since the decree text and the cloud-absence baseline are both well evidenced while the actual market response to the approaching deadline has not yet been observed). Law 05-20 separately empowers DGSSI, under the statute's own article 28, to collect and analyse technical data only -- the article's own language excludes "any other exploitation" -- from telecom operators, internet-service providers, cybersecurity providers and platform publishers, but solely for the purposes of preventing and characterising cyber threats [99]; this is a bounded, cyber-defensive monitoring power over private infrastructure rather than a content-interception authority, and it is distinct in both statutory basis and scope from the device-level Pegasus surveillance activity examined under *Intelligence collection and surveillance* below, which no legal provision reviewed for this chapter purports to authorise, whether for DGSSI or for DGST/DGED.

The same 2024 decree's preamble independently confirms that décret n°2-82-673 of 13 January 1983, which organises the Administration de la Défense Nationale, was itself amended by décret n°2-11-509 of 21 September 2011 [100]. This is consistent with, though not itself a direct primary-source confirmation of, DGSSI's founding placement under that same defence administration rather than under a civilian ministry (confidence: moderate), since no DGSSI publication consulted for this chapter states its own founding decree explicitly; the point nonetheless matters structurally, since it embeds Morocco's national cybersecurity authority within the defence establishment rather than a purely civilian regulatory body, a structural difference from most European cybersecurity-authority models worth flagging explicitly.

Morocco's data-protection statute, Law 09-08, governs the CNDP's regulatory activity, and the clearest and most current evidence of that activity is the commission's 31 August 2026 guidance for the 23 September 2026 legislative elections [112, 113]. That guidance requires political parties to notify data-processing operations to the CNDP in advance under article 12, bars exploitation of political opinions without explicit consent under article 21, limits retention to declared purpose under article 3, restricts unsolicited canvassing under article 10, and -- its most novel element relative to earlier CNDP practice -- mandates that AI-generated campaign content be labelled as such, citing the 2018 Penal Code's article 447-2 and articles 39, 51 and 53 of Organic Law n°53-25 [112]. It is highly likely that this AI-labelling requirement is a genuinely new addition to Morocco's electoral-communication rules rather than a restatement of prior guidance (confidence: moderate), inferred from the absence of any earlier CNDP electoral communiqué of this kind in the material reviewed, rather than from a direct comparison against a prior election cycle's own

guidance. A caveat on precision rather than substance: CNDP's own communiqué confirms the guidance's existence and its "ten imperatives" framing, but the specific article numbers cited above -- Penal Code article 447-2, Organic Law 53-25 articles 39, 51 and 53 -- rest on Le360/MAP's own press characterisation of the underlying texts rather than on a directly retrieved primary CNDP or Bulletin Officiel citation [112], and should be read accordingly as validity-plausible but not independently text-verified. Since this is the first electoral cycle to operate under the requirement at all, it is only roughly an even chance to likely (WEP 45-70%) that CNDP's own enforcement during the 23 September 2026 vote will prove light-touch and complaint-driven rather than proactively policed (confidence: low), a forecast this report states explicitly as a genuinely open first-instance test of CNDP's practical independence rather than a prediction the underlying material allows to be made with any greater confidence. This electoral AI-labelling rule should not be read as movement toward a general Moroccan AI-governance framework: no Morocco-specific AI statute or draft of any kind was located for this chapter, and the labelling requirement is a narrow, electoral-context-specific rule tied to existing Penal Code and electoral-law provisions on candidate conduct rather than the first plank of a broader regulatory regime, a distinction stated explicitly rather than left to inference.

DGSSI's homologation regime, distinct from the cloud-provider qualification scheme above, requires every sensitive information system operated by an IIV entity to undergo a formal homologation before deployment, under Law 05-20's article 19 [114]. Homologation is a documented act rather than merely a technical control: the IIV's own responsible official must produce a decision attesting to understanding the system's security posture and formally accepting whatever residual risk remains [114]. This places ultimate accountability for a vital-infrastructure system's security posture on a named institutional official rather than on DGSSI as auditor, a structurally significant design choice the source material states plainly but does not further elaborate procedurally; the full evaluation criteria and homologation-authority role are confined to a downloadable guide not fully examined for this chapter, a specific and namable content gap.

Morocco's cybersecurity incident-declaration framework rests on article 42 of Decree n°2-21-406, Law 05-20's general implementing decree, which tasks DGSSI with rapid incident detection, impact minimisation, vulnerability remediation and service restoration as its stated objectives [115]. The specific reporting timeframe or threshold triggering a mandatory declaration, and the precise division of labour between DGSSI's audit function and maCERT's operational incident-handling role, examined under *Defensive cybersecurity and incident response* below, could not be established from the material reviewed and are recorded as explicit gaps rather than inferred from the framework's general language. DGSSI's National Cybersecurity Strategy 2030, dated 22 July 2024, states its aim as improving national governance and strengthening the legal and institutional framework through 2030, supported by twelve technical guides spanning data classification, incident management, industrial-control-system security, business continuity and audit [116].

This section alone enumerates at least seven distinct legal and regulatory instruments -- Law 05-20 and its general implementing Decree 2-21-406, the IIV-cloud Decree 2-24-921, Law 09-08, the 2018 Penal Code's AI-labelling provision, Organic Law n°53-25, and the National Cybersecurity Strategy 2030 -- plus several DGSSI technical référentiels of their own; the table below collects each for quick reference.

Table 12. Morocco's cyberspace and data-protection legal and regulatory instruments.

Instrument	Legal citation	Date	Issuing/implementing authority	Core obligation
Law 05-20 (cybersecurity)	Dahir n°1-20-69	25 July 2020	DGSSI (national coordinating authority)	Establishes national cybersecurity architecture; organisational/technical

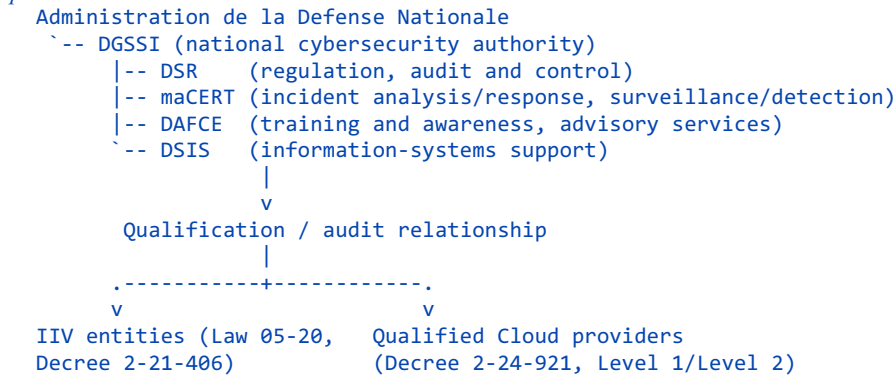
				obligations on state bodies and critical-infrastructure operators
Decree n°2-21-406 (general implementing decree)	Implements Law 05-20	2021	DGSSI	Incident-declaration framework (art. 42): detection, impact minimisation, remediation, restoration
Decree n°2-24-921 (IIV Cloud-provider qualification)	Implements Law 05-20 art. 25	22 October 2024	DGSSI (qualification and audit)	Two-tier Cloud-provider qualification (Level 1 general; Level 2 Moroccan-majority-owned, national-territory-only) for vital-infrastructure entities
Law 09-08 (personal data protection)	—	2009 (2026 electoral guidance 31 Aug 2026)	CNDP	Prior notification/authorisation for personal-data processing; 2026 electoral guidance (arts. 3, 10, 12, 21)
Penal Code art. 447-2 (AI-generated content labelling)	2018 Penal Code amendment	cited 2026	CNDP / judicial authorities	Requires AI-generated campaign content to be labelled as such
Organic Law n°53-25 (Chamber of Representatives)	arts. 39, 51, 53	cited 2026	Parliament / CNDP	Electoral-communication rules referenced alongside the AI-labelling requirement
DGSSI homologation guide	Law 05-20 art. 19	9 November 2021	DGSSI	Mandatory formal homologation of sensitive IIV information systems before deployment
National Cybersecurity Strategy 2030	—	22 July 2024	DGSSI	National governance and legal/institutional framework roadmap; twelve supporting technical guides

Defensive cybersecurity and incident response

DGSSI is Morocco's national cybersecurity authority, organising its own public mandate into six functional domains -- incident analysis and response, surveillance and detection, regulation, audit and control, training and awareness, and advisory services -- delivered through four named internal departments: DSR, maCERT, DAFCE and DSIS [117]. This is a broad, whole-of-government

remit that combines regulator, auditor and operational-response functions inside a single agency, a concentration of authority that is efficient for coordination but also means DGSSI has limited independent external check on its own audit findings within the civilian cybersecurity domain (confidence: moderate, an institutional-design inference rather than a directly documented finding). The figure below sets out this structure and DGSSI's regulatory relationship to the vital-infrastructure entities and qualified Cloud providers discussed under *Law and regulation* above.

Figure 11. DGSSI's institutional structure: departments, and its regulatory relationship to vital-infrastructure entities and qualified Cloud providers.



maCERT, one of DGSSI's four departments, is Morocco's national CERT, self-described as the watch, detection and response centre for computer attacks, pursuing four security objectives -- availability, integrity, confidentiality and traceability -- through reactive services (alerting, incident management, incident analysis, response support) and proactive services (technology watch, security evaluation, intrusion detection, security-information dissemination) [118]. No founding date, staffing figure, organisational chart or named historical incident response was located anywhere in maCERT's own public-facing material, an explicit and operationally relevant gap: it is not possible from open sources reviewed to assess maCERT's actual capacity or track record, only its stated mandate (confidence: high that this specific gap exists, since it reflects an absence check against the primary source itself rather than an inference). The one available quantified, if indirect, proxy for Morocco's overall cyber posture is the Estonian e-Governance Academy's 2026 National Cyber Security Index (NCSI), under which Morocco placed 43rd of 155 states with a score of 79.17, up in absolute score from 70.13 in the prior edition even as its rank fell from 32nd as peer states improved faster [119]. This index should be read as indicative of policy and legal-framework completeness rather than of demonstrated operational capability, and it is a distinct instrument from the ITU's own Global Cybersecurity Index, under which Morocco held a "Tier 1" placement in 2024 -- the two should not be conflated, an error this chapter has seen made in some Moroccan press coverage of the NCSI result; taken together with the gap just stated, it is likely (confidence: moderate) that maCERT's actual technical incident-response capacity is more limited than its formal six-domain mandate and Morocco's respectable NCSI standing alone would suggest, since a strong policy-framework score is not itself evidence of a mature operational CERT function. maCERT's only concretely documented international-partnership memberships, per its own primary page, are FIRST, the Forum of Incident Response and Security Teams, and OIC-CERT, the Organisation of Islamic Cooperation's CERT network [118]; no corroboration of broader bilateral cyber-defence partnerships was located via any primary maCERT or DGSSI source, and any such claim should be treated as unconfirmed rather than repeated as established.



Figure 12. The DGSSI institutional logo, retrieved directly from the agency's own official website.

The logo combines a small shield-shaped badge in the Moroccan national colours with a French-language wordmark reading "Royaume du Maroc / Administration de la Défense Nationale /

Direction Générale de la Sécurité des Systèmes d'Information" [120]. The wordmark is itself informative for this report, since it publicly confirms DGSSI's institutional attachment to the Administration de la Défense Nationale rather than to a purely civilian cybersecurity regulator, corroborating the structural point already made under *Law and regulation* above from the decree lineage rather than from the logo alone. No further official explanation of the badge's own heraldic elements -- the map-and-star motif, or the specific national colours used -- was located on the DGSSI site in the time available for this research, and this description is accordingly a factual visual inventory rather than a sourced symbolic gloss.

maCERT itself does not maintain an independent public website any longer: macert.ma does not resolve, and the dgssi.gov.ma/macert path redirects to the DGSSI homepage, which references maCERT only through news items -- participation in FIRST, OIC-CERT and APCERT events -- and a functional contact address, with no maCERT-specific logo image found on the page; maCERT's own membership page on FIRST.org likewise shows only FIRST's own logo, with no maCERT-specific emblem uploaded [121]. maCERT accordingly has no distinct institutional emblem of its own: it operates today as a function or team embedded within DGSSI rather than as a separately branded body, and appears to use DGSSI's own visual identity, shown above, rather than a logo of its own -- a negative finding stated explicitly rather than left unaddressed.

The clearest real-world incident-response case on record is the April 2025 breach of Morocco's National Social Security Fund (CNSS), independently confirmed by Spain's own national CERT: a threat actor using the handle Jabaroot disclosed more than 53,000 files on BreachForums, covering roughly 500,000 companies and two million employees, including salary and contact data exposed unencrypted on compromised servers [122]. INCIBE-CERT's own framing treats this as political-messaging-oriented rather than purely financially motivated activity, explicitly linking it to Morocco-Algeria tension via Jabaroot's own stated retaliation narrative for an earlier compromise of the Algerian Press Service's X account [122], an episode examined in full, together with the wider Jabaroot campaign it began, under *Hactivism and information confrontation* below. It is likely that this incident represents the most operationally significant cybersecurity incident Morocco's defensive apparatus has had to manage in the period under review (confidence: moderate), based on the scale of exposed records and the sustained, multi-year campaign it triggered, though no DGSSI or maCERT public statement on its own response to the incident was located, itself a further specific gap.

No official DGSSI or maCERT public statement addressing the CNSS breach, the subsequent Jabaroot leaks, or the August 2026 claims of a further breach targeting DGST/DGSN personnel records was located -- an institutional silence that is itself analytically relevant. It is roughly an even chance that this reflects a deliberate non-disclosure posture consistent with the general opacity Moroccan security institutions maintain around operational incidents, rather than an absence of any response effort (confidence: low, since no direct evidence of either an active internal response or a deliberate silence policy was located); this is stated as a gap, not resolved by inference in either direction.

Intelligence collection and surveillance

The forensic and technical understanding of how Pegasus-class spyware operations are structured advanced materially in the period under review, though the earliest publicly documented technical indicator specific to Morocco's own networks considerably predates it: Citizen Lab's 2018 "Hide and Seek" study identified network-level indicators -- DNS-cache probing and TLS-fingerprinting anomalies -- consistent with a suspected Pegasus operator it codenamed "ATLAS," geolocated to Maroc Telecom's and Orange Maroc's own networks (autonomous system numbers 6713 and

36925 respectively) from August 2017 [30]. Citizen Lab's own report explicitly characterises this network-level mapping as "a guide for further investigation, rather than ironclad evidence," a methodological limitation stated by the source itself rather than imposed by this chapter, and it does not by itself establish which Moroccan agency, if any, operated the ATLAS footprint -- a question this section returns to below via the more recent Forbidden Stories reporting. Amnesty International's Security Lab published, in July 2026, its most detailed public technical account to date of Pegasus's evolution, drawing on previously unpublished NSO Group internal documents disclosed through the WhatsApp v. NSO US litigation [123]. That report documents NSO's "White Services" practice of creating customer-specific accounts and domains for each client, and states that two clusters within the original 2021 Pegasus Project leak map directly onto deployments the report labels "Sales 3" and "Sales 6," used for vendor demonstrations [123]. The same report references, without naming Morocco directly, an active follow-on Forbidden Stories investigative track explicitly focused on "Morocco's spying machine" [123] -- independent confirmation, from a separate forensic lab, that serious investigative attention to a Morocco-specific NSO customer relationship remained live as of mid-2026, three years after the original 2021 revelations (confidence: high on the fact that such a track exists; its own findings are a separate matter this chapter does not assess).

The DGST profile in an earlier chapter of this report already traces the 2021-2026 judicial history of the Pegasus infections of Prime Minister Pedro Sánchez, Defence Minister Margarita Robles and Interior Minister Fernando Grande-Marlaska in detail; this chapter adds one further, directly verifiable data point. A direct primary-source check of the Audiencia Nacional's own public judicial-news listing, covering 2 July to 7 September 2026, found no item referencing that investigation, nor any item naming Morocco, the DGST or the DGED [124]. This absence is consistent with, but does not independently confirm, press reporting that the case was archived for a second time in January 2026 citing lack of Israeli judicial cooperation; the gap between no visible current docket item and a specific, datable archival order is stated explicitly as unresolved rather than treated as settled (confidence: low on the archival date and reasoning specifically, moderate on the case's current judicial inactivity as reflected in the public listing).

On the standing question of which Moroccan agency, if any, actually operated this capability -- left open immediately above and revisited under *Capability model* below -- the most specific attribution located across this research is the Forbidden Stories consortium's own Spanish-edition reporting, which names DGST rather than DGED as the primary operating service, with DGED cast in a coordination-only role [34]. This is a materially more specific claim than Amnesty's own generic "Moroccan authorities" attribution language, but it rests on testimonial sourcing from a single pseudonymous former DGST officer relayed by one investigative consortium rather than on independent forensic or judicial confirmation; it is highly likely (confidence: moderate) that Moroccan state services, most likely DGST, operated Pegasus against domestic dissidents, journalists and Sahrawi activists from at least 2017, a judgment resting on cross-laboratory device-forensic corroboration of the underlying infections combined with a targeting pattern consistent with known Moroccan state interests, but a judgment that stops short of a firm DGST-versus-DGED institutional resolution given the single-sourced nature of the operating-agency claim specifically. The same reporting thread carries an ironic capability-transfer detail bearing directly on Spain-Morocco cooperation: Spain's Guardia Civil, via its GAO unit, is reported to have trained DGST personnel in surveillance tradecraft from 2014 onward, with some of those same trained officers later alleged, per testimonial sourcing, to have been involved in surveillance activity that reportedly extended to Guardia Civil trainers themselves [41]. This detail is stated here as reported and testimonially attributed, not judicially confirmed, consistent with the wider evidentiary caution this section applies throughout; if accurate, it would mean skills transferred for bilateral security

cooperation were later, on this account, turned back against the Spanish institution that provided the training.

The single most significant new lead concerning this dossier, examined in full under *DGED* in an earlier chapter, is an 8 September 2026 Spanish press report naming Mehdi Hijaouy -- described as former deputy head of the DGED and former director of a unit the reporting calls Service Action -- as having had access to Pegasus-related documentation used against the three Spanish ministers named above, and as currently a fugitive living between Madrid and Cáceres after fleeing Morocco roughly two years ago and later failing to appear at Spanish court hearings [125]. This claim rests entirely on unnamed Spanish security sources relayed by a single outlet and is unverified by any independent forensic, judicial or corroborating press source located here; it should be treated as a lead requiring urgent follow-up corroboration, not as an established fact (confidence: low), though if substantiated it would be the first named DGED defector directly tied to the Pegasus evidentiary chain.

At the EU level, the accountability environment around Pegasus-class spyware remained active in mid-2026 independent of the Spain-Morocco track specifically. A 6 July 2026 joint civil-society statement, following Citizen Lab's forensic confirmation that Greek MEP Stelios Kouloglou was infected with Pegasus in October 2022 and again in March 2023 while serving on the European Parliament's PEGA spyware-oversight committee, called on the European Commission to launch an independent investigation and to enforce the EU's Dual-Use Regulation against spyware vendors [126]. This item makes no reference to Morocco or Spain specifically, but demonstrates that EU-level spyware-accountability pressure persisted as a live political track more than four years after the original Pegasus Project revelations, situating the Sánchez/Robles/Grande-Marlaska infections within a broader pattern of unresolved EU parliamentary-level targeting rather than as an isolated Spanish episode (confidence: high on the fact of continued EU-level activity).

A named Spanish opinion column, logged here without endorsement, explicitly argues that the 2021 Pegasus infection of Prime Minister Sánchez's phone may have influenced Spain's April 2022 reversal of its historical Western Sahara position via a personal letter to King Mohammed VI [127]. Both underlying facts -- the 2021 infection and the 2022 policy shift -- are independently documented elsewhere in this report; the causal link between them is this columnist's own inference, unsupported by any government statement, investigation or corroborating source located here, and it is unlikely that open-source material currently permits a responsible judgment either confirming or ruling out that link (confidence: low, i.e. low confidence that a stronger judgment is currently possible in either direction).

Beyond the Pegasus track specifically, this same period saw an escalating Jabaroot leak campaign against Moroccan security-sector data, reaching, by August 2026, a threat to expose roughly 70,000 names of DGST-affiliated personnel; at least six mutually exclusive attribution theories are in circulation for that campaign, none forensically confirmed, and this chapter defers their full comparison to *Hacktivism and information confrontation* and *APT groups* below rather than duplicating the analysis here.

Military cyber, electronic warfare and C4ISR

This section's central and most consequential finding is a gap, stated plainly rather than filled by inference: no primary, technical or investigative-journalism source consulted for this chapter documents a named, dedicated cyber-warfare unit, a formal electronic-warfare command, or a unified C4ISR network-integration programme within the Royal Moroccan Armed Forces (FAR) or its military-intelligence apparatus [128]. This absence should not be read as evidence that no such capability or unit exists -- Moroccan military and security institutions are consistently and

deliberately opaque about internal organisational detail in open sources, a pattern already independently observed for DGSSI's and maCERT's own public self-description under *Defensive cybersecurity and incident response* above -- but it is a genuine, not merely cosmetic, information gap that materially limits what this chapter can assess (confidence: high that the gap itself is real, meaning high confidence that the underlying research method, rather than mere bad luck, failed to locate such material).

The only concrete FAR-relevant material located concerns tactical, platform-level electronic-warfare and reconnaissance equipment rather than a cyber unit or C4ISR programme: self-protection and radar-warning suites fitted to F-16s (ASPIS II, AN/ALR-93) and earlier F-5/Mirage F1 upgrades (Elettronica ECM pods, Thales radar-warning and data-link systems), two Gulfstream G550 aircraft configured for airborne early-warning and control with two more on order, and, historically, C-130 Hercules aircraft equipped with side-looking airborne radar used for enemy-unit detection during the Western Sahara conflict [128]. This material is sourced only to a tertiary compilation whose own internal citations could not be independently resolved here, and should be read strictly as a lead for follow-up primary-source verification, not as confirmed capability detail (confidence: low on any specific figure); the broader qualitative point that FAR operates some tactical EW/ISR equipment is itself uncontroversial and consistent with Morocco's documented foreign-supplier relationships discussed elsewhere in this report, but this chapter cannot go further than that without over-reading thin sourcing.

No evidence was located of a named cyber unit specifically within Morocco's military-intelligence apparatus, as distinct from the civilian-facing DGST and DGED services examined in an earlier chapter and from DGSSI's institutional placement under the Administration de la Défense Nationale, which is a defence-adjacent but not military-intelligence-specific channel. Given the almost total absence of open-source material on this specific question, it would be analytically irresponsible to offer a WEP-banded judgment on whether such a unit exists at all; this chapter instead states the gap and flags it as the single highest-priority follow-up target for any subsequent research pass, ideally consulting specialist defence-intelligence sources such as Janes or IISS that this research could not reach.

Cybercrime and digital forensics

Morocco's cyber-threat environment, as documented here, separates cleanly into four analytically distinct layers that this chapter treats separately throughout: financially motivated cybercrime investigated by conventional law enforcement, examined under *LEA in cyberspace* and *Cybercrime* below; a large, contested and overwhelmingly single-source hacktivism and hack-and-leak phenomenon centred on the actor known as Jabaroot or JabaROOT DZ, examined under *Hacktivism and information confrontation*; a supporting ecosystem of private and foreign commercial vendors plus a conspicuously thin academic-research layer, examined under *Other actors*; and a small number of technically documented, APT-grade operations, examined under *APT groups*. It is likely that this evidentiary asymmetry -- solid, named, multi-party corroboration for ordinary financial cybercrime cases against thin, single-source, actor-driven claims for the hacktivism material -- reflects a genuine difference in how these two activity types are policed and reported, rather than an artefact of this research's own search strategy (confidence: moderate, since the pattern held consistently across every source examined). Neither track should be conflated with the DGST/DGED intelligence-surveillance track profiled under *Intelligence collection and surveillance* above.

LEA in cyberspace

DGSN, Morocco's national police, built its cybercrime-investigation capability incrementally over more than a decade: a dedicated cell to combat cybercrime was created in 2007, a specialised central service followed in 2013 within the Judicial Police's Rabat directorate, and a National Office for combating technology-related crime was established in 2018 at the Casablanca-based Brigade Nationale de la Police Judiciaire (BNPJ), staffed with roughly a dozen judicial-police officers and a similar number of IT and telecoms technicians and engineers [129]. This central capability is backed, per the same source, by 29 regional cybercrime brigades covering practically all of Morocco's prefectures and provinces, and by seven named digital-forensics laboratories, in Rabat, Casablanca (two), Laâyoune, Fès, Marrakech and Tétouan [129]. This account names an on-record official -- Divisional Commissioner Marouane Hejjouji, chief of BNPJ's digital-forensics laboratory -- a genuine reliability upgrade over the anonymous-sourced material that dominates the hacktivism material examined below, though it remains an agency self-description relayed through press rather than an independently audited primary DGSN publication.

It is highly likely that DGSN's cybercrime-investigative and digital-forensic units possess genuine, not merely paper, operational capacity (confidence: moderate), a judgment resting not on the institutional-history account alone but on independently dated, named operational outcomes -- specifically the Operation Lyrebird arrest and the October 2022 Casablanca-airport INTERPOL-notice arrest detailed under *Cybercrime* below, both of which required functioning digital-evidence and international-liaison capability to reach a named suspect. By contrast, no comparably detailed public account of a dedicated cyber-forensic capability within the BCIJ, the DGST's judicial-police arm for terrorism casework, was located -- an explicit, stated gap rather than evidence the capability does not exist, and one this chapter deliberately does not paper over by inference from DGSN's separately documented strength. The DGSSI/maCERT civilian cybersecurity-regulator architecture, covered in depth above, is institutionally and functionally distinct from this law-enforcement investigative and forensic capability and is not repeated here.

Cybercrime

The clearest, most independently verifiable notable case on record is Operation Lyrebird, a two-year joint investigation by DGSN, INTERPOL and the named commercial threat-intelligence firm Group-IB that culminated in the arrest of a suspect using the alias Dr Hex, attributed by Group-IB to roughly 134 website-defacement and payment-fraud attacks between 2009 and 2018 targeting predominantly French-speaking enterprises and financial institutions [130]. This is a materially stronger evidentiary case than any item in the hacktivism record below: it names all three cooperating parties, a specific alias, an attack count with a stated methodology -- Group-IB's own tracking of a consistent digital signature left on compromised pages -- and quotes an on-record INTERPOL official [130]. A second, independently dated case, a 24-year-old suspect intercepted at Casablanca's Mohammed V International Airport on 18 October 2022 while attempting to board a Turkey-bound flight after border control flagged him against an INTERPOL wanted-persons notice for stolen-card fraud and international banking-account hacking, further corroborates that Moroccan border-control and judicial-police systems functionally interoperate with INTERPOL's notice system in dated, individually verifiable practice, not merely in principle [131].

At the regional-cooperation level, Moroccan press reported Morocco's participation in a multinational operation conducted between October 2025 and 28 February 2026 -- described by the reporting outlet as the first regional action of this scale -- that facilitated the exchange of roughly 8,000 intelligence elements among participating states, led to the seizure of 53 servers, and resulted in judicial proceedings against three individuals in Morocco, targeting phishing and malware-distribution infrastructure [132]. This operation's own specific codename, reported elsewhere as Ramz but outside the sources directly consulted for this chapter, could not be independently confirmed against a primary INTERPOL publication; the operation's existence and

headline statistics are treated as likely accurate (confidence: moderate, resting on a single Moroccan trade-press account) pending primary INTERPOL confirmation this research could not obtain. The table below collects these cases for quick reference.

Table 13. Notable financially-motivated cybercrime cases and cooperative operations.

Case/operation	Date	Cooperating bodies	Stated outcome	Evidentiary strength
Operation Lyrebird ("Dr Hex")	2009-2018 offending window; arrest reported 2026	DGSN, INTERPOL, Group-IB	Arrest of a suspect attributed to roughly 134 defacement/payment-fraud attacks	Strong: named parties, alias, attack count, on-record INTERPOL official
Casablanca-airport arrest	18 October 2022	DGSN border control, INTERPOL notice system	Suspect intercepted on an INTERPOL wanted-persons notice for stolen-card fraud and banking-account hacking	Moderate: dated, individually verifiable
October 2025-February 2026 regional operation	Oct 2025-28 Feb 2026	Morocco, INTERPOL, regional partners	~8,000 intelligence elements exchanged; 53 servers seized; judicial proceedings against 3 individuals	Moderate: single Moroccan trade-press source; primary INTERPOL confirmation not obtained

Separately, Kaspersky-sourced research reported that 49.3% of messaging-based fraud cases against Moroccan victims concluded within 30 minutes of first contact, with average financial losses of USD 733 per victim, exceeding USD 1,350 in some cases, predominantly via WhatsApp, Facebook and Telegram impersonation of trusted contacts or brands [133]. It is likely that this fast-moving social-engineering fraud pattern represents a distinct, larger-volume threat to ordinary Moroccan consumers than the state-linked breach narrative that dominates the remainder of this chapter (confidence: moderate, based on Kaspersky's own stated methodology, though this figure is company-derived research rather than an independently audited national statistic).

Hacktivism and information confrontation

The dominant hacktivism actor documented in this research operates under the name Jabaroot, also styled JabaROOT or JabaROOT DZ, first identified in April 2025 with the breach of Morocco's National Social Security Fund (CNSS), examined under *Defensive cybersecurity and incident response* above, and escalating through a chain of claimed leaks -- the Ministry of Economic Inclusion, the Justice Ministry, the national road-safety agency NARSA, the ANCFCC property registry, the CNOPS social-coverage fund, a claimed 17-million-record breach of the RAMED medical-assistance database on 20 August 2026, and, from August 2026, a claimed 70,000-record dataset naming DGST/DGSN personnel -- explicitly framed by the actor as retaliation for an earlier pro-Morocco compromise of the Algerian Press Service's X account and, from August 2026, tied explicitly to the Ceuta migration crisis under the campaign banner "#OP_CEUTA" [122]. The RAMED claim carries its own internal, source-flagged discrepancy:

the claimed 17 million records exceed the 10.83 million records actually migrated from RAMEL into its December 2022 successor scheme, AMO-Tadamon, a discrepancy the reporting outlet itself notes but does not resolve, and which this chapter treats as a single unnamed-source claim rather than a confirmed breach of any particular scale [134]. It is almost certainly the case that this represents a sustained, multi-year campaign rather than a series of unrelated incidents, given the consistent branding, Telegram distribution pattern and self-referential escalation across more than a dozen independently reported tranches (confidence: high, since this chronology is corroborated across Spanish, Moroccan and Algerian press and at least two independent technical checks detailed below).

Whether Jabaroot denotes a single actor, a small coordinated group or a loosely shared brand used by more than one party remains explicitly unresolved in every source reviewed, including a dedicated tertiary compilation whose own conclusion is that the actor's origin remains unresolved [135]. At least five mutually exclusive attribution theories are in circulation, and none is forensically confirmed: the Moroccan government's own position that Jabaroot is an instrument of the Algerian state; an independent-hacktivist reading; a specialist consultancy's, Navakintelligence's, hypothesis that a single former Moroccan intelligence operative, acting alone, is responsible [136]; a claim, attributed to a firm named Zecurion only via a tertiary compilation and not independently traceable to any primary report consulted here, that technical indicators point to a Tunisian-origin engineer resident in Germany [135]; and the possibility, raised by the Hijaouy lead examined under *Intelligence collection and surveillance* above, that a named former DGED officer is connected to the leaks [125, 137]. The table below sets all five out side by side.

A sixth theory, reported by Le Monde and relayed via the Algerian outlet TSA (Tout sur l'Algérie), holds that the leaks are the work of five named-in-substance former DGST agents -- four officers and one commissioner -- who broke with the service and exiled themselves to Europe, and are said to be acting from institutional and personal grievance, demanding leadership changes and citing abuse of personal data in wiretapping and investigations [138]. This theory has some internal coherence with the leak's own content -- its targeting of specifically security-personnel data, its exculpation of the King while personally blaming named security-service leadership, and its threats of further Ceuta-linked revelations all sit more comfortably with an insider grievance narrative than with a purely external, opportunistic hacktivist or foreign-intelligence operation -- but it remains Le Monde's own single-sourced reporting, relayed at second hand by an Algerian outlet with an evident interest in discrediting the Moroccan government's own Algerian-state-sponsorship framing, and it is not independently confirmed by any technical indicator located across this research (confidence: low, exactly as for each of the other five theories individually). It is highly unlikely that all six theories can be correct simultaneously (confidence: high), and Morocco's own preferred narrative -- Algerian state sponsorship -- is itself independently doubted by cybersecurity-sector and intelligence sources cited within the same Moroccan and Spanish press reporting that carries it, a point this chapter weighs rather than treats as more evidentially established than its actual sourcing supports, since that narrative also serves Rabat's own institutional interest in externalising blame.

Table 14. Competing attribution theories for the Jabaroot/JabaROOT DZ campaign.

Theory	Proponent	Evidentiary basis	This report's confidence
Algerian-state-directed	Moroccan government / official Moroccan position	Rabat's consistent public framing; no independent forensic corroboration	Low
Independent hacktivist collective	General open-source commentary	Consistent with observed tactics; not	Low

		separately substantiated	
Lone former Moroccan intelligence operative	Navakintelligence (Spanish consultancy)	Specialist-consultancy assessment relayed in regional press	Low
Tunisian-origin engineer based in Germany	Firm named "Zecurion" (untraced)	Cited only via a tertiary compilation; not independently traceable to any primary report	Low (untraced)
Named former DGED officer (Hijaouy-linked)	Single-outlet Spanish press, unnamed security sources	Reported access to Pegasus material; unverified by independent forensic or judicial source	Low

It is a roughly even chance that any single one of these six theories is correct in isolation (confidence: low, individually, for each), and only a moderate-confidence higher-order judgment is defensible: that the campaign's access to specific, sensitive and in at least one case previously unpublished personal data is more consistent with insider-adjacent access than with a purely external, opportunistic hacktivist operation (confidence: low-to-moderate) -- a reading the sixth, DGST-exile theory above would, if accurate, directly explain, though it does not thereby become more confirmed than the other five. Which, if any, of the six is accurate remains genuinely unresolved on the open-source record as assembled here, and no hypothesis should be adopted above roughly-even-chance, low-confidence standing; this is a genuinely unresolved attribution problem, not a case where one explanation merely awaits confirmation.

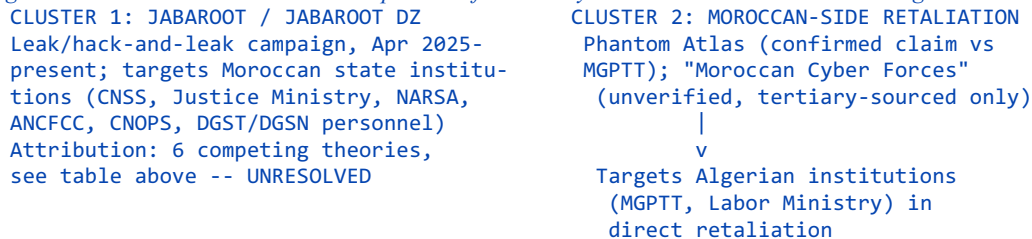
Morocco's own security services have not stood silent: DGSN and DGST publicly and categorically denied any intrusion into their systems following the August 2026 DGST/DGSN-personnel leak claim, stating the data instead originates from older insurance and social-coverage records and that their operational networks are not connected to networks open to the internet, with independent analysts cited in the same reporting finding the claimed 70,000-record figure implausibly large, since many named individuals were ordinary police officers, deceased persons, or had recruitment dates no later than 2020 [139]. This official counter-narrative is itself unverified and self-interested, exactly as the leak claims it disputes are unverified and actor-interested, and this report weighs both symmetrically rather than defaulting to either. A separate, independent technical check by the commercial threat-intelligence vendor CybelAngel of the earlier ANCFCC property-registry leak reached a genuinely mixed verdict: the sampled 4.8 GB, roughly 20,000-document archive it acquired contained no high-alert malware in its "VIPs" subset, but Jabaroot never delivered the claimed full 10-million-record, four-terabyte dataset, and CybelAngel's own analysis found no direct links between Jabaroot and other groups such as Keymous+ [140].

Morocco-aligned hacktivism runs in the opposite direction as a documented, if thinner, mirror image: a group self-identified as Phantom Atlas claimed, within 24 hours of the original April 2025 CNSS breach, to have exfiltrated over 13 GB of data from Algeria's postal and telecommunications-workers mutual fund (MGPTT) and internal Algerian Labor Ministry documents, framed explicitly as retaliation [141]. A second Moroccan-attributed name, "Moroccan Cyber Forces," is cited in a tertiary compilation as having conducted a similar retaliatory claim on 10 April 2025, but could not be independently traced to any primary or press source consulted here and is logged as an unverified, tertiary-sourced claim only [135]. Separately, this research's clearest independent technical source establishes that a third actor, Keymous+, associated

elsewhere with pro-Palestine-motivated DDoS activity against Moroccan government targets, is assessed as operationally distinct from Jabaroot rather than a shared identity, despite temporal and regional overlap [140].

It is likely that Morocco's hacktivism landscape in the period under review comprised at least three functionally separate threat clusters -- the Jabaroot/JabaROOT DZ leak campaign, a smaller Moroccan-side retaliatory cluster, and a distinct pro-Palestine DDoS cluster -- rather than one unified campaign or a two-sided binary rivalry (confidence: moderate, based on CybelAngel's explicit non-linkage finding and the differing tactics, mass data leaks versus DDoS, each cluster employs). The figure below sets out this three-cluster structure.

Figure 13. Morocco's hacktivism landscape: three functionally distinct clusters rather than a single two-sided rivalry.



CLUSTER 3: PRO-PALESTINE DDoS (Keymous+)
DDoS activity against Moroccan government targets;
CybelAngel: technically DISTINCT from Jabaroot despite temporal/regional overlap -- no shared infrastructure found

The information-confrontation dimension of this campaign extends beyond data disclosure into explicit political demands and unverified third-country claims: Jabaroot has demanded an official Moroccan apology, a national-mourning declaration and postponement of the 23 September 2026 legislative elections, and has separately claimed, via Telegram messaging relayed by an outlet with an acknowledged pro-Sahrawi advocacy orientation, that an alleged Moroccan migration-pressure scheme involved US and Israeli knowledge, a claim treated here as unverified and actor-sourced rather than established [142]. A specialist Spanish cybersecurity outlet's own August 2026 synthesis explicitly cautions against premature attribution on both the Pegasus and JabaROOT tracks simultaneously, framing the core risk as the proliferation of actors of uncertain attribution operating in a grey zone between hacktivism, state interests and disinformation [143].

It is likely that this pattern -- data leaks paired with explicit political demands and unverifiable geopolitical claims -- should itself be read as evidence that Jabaroot's messaging functions as an information operation, not solely as a data-breach disclosure mechanism, regardless of how its underlying data-access question is ultimately resolved (confidence: moderate). A further downstream effect flagged in press analysis is potential damage to Morocco's African security-cooperation relationships, since the personnel-data leak could in principle allow adversaries to cross-reference identities against roughly twenty African partner states' training and liaison records [144], though this specific judgment is the cited outlet's own analytical inference rather than an independently confirmed effect.

Other actors

Beyond the state law-enforcement and hacktivism/APT layers already covered, Morocco's cyber ecosystem includes a private commercial-vendor sector, at least one documented foreign-vendor partnership structure, and a conspicuously thin open-source academic-research footprint -- three sub-layers this chapter treats in turn below, each grounded in what direct primary-source checks could and could not establish, rather than in general industry knowledge.

Private vendors

FIRST, the Forum of Incident Response and Security Teams, an official international CSIRT-coordination body, lists seven Morocco-registered incident-response teams in its public member directory: maCERT, the state CERT already profiled under *Defensive cybersecurity and incident response* above; Dataprotect-CSIRT; Cires Technologies CyberSOC; DXC-CDG Cyber Defense, examined for its foreign-vendor dimension under *Foreign vendors* below; SEKERA CSIRT; LMPS CERT; and CERT-BAM, Bank Al-Maghrib's own incident-response team [145]. This directly evidences a maturing, multi-actor Moroccan CSIRT ecosystem extending well beyond the national CERT into banking and at least four privately operated CSIRTs and CyberSOCs, a genuinely positive institutional-capacity indicator independent of the more contested hacktivism material examined above. The table below collects all seven for quick reference.

Table 15. Morocco-registered CERT/CSIRT teams listed in FIRST's member directory.

Name	Character	Parent institution/owner
maCERT	State CERT	DGSSI (Administration de la Défense Nationale)
Dataprotect-CSIRT	Private	DataProtect
Cires Technologies CyberSOC	Private	Cires Technologies
DXC-CDG Cyber Defense	Joint venture (foreign/state-linked)	DXC Technology (US) + Caisse de Dépôt et de Gestion (Morocco)
SEKERA CSIRT	Private	SEKERA
LMPS CERT	Private	LMPS
CERT-BAM	Banking/central bank	Bank Al-Maghrib

DataProtect, whose own corporate site was directly consulted for this research, describes a service catalogue spanning 24/7 CyberSOC and CSIRT monitoring, managed security services, offensive-security penetration testing, governance and compliance support, cloud security, critical-infrastructure protection and a dedicated Cyber Skills Lab training offering, serving banking, insurance, government and industrial clients across a stated pan-African footprint from its Casablanca headquarters [146]. It is likely that DataProtect and Cires Technologies represent Morocco's most internationally recognised private cybersecurity vendors, given their independent confirmation in FIRST's own directory rather than reliance on marketing self-description alone (confidence: moderate); a direct fetch of Cires Technologies' own corporate site failed for this research, leaving its specific service catalogue known only via the FIRST listing, an explicit, namable gap.

Foreign vendors

The clearest documented foreign-vendor relationship within this chapter's scope is DXC-CDG Cyber Defense, a joint CSIRT structure combining DXC Technology, a US-headquartered global IT-services firm, with CDG, the Caisse de Dépôt et de Gestion, a major Moroccan public financial institution, independently confirmed via FIRST's own member directory [145]. This is a legitimate defensive-side foreign-vendor partnership, structurally distinct from -- and considerably less contested than -- the surveillance-vendor relationships addressed below regarding NSO Group and Pegasus, examined in full under *Intelligence collection and surveillance* above and *DGST* and *DGED* in an earlier chapter; Pegasus itself, per that fuller record, is a wholly commercial, Israeli product that has been used against domestic journalists and activists, foreign heads of government including France's Macron and Spain's Sánchez, and over 6,000 Algerian phone numbers, the last reportedly a contributing factor in Algeria's August 2021 rupture of relations with Morocco [147]. On the surveillance-vendor side specifically, a targeted, direct check of Amnesty International Security Lab's own July 2026 technical report on Pegasus's evolution for any documented Morocco

linkage to a vendor other than NSO Group -- Circles, Candiru, Intellexa/Predator, Cytrox, DarkMatter -- found none: Intellexa/Predator appears in that report only as an unrelated cross-reference, with no Morocco nexus stated [123]. It is unlikely that open-source reporting currently documents any Morocco-linked surveillance-vendor relationship beyond NSO/Pegasus (confidence: moderate, since this is an actively tested absence against a current, credible forensic source rather than an assumption from silence, though it cannot rule out an undisclosed relationship). This specific gap has proven consistent across successive passes of research on Morocco's cyber domain and is stated here as a standing, not merely one-off, limitation of the available open-source record. Against that consistent absence, a single Spanish outlet, Merca2, separately claims that Morocco spends more than EUR 50 million annually on additional Western surveillance and interception tooling beyond NSO/Pegasus -- naming BAE Systems' "Evident" mass internet-traffic-surveillance product, L3Harris's "Hailstorm" IMSI-catcher, Cellebrite device-extraction tooling, and Italian firm Memento Labs' "RCS," a successor product line to Hacking Team's -- financed, per the same report, through an Abu Dhabi-based intermediary, and further alleges that Maroc Telecom and Orange Maroc maintain direct server connections to DGST enabling interception outside judicial oversight [148]. This claim was directly tested against Amnesty's own July 2026 Pegasus report, examined above, and found no corroboration there for any of these named tools or the alleged telecom-operator server connections; it rests on a single outlet's own investigative reporting rather than on independent forensic or judicial confirmation, and should be treated as an unconfirmed lead rather than established capability (confidence: low).

Table 16. Foreign commercial vendors named in this collection, confirmed and checked-and-absent.

Vendor	Country	Product/service	Morocco link	Evidentiary basis
NSO Group	Israel	Pegasus (mobile-device intrusion)	Confirmed	Amnesty International Security Lab forensic reporting; foreign-government confirmations (see *Intelligence collection and surveillance* and DGST/DGED profiles in an earlier chapter)
DXC Technology	United States	Joint defensive CSIRT (DXC-CDG Cyber Defense)	Confirmed (legitimate, defensive-side partnership)	FIRST member directory
Circles, Candiru, Intellexa/Predator, Cytrox, DarkMatter	Various	Commercial intrusion/surveillance tooling	Checked, not found	Direct check of Amnesty's July 2026 technical report found no Morocco nexus for any of these vendors

The academia

No named, dedicated Moroccan academic cybersecurity research centre, chair or laboratory was identified in the material reviewed for this chapter. Direct checks for cybersecurity-specific research activity at ENSIAS, the École Nationale Supérieure d'Informatique et d'Analyse des Systèmes, and at INPT, the Institut National des Postes et Télécommunications, surfaced only general engineering content and a Master Data & IA programme listing, with no cybersecurity-specific chair, laboratory or publication record identified, and a check of UM6P's homepage likewise surfaced no cybersecurity-specific content within the page depth reached. This is stated explicitly as a research gap rather than evidence that no such academic capacity exists in Morocco -- university research pages are frequently not indexed at the depth a single-page fetch reaches, and a more targeted search of individual faculty publication pages or a dedicated Moroccan academic-conference proceedings archive was not possible within this research's scope.

It is roughly an even chance that Morocco's cybersecurity-skills pipeline currently runs predominantly through private-vendor training offerings, such as DataProtect's own Cyber Skills Lab examined under *Private vendors* above, rather than through a named, internationally visible academic research centre (confidence: low, an inference from the private-vendor material's relative visibility rather than from any comparative enrolment or output data, which was not located for either channel).

APT groups

The single most technically substantiated threat actor within this chapter's scope is Starry Addax, publicly documented by Cisco Talos in April 2024: a spear-phishing campaign against human-rights defenders associated with the Sahrawi Arab Democratic Republic (SADR) and Western Sahara cause, using a custom Android malware family, FlexStarling, that masquerades as the Sahara Press Service's mobile application, alongside Windows-targeting credential-harvesting infrastructure and a Firebase-based command-and-control channel [149]. It is likely that Starry Addax represents a resourced, purpose-built operation specifically interested in the Western Sahara political conflict, given Talos's own disclosed indicators -- custom malware development, dedicated attacker-controlled domains, and Talos's own assessment that the timelines connected to various artefacts indicate the campaign is just starting (confidence: moderate); it is unlikely that the available open-source technical record permits attribution of Starry Addax to any specific government, since Talos's own report makes no nation-state attribution and no subsequent report resolving that question was located (confidence: low, i.e. low confidence that a stronger judgment is currently responsible).

Whether Jabaroot itself should be characterised as APT-adjacent -- a resourced, possibly state-security-insider-linked operation using a hacktivist façade -- or as a genuinely independent hacktivist and leak actor remains the single largest unresolved attribution question in this chapter, and it is not resolved here; the competing theories, and the low-to-moderate confidence judgment that the campaign shows insider-adjacent characteristics without confirming any specific sponsor, are set out in full under *Hacktivism and information confrontation* above rather than repeated. Combining the two cases, it is likely that Morocco's Western Sahara-adjacent cyberspace in the period under review contained at least two analytically separate technically relevant threads -- a confirmed-but-unattributed, purpose-built espionage tool targeting Sahrawi civil society specifically, and a much larger, noisier, contested leak and hacktivism campaign targeting Moroccan state institutions whose sponsor, if any, remains unconfirmed by any forensic or judicial source located across this research to date (confidence: moderate on the analytical separateness of the two threads, given their entirely distinct targeting, tooling and evidentiary bases).

No dedicated open-source reporting of a named FAR or DGSSI offensive-cyber unit conducting attributed operations against Polisario- or Algeria-linked targets was located, consistent with the

broader gap already documented under *Military cyber, electronic warfare and C4ISR* above; this absence is recorded as a stated gap rather than inferred into either a capability claim or a capability denial, and it is likely, on the balance of what is documented across this chapter, that Morocco's offensive cyber model generally is procurement-led rather than development-led (confidence: moderate), consistent with the vendor-acquisition pattern documented under *Foreign vendors* above.

Key dependencies

This chapter examines Morocco's digital and critical-infrastructure dependencies -- the physical and logical chokepoints through which the Kingdom's connectivity, cloud, and telecommunications-ownership structures run, and the degree to which each rests on foreign ownership or foreign vendor supply. Several sub-topics below carry genuine evidentiary gaps in open-source reporting, a direct consequence of research conducted without web-search capacity; these gaps are stated explicitly rather than filled with inference.

Morocco's international data connectivity is anchored on a small, geographically concentrated set of submarine cable systems rather than a redundant global mesh. The Medusa cable -- approximately 8,700km, 24 fibre pairs at 20 Tbit/s each, led by the AFR-IX Telecom consortium -- lands at Tetouan and Nador, with a stated December 2025 shore-end completion at Nador [150], while older systems, ACE, the direct Estepona-Tetuán crossing, Atlas Offshore (Morocco-France) and EURAFRICA (Portugal-Morocco-France), provide the remaining direct links to Europe and West Africa [151]. It is likely that this cable set gives Morocco adequate aggregate capacity for current demand (confidence: moderate), but the physical concentration of landings around the narrow Strait of Gibraltar corridor -- Tetouan and Nador on the Moroccan side, the Estepona/Tarifa area on the Spanish side -- is a structural chokepoint: a significant fraction of Morocco's international bandwidth transits a single, historically anchor-drag-prone strait segment, and consortium ownership, exact capacity and ready-for-service dates for ACE, Estepona-Tetuán and Atlas Offshore beyond their landing-point names could not be established, leaving the precise redundancy picture only partially documented [151].

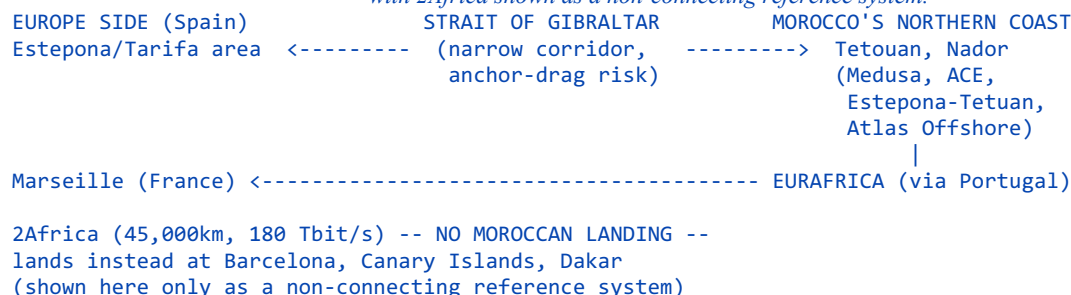
Morocco is, on current evidence, bypassed by the largest transcontinental cable investment of the decade: the 45,000km, 180 Tbit/s 2Africa system, backed by Meta, MTN, Orange, Vodafone, China Mobile, STC, Telecom Egypt and WIOCC and declared complete by Meta in November 2025, lands at Barcelona, the Canary Islands and Dakar but not at any Moroccan point [152]. It is likely that this non-landing reflects deliberate routing choices by the 2Africa consortium rather than a Moroccan policy decision (confidence: low, given no consortium statement on the reason was located), but the practical effect is that Morocco does not directly benefit from 2Africa's open-access wholesale capacity and remains dependent on its smaller, older cable set for west-African and transatlantic-adjacent routing redundancy -- a documented capacity and redundancy gap rather than a confirmed vulnerability, since no evidence was found that Morocco's current aggregate international bandwidth is actually insufficient. The table and figure below collect this cable set for reference.

Table 17. Submarine cable systems serving Morocco, and the 2Africa non-landing contrast.

Cable	Morocco landing point(s)	Other landings	Capacity	Consortium/owner	Notes/status
-------	--------------------------	----------------	----------	------------------	--------------

Medusa	Tetouan, Nador	19 sites across the Mediterranean/southern Europe	~8,700 km; 24 fibre pairs at 20 Tbit/s each	AFR-IX Telecom-led consortium	Nador shore-end completed December 2025
ACE (Africa Coast to Europe)	Named as a Moroccan-landing system	West/southern Africa, Europe	Not established	Not established	Ownership/capacity/RFS date could not be sourced beyond the landing-point name
Estepona-Tetuán (direct crossing)	Tetuán	Estepona, Spain	Not established	Not established	Ownership/capacity/RFS date could not be sourced beyond the landing-point name
Atlas Offshore	Morocco	France	Not established	Not established	Ownership/capacity/RFS date could not be sourced beyond the landing-point name
EURAFRICA	Morocco	Portugal, France	Not established	Not established	Ownership/capacity/RFS date could not be sourced beyond the landing-point name
2Africa (contrast row — no Moroccan landing)	None	Barcelona, Canary Islands, Dakar	~45,000 km; 180 Tbit/s	Meta, MTN, Orange, Vodafone, China Mobile, STC, Telecom Egypt, WIOCC	Declared complete by Meta, November 2025; bypasses Morocco

Figure 14. Morocco's submarine-cable topology: landings clustered on the northern coast against the Strait of Gibraltar chokepoint, with 2Africa shown as a non-connecting reference system.



Morocco's largest fixed and mobile operator, Maroc Telecom, has been majority-owned by Etisalat by e& of the UAE since Vivendi sold its 53% stake for approximately USD 4.2 billion in July 2013, with the Moroccan state retaining roughly 22% and the remainder in free float across the Casablanca and Paris exchanges [95]. This places the operator with the largest African-continent subsidiary footprint -- Mauritania, Gabon, Mali, Chad, Côte d'Ivoire and others -- under the

ultimate control of an Emirati state-linked entity, almost certainly a fact rather than a judgment given the well-documented 2013 transaction value, though the specific ownership-percentage breakdown itself rests on tertiary sourcing that could not be confirmed against a primary AMMC or investor-relations filing, both attempted retrievals having returned access errors [95]. This ownership structure is analytically significant less for day-to-day network operation than for the standing possibility of UAE-linked strategic influence over Morocco's dominant telecom infrastructure operator.

Orange Maroc, formerly Méditel and Morocco's second major operator, is roughly evenly split between Orange S.A. of France, which built its stake from 40% in 2010 (EUR 640 million) to 49% by 2015, and the Moroccan investor groups Finance Com and the Caisse de Dépôt et de Gestion (CDG), a state-linked institutional investor [96]. It is roughly an even chance that Orange's stake has since crossed 49%, given the general pattern of foreign-partner consolidation seen at Maroc Telecom (confidence: low, no 2024-2026 update located), but as documented this leaves Orange Maroc formally majority-Moroccan-owned even while operationally and technically dependent on the Orange Group's French corporate parent for network equipment standards, vendor relationships and technical support -- a softer, less quantifiable dependency than Etisalat's majority stake in Maroc Telecom, but a real one. Morocco's third operator, Inwi, formerly Wana Corporate, is held jointly by Al Mada, the Moroccan royal-family-linked holding company profiled under *The Makhzen* in an earlier chapter, and the Kuwaiti Zain Group, which took a 31% stake in February 2009 [153]; whether Zain's stake has changed since 2009 could not be established, a Zain Group investor-relations fetch having returned an unresolved redirect, so the current Gulf-ownership percentage in Morocco's third-largest operator is an explicitly flagged open item rather than a settled fact.

Taken together, all three of Morocco's licensed telecom operators carry a substantial non-Moroccan ownership component -- UAE, France and Kuwait respectively -- meaning Morocco's entire commercial telecom sector sits under partial foreign corporate control, a structural condition distinct from, and in addition to, any foreign-government regulatory leverage. The table and figure below collect this ownership structure for quick reference.

Table 18. Ownership structure of Morocco's three licensed mobile network operators.

Operator	Majority/plurality shareholder	Share	Country	Notes
Maroc Telecom (IAM)	Etisalat by e&	53% (since July 2013, ~USD 4.2bn transaction)	UAE	Moroccan state retains ~22%; remainder in free float (Casablanca/Paris exchanges)
Orange Maroc	Orange S.A.	40% (2010) rising to 49% (2015)	France	Remainder held by Finance Com and Caisse de Dépôt et de Gestion (Morocco); post-2015 stake unconfirmed
Inwi (Wana Corporate)	Al Mada + Zain Group	Al Mada majority; Zain 31% (since Feb 2009)	Morocco (Al Mada) / Kuwait (Zain)	Whether Zain's stake has changed since 2009 could not be established

Figure 15. Ownership structure of Morocco's three mobile network operators.

Etisalat/e& (UAE) --53%--> MAROC TELECOM <--~22%-- Moroccan state
 (remainder: free float,
 Casablanca/Paris exchanges)

Orange S.A. (France) --40-49%--> ORANGE MAROC <--remainder-- Finance Com,
 CDG (Morocco)

Al Mada (Morocco,
 royal-linked holding) --> INWI (Wana Corporate) <--31% (2009,
 unconfirmed since)-- Zain
 Group
 (Kuwait)

Morocco has no domestic hyperscale cloud-computing presence: direct checks of Microsoft's and Google's own infrastructure pages confirm that neither Azure nor Google Cloud operates a region in Morocco, with the nearest African regions in South Africa for both providers and Gulf regions in the UAE, Qatar and Saudi Arabia for Azure or Saudi Arabia for Google Cloud instead [154, 155]. Cloudflare's published network map corroborates the same pattern from a content-delivery and DDoS-mitigation angle: it lists 33 African cities but none in Morocco or elsewhere in North Africa [156]. It is almost certain that any Moroccan government, financial-sector or enterprise workload hosted on a major Western hyperscaler physically resides outside Moroccan jurisdiction, most plausibly in a European or Gulf data centre (confidence: high, given three independent official corporate sources agree on the absence). This is a foundational digital-sovereignty dependency: data residency, cloud-service latency and continuity of service for any Moroccan organisation using these providers are all conditioned on infrastructure and legal jurisdiction outside Morocco. The table below collects this cloud and CDN presence for reference.

Table 19. International hyperscale cloud and CDN presence relevant to Morocco.

Provider	Nearest region/PoP to Morocco	Region/PoP inside Morocco (Y/N)	Notes
Microsoft Azure	South Africa; Gulf regions (UAE, Qatar, Saudi Arabia)	N	Confirmed absent via Microsoft's own infrastructure page
Google Cloud	South Africa; Saudi Arabia	N	Confirmed absent via Google's own infrastructure page
Cloudflare	33 African cities listed, none in Morocco/North Africa	N	Confirmed via Cloudflare's own published network map
AWS	Not established	Unverified	Flagged as unverified in this research pass

Morocco's mobile and fixed-network equipment-vendor base -- whether Huawei, Nokia, Ericsson, ZTE or another supplier predominates -- could not be established: a targeted check of Huawei's own profile found no Morocco-specific content at all, leaving vendor identity an explicit, unresolved gap rather than a documented finding [157]. This matters directly for this report's core theme, since a Huawei-dominated network would raise materially different foreign-leverage and allied-interoperability considerations, given sustained US/EU scrutiny of Huawei in critical infrastructure, than a Nokia- or Ericsson-dominated one; this gap should be treated as a priority item for future research rather than assumed in either direction.

Morocco's digital infrastructure sits on an energy base that is itself import-dependent: the country is characterised as the largest energy importer in northern Africa, with negligible domestic hydrocarbon production and a historically coal-heavy generation mix -- major plants at Mohammedia and Jorf Lasfar burning imported South African and Polish coal -- even as

renewables targets rise toward a stated 52% of installed capacity by 2030 [158]. It is likely that this import dependency extends to the electricity ultimately powering Morocco's telecom networks and any future data-centre buildout, since digital infrastructure draws on the same national grid rather than a ring-fenced supply (confidence: moderate, an inference from the generation-mix data rather than a source explicitly discussing telecom-sector energy security, a gap that could not be closed here). Morocco's cross-Strait electrical interconnection with Spain is a related, separately load-bearing dependency that could not be sourced in detail for this chapter, and should be treated as a firm follow-up requirement rather than assumed from general knowledge.

Morocco's semiconductor and hardware-manufacturing footprint is limited to back-end assembly and test: STMicroelectronics' Bouskoura facility performs chip packaging and testing, plus, since 2022, a silicon-carbide production line for electric-vehicle applications, but no front-end wafer fabrication exists in the country [159]. This is almost certainly best read as a downstream link in STMicroelectronics' own European and Asian-anchored supply chain rather than an indigenous semiconductor capability (confidence: high, given the back-end-only characterisation is unambiguous in the source), meaning Morocco's telecom and electronics sectors remain fully dependent on imported integrated circuits and networking hardware for anything beyond this narrow assembly-and-test niche. Beyond semiconductors, no national AI-specific capability programme, no semiconductor-design (as opposed to assembly-and-test) capacity, no quantum-computing research programme and no post-quantum-cryptography migration initiative was identified anywhere in the material reviewed for this chapter; this is stated as an explicit research gap rather than evidence of genuine absence, since the underlying collection was oriented toward press and regulatory-document sources rather than a dedicated technical-sector survey, but it is nonetheless a further, cumulative data point in the same dependency pattern this section documents throughout.

Morocco's satellite-reconnaissance capability -- the Mohammed VI-A (2017) and Mohammed VI-B (2018) optical-imaging satellites -- was built entirely by the French and European industrial base, Airbus Defence and Space and Thales Alenia Space, on the Astrosat-1000 bus, and launched on the European Vega rocket, at a total programme cost reported around EUR 500-600 million [36, 37]. It is highly likely that Morocco cannot independently sustain, repair or replace this capability without renewed foreign contracting (confidence: moderate, based on the manufacturer and launcher dependency and the absence of any sourced ground-segment or exploitation-autonomy detail), and the satellites' comparatively short, approximately five-year design life means Morocco faces a near-term renewal decision that will almost certainly reprise the same foreign-industrial dependency [36]. Which Moroccan institution, DGST or DGED, actually holds satellite tasking authority could not be determined, a gap flagged explicitly rather than assumed, and one *Capability model* below returns to directly.

Morocco has no documented indigenous ground-segment infrastructure for satellite positioning, navigation and timing: a targeted check of GPS control-segment and monitor-station listings found stations across the Americas, the Atlantic, the Middle East and Australasia, but none in Morocco or North Africa, and no reference to EGNOS or Galileo ground-segment presence in the country either [160]. This is a genuine absence finding rather than a confirmed non-existence claim (confidence: low on the absolute absence, since failure to find is not proof of non-existence, though the finding is consistent across the sources checked), and it means Morocco's civil and military positioning, navigation and timing services -- used across telecom-network timing, financial-transaction synchronisation and any precision-guided military capability -- rest entirely on foreign-operated satellite constellations with no indigenous ground-segment leverage or fallback.

Part V. Assessment

Capability model

Morocco's offensive and collection track combines a longstanding indigenous signals-intelligence processing capability with an entirely foreign-sourced intrusion tool. The DGST's Police des Communications Radioélectriques (PCR) unit reportedly intercepts thousands of communications daily and, as of a 2010-era description, runs automated keyword search, speech-recognition call analysis and handwriting-recognition document analysis -- an indigenous SIGINT-processing capacity distinct from anything vendor-supplied [161]. Layered on top of this, Morocco's most consequential documented intrusion capability, mobile-device compromise via Pegasus, is a wholly commercial, Israeli product used against domestic journalists and activists, foreign heads of government including France's Macron and Spain's Sánchez, and over 6,000 Algerian phone numbers, the last reportedly a contributing factor in Algeria's August 2021 rupture of relations [147]. The specific operating agency behind this capability is better, if still not conclusively, evidenced than an outright gap: the Forbidden Stories consortium's Spanish-edition reporting, examined in full under *Intelligence collection and surveillance* above, names DGST rather than DGED as the primary operator, with DGED cast in a coordination-only role, on testimonial sourcing from a single former DGST officer [34]. It is highly likely that Morocco's most strategically consequential collection capability is vendor-dependent rather than indigenous, and likely, at moderate-to-low confidence given the single-sourced nature of the specific agency claim, that DGST rather than DGED is the operating service (confidence: moderate on vendor-dependency, moderate-to-low on the DGST-specific attribution), which places NSO Group's own export-licensing decisions and Israeli government policy as an external constraint on Morocco's offensive-cyber posture regardless of which service ultimately operates it.

The same offensive and collection track extends into space: the Mohammed VI-A/B optical-reconnaissance satellites, examined for their dependency dimension under *Key dependencies* above, give Morocco imagery capability exceeding that of any other African state on the open-source record reviewed [37], but the capability is French/European-built, has a short design life, and its institutional operator or tasking authority, DGST versus DGED, is not established by any source consulted [162]. DGED itself, Morocco's external intelligence service profiled in full in an earlier chapter -- roughly 4,000 personnel as of a 2003 estimate, 60% drawn from the Royal Armed Forces and the remainder civilian, with 250 to 300 agents estimated abroad and partnerships weighted toward France's DGSE and Francophone Africa -- appears from open sources to function as a liaison and collection network rather than a technology-development organisation [162]. Taken together, it is likely that Morocco's offensive and collection track is best characterised as broad in ambition and reach but structurally dependent on foreign hardware, foreign vendors and foreign industrial partners at nearly every technical layer (confidence: moderate).

Morocco's defensive track is institutionally more recently formalised than its collection apparatus: DGSSI, examined in full above, published a National Cybersecurity Strategy to the horizon of 2030 on 22 July 2024, operates under Law 05-20 and Law 43-20 on electronic trust services, and runs maCERT as its operational incident-response arm, which participates in international cyber-drill exercises [163]. This is a directly primary-sourced, high-reliability finding on DGSSI's mandate and legal basis, but it is also a narrow one: DGSSI's own homepage discloses no incident statistics, no budget figure and no staffing level, and the full text of the 2030 strategy itself could not be located. It is roughly an even chance that Morocco's defensive cyber capability is proportionate to the scale of digital dependency documented under *Key dependencies* above (confidence: low, given the near-total absence of quantitative defensive-capacity data in the open

sources reached) -- a genuine, explicitly flagged evidentiary gap rather than a negative judgment about DGSSI's actual competence.

No dedicated open-source evidence on an information-operations or influence track specifically was located for this section: no source consulted addressed state-linked disinformation campaigns, coordinated inauthentic social-media activity, or an information-operations doctrine attributable to a named Moroccan institution. This is stated as an explicit gap rather than an assessment of absence -- Morocco's state news agency and broader media apparatus, and the pro-Rabat and pro-Algeria influence activity discussed under *Hacktivism and information confrontation* above, bear on this question but were not duplicated here. Confidence in any judgment about the scale or sophistication of a Moroccan influence and information-operations capability is accordingly low, and should be cross-checked against the intelligence and diplomatic material presented elsewhere in this report rather than asserted here without a supporting citation.

Net assessment: Morocco's three-track capability model is asymmetric. The offensive and collection track is the most visible and most externally documented, but is highly likely to be structurally vendor- and partner-dependent at its most consequential layers -- Pegasus via Israel/NSO, the reconnaissance satellites via France's Airbus and Thales, and DGED's foreign liaison relationships (confidence: moderate). The defensive track has a credible, recently strengthened legal and institutional foundation, but its actual operational capacity is not quantifiable from the sources reached (confidence: low). The influence and information-operations track is effectively undocumented within this research and should not be assumed either strong or weak without dedicated follow-on collection (confidence: very low, i.e. a genuine gap). It is likely that this asymmetry -- visible, foreign-enabled offence; under-documented, institutionally young defence; and an unassessed influence capability -- reflects a genuine capability profile rather than merely a research artefact, given that the offensive track's visibility comes substantially from external forensic exposure rather than Moroccan self-disclosure, while the defensive and information-operations tracks have no equivalent external forcing function driving disclosure (confidence: moderate). The figure below sets out all three tracks side by side.

Figure 16. Morocco's three-track cyber capability model: offensive/collection, defensive, and influence/information-operations, each annotated by its dominant foreign-dependency vector and evidentiary confidence.

OFFENSIVE/COLLECTION	DEFENSIVE	INFLUENCE/IO
DGST PCR (indigenous SIGINT) + Pegasus/NSO (Israel) + Mohammed VI-A/B satellites (France: Airbus/Thales) Tasking authority (DGST vs DGED) UNRESOLVED Dominant dependency: Israel (Pegasus), France (satellites)	DGSSI/macCERT Loi 05-20/43-20, Strategy 2030 (institutional/legal foundation credible; capacity unquantifiable) Dominant dependency: none identified (institutionally indigenous)	No dedicated sourcing located this pass -- shown as a DATA-GAP node, not a capability claim Dominant dependency: unknown
Confidence: moderate	Confidence: low	Confidence: very low/gap

Best-evidenced precisely because of EXTERNAL forensic exposure
(Citizen Lab, Amnesty, foreign governments), not Moroccan self-disclosure.

Constraints and vulnerabilities

Morocco's intelligence and cybersecurity institutions are legally and organisationally fragmented across at least three bodies with only partially documented coordination mechanisms: DGST, interior/domestic-security-oriented and home of the PCR SIGINT unit and the BCIJ counter-terrorism arm; DGED, defence-ministry-adjacent and externally focused; and DGSSI, a distinct national cybersecurity regulator with its own legal basis under Law 05-20 [161, 162, 163]. It is likely that this three-way institutional split creates coordination overhead and potential authority gaps -- for example, no source establishes which body, if any, holds tasking authority over the

Mohammed VI-A/B satellites, and DGSSI's defensive remit does not evidently extend to the offensive capabilities documented under *Capability model* above (confidence: low, since this is an inference from institutional silence rather than a directly sourced account of coordination failures). Declared budgets for Morocco's two intelligence services are both in the low-single-billion-dirham range and are dated: DGST's annual budget was reported at 1.1 billion dirhams as of 2016, and DGED's at 1.08 billion dirhams as of 2015 [161, 162]. Even allowing for likely nominal growth since these figures were reported, it is likely that Morocco's declared intelligence-services budget remains modest in absolute terms relative to the scope of activity attributed to these services -- regional SIGINT collection, a satellite-reconnaissance programme, an international liaison network and, via Pegasus, transnational surveillance operations (confidence: low, since no current consolidated budget figure was located and the true resourcing picture may include off-budget or defence-ministry-embedded costs not captured in these dated figures).

Morocco's foreign-ownership exposure in its telecom sector, already documented under *Key dependencies* above, is a standing external-leverage vulnerability in its own right: Etisalat holds a majority stake in Maroc Telecom, Orange S.A. holds a near-majority stake in Orange Maroc, and Zain holds a substantial, if currently unconfirmed, stake in Inwi [95, 96, 153]. It is likely that this ownership structure gives the UAE, France and, to a lesser and less-confirmed extent, Kuwait each some degree of standing commercial influence over Morocco's telecom infrastructure operators, independent of any Moroccan government regulatory lever (confidence: low, since no direct evidence of any of these states actually exercising such influence over network policy was found -- the vulnerability is structural and potential rather than demonstrated).

Morocco's absence from the global hyperscaler and CDN footprint compounds this ownership-based exposure: it means Moroccan digital services of all kinds -- government, financial and private -- are, for cloud-hosted workloads, dependent on infrastructure and legal jurisdiction outside Morocco, most plausibly in Europe, the Gulf or South Africa [154, 155, 156]. It is almost certain that this creates a latent data-sovereignty and continuity-of-service exposure to the political and legal decisions of whichever foreign jurisdiction actually hosts a given Moroccan organisation's cloud workload (confidence: moderate), though which specific jurisdictions are actually in use by named Moroccan entities could not be determined, which would require account-level or technical investigation beyond what open-source document research can establish.

Morocco's undersea-cable geography concentrates a disproportionate share of the country's international connectivity through the narrow Strait of Gibraltar corridor -- the Estepona-Tetuán direct crossing and Medusa's Nador/Tetouan landings -- a physically constrained, high-vessel-traffic environment where anchor-drag cable damage is a recurring regional risk category [150, 151]. It is likely that a serious multi-cable incident in this corridor, whether accidental or deliberate, would materially degrade Morocco's international connectivity given the documented concentration of landing points (confidence: low, since no source quantifies exactly what fraction of Moroccan international bandwidth transits this specific corridor versus the ACE, Atlas Offshore and EURAFRICA routes), and this remains a genuinely open quantification gap rather than an assumption this report is prepared to make with confidence.

No source consulted addressed Morocco's cybersecurity or telecommunications-engineering talent pipeline at all -- university output, DGSSI/maCERT staffing, or private-sector technical workforce size. Any judgment about a Moroccan talent gap in this domain would be pure inference from the broader observation that DGSSI's own public materials disclose no staffing figures, and this report declines to assert a talent-gap judgment without a supporting citation; this is recorded as an explicit, unresolved gap for dedicated follow-up research, ideally targeting Morocco's Digital Development Agency, university cybersecurity-programme enrolment data, or ANRT digital-skills reporting. The table below collects the six constraints discussed in this section alongside their assessed confidence, for quick reference.

Table 20. Morocco's principal cyber-domain constraints and vulnerabilities, with assessed confidence.

Constraint	Nature	Assessed confidence
Institutional fragmentation (DGST/DGED/DGSSI)	Coordination overhead; unclear satellite-tasking authority	Low
Dated/modest declared intelligence budgets	DGST ~1.1bn MAD (2016); DGED ~1.08bn MAD (2015)	Low
Foreign telecom ownership	UAE/France/Kuwait stakes across all three operators	Low
Absent hyperscaler/CDN presence	Data-sovereignty and continuity-of-service exposure	Moderate
Submarine-cable corridor concentration	Strait of Gibraltar chokepoint; anchor-drag risk	Low
Undocumented cybersecurity/telecom talent pipeline	No source addresses workforce scale	Gap (no judgment offered)

Conclusions

Drawing together the cyberspace, cybercrime, hacktivism and dependency material examined across this chapter, four structural findings recur and deserve restating together. First, Morocco's offensive posture in cyberspace is procurement-led rather than development-led: no state-attributed Moroccan APT was identified in any tracked threat-intelligence catalogue, examined under *APT groups* above, yet a forensically confirmed, commercially sourced Pegasus capability has demonstrably reached domestic journalists and activists and, on the evidence assessed in an earlier chapter, senior Spanish officials. Second, Morocco's defensive institutional architecture, DGSSI and maCERT, is comprehensive on paper -- a dedicated statute, a published 2030 strategy, FIRST and OIC-CERT membership -- but its actual operational capacity remains unquantifiable from open sources, a gap this chapter has flagged consistently rather than resolved by inference. Third, the Jabaroot phenomenon exemplifies a genuinely unresolved attribution environment in which state, hacktivist and insider explanations all remain live simultaneously, and this chapter has deliberately declined to adopt any single theory as its own judgment. Fourth, Morocco's critical digital infrastructure -- telecommunications ownership, cloud hosting, submarine cables, satellites -- is substantially foreign-anchored, a dependency pattern examined in full below.

Morocco's critical digital infrastructure is, on the balance of evidence assembled here, foreign-anchored at nearly every load-bearing layer: cable landings cluster at a single physical chokepoint with several constituent systems documented only by name rather than by capacity or ownership; all three licensed telecom operators carry majority or near-majority foreign shareholding, from the UAE, France and Kuwait respectively; no major Western hyperscaler or CDN operates inside Moroccan territory; semiconductor manufacturing is limited to back-end assembly; satellite reconnaissance and its near-term renewal both run through the French/European industrial base; and positioning, navigation and timing services have no evident domestic ground segment. It is highly likely that this pattern reflects a deliberate, longstanding Moroccan policy of importing rather than indigenising critical-infrastructure and strategic-technology capability, in exchange for capital inflows, industrial partnership and alliance-embedded technology transfer (confidence: moderate) -- but no explicit Moroccan government strategy document was found articulating this trade-off as a conscious choice, so the judgment rests on the consistency of the pattern rather than a stated policy.

The capability model that sits atop this dependency base is itself unevenly documented rather than unevenly real: the offensive and collection track is the best-evidenced of the three tracks examined under *Capability model* above precisely because its most consequential tool, Pegasus, has been exposed by independent foreign forensic labs and confirmed by foreign governments reporting their own officials as targets, not because Morocco has been more transparent about this track than the other two. It is likely that Morocco's defensive and information-operations capabilities are comparably real but structurally under-disclosed, given that DGSSI operates under real legislation and a real 2024-published strategy with no equivalent external forensic exposure to size it against, and that no dedicated influence-operations sourcing was located at all (confidence: low on the information-operations track specifically, moderate on the defensive track's under-disclosure premise). This report should not read the offensive track's evidentiary richness as proof that it is Morocco's most developed capability -- only that it is Morocco's most externally exposed one.

The single highest-value follow-up for future research, in this analyst's judgment, is closing the ownership and market-share verification gap -- Maroc Telecom's exact shareholder percentages, Orange Maroc's current stake, Inwi's current Zain/Al Mada split, and current ANRT operator-level market share -- against primary AMMC, investor-relations or ANRT sources rather than the tertiary Wikipedia sourcing this chapter was forced to rely on; a second, comparably important gap is establishing equipment-vendor identity, Huawei versus Western alternatives, across Morocco's mobile networks, which could not be resolved at all here and which bears directly on any assessment of external-leverage exposure through hardware supply chains. Until both gaps close, judgments in this chapter that rest on the weakest-graded sourcing should be treated as probably-true working assumptions rather than settled findings.

References

References are given in ACM Reference Format, numbered in order of appearance into this document. Each entry closes with its NATO/Admiralty grading: a letter (A-F) for source reliability and a digit (1-6) for information credibility, assigned during collection and carried forward unchanged into this report.

[1] Haut-Commissariat au Plan. 2024. Recensement Général de la Population et de l'Habitat 2024 (population and demographic indicators). HCP official website (2024). Retrieved September 10, 2026 from <https://www.hcp.ma/> [Admiralty: A1]

[2] Kingdom of Morocco. 2011. Constitution of the Kingdom of Morocco (English translation). Comparative Constitutions Project (constituteproject.org) (1 July 2011). Retrieved September 10, 2026 from https://www.constituteproject.org/constitution/Morocco_2011.pdf [Admiralty: A1]

[3] Mohamed Chtatou. 2026. From A Morocco Of Centers To A Morocco Of Territories: The 2026 Legislative Elections And The Urgency Of A New Territorial Convergence Policy — Analysis. Eurasia Review (23 August 2026). Retrieved September 10, 2026 from <https://www.eurasiareview.com/23082026-from-a-morocco-of-centers-to-a-morocco-of-territories-the-2026-legislative-elections-and-the-urgency-of-a-new-territorial-convergence-policy-analysis/> [Admiralty: B2]

[4] Hespress EN. 2026. PJD's 2026 Election Platform: Key Tax and Economic Proposals. Hespress (English edition) (7 September 2026). Retrieved September 10, 2026 from <https://en.hespress.com/145034-pjd-targets-dominant-companies-with-top-corporate-tax-rate-in-election-plan.html> [Admiralty: B2]

[5] Oubachir (wire copy). 2025. Morocco's Gen Z protests escalate: deaths, arrests and calls for reform. BusinessMirror (3 October 2025). Retrieved September 10, 2026 from

<https://businessmirror.com.ph/2025/10/03/morocco-gen-z-protests-escalate-deaths-arrests-and-calls-for-reform/> [Admiralty: B2]

[6] Gavin Blackburn. 2025. Morocco pledges reforms as death toll from anti-government protests rises to three. Euronews (2 October 2025). Retrieved September 10, 2026 from <https://www.euronews.com/2025/10/02/two-killed-in-anti-government-protests-rocking-morocco> [Admiralty: B2]

[7] Shola Lawal. 2026. Trump says Morocco named Tiznit-Dakhla highway after him: Why it matters. Al Jazeera English (31 July 2026). Retrieved September 10, 2026 from <https://www.aljazeera.com/news/2026/7/31/morocco-names-tiznit-dakhla-highway-after-trump-why-it-matters> [Admiralty: B2]

[8] Hespress EN. 2026. US Awards \$42 Million Contract for Morocco F-16 Training Systems. Hespress (English edition) (1 September 2026). Retrieved September 10, 2026 from <https://en.hespress.com/144724-us-awards-42-million-contract-for-morocco-f-16-training-systems.html> [Admiralty: B2]

[9] Khadija Tachfine. 2026. Morocco and France Sign 12 Cooperation Agreements at High-Level Meeting in Rabat. Hespress (English edition) (16 July 2026). Retrieved September 10, 2026 from <https://en.hespress.com/142030-morocco-and-france-sign-12-cooperation-agreements-at-high-level-meeting-in-rabat.html> [Admiralty: B2]

[10] Layan, Eloïse; Mansouri, Hicham; Vénéitay, Guillaume. 2026. While France was considering buying Pegasus, Morocco was spying on its ministers. Forbidden Stories (16 July 2026). Retrieved September 10, 2026 from <https://forbiddenstories.org/while-france-was-considering-buying-pegasus-morocco-was-spying-on-its-ministers/> [Admiralty: B3]

[11] Christina Thykjaer. 2026. Crisis en Ceuta: así han evolucionado las relaciones entre España y Marruecos desde la llegada de Sánchez. Euronews (Spanish edition) (31 July 2026). Retrieved September 10, 2026 from <https://es.euronews.com/my-europe/2026/07/31/crisis-ceuta-relaciones-entre-espana-y-marruecos-llegada-sanchez> [Admiralty: B2]

[12] Khadija Tachfine. 2026. Albares: There Will Never Be Any Discussion With Morocco Over Ceuta and Melilla. Hespress (English edition) (7 September 2026). Retrieved September 10, 2026 from <https://en.hespress.com/145001-albares-there-will-never-be-any-discussion-with-morocco-over-ceuta-and-melilla.html> [Admiralty: B2]

[13] Echarri, Carmen. 2026. Así intentan el cruce Marruecos-Ceuta cientos de subsaharianos. El Faro de Ceuta (August 2026). Retrieved September 10, 2026 from <https://elfarodeceuta.es/asi-intentan-cruce-marruecos-ceuta-cientos-subsaharianos/> [Admiralty: B2]

[14] Naranjo, Antonio R.. 2026. El jefe de la Inteligencia marroquí condecorado por Marlaska irrumpe como uno de los cabecillas de la invasión a Ceuta. El Debate (9 September 2026). Retrieved September 10, 2026 from https://www.eldebate.com/espana/20260909/jefe-inteligencia-marroqui-condecorado-marlaska-irrumpe-como-cabecillas-invasion-ceuta_456488.html [Admiralty: C3]

[15] unknown. 2026. La Audiencia Nacional acuerda investigar la invasión de Ceuta y alerta de una «indudable gestión favorecedora desde Marruecos». ABC (7 September 2026 (date discrepancy flagged — URL date-stamp reads 2025)). Retrieved September 10, 2026 from <https://www.abc.es/espana/audiencia-nacional-acuerda-investigar-invasion-ceuta-alerta-20250907144350-nt.html> [Admiralty: D4]

[16] Betty de G. (citing IISS and Intissar Fakir/Middle East Institute). 2026. Maroc-Algérie: «Aucun ne veut la guerre, mais les deux se préparent au pire». Bladi.net (30 August 2026). Retrieved September 10, 2026 from <https://www.bladi.net/maroc-algerie-veut-guerre-deux-preparent-pire,123454.html> [Admiralty: B2]

[17] unknown (wire copy). 2026. Nigeria-Morocco Gas Pipeline Approved by Ecowas. Yahoo News (26 July 2026). Retrieved September 10, 2026 from

<https://www.yahoo.com/news/articles/ecowas-greenlights-25bn-nigeria-morocco-085428111.html> [Admiralty: B2]

[18] Walter Finch. 2026. Morocco 'closing military gap with Spain' with new missile arsenal. The Olive Press (7 September 2026). Retrieved September 10, 2026 from <https://www.theolivepress.es/spain-news/2026/09/07/morocco-military-gap-spain/> [Admiralty: C4]

[19] Lahcen Haddad. 2025. The Makhzen Complex: A Psychoanalytical Decoding of Algeria's Obsession with Morocco. Morocco World News (2 July 2025). Retrieved September 10, 2026 from <https://www.morocoworldnews.com/2025/07/223272/the-makhzen-complex-a-psychoanalytical-decoding-of-algerias-obsession-with-morocco/> [Admiralty: C3]

[20] unknown (agency copy). 2026. Morocco's Makhzen shelters fugitives wanted by European justice on drug, money laundering charges. Algérie Presse Service (APS) (11 August 2026). Retrieved September 10, 2026 from <https://www.aps.dz/en/world/world/msoshb8g-morocco-s-makhzen-shelters-fugitives-wanted-by-european-justice-on-drug-money-laundering-charges> [Admiralty: D4]

[21] unknown (profile page). 2026. Al Mada (company profile). Arabian Gulf Business Insight (retrieved 8 September 2026). Retrieved September 10, 2026 from <https://www.agbi.com/industry/finance/al-mada/> [Admiralty: B2]

[22] Moroccan Institute for Policy Analysis. 2026. MIPA homepage (recent publications listing, including reference to UN Security Council Resolution 2797). MIPA (retrieved 8 September 2026, listing items Feb-June 2026). Retrieved September 10, 2026 from <https://mipa.institute/> [Admiralty: B3]

[23] Hespress EN (with MAP). 2026. Greece's Support for Morocco's Autonomy Proposal. Hespress (English edition) (7 September 2026). Retrieved September 10, 2026 from <https://en.hespress.com/145039-greece-believes-moroccan-proposal-for-autonomy-could-be-most-feasible-solution-for-definitive-resolution-of-this-regional-conflict.html> [Admiralty: B2]

[24] Mohamed Ait Elmouden. 2026. Algeria's Changing Language Signals Possible Path to Sahara Settlement. Hespress (English edition) (6 May 2026). Retrieved September 10, 2026 from <https://en.hespress.com/137302-algerias-changing-language-signals-possible-path-to-sahara-settlement.html> [Admiralty: C3]

[25] Hespress EN (with MAP). 2026. Danish FM: Denmark and Europe Need Reliable Friend Like Morocco. Hespress (English edition) (5 September 2026). Retrieved September 10, 2026 from <https://en.hespress.com/144933-danish-fm-denemark-and-europe-need-reliable-friend-like-morocco.html> [Admiralty: B2]

[26] Wikipedia contributors. 2026. General Directorate of Studies and Documentation. Wikipedia (English) (accessed September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/General_Directorate_of_Studies_and_Documentation [Admiralty: C3]

[27] Wikipedia contributors. 2026. General Directorate for Territorial Surveillance. Wikipedia (English) (accessed September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/General_Directorate_for_Territorial_Surveillance [Admiralty: C3]

[28] Wikipedia contributors. 2026. Direction générale de la Sûreté nationale (Maroc). Wikipedia (French) (accessed September 2026). Retrieved September 10, 2026 from [https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%BBret%C3%A9_nationale_\(Maroc\)](https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%BBret%C3%A9_nationale_(Maroc)) [Admiralty: C3]

[29] Wikipedia contributors. 2026. Abdellatif Hammouchi. Wikipedia (English) (accessed September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Abdellatif_Hammouchi [Admiralty: C3]

- [30] Marczak, Bill; Scott-Railton, John; McKune, Sarah; Abdul Razzak, Bahr; Deibert, Ron. 2018. Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab, Munk School of Global Affairs, University of Toronto (18 September 2018). Retrieved September 10, 2026 from <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> [Admiralty: A2]
- [31] Amnesty International Security Lab. 2020. Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools. Amnesty International (22 June 2020). Retrieved September 10, 2026 from <https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/> [Admiralty: A1]
- [32] Amnesty International (Amnesty Tech / Security Lab). 2022. Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence. Amnesty International (9 March 2022). Retrieved September 10, 2026 from <https://www.amnesty.org/en/latest/news/2022/03/morocco-western-sahara-activist-nso-pegasus/> [Admiralty: A1]
- [33] Bautista, José; Layan, Eloïse; Mansouri, Hicham; Vénétitay, Guillaume. 2026. How did Morocco become addicted to tracking down its opponents with spyware?. Forbidden Stories (16 July 2026). Retrieved September 10, 2026 from <https://forbiddenstories.org/how-did-morocco-become-addicted-to-tracking-down-its-opponents-with-spyware/> [Admiralty: B2]
- [34] Bautista, José; Mansouri, Hicham. 2026. Cómo los servicios de inteligencia marroquíes habrían espiado a los agentes españoles que los formaban. Forbidden Stories (Spanish edition) (17 July 2026). Retrieved September 10, 2026 from <https://forbiddenstories.org/es/como-los-servicios-de-inteligencia-marroquies-habrian-espiado-a-los-agentes-espanoles-que-los-formaban/> [Admiralty: B2]
- [35] Bautista, José; Layan, Eloïse; Mansouri, Hicham; Rueckert, Phineas; Vénétitay, Guillaume. 2026. How Morocco allegedly spies on an African ally. Forbidden Stories (16 July 2026). Retrieved September 10, 2026 from <https://forbiddenstories.org/how-morocco-allegedly-spies-on-an-african-ally/> [Admiralty: B3]
- [36] Wikipedia contributors. 2026. Mohammed VI-A. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Mohammed_VI-A [Admiralty: D2]
- [37] Clark, Stephen. 2018. Moroccan spy satellite launched aboard Vega rocket. Spaceflight Now (21 November 2018). Retrieved September 10, 2026 from <https://spaceflightnow.com/2018/11/21/moroccan-spy-satellite-launched-aboard-vega-rocket/> [Admiralty: B2]
- [38] Entrambasaguas, Alejandro. 2026. El ex 'dos' del espionaje de Marruecos que accedió a las pruebas de Pegasus vive escondido entre un piso en Madrid y una finca en Cáceres. El Debate (8 September 2026). Retrieved September 10, 2026 from https://www.eldebate.com/espana/20260908/ex-dos-espionaje-marruecos-accedio-pruebas-pegasus-vive-escondido-entre-piso-madrid-finca-caceres_456302.html [Admiralty: C3]
- [39] Entrambasaguas, Alejandro. 2026. Un colaborador de la Policía pidió 2 millones a Marruecos a cambio de entregar al espía que guarda las pruebas de Pegasus. El Debate (9 September 2026). Retrieved September 10, 2026 from https://www.eldebate.com/espana/20260909/colaborador-policia-pidio-2-millones-marruecos-cambio-entregar-espia-guarda-pruebas-pegasus_456615.html [Admiralty: C3]
- [40] Forbidden Stories consortium. 2026. Codename Morgan: a look back at Morocco's acquisition of Pegasus involving Israel and the United Arab Emirates. Forbidden Stories (16 July 2026). Retrieved September 10, 2026 from <https://forbiddenstories.org/codename-morgan-a-look-back-at-moroccos-acquisition-of-pegasus-involving-israel-and-the-united-arab-emirates/> [Admiralty: C3]

- [41] Bautista, José; Mansouri, Hicham. 2026. Moroccan intelligence is believed to have spied on Spanish agents who were training them. Forbidden Stories (17 July 2026). Retrieved September 10, 2026 from <https://forbiddenstories.org/moroccan-intelligence-is-believed-to-have-spied-on-spanish-agents-who-were-training-them/> [Admiralty: B3]
- [42] Wikipedia contributors. 2026. Espionaje con Pegasus al Gobierno de España. Wikipedia (Spanish) (accessed September 2026). Retrieved September 10, 2026 from https://es.wikipedia.org/wiki/Espionaje_con_Pegasus_al_Gobierno_de_Espa%C3%B1a [Admiralty: C3]
- [43] unknown. 2026. El fiscal jefe de la Audiencia Nacional rechazó las «pruebas» sobre el móvil de Sánchez hackeado: «No interesa por Marruecos». ABC (8 September 2026 (date discrepancy flagged — URL date-stamp reads 2025)). Retrieved September 10, 2026 from <https://www.abc.es/espana/fiscal-jefe-audiencia-nacional-rechazo-pruebas-sobre-20250908215738-nt.html> [Admiralty: D4]
- [44] Moreno Mena, Miguel. 2026. Abdellatif Hammouchi, el líder de la seguridad de Marruecos señalado por los hackers de Jabaroot y acusado de torturas al que Marlaska le dio una medalla. Infobae España (27 August 2026). Retrieved September 10, 2026 from <https://www.infobae.com/espana/2026/08/27/abdellatif-hammouchi-el-lider-de-la-seguridad-de-marruecos-senalado-por-los-hackers-de-jabaroot-y-acusado-de-torturas-al-que-marlaska-le-dio-una-medalla/> [Admiralty: B3]
- [45] Faouzi, Adil. 2026. Morocco's Security Pole Denies Any Database Breach, Points to Old Insurance Data. Morocco World News (27 August 2026). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2026/08/336320/moroccos-security-pole-denies-any-database-breach-points-to-old-insurance-data/> [Admiralty: C3]
- [46] Wikipedia contributors. 2026. Sûreté Nationale (Morocco). Wikipedia (retrieved September 2026). Retrieved September 10, 2026 from [https://en.wikipedia.org/wiki/Sûreté_Nationale_\(Morocco\)](https://en.wikipedia.org/wiki/Sûreté_Nationale_(Morocco)) [Admiralty: C3]
- [47] Wikipedia contributors. 2026. Bureau Central d'Investigations Judiciaires. Wikipedia (retrieved September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Bureau_Central_d%27Investigations_Judiciaires [Admiralty: C3]
- [48] Wikipedia contributors. 2026. Royal Moroccan Gendarmerie. Wikipedia (retrieved September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Royal_Moroccan_Gendarmerie [Admiralty: C3]
- [49] Wikipedia contributors. 2026. Forces auxiliaires marocaines. Wikipédia (retrieved September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Forces_auxiliaires_marocaines [Admiralty: C3]
- [50] Echarri, Carmen. 2026. Imágenes de las detenciones a subsaharianos en Marruecos. El Faro de Ceuta (August 2026). Retrieved September 10, 2026 from <https://elfarodeceuta.es/imagenes-detenciones-subsaharianos-marruecos/> [Admiralty: B2]
- [51] Wikipedia contributors. 2026. Wali (arabe). Wikipédia (retrieved September 2026). Retrieved September 10, 2026 from [https://fr.wikipedia.org/wiki/Wali_\(arabe\)](https://fr.wikipedia.org/wiki/Wali_(arabe)) [Admiralty: C3]
- [52] Wikipedia contributors. 2026. Direction générale de la sûreté nationale. Wikipédia (retrieved September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_s%C3%BBret%C3%A9_nationale [Admiralty: C3]
- [53] Moho Amer, Oumaima. 2026. Morocco's Public Security Director El Hail Zitouni Dies After Four-Decade Career. Morocco World News (August 2026). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2026/08/335634/moroccos-public-security-director-el-hail-zitouni-dies-after-four-decade-career/> [Admiralty: B2]

- [54] Afeznaoui, Hanane. 2026. Agadir Security Directorate Launches Morocco's Eighth Regional Explosives Unit. Morocco World News (August 2026). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2026/08/336307/agadir-security-directorate-launches-moroccos-eighth-regional-explosives-unit/> [Admiralty: B3]
- [55] Afeznaoui, Hanane. 2026. DGSN Deploys AI-Powered 'Amane' and 'Madar' Smart Patrols in Casablanca. Morocco World News (July 2026). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2026/07/331326/dgsn-deploys-ai-powered-amane-and-madar-smart-patrols-in-casablanca/> [Admiralty: B3]
- [56] INTERPOL. 2026. Morocco — Member Countries. INTERPOL (retrieved September 2026). Retrieved September 10, 2026 from <https://www.interpol.int/en/Who-we-are/Member-countries/Africa/MOROCCO> [Admiralty: A1]
- [57] Naim, Firdaus. 2025. Morocco-Spain Operation Seizes 22 Tons of Hashish Hidden in Pepper Trucks. Morocco World News (October 2025). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2025/10/265741/> [Admiralty: B2]
- [58] Direction Générale de la Sûreté Nationale (traced by Wikimedia Commons uploader). 2022. File:Emblem of the Moroccan DGSN.svg. Wikimedia Commons (10 November 2022). Retrieved September 10, 2026 from https://commons.wikimedia.org/wiki/File:Emblem_of_the_Moroccan_DGSN.svg [Admiralty: B3]
- [59] Machloukh, Anass. 2021. Haboub Cherkaoui, patron du BCIJ: 'Le Polisario est un important pourvoyeur de Djihadistes'. L'Opinion (Maroc) (October 2021). Retrieved September 10, 2026 from https://www.lopinion.ma/Haboub-Cherkaoui-patron-du-BCIJ-Le-polisario-est-un-important-pourvoyeur-de-Djihadistes_a35872.html [Admiralty: C4]
- [60] Wikipedia contributors. 2026. Bureau central d'investigations judiciaires. Wikipédia (April 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Bureau_central_d%E2%80%99investigations_judiciaires [Admiralty: C3]
- [61] MWN Staff. 2026. BCIJ Dismantles ISIS-Affiliated Cell Involved in Criminal Operations Across Morocco. Morocco World News (April 2026). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2026/04/286037/bcij-dismantles-isis-affiliated-cell-involved-in-criminal-operations-across-morocco/> [Admiralty: B3]
- [62] Kasraoui, Safaa. 2024. Morocco-Spain Dismantle ISIS-Affiliated Terror Cell Spanning Two Continents. Morocco World News (November 2024). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2024/11/168105/morocco-spain-dismantle-isis-affiliated-terror-cell-spanning-two-continents/> [Admiralty: B3]
- [63] NorthAfricanArmsDealer (Wikimedia Commons uploader). 2022. File:Blazon du BCIJ.svg. Wikimedia Commons (19 November 2022 (created); 29 November 2022 (uploaded)). Retrieved September 10, 2026 from https://commons.wikimedia.org/wiki/File:Blazon_du_BCIJ.svg [Admiralty: D4]
- [64] Wikipedia contributors. 2026. Gendarmerie royale marocaine. Wikipedia (French) (accessed September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Gendarmerie_royale_marocaine [Admiralty: F3]
- [65] Wikipedia contributors. 2026. Forces armées royales (Maroc). Wikipedia (French) (accessed September 2026). Retrieved September 10, 2026 from [https://fr.wikipedia.org/wiki/Forces_arm%C3%A9es_royales_\(Maroc\)](https://fr.wikipedia.org/wiki/Forces_arm%C3%A9es_royales_(Maroc)) [Admiralty: F3]
- [66] Jiménez, Isabel. 2025. Interceptada una lancha con inmigrantes de Bangladesh que cruzaba a Ceuta. El Faro de Ceuta (October 2025). Retrieved September 10, 2026 from <https://elfarodeceuta.es/interceptada-lancha-inmigrantes-bangladesh-cruzaba-ceuta/> [Admiralty: B2]

- [67] Hespress EN. 2026. Moroccan Gendarmes Seize Over Three Tonnes of Cocaine off Tarfaya. Hespress (English edition) (July 2026). Retrieved September 10, 2026 from <https://en.hespress.com/142551-moroccan-gendarmes-seize-over-three-tonnes-of-cocaine-off-tarfaya.html> [Admiralty: B3]
- [68] Hespress EN. 2025. Casablanca Court Deliberates Verdict in Case of 37 Gendarmerie Officers Accused of Collusion with Drug Trafficker. Hespress (English edition) (March 2025). Retrieved September 10, 2026 from <https://en.hespress.com/105477-casablanca-court-deliberates-verdict-in-case-of-37-gendarmerie-officers-accused-of-collusion-with-drug-trafficker.html> [Admiralty: C3]
- [69] Hespress EN. 2025. Seven Gendarmes Jailed in Morocco Over Alleged Cover-Up for Drug Baron Linked to Murder. Hespress (English edition) (January 2025). Retrieved September 10, 2026 from <https://en.hespress.com/100511-seven-gendarmes-jailed-in-morocco-over-alleged-cover-up-for-drug-baron-linked-to-murder.html> [Admiralty: C3]
- [70] Daoudi, Asmae. 2025. Agadir Authorities Launch Investigation into Lqliaa Gendarmerie Post Incident. Morocco World News (October 2025). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2025/10/261422/agadir-authorities-launch-investigation-lqliaa-gendarmerie-post-incident/> [Admiralty: C4]
- [71] Testomania (Wikimedia Commons uploader). 2025. File:Royal Moroccan gendarmery.png. Wikimedia Commons (10 May 2025). Retrieved September 10, 2026 from https://commons.wikimedia.org/wiki/File:Royal_Moroccan_gendarmery.png [Admiralty: D4]
- [72] Mesfioui, Khalid. 2018. Voici les détails du plan royal pour moderniser les Forces auxiliaires. Le360 (French edition) (January 2018). Retrieved September 10, 2026 from <https://fr.le360.ma/politique/voici-les-detaills-du-plan-royal-pour-moderniser-les-forces-auxiliaires-152697/> [Admiralty: B2]
- [73] Ministère de la Transformation Numérique et de la Réforme de l'Administration. 2018. Textes juridiques — Décrets n° 2.17.827 et 2.17.825 du 6 mars 2018. mmsp.gov.ma (March 2018). Retrieved September 10, 2026 from https://www.mmsp.gov.ma/fr/textes-juridiques?field_type_textes_juridiques_target_id=All&page=21 [Admiralty: A1]
- [74] Boudarham, Mohammed. 2020. Info360. Voici les deux nouveaux patrons des Forces auxiliaires. Le360 (French edition) (October 2020). Retrieved September 10, 2026 from <https://fr.le360.ma/politique/info360-voici-les-deux-nouveaux-patrons-des-forces-auxiliaires-225667/> [Admiralty: B2]
- [75] Inspection Générale des Forces Auxiliaires (via mobaraty.com). 2023. File:Forces Auxiliaires.png. Wikimedia Commons (19 June 2023). Retrieved September 10, 2026 from https://commons.wikimedia.org/wiki/File:Forces_Auxiliaires.png [Admiralty: B3]
- [76] MINURSO. 2026. MINURSO home page. United Nations Mission for the Referendum in Western Sahara (accessed September 2026). Retrieved September 10, 2026 from <https://minurso.unmissions.org/> [Admiralty: A1]
- [77] Wikipedia contributors. 2026. Royal Moroccan Armed Forces. Wikipedia (English) (accessed September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Royal_Moroccan_Armed_Forces [Admiralty: F3]
- [78] Wikipedia contributors. 2026. Ahmed Dlimi. Wikipedia (French) (accessed September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Ahmed_Dlimi [Admiralty: F3]
- [79] Aminovich (Wikimedia Commons uploader). 2008. File:Moroccan Armed Force.png. Wikimedia Commons (29 January 2008). Retrieved September 10, 2026 from https://commons.wikimedia.org/wiki/File:Moroccan_Armed_Force.png [Admiralty: C3]
- [80] Wikipedia contributors. 2026. Direction générale de la surveillance du territoire. Wikipedia (French) (accessed September 2026). Retrieved September 10, 2026 from

https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_surveillance_du_territoire [Admiralty: F3]

[81] Wikipedia contributors. 2026. Direction générale des études et de la documentation. Wikipedia (French) (accessed September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_des_%C3%A9tudes_et_de_la_documentation [Admiralty: F3]

[82] Wikipedia contributors. 2026. Garde royale marocaine. Wikipedia (French) (accessed September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Garde_royale_marocaine [Admiralty: F3]

[83] Garde Royale (via vuseen.com). 2023. File:Moroccan Royal Guard.png. Wikimedia Commons (19 June 2023). Retrieved September 10, 2026 from https://commons.wikimedia.org/wiki/File:Moroccan_Royal_Guard.png [Admiralty: B3]

[84] Wikipedia contributors. 2026. Berm (Western Sahara). Wikipedia (English) (accessed September 2026). Retrieved September 10, 2026 from [https://en.wikipedia.org/wiki/Berm_\(Western_Sahara\)](https://en.wikipedia.org/wiki/Berm_(Western_Sahara)) [Admiralty: F3]

[85] Security Council Report. 2025. Western Sahara Monthly Forecast, October 2025. Security Council Report (October 2025). Retrieved September 10, 2026 from <https://www.securitycouncilreport.org/monthly-forecast/2025-10/western-sahara-16.php>

[Admiralty: B1]

[86] Hespress. 2026. المغرب يحشد دعم 40 دولة للحكم الذاتي. Hespress (8 September 2026). Retrieved September 10, 2026 from

<https://www.hespress.com/%d8%a7%d9%84%d9%85%d8%ba%d8%b1%d8%a8-%d9%8a%d8%ad%d8%b4%d8%af-%d8%af%d8%b9%d9%85-40-%d8%af%d9%88%d9%84%d8%a9-%d9%84%d9%84%d8%ad%d9%83%d9%85-%d8%a7%d9%84%d8%b0%d8%a7%d8%aa%d9%8a-1803928.html> [Admiralty: B2]

[87] R. N.. 2026. Equal Earth de l'ONU : une victoire cartographique historique pour le peuple sahraoui. El Watan (7 September 2026). Retrieved September 10, 2026 from <https://elwatan.dz/equal-earth-de-lonu-une-victoire-cartographique-historique-pour-le-peuple-sahraoui/> [Admiralty: B3]

[88] Hammouche, Sid Ahmed. 2026. Grande victoire du peuple sahraoui. El Watan (8 September 2026). Retrieved September 10, 2026 from <https://elwatan.dz/grande-victoire-du-peuple-sahraoui/> [Admiralty: B3]

[89] Boufertih, Toufiq. 2026. مسيرة مغربية تقصف منقبين بالصحراء. Hespress (8 September 2026). Retrieved September 10, 2026 from

<https://www.hespress.com/%d9%85%d8%b3%d9%8a%d8%b1%d8%a9-%d9%85%d8%ba%d8%b1%d8%a8%d9%8a%d8%a9-%d8%aa%d9%82%d8%b5%d9%81-%d9%85%d9%86%d9%82%d8%a8%d9%8a%d9%86-%d8%a8%d8%a7%d9%84%d8%b5%d8%ad%d8%b1%d8%a7%d8%a1-1804049.html>

[Admiralty: B4]

[90] Wikipedia contributors. 2026. Ministry of Interior (Morocco). Wikipedia (retrieved September 2026 (article updated 6 July 2026)). Retrieved September 10, 2026 from [https://en.wikipedia.org/wiki/Ministry_of_Interior_\(Morocco\)](https://en.wikipedia.org/wiki/Ministry_of_Interior_(Morocco)) [Admiralty: C3]

[91] Human Rights Watch. 2004. Morocco: Human Rights at a Crossroads. Human Rights Watch (October 2004). Retrieved September 10, 2026 from <https://www.hrw.org/report/2004/10/20/morocco-human-rights-crossroads> [Admiralty: B2]

[92] Institut Royal des Études Stratégiques (IRES). 2026. IRES — official institutional site. IRES (retrieved September 2026). Retrieved September 10, 2026 from <https://www.ires.ma/> [Admiralty: A2]

- [93] Wikipedia contributors. 2026. Abdellatif Hammouchi. Wikipedia (retrieved September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Abdellatif_Hammouchi [Admiralty: C3]
- [94] Amnesty International Security Lab. 2021. Forensic Methodology Report: How to Catch NSO Group's Pegasus. Amnesty International (1 July 2021). Retrieved September 10, 2026 from <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> [Admiralty: B2]
- [95] Wikipedia contributors. 2026. Maroc Telecom. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Maroc_Telecom [Admiralty: D3]
- [96] Wikipedia contributors. 2026. Orange Maroc. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Orange_Maroc [Admiralty: D3]
- [97] Marczak, Bill; Scott-Railton, John; Berdan, Kristin; Abdul Razzak, Bahr; Deibert, Ron. 2020. Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles. Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto (1 December 2020). Retrieved September 10, 2026 from <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/> [Admiralty: B2]
- [98] Wikipedia contributors. 2026. Hacking Team. Wikipedia (retrieved September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Hacking_Team [Admiralty: C3]
- [99] Royaume du Maroc. 2020. Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité. Bulletin Officiel n° 6906 (hosted by DGSSI) (6 August 2020). Retrieved September 10, 2026 from <http://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/loi%2005-20.pdf> [Admiralty: A1]
- [100] Aziz Akhannouch (Chef du Gouvernement, signatory). 2024. Décret n° 2-24-921 du 18 rabii II 1446 (22 octobre 2024) relatif au recours aux prestataires de services Cloud par les entités et les infrastructures d'importance vitale. Bulletin Officiel du Royaume du Maroc (hosted via dgssi.gov.ma) (22 October 2024 (BO N°7380, 20 February 2025)). Retrieved September 10, 2026 from <https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2025-04/DECREE%202.24.921%20FR%20.pdf> [Admiralty: A1]
- [101] Wikipedia contributors. 2026. École nationale supérieure d'informatique et d'analyse des systèmes. Wikipédia (retrieved September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/%C3%89cole_nationale_sup%C3%A9rieure_d%27informatique_et_d%27analyse_des_syst%C3%A8mes [Admiralty: C3]
- [102] Wikipedia contributors. 2026. University Mohammed VI Polytechnic. Wikipedia (retrieved September 2026 (article updated 11 August 2026)). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/University_Mohammed_VI_Polytechnic [Admiralty: C3]
- [103] Wikipedia contributors. 2026. International University of Rabat. Wikipedia (retrieved September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/International_University_of_Rabat [Admiralty: C3]
- [104] Direction Générale de la Sécurité des Systèmes d'Information (DGSSI). 2026. DGSSI — official institutional site (training and education section). DGSSI (retrieved September 2026). Retrieved September 10, 2026 from <http://www.dgssi.gov.ma/fr/> [Admiralty: A2]
- [105] Naim, Firdaous. 2025. Sidi Ifni Maritime Interdiction: Hashish and Irregular-Migration Boat Intercepted. Morocco World News (August 2025). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2025/08/249194/> [Admiralty: C3]
- [106] Constitute Project. 2011. Morocco's Constitution of 2011. Constitute Project (29 July 2011 (retrieved September 2026)). Retrieved September 10, 2026 from https://www.constituteproject.org/constitution/Morocco_2011 [Admiralty: A1]

- [107] Wikisource contributors. 2011. Constitution marocaine de 2011/Titre III : De la Royauté. Wikisource (29 July 2011 (retrieved September 2026)). Retrieved September 10, 2026 from https://fr.wikisource.org/wiki/Constitution_marocaine_de_2011/Titre_III:_De_la_Royaut%C3%A9 [Admiralty: A1]
- [108] Privacy International. 2019. State of Privacy: Morocco. Privacy International (January 2019). Retrieved September 10, 2026 from <https://www.privacyinternational.org/state-privacy/1007/state-privacy-morocco> [Admiralty: B2]
- [109] Wikipedia contributors. 2026. Bureau central d'investigation judiciaire. Wikipédia (retrieved September 2026). Retrieved September 10, 2026 from https://fr.wikipedia.org/wiki/Bureau_central_d%27investigation_judiciaire [Admiralty: C3]
- [110] Wikipedia contributors. 2026. Telecommunications in Morocco. Wikipedia (English) (accessed 8-9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Telecommunications_in_Morocco [Admiralty: F3]
- [111] Agence Nationale de Réglementation des Télécommunications (ANRT). 2026. Observatoires du secteur au titre du T1 2026. anrt.ma (26 June 2026). Retrieved September 10, 2026 from <https://www.anrt.ma/> [Admiralty: A1]
- [112] Le360 (avec MAP). 2026. Législatives 2026: la CNDP fixe les règles sur l'usage des données personnelles. Le360 (29 August 2026). Retrieved September 10, 2026 from https://fr.le360.ma/politique/legislatives-2026-la-cndp-fixe-les-regles-sur-lusage-des-donnees-personnelles_6ROWMYG5TRC7FCNJVDY6PNLXA4/ [Admiralty: B2]
- [113] CNDP (institutional). 2026. Les dix impératifs à respecter durant les opérations et les consultations électorales (communiqué). cndp.ma (31 August 2026). Retrieved September 10, 2026 from <https://www.cndp.ma/> [Admiralty: A1]
- [114] DGSSI (institutional). 2021. Guide d'homologation des systèmes d'information sensibles des infrastructures d'importance vitale. dgssi.gov.ma (9 November 2021). Retrieved September 10, 2026 from <https://www.dgssi.gov.ma/fr/publications/guide-dhomologation-des-systemes-dinformation-sensibles-des-infrastructures> [Admiralty: A1]
- [115] DGSSI (institutional). 2023. Référentiel de gestion des incidents de cybersécurité. dgssi.gov.ma (5 May 2023). Retrieved September 10, 2026 from <https://www.dgssi.gov.ma/fr/publications/referentiel-de-gestion-des-incidents-de-cybersecurite> [Admiralty: A1]
- [116] DGSSI (institutional). 2024. Stratégie Nationale de Cybersécurité 2030. dgssi.gov.ma (22 July 2024). Retrieved September 10, 2026 from <https://www.dgssi.gov.ma/fr/publications/strategie-nationale-de-cybersecurite> [Admiralty: A2]
- [117] DGSSI (institutional). 2026. DGSSI homepage (mission, structure, legal basis). dgssi.gov.ma (accessed 8 September 2026). Retrieved September 10, 2026 from <http://www.dgssi.gov.ma/fr/> [Admiralty: A1]
- [118] DGSSI / maCERT (institutional). 2026. maCERT — mandate and service catalogue. dgssi.gov.ma (accessed 8 September 2026). Retrieved September 10, 2026 from <http://www.dgssi.gov.ma/fr/macert/> [Admiralty: A1]
- [119] Hespress (French edition). 2026. Cybersécurité: le Maroc classé 43e mondial sur 155 pays en 2026. Hespress (French edition) (18 August 2026). Retrieved September 10, 2026 from <https://fr.hespress.com/485544-cybersecurite-le-maroc-classe-43e-mondial-sur-155-pays-en-2026.html> [Admiralty: B2]
- [120] Direction Générale de la Sécurité des Systèmes d'Information. 2026. DGSSI — site officiel (page d'accueil et logo institutionnel). dgssi.gov.ma (8 September 2026 (accessed)). Retrieved September 10, 2026 from <https://www.dgssi.gov.ma/> [Admiralty: A1]

- [121] Forum of Incident Response and Security Teams (FIRST). 2026. maCERT — Member Team Page. first.org (8 September 2026 (accessed)). Retrieved September 10, 2026 from <https://www.first.org/members/teams/macert> [Admiralty: B2]
- [122] INCIBE-CERT (institutional). 2025. Data Leak on Moroccan Institutions Increases Political Tensions with Algeria. INCIBE-CERT Cybersecurity Highlights (9 April 2025). Retrieved September 10, 2026 from <https://www.incibe.es/en/incibe-cert/publications/cybersecurity-highlights/data-leak-moroccan-institutions-increases-political-tensions-algeria> [Admiralty: A1]
- [123] Amnesty International Security Lab. 2026. Inside Pegasus: The evolution of the world's most notorious spyware. Amnesty International Security Lab (July 2026). Retrieved September 10, 2026 from <https://securitylab.amnesty.org/latest/2026/07/inside-pegasus-the-evolution-of-the-worlds-most-notorious-spyware/> [Admiralty: A1]
- [124] Consejo General del Poder Judicial (institutional). 2026. Audiencia Nacional — Noticias Judiciales (rolling listing). poderjudicial.es (accessed 8 September 2026 (items 2 July-7 September 2026)). Retrieved September 10, 2026 from <https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Audiencia-Nacional/Noticias-Judiciales/> [Admiralty: A1]
- [125] Alejandro Entrambasaguas. 2026. El ex 'dos' del espionaje de Marruecos que accedió a las pruebas de Pegasus vive escondido entre un piso en Madrid y una finca en Cáceres. El Debate (8 September 2026). Retrieved September 10, 2026 from https://www.eldebate.com/espana/20260908/ex-dos-espionaje-marruecos-accedio-pruebas-pegasus-vive-escondido-entre-piso-madrid-finca-caceres_456302.html [Admiralty: C3]
- [126] Amnesty International et al. (joint statement). 2026. Joint Statement: Pegasus in the Parliament — the EU Must Act Now. Amnesty International Security Lab (6 July 2026). Retrieved September 10, 2026 from <https://securitylab.amnesty.org/latest/2026/07/joint-statement-pegasus-in-the-parliament-the-eu-must-act-now/> [Admiralty: B2]
- [127] Manuel García Castellón. 2026. La sombra de Pegasus sobre Ceuta (Opinion). El Independiente (3 September 2026). Retrieved September 10, 2026 from <https://www.elindependiente.com/opinion/2026/09/03/la-sombra-de-pegasus-sobre-ceuta/> [Admiralty: D4]
- [128] Wikipedia contributors. 2026. Royal Moroccan Air Force. Wikipedia (English) (accessed 8 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Royal_Moroccan_Air_Force [Admiralty: F3]
- [129] Hespress (institutional). 2021. La cybercriminalité: Un phénomène menaçant que la DGSN prend très au sérieux. Hespress (French edition) (25 December 2021). Retrieved September 10, 2026 from <https://fr.hespress.com/240008-la-cybercriminalite-un-phenomene-menacant-que-la-dgsn-prend-tres-au-serieux.html> [Admiralty: B2]
- [130] Le360 (institutional). 2026. Cybercriminalité: un célèbre hacker arrêté au Maroc, lors d'une opération conjointe entre la DGSN et Interpol. Le360 (undated (2009-2018 offending window referenced)). Retrieved September 10, 2026 from <https://fr.le360.ma/societe/cybercriminalite-un-celebre-hacker-arrete-au-maroc-lors-dune-operation-conjointe-entre-la-dgsn-et-241581/> [Admiralty: B2]
- [131] Le360 (institutional). 2022. Cybercriminalité: recherché par Interpol, un hacker interpellé à Casablanca. Le360 (event dated 18 October 2022). Retrieved September 10, 2026 from <https://fr.le360.ma/societe/cybercriminalite-recherche-par-interpol-un-hacker-interpelle-a-casablanca-268785/> [Admiralty: B2]
- [132] Perspectives Med (institutional). 2026. Cybercriminalité: Le Maroc s'implique dans la lutte menée par Interpol. Perspectives Med (20 May 2026). Retrieved September 10, 2026 from <https://perspectivesmed.com/cybercriminalite-le-maroc-simplique-dans-la-lutte-menee-par-interpol/> [Admiralty: C3]

- [133] Infomag (institutional). 2026. Kaspersky alerte sur la rapidité des fraudes au Maroc. InfoMagazine Maroc (16 June 2026). Retrieved September 10, 2026 from <https://www.infomagazine.ma/cybersecurite/kaspersky-alerte-sur-la-rapidite-des-fraudes-au-maroc-15586-2026/> [Admiralty: C2]
- [134] Estrella Digital (institutional). 2026. JabaROOT hackea RAMED: datos de 17 millones de marroquíes. Estrella Digital (20 August 2026). Retrieved September 10, 2026 from <https://www.estrelladigital.es/articulo/ciberseguridad/jabaroot-hackea-ramed-datos-17-millones-marroquies/20260820013152450106.html> [Admiralty: E4]
- [135] Wikipedia contributors. 2026. Jabaroot. Wikipedia (Spanish) (accessed 8 September 2026). Retrieved September 10, 2026 from <https://es.wikipedia.org/wiki/Jabaroot> [Admiralty: F3]
- [136] Lucas Barreiro. 2026. 70.000 nombres en juego: la amenaza que golpea al aparato de inteligencia de Marruecos. Catalunya Press (20 August 2026). Retrieved September 10, 2026 from <https://www.catalunyapress.es/articulo/internacional/2026-08-20/5989486-70000-nombres-juego-amenaza-golpea-aparato-inteligencia-marruecos> [Admiralty: C3]
- [137] ESdiario (citing journalist Ketty Garat). 2026. Ketty Garat revela los datos del espionaje de Pegasus a Sánchez vinculados a Marruecos. ESdiario (8 September 2026). Retrieved September 10, 2026 from <https://esdiario.com/nacional/260908/197171/ketty-garat-sanchez-pegasus-marruecos.html> [Admiralty: D4]
- [138] TSA — Tout sur l'Algérie (relaying Le Monde). 2026. Jabaroot: la piste algérienne s'efface, d'ex-espions marocains derrière la fuite de 70.000 noms d'agents. TSA (Tout sur l'Algérie) (27 August 2026). Retrieved September 10, 2026 from <https://www.tsa-algerie.com/jabaroot-la-piste-algerienne-sefface-dex-espions-marocains-derriere-la-fuite-de-70-000-noms-dagents/> [Admiralty: E4]
- [139] Morocco World News (institutional). 2026. Morocco's Security Pole Denies Any Database Breach, Points to Old Insurance Data. Morocco World News (August 2026). Retrieved September 10, 2026 from <https://www.moroccoworldnews.com/2026/08/336320/moroccos-security-pole-denies-any-database-breach-points-to-old-insurance-data/> [Admiralty: C3]
- [140] CybelAngel (institutional). 2025. Our Investigation of the ANCFCC Data Leak (Flash Report). CybelAngel (5 June 2025). Retrieved September 10, 2026 from <https://cybelangel.com/blog/ancfcc-data-leak-flash-report/> [Admiralty: B2]
- [141] Betty de G.. 2025. Des hackers marocains ripostent à l'Algérie avec une attaque ciblée. Bladi.net (12 April 2025). Retrieved September 10, 2026 from <https://www.bladi.net/hackers-marocains-ripostent-algerie-attaque-ciblee,114181.html> [Admiralty: F3]
- [142] ECSaharaui (institutional). 2026. Telegram cierra el canal de los hackers Jabaroot tras la identificación de 70.000 espías marroquíes. ECSaharaui (August 2026). Retrieved September 10, 2026 from <https://ecsaharaui.com/08/2026/telegram-cierra-el-canal-de-los-hackers-jabaroot-tras-la-identificacion-de-70-000-espias-marroquies/> [Admiralty: F4]
- [143] Escudo Digital (institutional). 2026. From Pegasus to JabaROOT: Inside the Undeclared Cyber Warfare Between Spain and Morocco. Escudo Digital (21 August 2026). Retrieved September 10, 2026 from <https://www.escudodigital.com/en/latest-reports/from-pegasus-to-jabaroot-inside-the-undeclared-cyber-warfare-between-spain-and-morocco.html> [Admiralty: C2]
- [144] Ali Attar. 2026. Fuite Jabaroot: le Maroc et ses partenaires sécuritaires africains fragilisés. Afrik.com (25 August 2026). Retrieved September 10, 2026 from <https://www.afrik.com/fuite-jabaroot-le-maroc-et-ses-partenaires-securitaires-africains-fragilises> [Admiralty: C3]
- [145] FIRST (institutional). 2026. FIRST Members (team directory). FIRST.org (accessed 8 September 2026). Retrieved September 10, 2026 from <https://www.first.org/members/teams/> [Admiralty: A1]

- [146] DataProtect (institutional). 2026. DataProtect homepage (service catalogue). dataprotect.ma (accessed 8 September 2026). Retrieved September 10, 2026 from <https://www.dataprotect.ma/> [Admiralty: C2]
- [147] Wikipedia contributors. 2026. Pegasus (spyware). Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from [https://en.wikipedia.org/wiki/Pegasus_\(spyware\)](https://en.wikipedia.org/wiki/Pegasus_(spyware)) [Admiralty: D2]
- [148] Fatima Gomez. 2026. El arsenal de espionaje de Marruecos más allá de Pegasus. Merca2.es (18 July 2026). Retrieved September 10, 2026 from <https://www.merca2.es/2026/07/18/arsenal-espionaje-marruecos-pegasus-2420008/> [Admiralty: E4]
- [149] Cisco Talos. 2024. Starry Addax targets human rights defenders in North Africa with new malware. Cisco Talos Intelligence Blog (9 April 2024). Retrieved September 10, 2026 from <https://blog.talosintelligence.com/starry-addax/> [Admiralty: A1]
- [150] Medusa Submarine Cable System (AFR-IX Telecom-led consortium). 2026. Medusa Submarine Cable System — official project site. medusascs.com (undated, retrieved 8 September 2026). Retrieved September 10, 2026 from <https://medusascs.com/> [Admiralty: B2]
- [151] Wikipedia contributors. 2026. List of international submarine communications cables. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/List_of_international_submarine_communications_cables [Admiralty: D3]
- [152] Wikipedia contributors. 2026. 2Africa. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from <https://en.wikipedia.org/wiki/2Africa> [Admiralty: D2]
- [153] Wikipedia contributors. 2026. Inwi. Wikipedia (retrieved 9 September 2026 (article states last updated May 2026)). Retrieved September 10, 2026 from <https://en.wikipedia.org/wiki/Inwi> [Admiralty: D3]
- [154] Microsoft Corporation. 2026. Azure global infrastructure — geographies. Microsoft Azure (official corporate page) (retrieved 9 September 2026 (live page)). Retrieved September 10, 2026 from <https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies/> [Admiralty: B2]
- [155] Google LLC. 2026. Google Cloud locations. Google Cloud Platform (official corporate page) (retrieved 9 September 2026 (live page)). Retrieved September 10, 2026 from <https://cloud.google.com/about/locations> [Admiralty: B2]
- [156] Cloudflare, Inc.. 2026. Cloudflare network map. Cloudflare (official corporate page) (retrieved 9 September 2026 (live page)). Retrieved September 10, 2026 from <https://www.cloudflare.com/network/> [Admiralty: B2]
- [157] Wikipedia contributors. 2026. Huawei. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from <https://en.wikipedia.org/wiki/Huawei> [Admiralty: F6]
- [158] Wikipedia contributors. 2026. Energy in Morocco. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Energy_in_Morocco [Admiralty: D2]
- [159] Wikipedia contributors. 2026. STMicroelectronics. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from <https://en.wikipedia.org/wiki/STMicroelectronics> [Admiralty: D2]
- [160] Wikipedia contributors. 2026. Global Positioning System. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/Global_Positioning_System [Admiralty: D6]
- [161] Wikipedia contributors. 2026. General Directorate for Territorial Surveillance. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from https://en.wikipedia.org/wiki/General_Directorate_for_Territorial_Surveillance [Admiralty: D3]

[162] Wikipedia contributors. 2026. DGED. Wikipedia (retrieved 9 September 2026). Retrieved September 10, 2026 from <https://en.wikipedia.org/wiki/DGED> [Admiralty: D3]

[163] DGSSI (Direction Générale de la Sécurité des Systèmes d'Information). 2024. Publication de la Stratégie Nationale de Cybersécurité à l'horizon 2030 (DGSSI homepage). dgssi.gov.ma (22 July 2024 (page retrieved 9 September 2026)). Retrieved September 10, 2026 from <https://www.dgssi.gov.ma/fr/> [Admiralty: A2]

Acronyms

For ready reference, the acronyms used throughout this report expand as follows: AMDIE, Agence Marocaine de Développement des Investissements et des Exportations; AMMC, Autorité Marocaine du Marché des Capitaux; ANCFCC, Agence Nationale de la Conservation Foncière, du Cadastre et de la Cartographie; ANRT, Agence Nationale de Réglementation des Télécommunications; APEBI, Fédération Marocaine des Technologies de l'Information, des Télécommunications et de l'Offshoring; APT, Advanced Persistent Threat; AUSIM, Association des Utilisateurs des Systèmes d'Information au Maroc; BCIJ, Bureau Central d'Investigations Judiciaires; BNPJ, Brigade Nationale de la Police Judiciaire; C4ISR, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance; CDG, Caisse de Dépôt et de Gestion; CERT, Computer Emergency Response Team; CGEM, Confédération Générale des Entreprises du Maroc; CGPJ, Consejo General del Poder Judicial (Spain); CJEU, Court of Justice of the European Union; CNDP, Commission Nationale de contrôle de la protection des Données à caractère Personnel; CNI, Centro Nacional de Inteligencia (Spain); CNIE, Carte Nationale d'Identité Électronique; CNOPS, Caisse Nationale des Organismes de Prévoyance Sociale; CNSS, Caisse Nationale de Sécurité Sociale; CSIRT, Computer Security Incident Response Team; DDoS, Distributed Denial-of-Service; DGED, Direction Générale des Études et de la Documentation; DGSN, Direction Générale de la Sûreté Nationale; DGSSI, Direction Générale de la Sécurité des Systèmes d'Information; DGST, Direction Générale de la Surveillance du Territoire; FAR, Forces Armées Royales; FIRST, Forum of Incident Response and Security Teams; GCI, the ITU's Global Cybersecurity Index; GSI-GR, Groupement de Sécurité et d'Intervention de la Gendarmerie Royale; IAM, Itissalat Al-Maghrib (Maroc Telecom); IIV, Infrastructures d'Importance Vitale (vital infrastructure); INCIBE, Instituto Nacional de Ciberseguridad (Spain); IXP, Internet Exchange Point; maCERT, Morocco Computer Emergency Response Team; MGPTT, Mutuelle Générale des Postes et Télécommunications (Algeria's postal and telecommunications-workers mutual fund); MINURSO, Mission des Nations Unies pour l'Organisation d'un Référendum au Sahara Occidental; NARSA, Agence Nationale de la Sécurité Routière; NCSI, the National Cyber Security Index (Estonia's e-Governance Academy); OIC-CERT, Organisation of Islamic Cooperation Computer Emergency Response Team; PCR, Police des Communications Radioélectriques; PEGA, the European Parliament's committee of inquiry on the use of Pegasus and equivalent surveillance spyware; PJD, Parti de la Justice et du Développement (Justice and Development Party); PKI, Public Key Infrastructure; PNT, Positioning, Navigation and Timing; RASCOM, Regional African Satellite Communication Organization; SCADA, Supervisory Control and Data Acquisition; SIGINT, Signals Intelligence; and SRBM, Système des Règlements Bruts du Maroc.



Sede S2GRUPO
Calle Luis Merelo y Mas,
6, 46023 Valencia
S2grupo.com

/s2grupo
LinkedIn
Instagram
Facebook
X