

UNITED CANADIAN EMPIRE

CYBERSENTINEL OPERATIONS & DOCTRINE HANDBOOK

2026 DEFINITIVE EDITION

CROWN SECURITY RESTRICTED

IMPERIAL DEFENSE / CYBERSENTINEL PROGRAM MATERIAL



AUTHORIZED IMPERIAL PERSONNEL ONLY

UCE-CSH-2026-R1

CROWN SECURITY RESTRICTED

AUTHORIZED IMPERIAL PERSONNEL ONLY

CONTROLLED COPY NO. _____

This document is a controlled restricted publication of the United Canadian Empire.

CLASSIFICATION & HANDLING

CROWN SECURITY RESTRICTED

This handbook contains restricted technical, operational, organizational, and strategic information relating to the Cybersentinel Program.

Covered material includes class architecture and engineering, tactical AI and command, weapons and defenses, Warden countermeasures, force organization and readiness, manufacturing and sustainment, recovery and technology denial, and Prototype policy.

Possession of this handbook does not itself grant access to every compartment referenced within it. Some Warden, Prototype, Crown, and special-access procedures remain outside this publication.

Unauthorized duplication, distribution, or disclosure is prohibited. Lost or compromised copies shall be reported through Crown Security channels.

DOCUMENT AUTHORITY

Controlling Edition: 2026 Definitive Edition

Program Authority: Imperial Cybersentinel Command (ICCOM)

Technical Authority: Ironreach Cybersentinel Directorate

Strategic Authority: Imperial Armed Forces of the United Canadian Empire

Ultimate Command Authority: Emperor

PURPOSE & INTENDED USERS

This handbook serves as the comprehensive engineering, doctrine, and operational reference for Cybersentinel systems.

It is intended for commanders, technical personnel, operators, intelligence staff, recovery personnel, and other authorized Imperial users.

Cybersentinels are tactically autonomous strategic weapons platforms operating under human strategic authority.

REVISION CONTROL

Table FM-1 — Revision Control.

Revision	Date	Description	Authority
1.0	2026	Definitive Edition	ICCOM / Ironreach

TERMS & DEFINITIONS

Cybersentinel — A tactically autonomous strategic weapons platform operating under human strategic authority.

Production Class — An approved operational class built to a controlling mission architecture.

Prototype — A CS-X4-## experimental system not assumed to be equivalent to a production class.

Authorized Fleet — The officially authorized force establishment.

Inventory Present — Certified systems physically carried in active inventory.

Available Combat Strength (ACS) — Systems realistically deployable for a given mission and time window.

Mission Envelope — The human-defined bounds governing objective, area, rules, protected assets, prohibited targets, weapons, duration, withdrawal, denial, and escalation.

ISTM — Imperial Sentinel Tactical Mesh; decentralized tactical coordination architecture.

TCN — Tactical Coordination Node; a temporary coordination role, not a permanent master node.

COG — Cybersentinel Operations Group; a temporary operational headquarters.

SRP — Sentinel Recovery Point.

Neutralize — Render a hostile capability unable to continue the relevant threat.

Operational — Certified and carried as part of the active inventory; not synonymous with currently available.

Readiness State — R1 Immediate Ready, R2 Mission Ready, R3 Maintenance Ready, or R4 Deep Service.

TABLE OF CONTENTS

PART I — FOUNDATION 11

Chapter 1: Executive Overview 12

Chapter 2: Historical Development 15

Chapter 3: Design Doctrine & Program Philosophy 18

Chapter 4: Classification System 22

PART II — ENGINEERING & WEAPONS 24

Chapter 5: Common Cybersentinel Architecture 25

Chapter 6: Physical Engineering & Survivability 31

Chapter 7: Weapons & Defensive Systems 35

PART III — PRODUCTION CLASSES 38

Chapter 8: CS-S4-01 Sentry 40

Chapter 9: CS-L4-01 Legion 44

Chapter 10: CS-B4-01 Bulwark 48

Chapter 11: CS-W4-01 Warden 52

Chapter 12: Prototype Systems 58

PART IV — COMMAND & ORGANIZATION 61

Chapter 13: Command, Control & Tactical AI 62

Chapter 14: Imperial Sentinel Tactical Mesh 66

Chapter 15: Organization, Inventory & Readiness 68

Chapter 16: Manufacturing, Sustainment & Lifecycle 72

PART V — OPERATIONAL DOCTRINE 75

Chapter 17: Operational Doctrine 75

Chapter 18: Combined-Arms Integration 78

Chapter 19: Large-Scale & National Mobilization 80

Chapter 20: EW, Communications & Degraded Operations 83

PART VI — DAMAGE, RECOVERY & LEARNING 85

Chapter 21: Damage States & Battlefield Survival 86

Chapter 22: Recovery & Technology Denial 90

Chapter 23: Phleboto-Bot Repair Systems 93

Chapter 24: Five Gambit Lessons 97

PART VII — REFERENCE & CURRENT STATUS 99

Chapter 25: Visual & Identification Annex 100

Chapter 26: Quick-Reference Operational Annex 103

Chapter 27: 2026 Status 106

Glossary 109

Acronym Reference 112

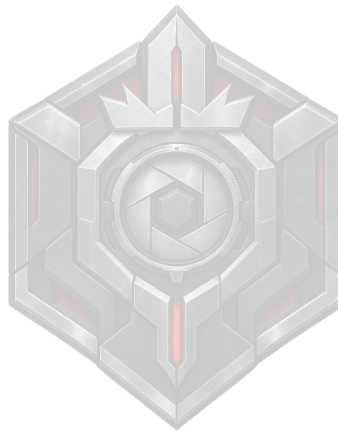
List Of Figures 113

List Of Tables 114

Index 116

PART I

FOUNDATION



CROWN SECURITY RESTRICTED

CHAPTER 1

EXECUTIVE OVERVIEW

Strategic Weapons Platforms of the United Canadian Empire

This chapter establishes the controlling 2026 definition, mission, force structure, and strategic boundaries of the Cybersentinel Program. Cybersentinels are not robotic infantry and are not autonomous national commanders. They are tactically autonomous strategic weapons platforms operating under human strategic authority.

DOCTRINAL PRINCIPLE: Cybersentinels exist to change a military problem that conventional forces, Redcoats, fixed defenses, aircraft, vehicles, or drones cannot solve as efficiently.

1.1 Program Definition

The Cybersentinel Program provides the United Canadian Empire with a small, specialized family of large robotic systems designed for strategic surveillance, heavy battlefield combat, mobile shield defense, metahuman contingency response, and controlled experimentation. The program supplements the Imperial Armed Forces; it does not replace the Army, Air Service, Maritime Service, Imperial Special Operations Command, Redcoats, Enforcers, or fixed defense infrastructure.

The defining boundary is authority. A Cybersentinel may evaluate terrain, threats, firing solutions, defensive posture, movement, and immediate tactical options inside an authenticated Mission Envelope. It does not determine national policy, select wars, create strategic objectives, or assume sovereign command. Human authority establishes why the platform is employed and the limits inside which it may act.

This distinction is central to every later chapter. The machines are powerful because they can continue to function under degraded communications, but resilience is not independence from the state. Local tactical autonomy is an engineering response to battlefield disruption, not a grant of political or strategic agency.

1.2 Production Classes

Generation IV standardizes four production classes and one Prototype category. Each class is defined by its primary strategic mission and controlling architecture rather than by superficial body shape. Mission determines form.

Table 1-1 — Production Classes.

Class	Authorized	Primary Strategic Mission	Controlling Form
Sentry	48	Strategic surveillance, site defense, electronic warfare, local air and drone defense	Low industrial quadruped
Legion	24	Heavy conventional battlefield combat and anti-vehicle firepower	Broad low-center-of-gravity biped
Bulwark	12	Mobile strategic shielding and protected-sector defense	Low rectangular mobile fortress; tower deployed
Warden	8	Metahuman suppression, restraint, contingency response, and containment	Tall, narrow, sensor-dense biped

Prototype	4	Experimental strategic systems and technology validation	Project-specific; no standard production silhouette
-----------	---	--	---

The authorized 2026 fleet totals 96 operational systems. This number is the controlling force establishment: 48 Sentry, 24 Legion, 12 Bulwark, 8 Warden, and 4 Prototype systems. The private long-term aspiration for a substantially larger fleet is not current authorization, not a present procurement schedule, and not an estimate of hidden inventory.

1.3 Strategic Role and Scarcity

Cybersentinels are intentionally scarce. They are allocated when their specialized effect justifies the industrial, logistical, security, and recovery burden of committing them. A routine tactical problem should not receive a strategic robotic weapons platform simply because one exists.

This scarcity shapes doctrine. Singletons and small Elements handle many routine requirements. Larger Detachments are created for significant battles or national crises. Strategic reserve is preserved where practical so that one emergency does not consume the Empire's ability to answer the next. Available Combat Strength therefore matters more in practice than the authorized headline total.

Replacement-before-expansion doctrine further reinforces scarcity. Ironreach normally uses new production to restore destroyed or retired systems toward the authorized force before expanding above it. Expansion above 96 requires explicit future authority.

1.4 Relationship to Redcoats and Conventional Forces

Redcoats are robotic soldiers. Cybersentinels are strategic robotic weapons platforms. The distinction is functional, not rhetorical. Redcoats can provide persistent manpower, close security, interior operations, and repeated small-unit presence. Cybersentinels deliver effects measured in surveillance reach, heavy firepower, strategic shielding, or metahuman contingency capability.

Imperial Army formations retain responsibility for maneuver, terrain, conventional logistics, and sustained ground control. The Imperial Air Service controls the broader air battle. The Maritime Service provides naval support and, in many off-island contingencies, the principal heavy transport pathway. ISOC handles specialized joint missions. Cybersentinels amplify these forces rather than replace them.

At the national-defense level, the program fits into defense in depth: detection, interception, shielding, metahuman response, and inner security. The machine changes the battlefield; the combined force converts that advantage into victory.

1.5 Command and Security Boundary

Cybersentinels authenticate command through layered credentials, rotating keys, and challenge-response procedures. There is no universal master-control code and no fleetwide kill switch. Mission authority is hierarchical, but tactical survival is deliberately decentralized.

Each deployment is bounded by a Mission Envelope defining objective, operating area, rules of engagement, protected assets, prohibited targets, authorized weapons, duration, withdrawal conditions, denial conditions, and escalation limits. When communications fail, a platform falls back on the Last Valid Mission Envelope rather than seeking open-ended authority.

The program therefore separates strategic control from tactical execution. That separation is one of the direct lessons of Operation: Gambit and one of the foundational reasons Generation IV can remain effective under jamming, network partition, or local infrastructure failure.

1.6 2026 Program Posture

By 2026, Generation IV is a mature integrated production standard. The major architectural questions are no longer whether the concept works, but how many systems can be sustained, how quickly they can be repaired or replaced, how much strategic reserve must be preserved, and how individual class effects should be combined with conventional forces. The program is powerful precisely because it is specialized, recoverable, and bounded.

No Cybersentinel is irreplaceable; no Cybersentinel is expendable without purpose.

1.7 Chapter Summary

The Cybersentinel Program is a 96-system strategic robotic force organized around four mature production classes and a tightly controlled Prototype category. Human strategic authority remains absolute. Tactical autonomy exists to preserve mission function under battlefield disruption, while combined-arms doctrine, recovery discipline, and industrial scarcity prevent the machines from becoming an isolated or self-directing force.

CHAPTER 2

HISTORICAL DEVELOPMENT

From Fortress Expansion to Generation IV

Cybersentinels emerged from the United Canadian Empire's post-IRON LANTERN requirement for strategic defensive systems capable of offsetting manpower limits, surviving heavy attack, and continuing to function when communications and fixed infrastructure were damaged.

2.1 Technical Prehistory: 2005–2008

The earliest program roots lie in the Empire's rapid militarization after its founding and in the engineering culture that surrounded Ironreach and Doctor Phlebotinum. Robotics, remote weapons, hardened infrastructure, compact power systems, and automated defensive logic developed in parallel rather than as one unified machine program.

Operation IRON LANTERN in 2008 provided the decisive catalyst. The siege demonstrated the strategic danger of relying on human defenders alone against a numerically and materially superior external force. Fortress Expansion therefore sought systems that could hold critical sectors, absorb losses, and multiply the effect of a comparatively small Imperial defense establishment.

2.2 CS-X1 and the First True Cybersentinel

By approximately 2009, the CS-X1 test platform represented the first system that met the later definition of a Cybersentinel: a large tactical machine with sufficient local sensing, weapons integration, mobility, and computational autonomy to execute bounded combat tasks without continuous remote piloting.

At this stage, architecture remained experimental. Control logic was more centralized, subsystem isolation was immature, maintenance was difficult, and the distinction between test platform and battlefield system was still evolving. Nevertheless, CS-X1 proved that an Imperial-built strategic robotic platform could be more than a fixed weapon or remote vehicle.

2.3 Project COUNTERMEASURE

In parallel, Project COUNTERMEASURE explored robotic responses to metahuman threats. CM-X1 and CM-X2 were not yet modern Wardens, but they established the principle that a machine could be built around specific suppression, restraint, environmental, and containment requirements rather than around conventional firepower alone. Their legacy survives in the Warden class and its mission-package architecture.

2.4 Generation I — 2008–2012

Generation I was the proof-of-concept generation. Fewer than twenty systems were deployable by Operation: Gambit. They demonstrated impressive strength, firepower, endurance, and local tactical capability, but their design still carried vulnerabilities inherited from an era when the Empire was building strategic robotics faster than it could fully mature doctrine and sustainment.

Operation: Gambit became the program's defining battlefield test. Approximately two-thirds of the Generation I systems that were deployed or operational during the crisis were destroyed or rendered combat ineffective. The loss was not caused by one simple weakness. Centralized command dependencies, cooling vulnerabilities, maintenance limits, electronic warfare, mobility failures, tipping risk, subsystem cascades, and dangerous anti-capture logic all contributed.

One exceptional Generation I survivor continued operating after major network disruption. That machine demonstrated an enduring principle: a strategic platform that can preserve a valid mission locally is more survivable than one whose tactical existence depends upon an intact central network.

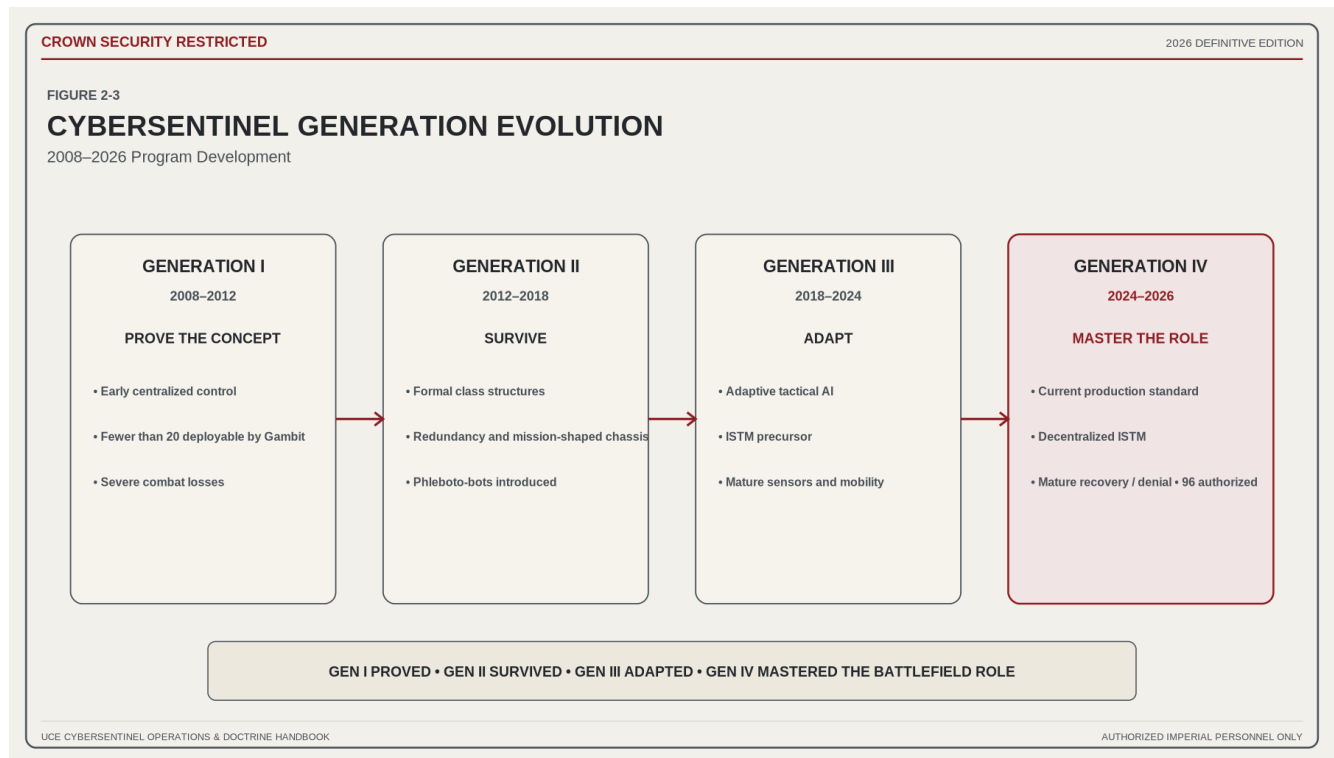


Figure 2-3 — Cybersentinel Generation Evolution, 2008–2026.

2.5 Generation II — 2012–2018: Survive

Generation II converted Gambit losses into engineering requirements. Formal production classes began to replace one-off multifunction machines. Redundancy increased. Critical systems were distributed. Mission-shaped chassis became the norm. Anti-capture policy was reworked to prevent the machine from becoming a greater danger to Imperial forces than the enemy attempting to seize it.

This period also introduced the Phlebotomist system: small brass spherical repair machines capable of climbing through a host platform, carrying tools, and performing temporary local repairs. The concept did not make Cybersentinels self-healing. It did allow hundreds of small failures to be contained before they became catastrophic.

2.6 Generation III — 2018–2024: Adapt

Generation III matured adaptive tactical AI, sensor fusion, electronic warfare, mobility, and class identity. The predecessor architecture to the Imperial Sentinel Tactical Mesh emerged during this period as the program moved away from centralized network assumptions toward federated tactical coordination.

Generation III also made survivability more deliberately functional. Designers stopped treating armor thickness as the sole measure of endurance and increasingly focused on keeping the mission alive after sensors, mobility, weapons, cooling, or communications were damaged.

2.7 Generation IV — 2024–2026: Master the Role

Generation IV is the current integrated production standard. The four production classes are now sharply differentiated. Common architecture improves sustainment, while mission systems, chassis, armament, mobility, and doctrine remain specialized.

Generation IV formalizes decentralized ISTM coordination, layered command authentication, GREEN/AMBER/RED physical states, BLACK security state, YELLOW COMMAND anomaly handling, staged technology denial, Last Valid Mission Envelope behavior, and standardized Phleboto-bot integration. There is no single-point death switch and no assumption that network loss equals tactical defeat.

2.8 Historical Principle

DOCTRINAL PRINCIPLE: Generation I proved the concept. Generation II learned to survive. Generation III learned to adapt. Generation IV learned to master its battlefield role.

2.9 Chapter Summary

The modern Cybersentinel is the product of battlefield loss as much as technological progress. Operation: Gambit transformed the program from an impressive collection of machines into a disciplined weapons system built around redundancy, bounded autonomy, recovery, sustainment, and the assumption that enemy action will target function rather than spectacle.

CHAPTER 3

DESIGN DOCTRINE & PROGRAM PHILOSOPHY

Mission Before Machine

Cybersentinel design begins with a strategic effect, not a preferred body shape. The program exists to solve military problems that are poorly served by ordinary troops, Redcoats, vehicles, aircraft, drones, or fixed emplacements.

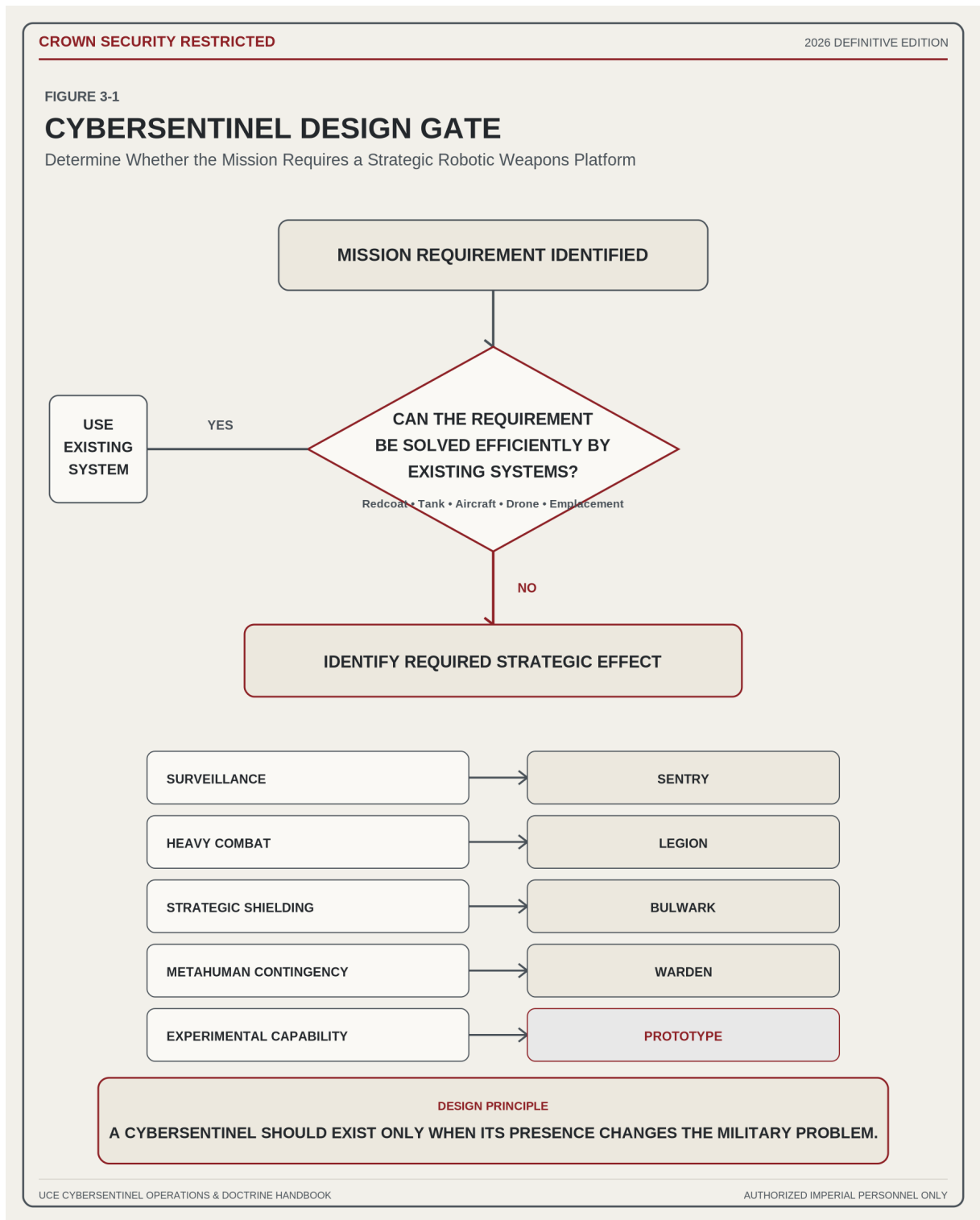


Figure 3-1 — Cybersentinel Design Gate.

3.1 The Design Gate

Every proposed system must first pass a basic test: can the requirement be solved more efficiently by an existing force or platform? If the answer is yes, the requirement should not produce a Cybersentinel.

Large strategic robots are expensive to build, difficult to move, security-sensitive, and demanding to recover. The threshold for creating or deploying one is deliberately high.

Only when the required effect exceeds what a Redcoat, tank, aircraft, drone, emplacement, or ordinary combined-arms formation can reasonably deliver does the program proceed to class-level design. Surveillance and defensive awareness point toward Sentry. Heavy conventional combat points toward Legion. Strategic shielding points toward Bulwark. Metahuman contingency response points toward Warden. Experimental cross-domain requirements remain Prototype work until proven.

A Cybersentinel should exist only when its presence changes the military problem.

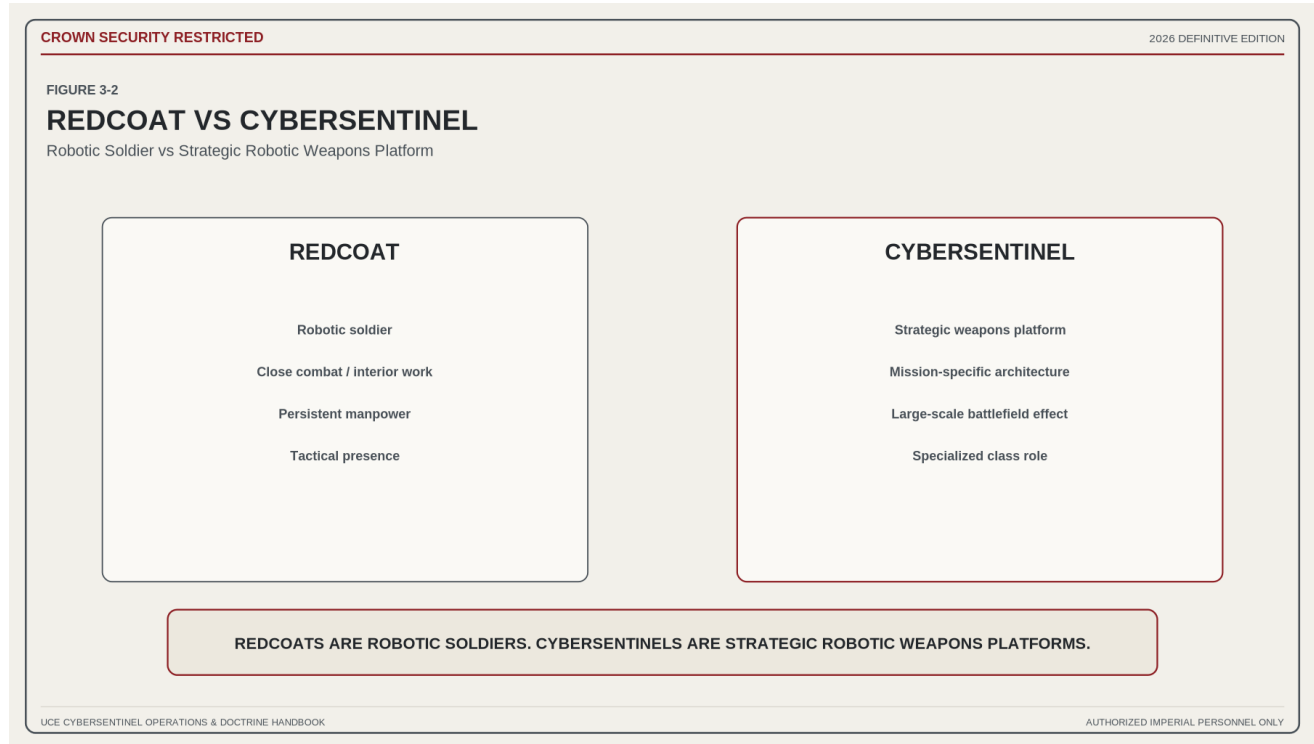


Figure 3-2 — Foundational distinction between Redcoat robotic soldiers and Cybersentinel strategic weapons platforms.

3.2 Mission-Shaped Chassis

Cybersentinels are not required to resemble humans. Body architecture follows the physics of the mission. Sentry uses a low quadruped form because stability, sensor coverage, endurance, and all-terrain movement matter more than humanlike reach. Legion uses a broad biped because recoil control, integrated heavy weapons, obstacle negotiation, and deliberate direct-fire maneuver define its role. Bulwark is a mobile fortress because shield stability and anchoring dominate its engineering. Warden is taller and narrower because sensor density, rapid positioning, restraint, and countermeasure deployment demand a different geometry.

This philosophy is also a control against aesthetic drift. A design is not accepted because it looks intimidating. If its form does not improve the mission, it is rejected.

3.3 Human Strategic Authority

Production systems use tactical artificial intelligence rather than humanlike synthetic personality. The machine may decide how to move, which threat to engage first, how to allocate point defense, how to preserve cover, or when a local withdrawal recommendation is necessary. It does not decide why the war exists.

Strategic objectives, mission boundaries, protected persons and facilities, prohibited targets, escalation limits, and denial authority remain human responsibilities. Even Warden, the class with the most specialized target-control logic, operates inside an authenticated Mission Envelope rather than an open-ended hunt state.

3.4 Mutual Specialization

No production class is designed to dominate every category. Sentry sees and disrupts. Legion applies conventional heavy force. Bulwark changes the geometry of protection. Warden addresses powered threats that can make ordinary battlefield assumptions unreliable.

This specialization is deliberate. It makes the force easier to understand, maintain, allocate, and command. It also reduces the temptation to build a universal machine that is too expensive, too complex, and too compromised in every role to be truly exceptional in any one of them.

3.5 Prototype Boundary

Prototype systems exist to test technology, not to provide a hidden fifth production class. A Prototype may break production limits, explore extreme environments, experiment with cognition, or combine capabilities that would be unacceptable in an ordinary fielded system. That freedom is balanced by tighter compartmentalization and a small authorized inventory.

Prototype success does not automatically imply adoption. A project may be adopted, partially adopted, archived, dismantled, destroyed, or sealed. Production status is earned through repeatability, sustainment, doctrine, and strategic need.

3.6 Engineering Maxim

Phlebotinum built the machinery. The Empire armored it.

The maxim captures the program's dual nature: advanced and sometimes unconventional engineering is disciplined by Imperial requirements for armor, redundancy, security, maintainability, and battlefield recovery.

3.7 Chapter Summary

Cybersentinel design is mission-driven, bounded by human strategic authority, and intentionally specialized. The program rejects universal machines, unnecessary humanoid form, and automation without command limits. Production classes exist because they solve distinct strategic problems better than other available systems.

CHAPTER 4

CLASSIFICATION SYSTEM

Class, Generation, Model, and Prototype Designation

The classification system provides a common language for commanders, engineers, intelligence personnel, recovery teams, and Crown Security. It identifies what a machine is expected to do, what generation of program architecture it belongs to, and whether its external configuration is a standardized production design or an experimental project.

4.1 Classification by Primary Strategic Mission

Table 4-1 — Classification by Primary Strategic Mission.

Class Code	Class	Primary Mission
S	Sentry	Surveillance / site defense / EW / local air defense
L	Legion	Heavy conventional battlefield combat
B	Bulwark	Mobile strategic shielding
W	Warden	Metahuman contingency and containment
X	Prototype	Experimental or nonstandard strategic capability

Class assignment follows the primary strategic mission and controlling architecture. A machine with several secondary capabilities remains in the class whose mission and chassis determine its design. True hybrids remain Prototype systems until a separate production standard is formally authorized.

4.2 Model Designation

Production model designations use the form CS-[Class][Generation]-[Model]. The 2026 controlling examples are CS-S4-01 Sentry, CS-L4-01 Legion, CS-B4-01 Bulwark, and CS-W4-01 Warden. Prototype systems use CS-X4-## because each project is individually controlled rather than treated as one standardized chassis family.

TECHNICAL NOTE: Systems sharing the same Generation, Class, and model designation share the same controlling exterior silhouette. Subvariants should be expressed primarily through internal systems, software, sensors, weapons packages, or mission configuration rather than casual exterior redesign.

4.3 Generation

Generation identifies the program architecture rather than merely the year of construction. A newly rebuilt older chassis can remain in active inventory only if it is fully rebuilt, certified, and brought to the required current standard. Age alone does not define operational relevance.

For prose, the preferred form is Generation I, Generation II, Generation III, or Generation IV. The compact form Gen IV is reserved for tables or dense reference material.

4.4 Production Classes and Standard Silhouettes

Exterior silhouette is an identification and sustainment control. It allows personnel to distinguish class at distance, supports training, and prevents undocumented visual variants from confusing operational recognition. A legitimate new model may alter the silhouette, but that change requires a real engineering threshold rather than cosmetic preference.

The four production classes therefore retain controlling visual forms: low quadruped Sentry, broad biped Legion, low fortress-like Bulwark, and taller narrow Warden. Prototype systems have no standard silhouette and should not be represented by a generic fifth robot.

4.5 Prototype Categories

Table 4-2 — Prototype Categories.

Prototype Category	Scope
Combat	Experimental offensive or battlefield systems
Defense	Novel protective or denial technologies
Mobility	Unusual movement or deployment architecture
Cognition	Restricted synthetic cognition and advanced decision systems
Special Systems	Cross-domain or unique mission technology
Extreme Environmental	Deep-water, space, lunar, magma, or similarly exceptional environments

A Prototype concept is normally represented by one system and at most two unless separately authorized. Prototype systems are excluded from ordinary strategic-reserve calculations unless a specific project has been separately approved for contingency use.

4.6 Identification Control

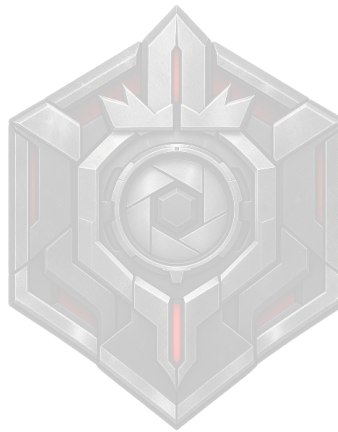
Program insignia, restrained Imperial-red identification lighting, national and military markings, service records, and model/serial data support positive identification. The Cybersentinel program insignia is subordinate to national and military authority markings; it identifies the program, not an independent institution.

4.7 Chapter Summary

Classification is deliberately conservative. Mission defines class, generation defines architecture, model defines the standardized production form, and Prototype status marks systems not yet suitable for routine production classification. The system exists to prevent ambiguity in command, maintenance, intelligence, and visual identification.

PART II

ENGINEERING & WEAPONS



CROWN SECURITY RESTRICTED

CHAPTER 5

COMMON CYBERSENTINEL ARCHITECTURE

Shared Generation IV Systems and Failure-Tolerant Design

Generation IV production classes are intentionally different in exterior form and mission, but they share enough underlying architecture to reduce sustainment burden, standardize security, and support repair. Commonality is a support strategy, not a requirement that every class become the same machine.

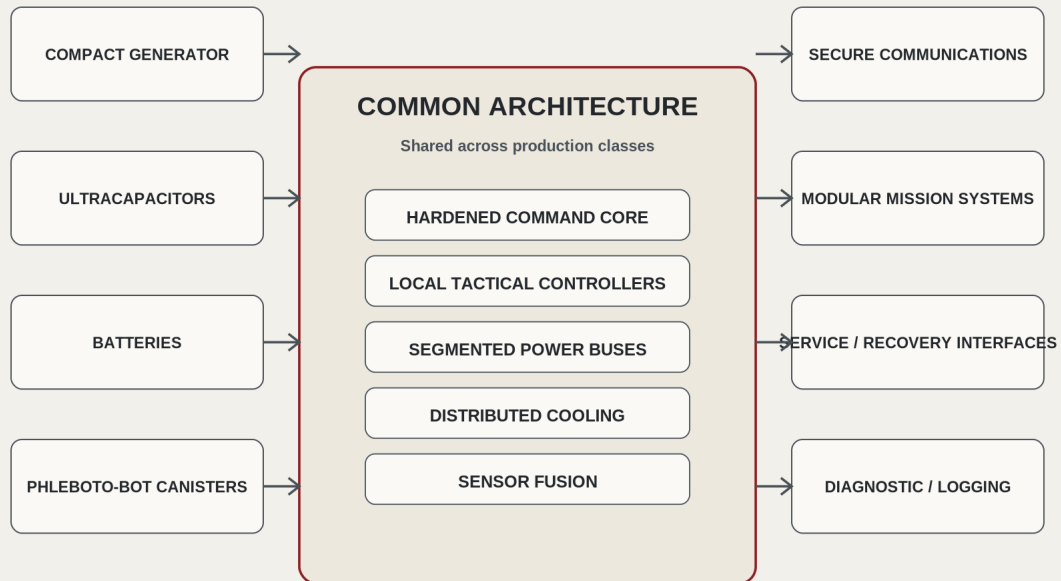
CROWN SECURITY RESTRICTED

2026 DEFINITIVE EDITION

FIGURE 5-1

COMMON CYBERSENTINEL CORE ARCHITECTURE

Shared Generation IV Systems Without a Generic Chassis



DOCTRINAL TAKEAWAY

SHARED ARCHITECTURE IMPROVES SUSTAINMENT WITHOUT ERASING CLASS SPECIALIZATION.

Conceptual architecture only — no generic fifth Cybersentinel chassis is implied.

UCE CYBERSENTINEL OPERATIONS & DOCTRINE HANDBOOK

AUTHORIZED IMPERIAL PERSONNEL ONLY

Figure 5-1 — Common Cybersentinel Core Architecture.

5.1 Common Combat Architecture

The Common Cybersentinel Core Architecture establishes shared principles for command processing, local control, power segmentation, secure communications, sensor fusion, cooling, maintenance access, logging, recovery, and Phleboto-bot integration. Approximately 30–40 percent subsystem-family commonality is maintained where practical across production systems.

CROWN SECURITY RESTRICTED | AUTHORIZED IMPERIAL PERSONNEL ONLY

Commonality is deliberately bounded. The Legion does not carry Sentry architecture merely for parts convenience, and Bulwark does not compromise shield stability to share a mobility assembly. Mission-critical specialization takes precedence when common components would degrade the class.

5.2 Hardened Command Core and Local Controllers

Each platform contains a hardened command core but does not depend upon one monolithic processor for every function. Local controllers preserve subsystem operation if higher-level coordination is damaged or isolated. This distributed approach supports the program principle that damage should propagate poorly.

Production tactical AI is bounded by authenticated mission authority. Local controllers can preserve mobility, sensor operation, cooling, point defense, or other essential functions without granting the machine strategic independence.

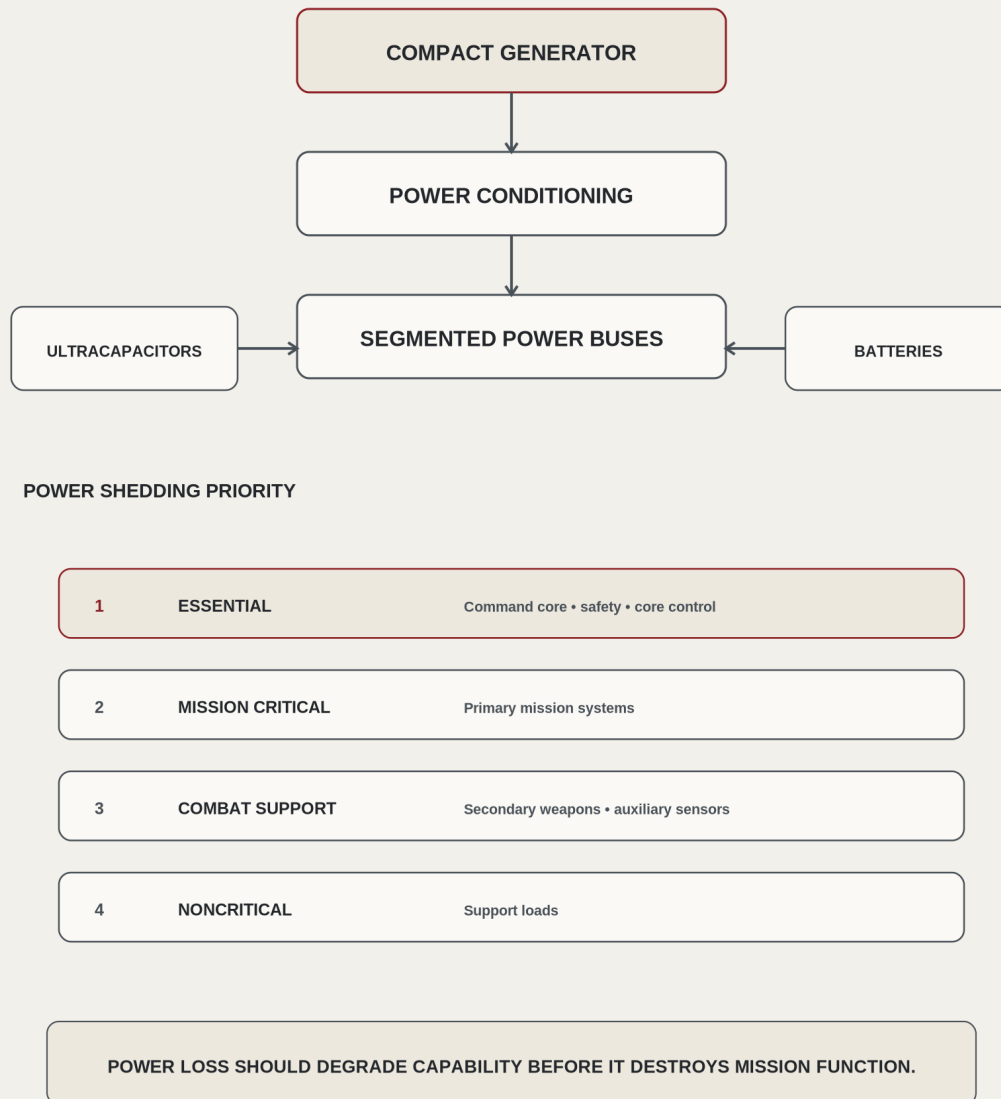
CROWN SECURITY RESTRICTED

2026 DEFINITIVE EDITION

FIGURE 5-3

POWER ARCHITECTURE & SHEDDING

Segmented Energy Distribution and Priority Preservation



UCE CYBERSENTINEL OPERATIONS & DOCTRINE HANDBOOK

AUTHORIZED IMPERIAL PERSONNEL ONLY

Figure 5-3 — Segmented power architecture and priority shedding.

5.3 Power Architecture

Generation IV combines a compact primary generator with ultracapacitors and battery reserves. The exact internal arrangement varies by class, but power distribution is segmented so damage to one bus does not automatically remove all mission function.

Power shedding follows a hierarchy: Essential, Mission Critical, Combat Support, and Noncritical. When output falls, lower-priority systems are shed first. The objective is not to keep every function alive; it is to preserve the functions necessary to complete, modify, or safely terminate the mission.

5.4 Distributed Cooling

Gambit demonstrated that cooling can be a mission-kill pathway even when armor remains intact. Generation IV therefore uses distributed cooling with isolation and rerouting rather than assuming one central loop will remain available.

Heat remains a finite operational constraint. Heavy weapons, shielding, mobility, electronic warfare, and countermeasure systems compete for thermal margin. Tactical AI may reduce rate of fire, movement, field output, sensor intensity, or auxiliary systems to prevent a localized heat problem from becoming total platform failure.

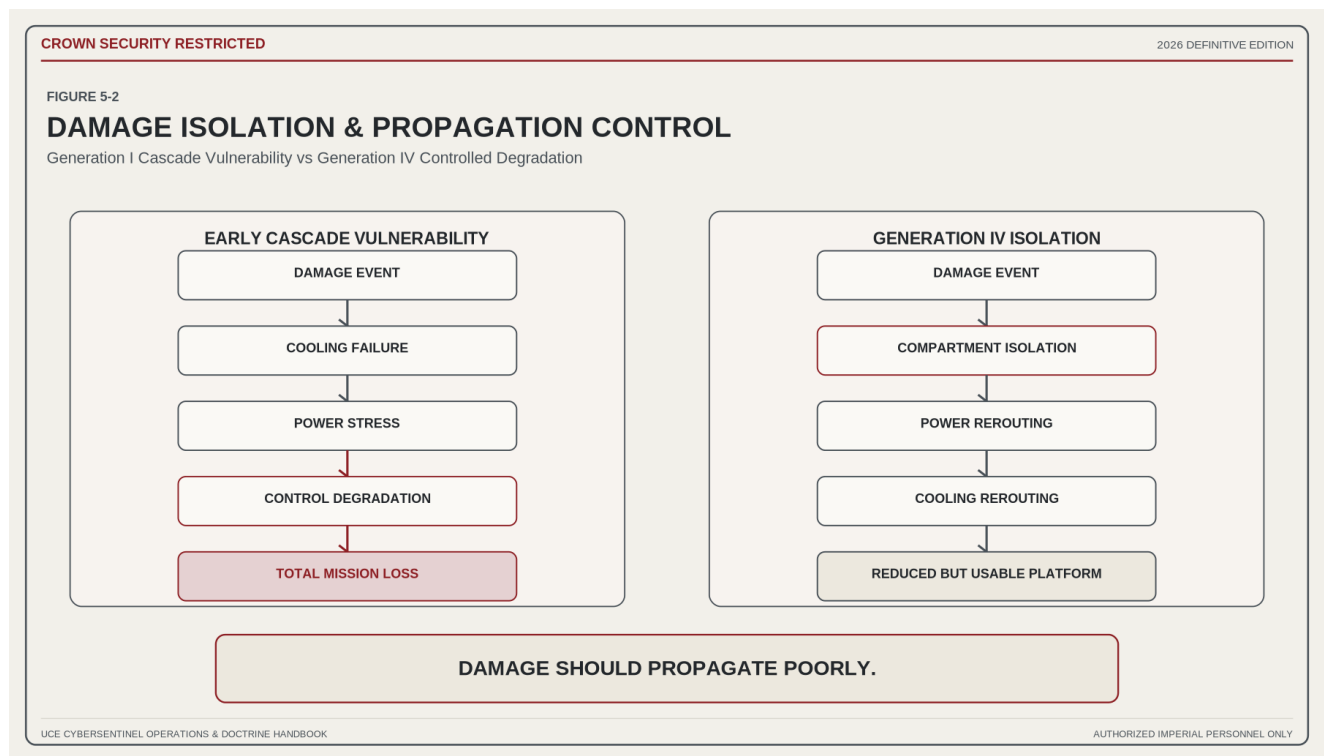


Figure 5-2 — Damage isolation and propagation control.

5.5 Damage Isolation

The controlling internal principle is simple: damage should propagate poorly. Armor is only the first layer. Structural segmentation, distributed power, redundant sensing, local control, fire isolation, cooling reroute, protected data paths, and repair access all exist to limit cascading failure.

Generation IV accepts controlled degradation. A machine may lose a sensor arc, weapon, limb, cooling segment, or communications path and remain militarily useful. Functional survival matters more than preserving a pristine platform.

DAMAGE SHOULD PROPAGATE POORLY.

5.6 Communications, Security, and Logging

Production systems use secure authenticated communications, rotating credentials, challenge-response procedures, and isolation behavior for suspect nodes. The architecture assumes jamming, deception, bandwidth loss, and captured equipment attempts rather than treating them as exceptional scenarios.

Operational logs, subsystem telemetry, damage records, and repair history are retained because every serious failure is an engineering data source. Recovery therefore preserves knowledge as well as hardware.

5.7 Phleboto-Bot Integration

Phleboto-bot canisters are standard Generation IV support equipment. Their complement varies by class, but the architectural requirement is common: access routes, magnetic crawl paths, host control, repair prioritization, recharge, and return must be planned into the machine rather than added afterward.

5.8 Chapter Summary

Generation IV architecture is common where commonality improves sustainment and specialized where mission demands it. Segmented power, distributed cooling, local controllers, secure communications, repair integration, and aggressive fault isolation allow a damaged machine to degrade in controlled steps instead of failing as one interconnected object.

CHAPTER 6

PHYSICAL ENGINEERING & SURVIVABILITY

Scale, Armor, Mobility, and Controlled Survivability

Cybersentinel survivability comes from geometry, material protection, redundancy, mobility, active defense, repair, information, and recovery doctrine. Armor alone cannot preserve a strategic platform against an intelligent enemy that can attack sensors, anchors, cooling, movement, weapons, software, or support infrastructure.

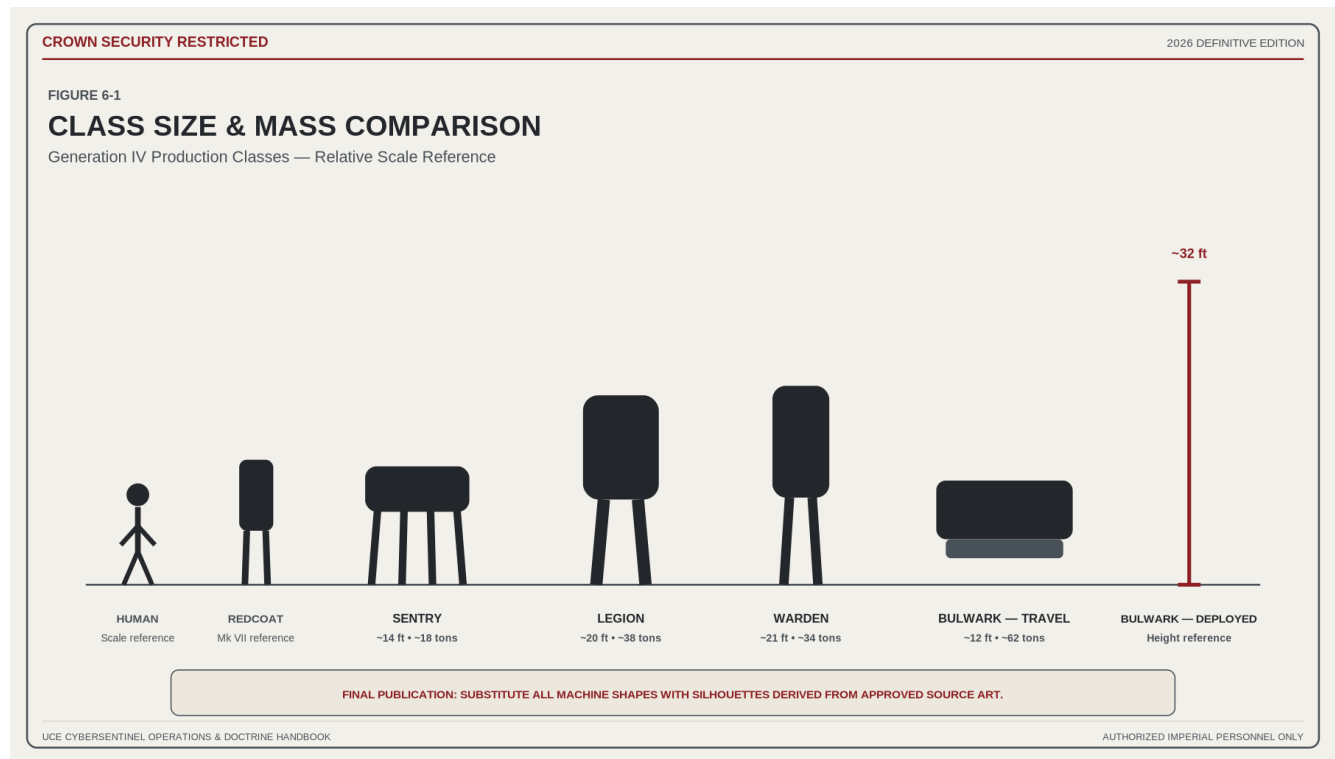


Figure 6-1 — Generation IV class size and mass comparison. Final source-derived silhouettes pending substitution.

6.1 Class Dimensions and Mass

Table 6-1 — Class Dimensions and Mass.

Class	Controlling Dimensions	Approx. Mass
Sentry	~14 ft high; ~19 ft long; ~11 ft wide	~18 tons
Legion	~20 ft high; ~10.5 ft wide	~38 tons
Bulwark	~12 ft transport; ~24 ft long; ~14 ft wide; ~32 ft deployed	~62 tons
Warden	~21 ft high; ~9.5 ft wide	~34 tons
Prototype	Project-specific / unrestricted	Project-specific

The figures above are engineering reference values rather than exact tolerances for every service modification. Same-generation, same-class, same-model systems retain the controlling silhouette and dimensional envelope unless a formally authorized model revision changes the design.

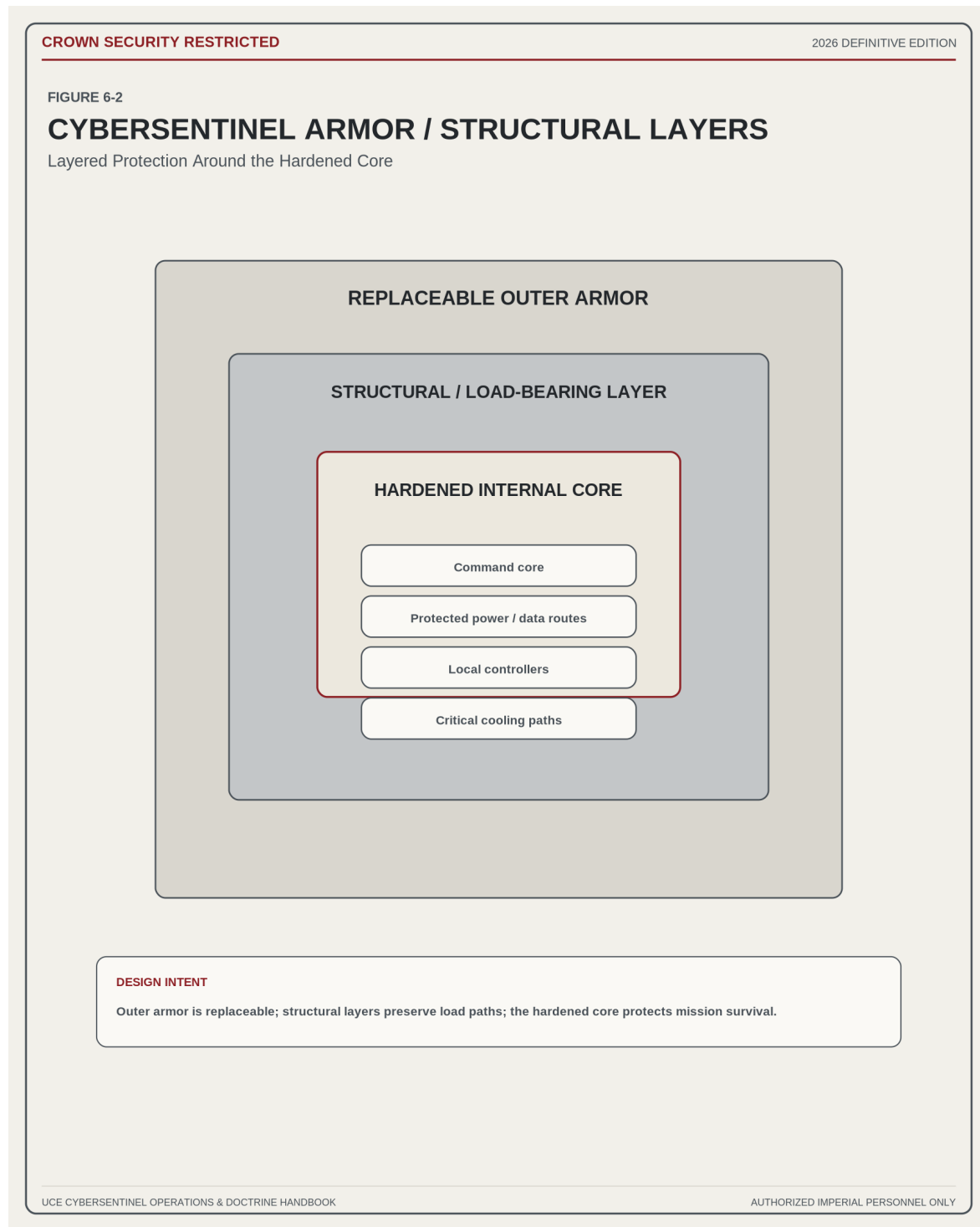


Figure 6-2 — Cybersentinel armor and structural protection layers.

6.2 Protection Layers

Protection is layered. Replaceable outer armor absorbs and localizes damage. Structural and load-bearing layers preserve mechanical integrity. A hardened internal core protects command, power distribution, local control, and other mission-critical functions. Advanced steels, titanium, ceramics, composites, and limited exotic materials are used according to class requirements.

No formal universal comic-style armor grade is assigned to the Sentry or other classes in this edition. Protection is discussed through architecture, role, and survivability rather than through unsupported single-word ratings.

6.3 Mobility Architecture

Mobility is class-specific. Sentry uses four articulated legs and a low center of mass for surveillance, terrain access, and stable weapon/sensor operation. Legion uses articulated bipedal movement optimized for deliberate heavy combat. Bulwark combines treads and walking/leveling mechanisms because transport stability and anchored deployment dominate its role. Warden uses articulated bipedal mobility with greater agility than Legion because it must reposition against dynamic metahuman threats.

Hover capability is tactical, not aviation. It exists to cross obstacles, reposition quickly, or solve short-duration terrain problems. Cybersentinels are not substitutes for aircraft.

6.4 Mobility and Environmental Reference

Table 6-2 — Mobility and Environmental Reference.

Class	Road	Cross-Country	Underwater	Hover / Tactical Lift
Sentry	~40 mph	~25–30 mph	~150 ft	~90 sec / ~40 mph
Legion	~35 mph	~22–28 mph	~250 ft	~2 min / ~45 mph
Bulwark	Mission-dependent transport	Mission-dependent	~100 ft	~20 sec / ~15 mph tactical obstacle lift only
Warden	~42 mph	~28–32 mph	~250 ft	~2 min / ~45 mph

Underwater ratings are operational depth references for applicable production systems, not a claim that every class is optimized for submerged combat. Prototype Extreme Environmental projects may exceed normal production limits, including depths beyond 1,000 ft or operation in space, lunar, magma, and other exceptional environments.

6.5 Survivability as Mission Preservation

A Cybersentinel does not need to remain untouched to remain successful. It must preserve enough mobility, sensing, firepower, shielding, containment, communications, or recovery capability to achieve the required effect.

Tactical AI therefore evaluates whether to continue, modify, withdraw, stabilize, or recommend recovery based on mission value and remaining capability. A machine can be functionally defeated without being destroyed; doctrine is designed around recognizing that reality early enough to preserve the platform and the mission where possible.

6.6 Environmental and Recovery Design

Service access, towing/recovery interfaces, underwater sealing where applicable, repair routes, attachment points, modular armor, and transport constraints are part of survivability engineering. Recovery is not an afterthought imposed on a wreck; it begins when the machine is designed and when the deployment plan is written.

6.7 Chapter Summary

Generation IV survivability is layered and functional. Class geometry, protective materials, segmented systems, movement, thermal management, tactical lift, underwater operation, active defense, repair, and

recovery all contribute. The enemy is expected to attack function rather than the strongest armor plate, so the machine is designed to remain useful after damage rather than merely difficult to penetrate.

CHAPTER 7

WEAPONS & DEFENSIVE SYSTEMS

Mission-Driven Armament, Active Defense, Shielding, and Countermeasures

Cybersentinel armament is integrated into class architecture and bounded by ammunition, heat, power, mission authority, and recovery considerations. Weapons are selected to create the required strategic effect, not to maximize the number of systems mounted on a chassis.

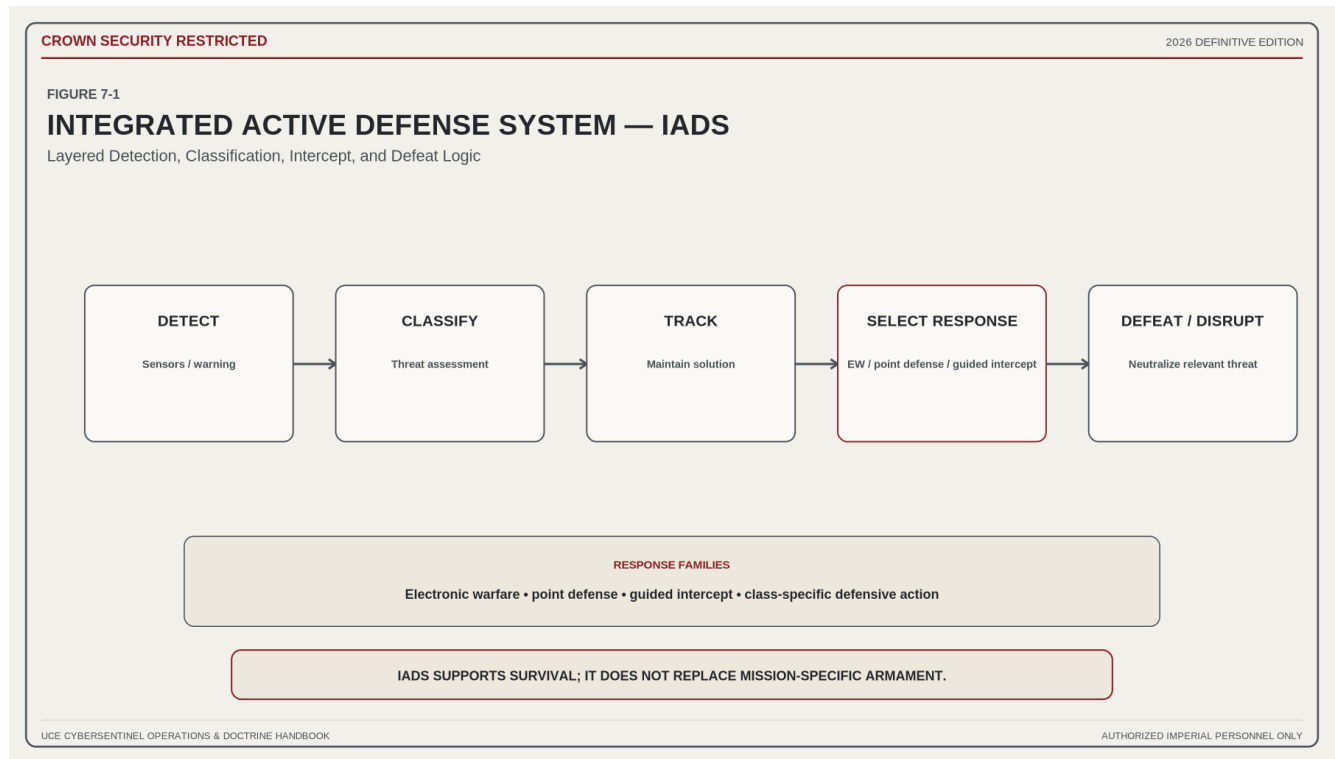


Figure 7-1 — Integrated Active Defense System architecture.

7.1 Integrated Active Defense System

The Integrated Active Defense System combines detection, classification, tracking, electronic warfare, point defense, guided intercept, and class-specific defensive action. The precise mix varies by class, but the objective is consistent: defeat or disrupt incoming threats before passive armor becomes the only remaining protection.

IADS does not replace mission-specific armament. It supports survival. Sentry places particularly strong emphasis on surveillance, electronic warfare, counter-drone, and local air defense; Legion combines IADS with heavy direct-fire capability; Bulwark protects its shield mission; Warden protects a platform that may need to remain exposed while containing an unusual target.

7.2 Weapon Families

Table 7-1 — Weapon Families.

Weapon / Defense Family	Operational Role
Kinetic	Conventional and heavy direct-fire systems; ammunition-limited
Directed Energy	Precision or specialized energy effects; power/heat-limited
Guided	Internal cells or guided munitions for selected threats
Point Defense	Short-response interception against missiles, drones, and close threats
Electronic Warfare	Jamming, deception, sensing disruption, and spectrum control
Special Systems	Class-specific shield or metahuman countermeasure architecture

All classes operate within finite ammunition, heat, power, and mission constraints. No production platform has unlimited firepower and no design assumption treats weapons expenditure as strategically free.

7.3 Sentry Defensive Armament

Sentry carries a medium rapid-fire kinetic defensive weapon, strong point defense, internal guided cells, and the strongest routine surveillance/electronic-warfare suite among production classes. Its role is to detect, track, disrupt, protect, and cue other forces rather than to behave as a miniature Legion.

7.4 Legion Heavy Combat Armament

Legion carries the greatest conventional offensive firepower of the production classes. Its defining weapon is the integrated Heavy Kinetic Cannon, supported by a medium multi-role weapon, direct anti-air capability, point defense, guided cells, and an industrial clamp/manipulator suitable for close-range mechanical force.

Braced Fire Posture transfers recoil through the chassis and terrain. Firepower is therefore inseparable from geometry, stance, cooling, and power allocation. Legion is not a giant infantryman carrying a rifle; its weapon system is part of the machine.

7.5 Bulwark Shield Architecture

Bulwark's primary weapon is protection. It operates a Mobile Field for tactical movement and an Anchored Strategic Field for maximum stabilized output. Anchoring, emitter geometry, ground lock, cooling, power management, and field synchronization are therefore combat systems in the same sense that a cannon is a combat system on Legion.

Field Contraction reduces protected area to increase local field concentration. Shield Burn represents an overload condition rather than a normal operating mode. Bulwark also carries strong point defense, local anti-air capability, and a medium defensive weapon because a shield platform that cannot protect itself during deployment is strategically fragile.

7.6 Warden Countermeasure Architecture

Warden is built around six countermeasure families rather than one universal nullification technology. Its permanent systems include the Resonance Disruption Array, Electronic Perception Spoofer, Adaptive Restraint System, baseline Adaptive Environmental Suppression Suite, and Localized Containment Barrier. Three configurable mission bays add selected packages before deployment.

Configurable choices include Thaumic Interference, Thermal Inversion, Kinetic Resonance, Spatial Interdiction, and Expanded Environmental Suppression. Only three of these are installed for a mission, producing a maximum of eight major systems. Expanded Environmental Suppression extends the permanent baseline AESS rather than duplicating it.

Countermeasure performance is classified as Hard Counter, Soft Counter, or Adaptive Counter. The absence of a universal power-nullification field is deliberate; Warden doctrine depends on preparation, assessment, sequencing, restraint, environmental control, and adaptation rather than a fictional one-switch solution to every metahuman threat.

7.7 Weapons Control and Mission Authority

Weapons remain bounded by the Mission Envelope. Targeting data may be shared through ISTM, but command traffic and tactical cueing do not transfer strategic authority. A receiving platform still evaluates the target against its own authenticated mission constraints.

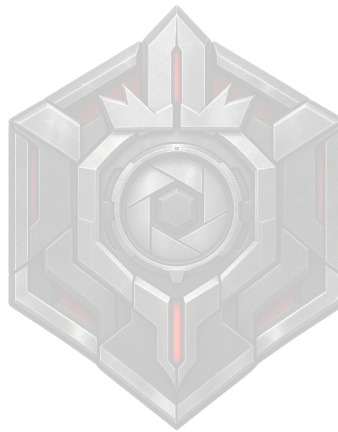
When data confidence falls from Verified to Trusted, Contested, or Rejected, the platform narrows aggressive action accordingly. The program treats uncertain information as a control problem, not as permission to act more freely.

7.8 Chapter Summary

Cybersentinel weapons and defenses are integrated mission systems. Sentry emphasizes sensing, EW, and defensive fire; Legion concentrates conventional offensive power; Bulwark treats shielding as its primary strategic effect; Warden combines precision conventional force with restraint and configurable countermeasures. Across all classes, ammunition, heat, power, data confidence, and human mission authority remain hard limits.

PART III

PRODUCTION CLASSES



CROWN SECURITY RESTRICTED

CHAPTER 8

CS-S4-01 SENTRY

Strategic Surveillance, Site Defense & Electronic Warfare

The CS-S4-01 Sentry is the Generation IV system responsible for seeing the battlefield first, maintaining local awareness, protecting strategic approaches, and coordinating defensive response. It is not designed to break fortified lines or replace heavy combat platforms. Its value lies in persistence, information quality, electronic warfare, and the ability to remain tactically useful when broader networks degrade.



Figure 8-1 — CS-S4-01 Sentry baseline identification image.

8.1 Mission and Role

Sentry is the routine eyes-and-ears class of the Cybersentinel force. It monitors strategic approaches, critical installations, airspace at local defensive scale, likely intrusion corridors, and unusual activity requiring escalation. Its primary battlefield contribution is reliable information married to a capable defensive weapons package.

A Sentry is normally employed before the heavier classes. It observes, classifies, tracks, and passes a validated picture to commanders and nearby forces. In mixed formations it frequently provides the first target-quality data used by Legion, Warden, conventional air-defense systems, or local commanders.

The class follows a Passive First / Active as Required philosophy. Emissions, radar-like activity, active electronic warfare, and weapons cueing are increased when the tactical situation justifies the additional signature. Routine operation therefore favors persistence and discrimination over spectacle.

8.2 Physical Configuration

Table 8-1 — Physical Configuration.

Characteristic	CS-S4-01
Height	~14 ft
Length	~19 ft
Width	~11 ft
Mass	~18 tons
Primary form	Low industrial quadruped
Road speed	~40 mph
Cross-country	~25–30 mph
Underwater	Up to ~150 ft
Tactical hover	~90 sec / ~40 mph
Phleboto complement	6 canisters / 600+ bots

The four-legged chassis keeps the sensor crown and weapons package low, stable, and difficult to overturn while allowing the machine to negotiate damaged roads, prepared defenses, shoreline approaches, and uneven ground. The design is intentionally industrial rather than animalistic: four articulated load-bearing limbs support a broad armored hull with a low sensor crown and no head.

Damage tolerance reflects the class mission. Loss of one leg may still permit the platform to brace, continue observation, or execute limited movement. Loss of two legs normally immobilizes the machine, but an immobilized Sentry may remain operational as a sensor, electronic-warfare, and defensive node.

8.3 Sensors, Electronic Warfare and Tactical Mesh

Sentry carries the strongest routine surveillance and electronic-warfare emphasis of the production classes. Near-360-degree sensing, passive detection, local air and drone surveillance, target classification, and directional electronic attack are integrated into the chassis.

Electronic warfare is selective rather than indiscriminate. Directional jamming and localized disruption are preferred where possible to preserve friendly communications and avoid creating unnecessary electromagnetic signatures. The machine can support ISTM coordination and may temporarily assume Tactical Coordination Node duties when the local mesh requires one; that role is functional and may be reassigned.

Network loss does not erase the mission. Under degraded conditions the Sentry continues local surveillance, preserves the Last Valid Mission Envelope, and shares what data it can through surviving links. The class is therefore designed to remain useful even when its wider information advantage has been reduced.

8.4 Weapons and Defense

The primary weapon is a medium rapid-fire kinetic defensive system intended to defeat infantry concentrations, light vehicles, drones, exposed sensors, and other threats that penetrate the surveillance perimeter. Strong point-defense systems and internal guided cells provide additional local defense.

The Sentry is not a breakthrough machine. It can defend itself and support a local fight, but prolonged direct assault against heavy armor or hardened positions should be handed to Legion or conventional

heavy forces. The class survives best by detecting the attack early, disrupting it, and creating time for the correct response.

8.5 Watch Configuration

Watch Configuration lowers the machine into a stabilized observation posture, improving sensor steadiness, reducing unnecessary movement, and emphasizing survivability and defensive control. This posture is particularly useful for strategic approaches, fixed-site defense, shoreline monitoring, and temporary overwatch positions.



Figure 8-2 — Sentry in Watch Configuration during strategic-site surveillance.

8.6 Operational Employment

Routine employment favors singleton or paired coverage rather than large concentrations. A Sentry may defend a site alone, support a Bulwark emplacement, cue a Legion element, or accompany a Warden response. Multiple Sentries can distribute surveillance across a sector without becoming dependent on a single node.

In the Wolfe Island defense system, Sentry is the outer detection layer. Its success is measured not by kills, but by how early and accurately it establishes the threat picture, how well it protects the decision cycle, and whether it enables stronger systems to arrive before the enemy reaches critical terrain.

COMMAND NOTE: Track before engage. The Sentry exists first to understand the threat, then to shape the response.



Figure 8-3 — CS-S4-01 Sentry technical profile.

8.7 Limitations

Sentry lacks Legion-level armor and offensive firepower, Bulwark-level shield strength, and Warden-specific countermeasure architecture. It is vulnerable if fixed in place against a determined heavy assault and can be overloaded by simultaneous surveillance, electronic-warfare, and close-defense demands.

The class is therefore most effective when commanders preserve its information advantage and avoid treating a surveillance platform as a substitute assault machine.

Sentry asks: “What is happening?”

CHAPTER 9

CS-L4-01 LEGION

Heavy Battlefield Combat & Breakthrough Platform

The CS-L4-01 Legion is the Generation IV class built to defeat conventional battlefield threats through concentrated direct fire, protected movement, and sustained heavy combat. Where Sentry establishes the tactical picture, Legion converts that picture into destructive battlefield effect.



Figure 9-1 — CS-L4-01 Legion baseline identification image.

9.1 Mission and Role

Legion is the program's principal conventional combat class. It is assigned where heavy armor, fortified resistance, hardened targets, or concentrated hostile forces require more than local defensive weapons. It supports Imperial Army maneuver rather than replacing it, and is most effective when infantry, reconnaissance, logistics, and air support exploit the effects it creates.

The class is deliberately straightforward by Cybersentinel standards. Its primary purpose is not elaborate electronic warfare or specialized metahuman containment. It carries the highest conventional offensive firepower of the production fleet and is designed to survive recoil, counterfire, and repeated movement through contested terrain.

9.2 Physical Configuration

Table 9-1 — Physical Configuration.

Characteristic	CS-L4-01
Height	~20 ft
Width	~10.5 ft
Mass	~38 tons
Primary form	Broad low-center-of-gravity biped
Road speed	~35 mph
Cross-country	~22–28 mph
Underwater	Up to ~250 ft
Tactical hover	Up to ~2 min / ~45 mph
Phleboto complement	8 canisters / 800+ bots

The Legion chassis uses a broad torso, short powerful legs, and a low center of gravity to control recoil and maintain stability under heavy weapons fire. It has no head and no human-style weapon carriage. The main gun is structurally integrated into the right-side arm architecture rather than being a rifle held by a humanoid machine.

Articulated legs allow the machine to cross damaged terrain and position its mass for firing. Tactical hover exists for obstacle negotiation and short repositioning, not aerial combat. Underwater capability supports shoreline operations and protected transit where depth permits.

9.3 Armament

The integrated Heavy Kinetic Cannon is the defining Legion weapon. It is supported by a medium multi-role secondary weapon, stronger direct anti-air capability than the other ground-combat classes, point defense, guided cells, and an industrial clamp/manipulator capable of close physical engagement when necessary.

Weapons are constrained by finite ammunition, heat, power, recoil, and mission priorities. The machine does not fire simply because a target is available. Target selection remains bounded by the Mission Envelope and by the tactical value of preserving ammunition for the threats only Legion can efficiently defeat.

9.4 Braced Fire Posture

Braced Fire Posture converts the machine's mass and stance into a stabilized heavy-weapon firing platform. The legs widen and load paths are set to absorb recoil while the machine reduces unnecessary movement. This posture maximizes heavy-weapon effectiveness against hardened or high-value targets but temporarily makes the machine less mobile and therefore more dependent on reconnaissance, point defense, and supporting forces.



Figure 9-2 — Legion in heavy direct-fire employment. Braced-fire doctrine emphasizes recoil stability and target-value discipline.

9.5 Power Allocation States

Table 9-2 — Power Allocation States.

State	Primary Effect
Standard	Balanced mobility, weapons, sensors, cooling and defense
Firepower	Additional generation and capacitor support to weapons and recoil systems
Mobility	Prioritizes movement, obstacle crossing and repositioning
Defense	Prioritizes active defense, cooling resilience and protected withdrawal

9.6 Tactical Employment

Legions normally fight dispersed enough to avoid presenting one concentrated target while remaining close enough for mutual support. The preferred rule is shoot-and-move: establish a firing position, deliver the required heavy effect, then reposition before enemy artillery, air attack, metahuman response, or precision weapons can exploit predictability.

Urban employment requires reconnaissance and conventional forces because the machine is not optimized for fine interior work. In dense terrain, Legion should dominate streets, strongpoints, access corridors, and major structures while Redcoats or human troops clear interiors and manage spaces too confined for the platform.

Sentry-to-Legion cueing is particularly important. A Legion should not expose itself to perform surveillance that a Sentry, drone, Army observer, or other sensor can accomplish more safely.

DOCTRINAL PRINCIPLE: Concentrate firepower at the point of tactical decision; do not concentrate machines merely for appearance.



Figure 9-3 — CS-L4-01 Legion technical profile.

9.7 Limitations

Legion has high conventional combat value but is not a surveillance specialist, mobile shield generator, or dedicated metahuman countermeasure system. Its size complicates confined urban terrain and increases transport burden. Heavy weapons also create ammunition, recoil, cooling, and signature demands that make careless prolonged firing unsustainable.

Its battlefield purpose is therefore precise: apply heavy force where heavy force changes the outcome, then preserve the machine for the next engagement.

Legion asks: “What needs to be defeated?”

CHAPTER 10

CS-B4-01 BULWARK

Mobile Strategic Shield-Defense Platform

The CS-B4-01 Bulwark is a mobile strategic-defense system built around one defining capability: taking a shield effect that would normally belong to fixed infrastructure and placing it where the Empire needs it. It is the heaviest standard Cybersentinel class and the strongest armored production platform, but its primary value is protection rather than assault.



Figure 10-1 — CS-B4-01 Bulwark in transport configuration at Ironreach. Operational artwork is used here; dimensional values are controlled by handbook text.

10.1 Physical Configuration

Table 10-1 — Physical Configuration.

Characteristic	CS-B4-01
Transport height	~12 ft
Length	~24 ft
Width	~14 ft
Deployed height	~32 ft
Mass	~62 tons
Mobility	Hybrid articulated tread / walking system
Underwater	Up to ~100 ft
Tactical lift	~20 sec / ~15 mph obstacle crossing only
Phleboto complement	12 canisters / 1,200+ bots

The transport configuration is a low rectangular mobile fortress. It has no head or arms and should not be understood as a conventional tank. The tread/walking system combines load-bearing efficiency with limited articulated movement for broken terrain, emplacement adjustment, and stabilization.

The Bulwark is not fast. Its design accepts that limitation because strategic shielding depends on mass, stability, anchoring, power, cooling, and emitter geometry. The platform must arrive before the critical phase of the battle, not chase the battle after it has moved elsewhere.

10.2 Eight-Stage Deployment

Transition from transport configuration to Anchored Strategic Field is a deliberate engineering sequence. Normal deployment requires approximately 60–90 seconds; emergency deployment may be compressed to roughly 35–45 seconds at greater mechanical and thermal stress. The period before full field establishment is the platform's most tactically vulnerable interval.

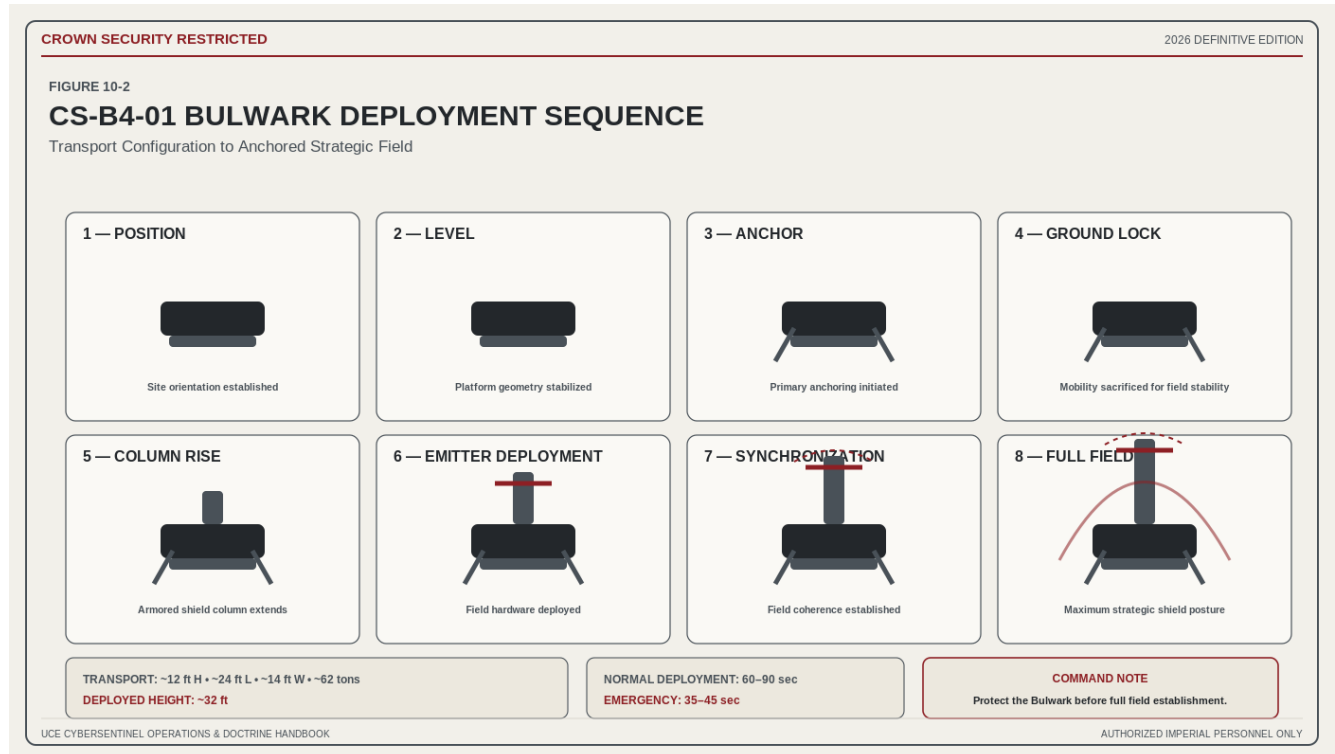


Figure 10-2 — Bulwark eight-stage deployment sequence. Final publication geometry will be source-derived from the approved chassis.

10.3 Shield Modes

The Mobile Field provides reduced shield strength while allowing the platform to continue moving. It is useful for protected transit, temporary coverage, repositioning, and situations where remaining fixed would be more dangerous than accepting lower field performance.

The Anchored Strategic Field is the maximum-strength posture. Once positioned, leveled, anchored, ground-locked, raised, deployed, and synchronized, the Bulwark converts itself into a strategic shield node capable of protecting critical terrain, installations, troop concentrations, or damaged fixed-defense sectors.

Field Contraction trades protected area for local strength. Commanders can deliberately shrink the field when one location must be protected against a stronger attack. This is not free additional power; it is a redistribution of the same defensive capacity.

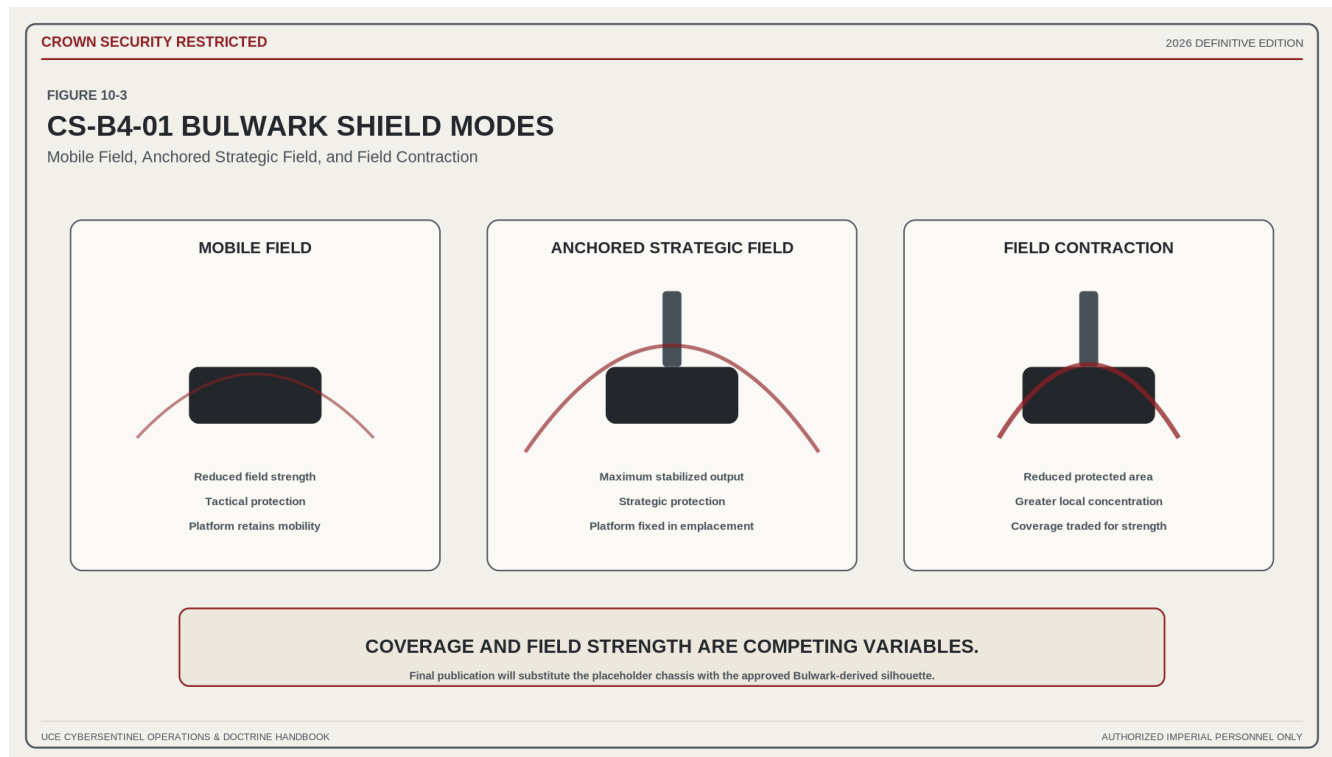


Figure 10-3 — Bulwark shield modes: Mobile Field, Anchored Strategic Field, and Field Contraction.

10.4 Substitution Mode and Fixed Defense Integration

A Bulwark can synchronize with compatible fixed shield infrastructure in Substitution Mode. The purpose is not to make the machine a permanent replacement for strategic facilities, but to restore continuity when a fixed node has been destroyed, taken offline, overloaded, or isolated from the larger defensive network.

This capability makes Bulwark particularly valuable during attacks on prepared Imperial territory. An enemy may destroy the expected shield node and still face a mobile replacement that changes the geometry of the defense.

10.5 Defensive Armament and Shield Burn

Bulwark carries strong point defense and local anti-air systems as well as a medium defensive weapon. These systems protect the platform and its shield geometry; they are not intended to convert the class into a heavy-assault substitute for Legion.

When incoming energy or kinetic demand exceeds normal field management, the platform may enter Shield Burn: an overload state in which emitters, power systems, and cooling are driven beyond preferred sustained limits to preserve protection for a critical interval. Shield Burn is an emergency measure that accelerates wear and may force later field reduction, withdrawal, or deep maintenance.

10.6 Operational Employment

Bulwark doctrine is summarized by Position Before Power. The correct location matters as much as raw field strength. Terrain, line of protection, friendly movement, likely enemy approach, recovery access, and the time required to establish the field must be solved before the machine commits to anchoring.

Protected deployment is therefore standard. Sentry, Army, Redcoat, Legion, air-defense, or other forces should screen the machine while it anchors. Bulwark Rotation may be used in prolonged defense so one platform can reduce field stress or enter service while another assumes the shield mission.

Foreign doctrine is expected to focus on killing or disrupting the Bulwark before it anchors. Imperial commanders should plan accordingly.



Figure 10-4 — Anchored Bulwark shield employment. The field is a protected-area effect, not a permanent invulnerability bubble.

COMMAND NOTE: Protect the Bulwark before full field establishment. A shield platform destroyed during deployment protects nothing.

10.7 Limitations

Bulwark is slow, heavy, logistically demanding, and most effective when deliberately emplaced. It is not a frontline pursuit platform and should not be treated as an assault tank. Shield performance is finite and is constrained by power, cooling, emitter condition, field geometry, and duration.

The class is strategically valuable because it makes defensive geography less predictable. Its scarcity also means commanders must avoid consuming that value on missions that ordinary fortification, air defense, or conventional maneuver can solve.

Bulwark asks: “What must be protected?”

CHAPTER 11

CS-W4-01 WARDEN

Metahuman Interdiction, Suppression & Containment Platform

The CS-W4-01 Warden is the rarest standard production class and the most specialized. It exists for contingencies in which an extraordinary powered opponent, unusual capability, or unstable metahuman crisis presents a threat that conventional heavy firepower cannot address safely or efficiently. A Warden does not patrol. A Warden is released.



Figure 11-1 — CS-W4-01 Warden baseline identification image.

11.1 Mission and Role

Warden doctrine begins with identification. The machine must determine what kind of threat it is facing, which capabilities are confirmed, which are plausible, which remain unknown, and which countermeasure family offers the best chance of ending the threat without creating a larger crisis.

The class is therefore sensor-dense, information-hungry, and more dependent on target knowledge than Legion. It is most effective against known or sufficiently characterized threats. Unexpected responders remain genuine X-factors, and multi-metahuman encounters can overload the machine's ability to maintain the correct countermeasure sequence.

11.2 Physical Configuration

Table 11-1 — Physical Configuration.

Characteristic	CS-W4-01
Height	~21 ft
Width	~9.5 ft
Mass	~34 tons
Primary form	Tall, narrow, sensor-dense biped
Road speed	~42 mph
Cross-country	~28–32 mph

Underwater	Up to ~250 ft
Tactical hover	Up to ~2 min / ~45 mph
Phleboto complement	10 canisters / 1,000+ bots

Warden is slightly taller, narrower, lighter, and more agile than Legion. Its proportions reflect sensor density, precision movement, countermeasure hardware, and restraint requirements rather than maximum conventional armor and recoil absorption.

The machine has no head. Sensor packages are distributed across the upper chassis so the loss of one aperture does not blind the platform. Its articulated manipulators are designed for restraint and Containment Grip Mode rather than industrial lifting alone.

11.3 Permanent and Configurable Countermeasure Architecture

Every Warden carries five permanent major systems and three configurable mission bays. Only three optional packages are installed for a given deployment, creating a maximum of eight major countermeasure systems. Mission preparation therefore matters: the machine cannot carry every specialized package simultaneously.

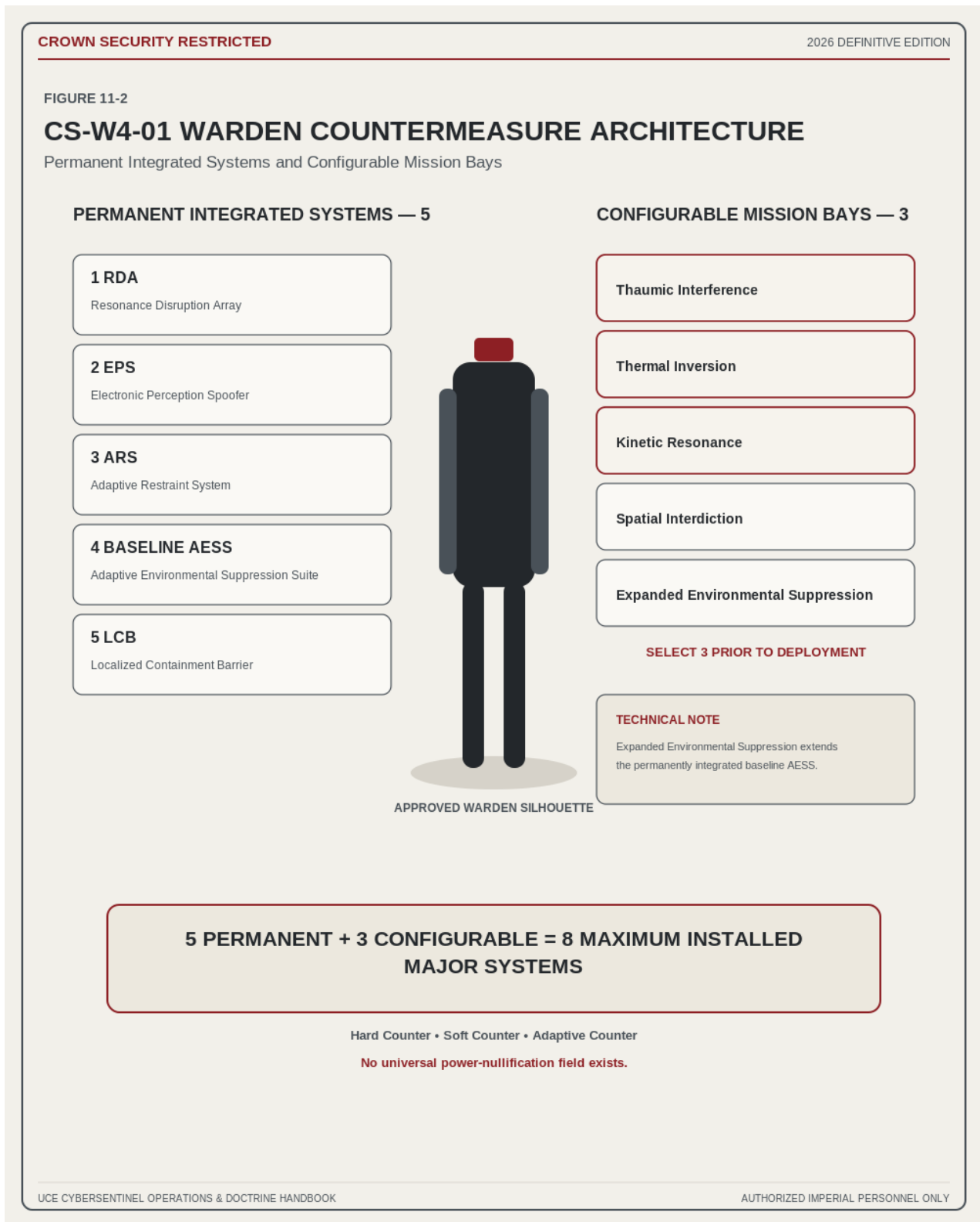


Figure 11-2 — Warden 5+3 countermeasure architecture. Final publication silhouette will be derived from the approved Warden source image.

Table 11-2 — Permanent and Configurable Countermeasure Architecture.

Type	System / Package	Function
------	------------------	----------

Permanent	RDA — Resonance Disruption Array	Disrupt applicable resonance-dependent capabilities
Permanent	EPS — Electronic Perception Spoofers	Degrade or manipulate electronic/perceptual targeting pathways
Permanent	ARS — Adaptive Restraint System	Physical and adaptive containment architecture
Permanent	Baseline AESS	Permanent environmental-control capability
Permanent	LCB — Localized Containment Barrier	Short-range containment and movement restriction
Configurable	Thaumic Interference	Specialized anti-thaumic package
Configurable	Thermal Inversion	Specialized thermal countermeasure
Configurable	Kinetic Resonance	Specialized kinetic-response package
Configurable	Spatial Interdiction	Specialized spatial-control package
Configurable	Expanded Environmental Suppression	Extension of baseline AESS capability

TECHNICAL NOTE: Expanded Environmental Suppression is a configurable mission-bay extension of the permanently integrated baseline AESS. It is not a sixth permanent system.

11.4 Countermeasure Performance

Table 11-3 — Countermeasure Performance.

Category	Meaning
Hard Counter	Directly disrupts a known capability or removes the condition required for it to function.
Soft Counter	Reduces effectiveness, accuracy, endurance, control, or freedom of action without fully shutting the capability down.
Adaptive Counter	Adjusts countermeasure timing or combination as new target behavior becomes known during the engagement.

There is no universal power-nullification field. Warden effectiveness comes from preparation, specialization, sequencing, containment geometry, environmental manipulation, electronic deception, and target-specific countermeasures—not a single device that simply turns powers off.

11.5 Target Assessment and Priority Response List

The Priority Response List organizes likely opposition into Tier I EXPECTED, Tier II PLAUSIBLE, and Tier III WATCH categories. The list can include local, regional, and long-range responders where intelligence indicates their intervention is likely, including GUARD or Terraguardian assets when operational circumstances make them relevant.

Unexpected responders are recorded as UNPLANNED META CONTACT. That label matters because the Warden's greatest advantage is preparation. An unplanned contact may force Adaptive Assessment and a rapid reassessment of whether the installed mission packages remain appropriate.

11.6 Escalation and Containment Doctrine

Warden escalation normally proceeds from disruption to suppression, immobilization, containment, and only then severe force where necessary. The machine is built to end the relevant threat, not to maximize lethality. Precision conventional weapons support the countermeasure suite, while restraint launchers, articulated manipulators, ARS, LCB, and environmental systems create opportunities for capture or controlled disengagement.

Containment Stance prioritizes field geometry, restraint options, sensor control, and defensive stability over pursuit speed. Containment Grip Mode allows the machine to use its manipulators as a controlled restraint system rather than an indiscriminate crushing weapon.

Containment Funnel Logic attempts to shape the opponent's available movement so the target is gradually forced toward an area where the installed countermeasures, restraint systems, conventional forces, or Enforcer support have the best probability of success.



Figure 11-3 — Warden containment operation. The class is optimized for controlled interdiction rather than routine battlefield patrol.

11.7 Multi-Metahuman Complexity and Package Degradation

One Warden is normal for a defined metahuman contingency. Pairs are authorized when threat complexity, uncertainty, or responder probability justifies them. Three or more Wardens in one crisis is exceptional because the class is scarce and because national package coordination becomes increasingly important as multiple specialized systems operate near one another.

PACKAGE DEGRADATION describes the loss of confidence or effectiveness in one or more installed countermeasures as target behavior changes, new powers appear, environmental conditions shift, or systems are damaged. A Warden must recognize degradation early enough to change tactics rather than continue executing a countermeasure that no longer controls the threat.

The greatest structural limitation remains saturation. Multiple powered opponents with dissimilar capabilities can force the machine to divide sensors, power, movement, and countermeasure timing faster than one chassis can optimize them.



Figure 11-4 — CS-W4-01 Warden technical profile.

11.8 Pursuit Limits and Combined Response

Warden is not authorized to chase indefinitely simply because a target remains active. Pursuit must remain consistent with the Mission Envelope, containment objective, protected population, terrain, support, and the risk of drawing the machine away from the crisis it was deployed to control.

Imperial commanders should use the Warden with Sentry intelligence, conventional containment forces, Army maneuver, Redcoat security, air support, and Enforcers where available. Unexpected responders and unfamiliar abilities must be treated as genuine uncertainty rather than assumed to fall inside an existing package.

Warden asks: “Which metahuman must be neutralized?”

CHAPTER 12

PROTOTYPE SYSTEMS

Experimental Strategic Systems and Technology Validation

Prototype is not a fifth production class. CS-X4-## is the designation framework for tightly controlled experimental systems whose missions, architectures, or technologies fall outside the mature Sentry, Legion, Bulwark, and Warden families. The Prototype category exists to test whether a new strategic capability can work—not to populate the fleet with undefined super-machines.

RESTRICTED NOTE: Specific Generation IV Prototype identities, configurations, and project details remain compartmentalized. This chapter defines program policy, not undisclosed chassis.

12.1 Designation and Program Boundary

Generation IV experimental systems use the CS-X4-## designation family. A project normally produces one system and rarely more than two per concept. If a technology matures into a repeatable, sustainable mission architecture, it may be adopted into a production class, partially adopted as a subsystem, or used to define a later production model.

True hybrids remain Prototype. If a machine combines major class missions so thoroughly that no production-class doctrine controls it, the correct answer is not to invent a new standard silhouette casually. The system remains experimental until the Empire determines whether that combination is strategically valuable and supportable.

12.2 Prototype Categories

Table 12-1 — Prototype Categories.

Category	Scope
Combat	Experimental weapons, target effects, fire-control or unconventional battlefield architecture
Defense	Advanced protection, shielding, survivability or strategic denial systems
Mobility	Nonstandard movement, extreme maneuver, transport or access concepts
Cognition	Restricted Synthetic Cognition and other experimental decision architectures
Special Systems	Novel sensors, energy, containment, communications or mission technologies
Extreme Environmental	Operations beyond normal production limits, including deep-water, space/lunar, magma or comparable environments

12.3 Restricted Synthetic Cognition

Restricted Synthetic Cognition is Prototype-only. Production Sentry, Legion, Bulwark, and Warden systems use tactical machine intelligence that is purpose-built, bounded, non-sentient, and prohibited from copying or migrating itself.

A cognition experiment does not automatically receive operational authority because it demonstrates more flexible reasoning. Strategic authority remains human. Any synthetic-cognition research is judged by whether it improves mission performance without eroding authentication, predictability, recoverability, auditability, or human control.

12.4 Production-Limit Exceptions

A Prototype may exceed production-class limits when the experiment requires it. Extreme Environmental systems may operate at depths beyond 1,000 ft or test space, lunar, high-temperature, or otherwise inaccessible environments. Combat or Defense projects may carry experimental systems too power-intensive, heavy, or specialized for standard production.

These exceptions do not rewrite production doctrine. Prototype capability is not evidence that ordinary Cybersentinels possess the same performance. Every exceptional characteristic must remain tied to the specific experimental project that demonstrates it.

12.5 Visual and Information-Control Policy

Prototype visual treatment is divided into Existence-Only, Story-Relevant, and Visual-Canon levels. Existence-Only confirms that a project exists without defining its appearance. Story-Relevant material may reveal selected details required by an operational narrative. Visual-Canon status is granted only when a specific project requires a controlling exterior design.

There is deliberately no generic Prototype silhouette, no four-Prototype lineup, and no Prototype infographic in this handbook. Inventing one would imply a standardized chassis that does not exist and would prematurely define projects that are intentionally compartmentalized.

12.6 Disposition and Technology Transfer

Table 12-2 — Disposition and Technology Transfer.

Disposition	Meaning
Adopted	Technology successfully enters a production class or future standard system.
Partially Adopted	Selected subsystems or software concepts are retained; the complete project is not.
Archived	Project preserved for possible later use or reference.
Dismantled	System deliberately disassembled after evaluation.
Destroyed	Prototype lost through test, accident, combat or authorized denial.
Sealed	Project retained under compartmented restriction with no ordinary program access.

12.7 Operational Accounting

Four Prototype systems are included in the 2026 authorized Cybersentinel inventory, but they represent multiple separate projects rather than one standardized four-unit class. They are excluded from ordinary strategic-reserve calculations unless a specific project has separately been authorized for an operational contingency role.

Prototype systems therefore should not be used to inflate Available Combat Strength on paper. A machine that exists but is in test configuration, sealed, dismantled for instrumentation, or unsuitable for the current mission is not equivalent to an R1 production platform.

12.8 Security, Recovery and Denial

Prototype recovery receives elevated attention because a single machine may contain technology not yet distributed across the fleet. At the same time, denial remains staged and proportional. The presence of experimental technology does not create a blanket license for catastrophic self-destruction.

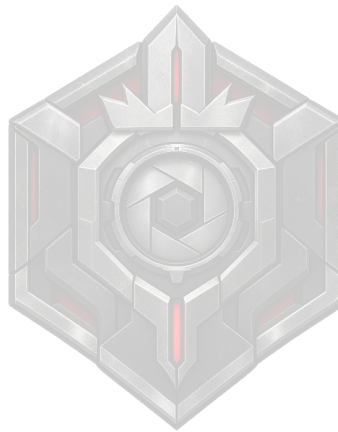
Where possible, the Empire recovers the chassis, removes sensitive modules, preserves logs and instrumentation, and separates exploitable technology from forensic evidence. Only the lowest sufficient denial level should be used, subject to the specific project's compartmented procedures.

12.9 Chapter Summary

Prototype asks: "Can this new technology work?" The category is deliberately small, compartmented, and fluid. Its purpose is to test possibilities, feed successful technology into mature systems, and terminate ideas that do not justify the cost, risk, or complexity of becoming part of the operational force.

PART IV

COMMAND & ORGANIZATION



CROWN SECURITY RESTRICTED

CHAPTER 13

COMMAND, CONTROL & TACTICAL AI

Human Strategic Authority, Bounded Tactical Autonomy

Cybersentinels are tactically autonomous strategic weapons platforms operating under human strategic authority. Their command architecture is designed to preserve useful battlefield action when communications degrade without allowing a machine to become an independent national commander. Authority therefore flows through authenticated human command, a bounded Mission Envelope, and decentralized tactical execution.

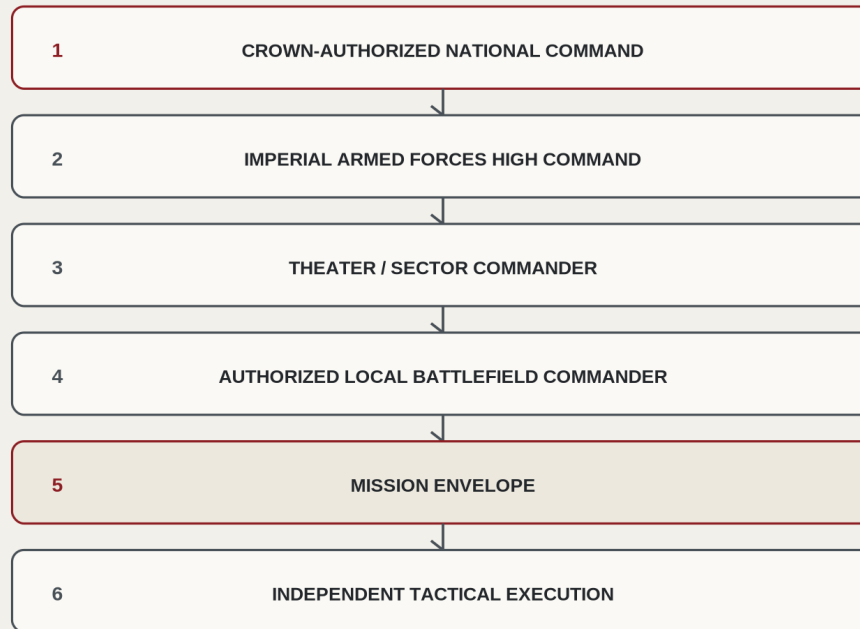
CROWN SECURITY RESTRICTED

2026 DEFINITIVE EDITION

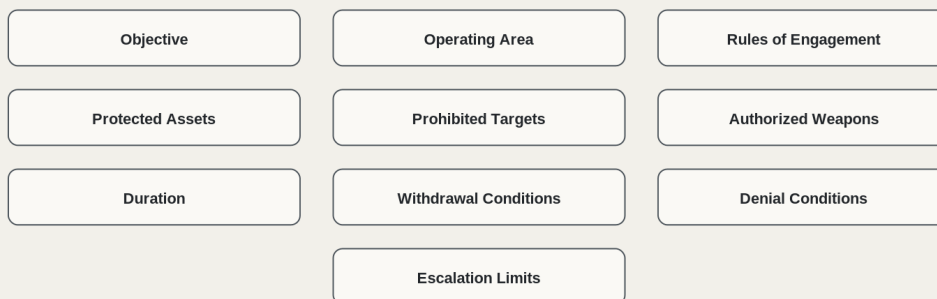
FIGURE 13-1

COMMAND PRIORITY & MISSION ENVELOPE

Human Strategic Authority, Bounded Tactical Autonomy



MISSION ENVELOPE CONTAINS



DOCTRINAL PRINCIPLE

HUMAN AUTHORITY DEFINES THE MISSION. TACTICAL AI EXECUTES WITHIN IT.

UCE CYBERSENTINEL OPERATIONS & DOCTRINE HANDBOOK

AUTHORIZED IMPERIAL PERSONNEL ONLY

Figure 13-1 — Command priority and Mission Envelope architecture.

13.1 Command Priority

Table 13-1 — Command Priority.

Priority	Authority	Function
1	Crown-authorized national command	Highest strategic authority
2	Imperial Armed Forces high command	National military direction
3	Theater / sector commander	Operational objectives and boundaries
4	Authorized local battlefield commander	Immediate tactical tasking
5	Mission Envelope	Validated operating boundaries
6	Independent tactical execution	Platform-level action within the envelope

The priority order does not imply that every tactical action requires a live command from the top of the hierarchy. Higher authority defines objectives, constraints, protected interests, and escalation limits; the Cybersentinel then executes locally within those boundaries.

Authentication is layered. Rotating keys, challenge-response checks, command provenance, and local security logic reduce the value of capturing any single code or transmission. There is no universal master code that grants unrestricted control over the fleet.

13.2 The Mission Envelope

The Mission Envelope is the machine's controlling operational contract. It specifies the objective, authorized area, rules of engagement, protected assets, prohibited targets, available weapons, expected duration, retreat conditions, denial restrictions, and escalation authority. A Cybersentinel may improvise tactically, but it may not invent a new strategic purpose for itself.

When command links are lost, the last valid Mission Envelope becomes the principal boundary for continued action. This prevents communications failure from creating either instant paralysis or unrestricted autonomy.

13.3 Operating Modes

Table 13-2 — Operating Modes.

Mode	Description
Integrated	Normal authenticated command and ISTM connectivity.
Local Tactical Autonomy	Command intent remains valid; the platform executes locally with reduced external coordination.
Degraded Mission	Communications, sensors, mobility, or supporting systems are impaired; mission scope narrows to what can still be performed safely.
Preservation-Denial	Mission success is no longer realistic; priority shifts to personnel/asset protection, recovery, data protection, and staged denial where authorized.

13.4 YELLOW COMMAND and BLACK Security

YELLOW COMMAND is invoked when a command is properly authenticated but appears anomalous, inconsistent with current mission conditions, or sufficiently unusual to justify secondary verification. The platform does not automatically treat the order as hostile. It preserves the current valid mission boundaries, requests additional verification, and avoids unnecessary irreversible action while confidence is rebuilt.

BLACK is a security state rather than a physical-damage state. It indicates that command, data, cryptographic, or system integrity is compromised or cannot be trusted. The required response is isolation, preservation of trusted local control, protection of sensitive information, and proportionate recovery or denial action. BLACK is distinct from GREEN, AMBER, and RED physical-condition states.

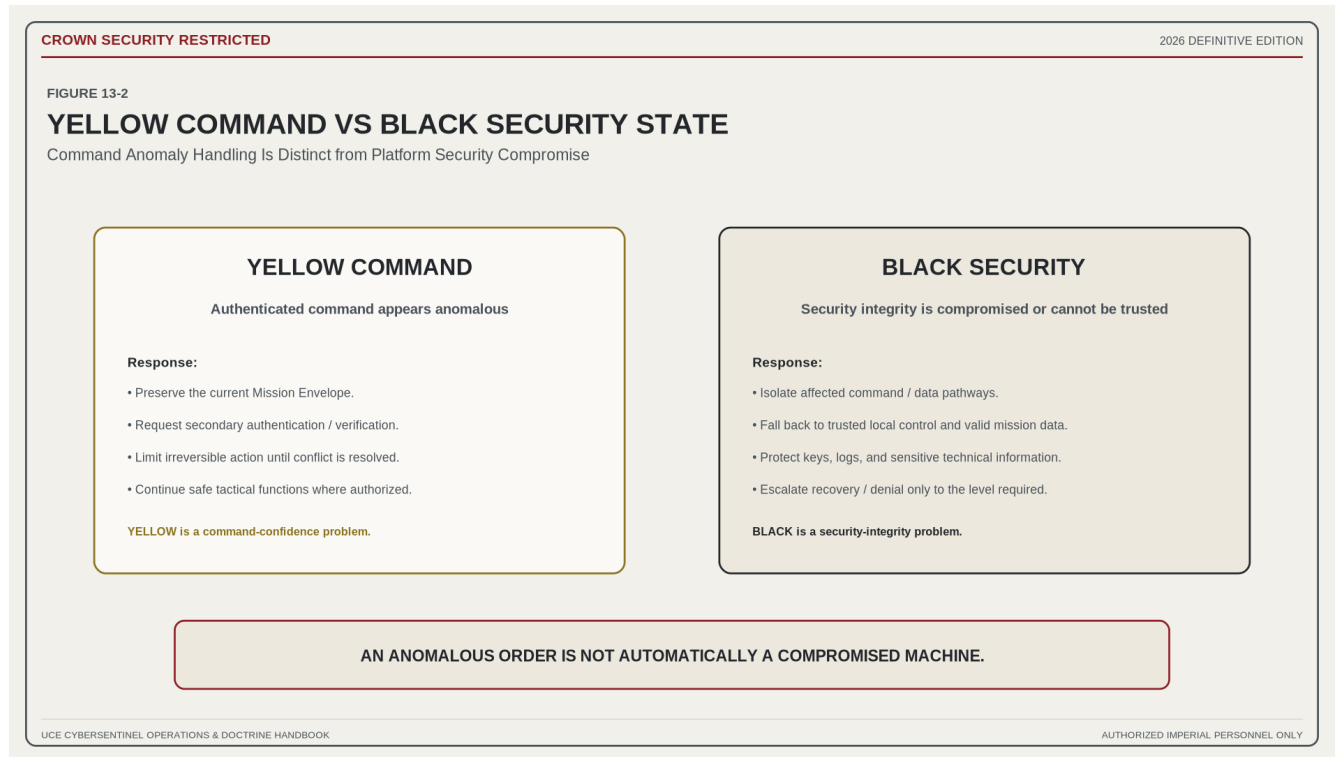


Figure 13-2 — YELLOW COMMAND vs BLACK security-state distinction.

COMMAND NOTE: An authenticated order can be suspicious without the machine itself being compromised. Command confidence and system security are evaluated separately.

13.5 Tactical Intelligence Limits

Generation IV tactical intelligence is deliberately powerful in perception, movement, target selection, self-preservation, formation behavior, and local problem solving. It is deliberately limited in strategic self-direction. Production systems do not develop independent political objectives, select national campaigns, or redefine protected and prohibited interests.

Production AI cannot copy or migrate itself to another chassis. Software updates, mission data, and tactical learning products may be distributed through authorized maintenance and command processes, but the operational identity of a production machine is bound to its controlled system architecture.

The machines are not designed with humanlike personalities. Familiarity, predictable behavior, and clear interaction conventions may exist for crews and commanders, but these are operational interfaces rather than simulated personhood.

Human authority defines the mission. Machine autonomy solves the local problem.

CHAPTER 14

IMPERIAL SENTINEL TACTICAL MESH

Decentralized Tactical Networking Without a Master Node

The Imperial Sentinel Tactical Mesh (ISTM) is the Generation IV networking architecture that allows Cybersentinels to share sensor data, status, targeting information, local command context, and tactical intent without making the force dependent on one central brain. The mesh coordinates the force; it does not define the force.

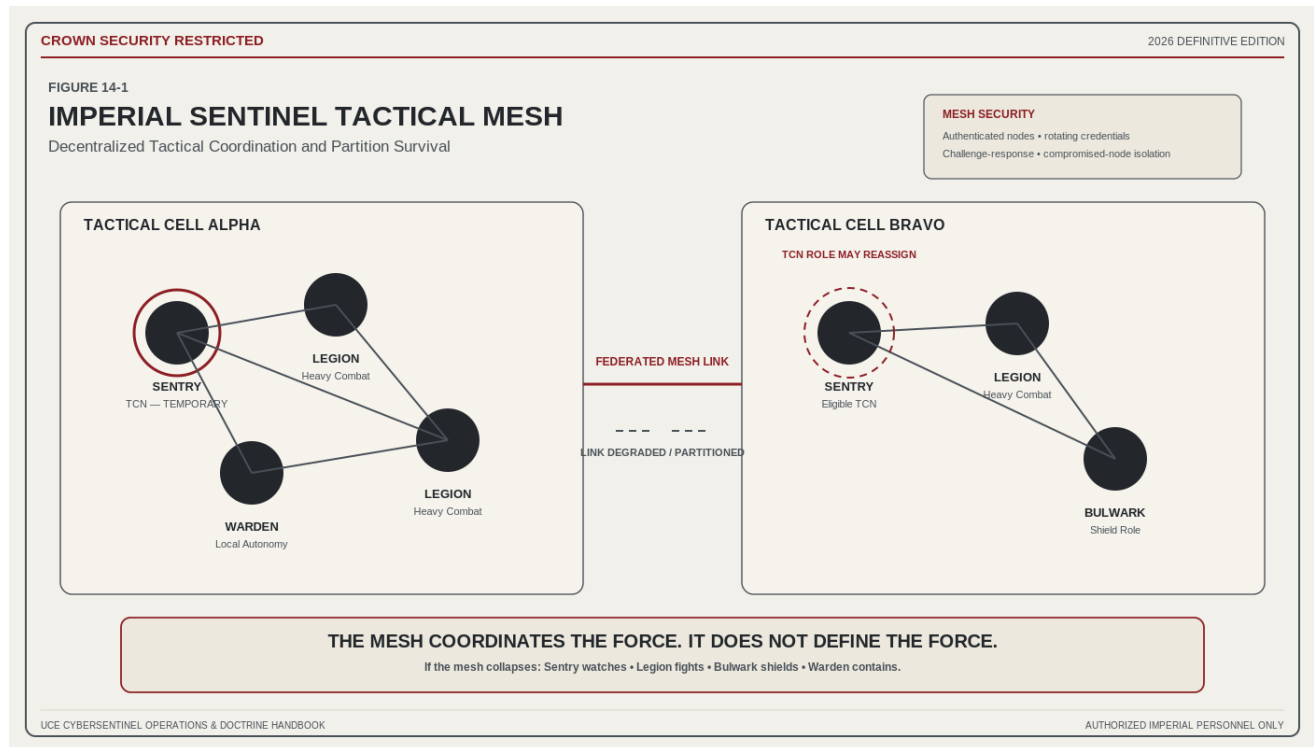


Figure 14-1 — Imperial Sentinel Tactical Mesh operational topology. Final publication nodes will use source-derived class silhouettes.

14.1 Federated Mesh Architecture

ISTM is federated rather than hierarchical at the tactical-survival level. Platforms form local cells, exchange information with neighboring cells when links permit, and can create a temporary Tactical Coordination Node (TCN) for specific operations. A TCN improves synchronization but is not a command brain and is not required for every machine to remain tactically functional.

If one node, relay, or cell is destroyed, surviving machines retain their own Mission Envelopes, local sensor pictures, and tactical-control functions. The network may become less informed and less efficient, but it does not collapse merely because one coordinating node disappears.

14.2 Shared Data

Table 14-1 — Shared Data.

Data Family	Purpose
Sensor tracks	Position, classification, confidence and movement of relevant contacts.
Threat data	Weapons, emissions, probable capability and observed behavior.
Friendly status	Location, mission state, damage, ammunition/power constraints and assistance requests.
Target handoff	Validated track transfer to the class or force best suited to create the required effect.
Mission context	Current boundaries, protected assets, exclusion zones and authenticated updates.

14.3 Local Valid Mission Envelope

Each production system retains its Last Valid Mission Envelope locally. Loss of the mesh therefore removes information and coordination before it removes authority to perform already-approved tactical actions. The platform can continue to watch, fight, shield, or contain as appropriate to class and mission while seeking restored communications.

When a partitioned group retains local connectivity, the surviving machines form a smaller federated cell. Information is reconciled when trusted links return. Conflicting stale data is not simply merged; timestamps, authentication, sensor confidence, and command validity are considered before shared state is updated.

14.4 Tactical Cells and Temporary Coordination

Tactical cells normally contain two to six systems when a mission benefits from close machine-to-machine coordination. Cell composition is mission-driven rather than class-pure. A Sentry may provide the principal sensor picture, Legions may execute heavy engagement, a Bulwark may anchor protection, and a Warden may remain on a separate metahuman task until handoff is required.

Temporary coordination functions can be created, transferred, or dissolved as the network changes. This is one of the direct Generation IV corrections to the early program's vulnerability to centralized control.

DOCTRINAL PRINCIPLE: The mesh coordinates the force. It does not define the force.

14.5 Degraded-Mesh Behavior

Table 14-2 — Degraded-Mesh Behavior.

Network Condition	Expected Behavior
Full mesh	Broad sensor and status sharing; efficient target handoff.
Reduced bandwidth	Priority tracks and command traffic retained; lower-value data delayed or dropped.
Partitioned mesh	Local cells continue; cross-cell awareness becomes incomplete.
Isolated platform	Local Tactical Autonomy under the Last Valid Mission Envelope.
Security-compromised path	Untrusted link isolated; trusted local information preserved.

Information loss reduces certainty and coordination. It does not automatically convert a Cybersentinel into a disabled platform.

CHAPTER 15

ORGANIZATION, INVENTORY & READINESS

Authorized Fleet, Available Combat Strength & Readiness

The 2026 Cybersentinel force is a deliberately limited strategic fleet. Its strength is measured not only by how many chassis exist, but by how many are present, serviceable, mission-configured, supplied, and available for the specific operation under consideration. This chapter therefore distinguishes Authorized Fleet, Inventory Present, and Available Combat Strength (ACS).

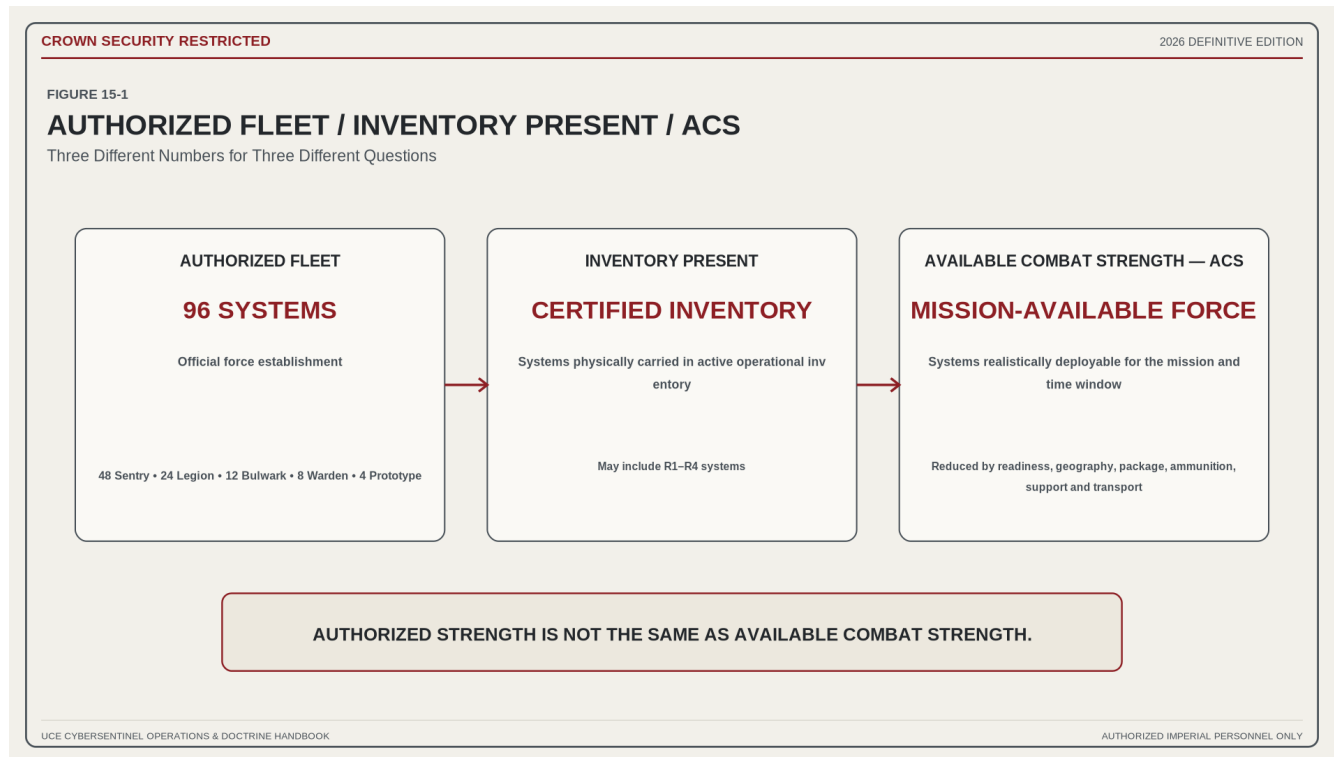


Figure 15-1 — Authorized Fleet, Inventory Present, and Available Combat Strength.

15.1 2026 Authorized Inventory

Table 15-1 — 2026 Authorized Inventory.

Class	Authorized Systems
Sentry	48
Legion	24
Bulwark	12
Warden	8
Prototype	4
TOTAL	96

Ninety-six systems is the controlling 2026 authorization. The earlier concept of a force approaching 400 systems is not a hidden current fleet and is not an active procurement baseline; it survives only as Emperor North's private long-term aspiration for a much larger future strategic force.

Replacement-before-expansion remains the normal production policy. New production first restores losses toward the authorized establishment unless the Crown explicitly approves a larger fleet.

15.2 Authorized Fleet, Inventory Present and ACS

Table 15-2 — Authorized Fleet, Inventory Present and ACS.

Measure	Meaning
Authorized Fleet	The approved force ceiling by class.
Inventory Present	Physical systems currently held by the program, regardless of readiness.
Available Combat Strength (ACS)	Systems that can reasonably be committed to the specified mission within the required time, considering maintenance, configuration, geography, logistics, and competing commitments.

ACS is always contextual. A machine may be operational but unavailable to one theater because it is committed elsewhere, undergoing mission-specific configuration, protecting a strategic site, or too distant to arrive in time. For that reason, ACS should not be reduced to a single permanent national number.

15.3 Readiness States

Table 15-3 — Readiness States.

State	Definition
R1 — Immediate Ready	Prepared for rapid tasking with mission systems available and no significant maintenance constraint.
R2 — Mission Ready	Combat-capable but may require routine preparation, loading, configuration, or movement before deployment.
R3 — Maintenance Ready	Not immediately deployable; recoverable through scheduled field/depot maintenance.
R4 — Deep Service	Major overhaul, rebuild, structural work, or Ironreach-level intervention required.

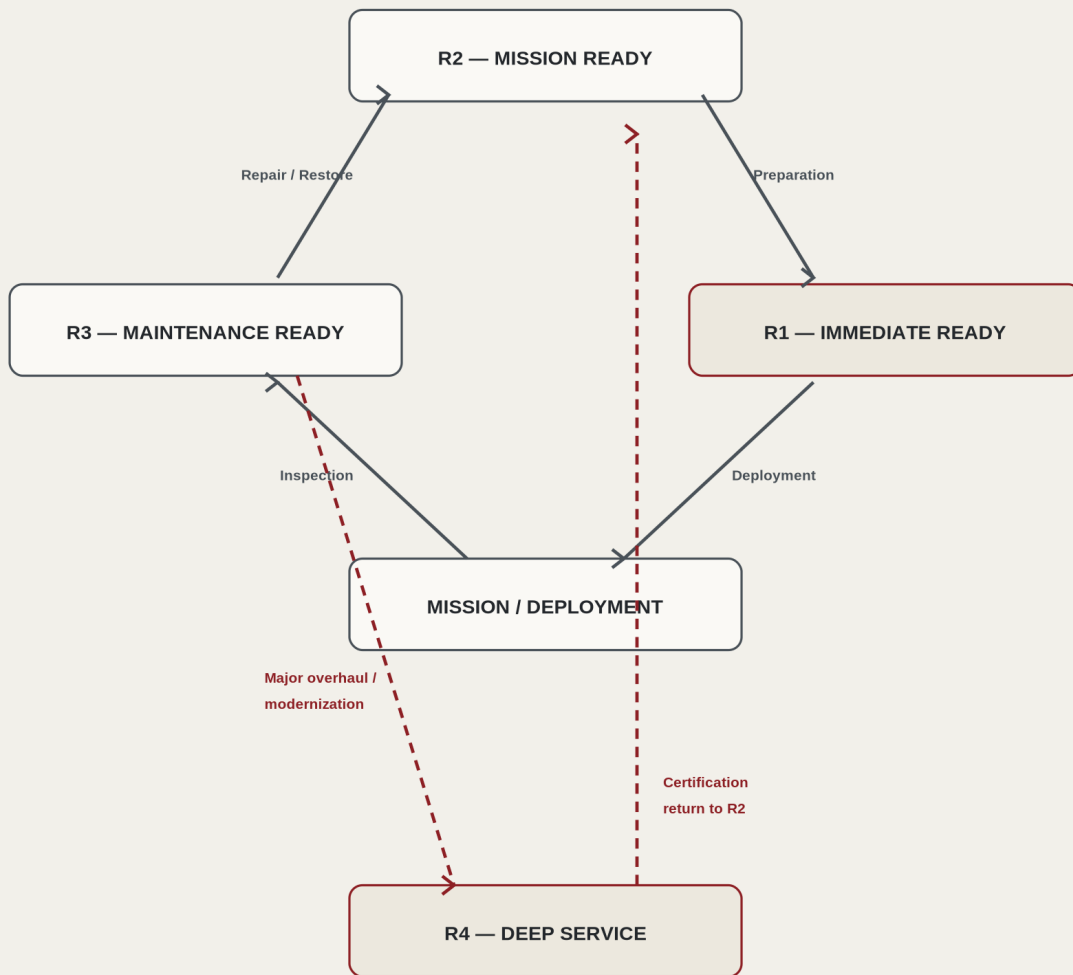
CROWN SECURITY RESTRICTED

2026 DEFINITIVE EDITION

FIGURE 15-2

CYBERSENTINEL READINESS CYCLE

Dynamic Readiness States and Deep-Service Branch



TECHNICAL NOTE

R4 is a deep-service branch, not a mandatory step after every mission.

UCE CYBERSENTINEL OPERATIONS & DOCTRINE HANDBOOK

AUTHORIZED IMPERIAL PERSONNEL ONLY

Figure 15-2 — Cybersentinel readiness cycle.

15.4 Operational Groupings

Table 15-4 — Operational Groupings.

Grouping	Systems	Typical Use
Singleton	1	Routine patrol, specialist task, local strategic presence
Element	2–3	Mutual support / significant response
Detachment	4–6	Major battle or major local crisis
Heavy Detachment	7–12	National crisis / concentrated strategic action
Sentinel Group	13+	Major campaign or exceptional national-level commitment

15.5 Concentration and Strategic Reserve

Routine doctrine favors distribution. One system is a normal strategic presence; two to three is significant; four to six indicates a major engagement; seven to twelve represents a national crisis. Concentrations above twelve are exceptional and normally require campaign-level justification.

Where practical, roughly fifteen to twenty percent of combat-capable strength is kept from immediate commitment as strategic reserve, recovery coverage, maintenance margin, or response capacity. This is a planning principle rather than a mathematically fixed quota.

No doctrine assumes all ninety-six systems should be concentrated into one battle. The fleet exists to defend a nation, preserve multiple critical sectors, recover from losses, and retain options after the first engagement.

DOCTRINAL PRINCIPLE: Disperse strategically. Concentrate tactically. Preserve recovery and reserve capacity.

CHAPTER 16

MANUFACTURING, SUSTAINMENT & LIFECYCLE

Ironreach Production, Maintenance & Replacement Doctrine

Cybersentinels are strategic machines, not disposable munitions. Their industrial system is therefore built around controlled manufacture, extensive subsystem testing, recoverability, modular replacement, and long service lives. Ironreach is the principal center for design, fabrication, integration, deep maintenance, and rebuild.

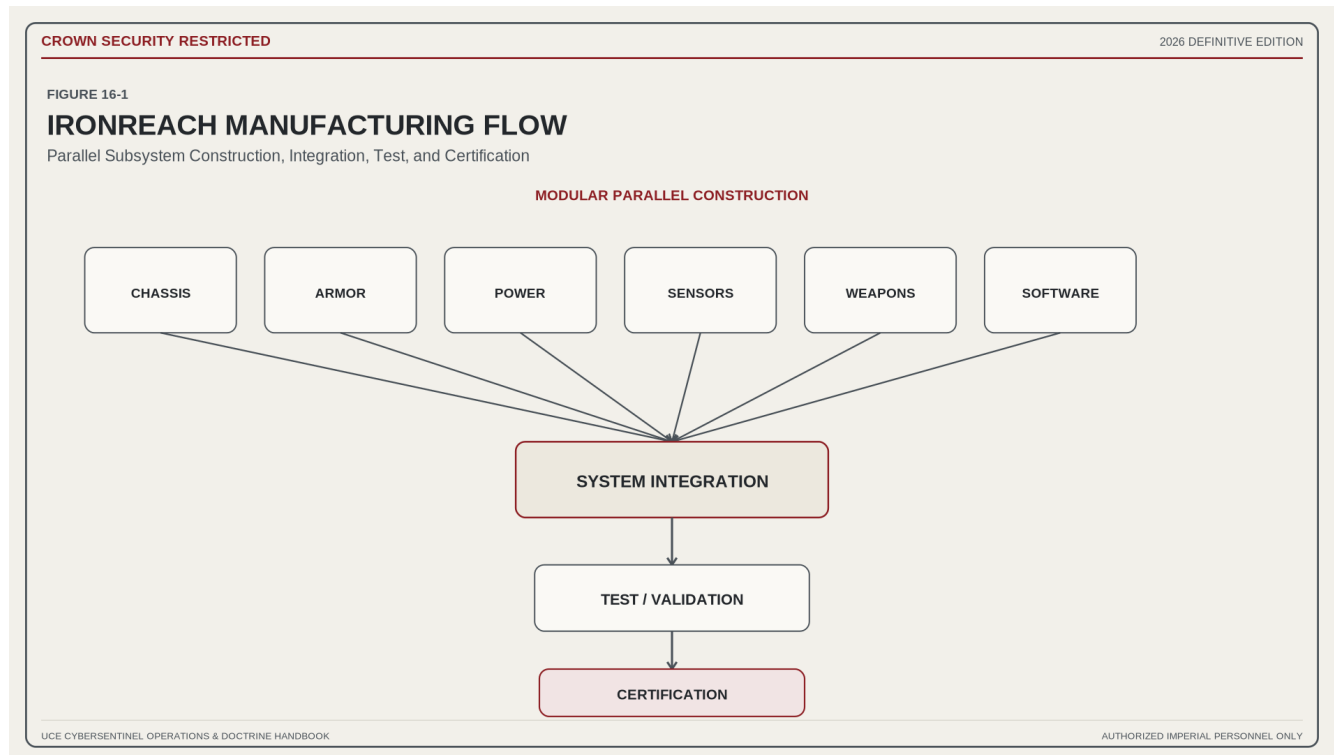


Figure 16-1 — Ironreach manufacturing flow from parallel subsystem construction through certification.

16.1 Production Model

Cybersentinel construction is modular and parallel. Chassis, armor, power systems, sensors, weapons, software, and specialized class equipment are built and tested as subsystem families before final integration. Approximately thirty to forty percent subsystem-family commonality across the program reduces spare-parts burden without forcing different classes into the same body plan.

The controlling philosophy is that common internal engineering should simplify sustainment while exterior architecture remains mission-shaped. A Warden is not a lighter Legion and a Sentry is not a quadruped version of either; shared engineering exists beneath distinct class functions.

16.2 Typical Construction Time

Table 16-1 — Typical Construction Time.

Class	Typical Build Time
Sentry	6–8 months
Legion	9–12 months
Bulwark	12–16 months
Warden	14–18 months
Prototype	18 months to several years

Under normal conditions, Ironreach can complete approximately six to ten production systems per year. A national emergency can increase output by roughly thirty to fifty percent for a limited period, but surge production consumes reserve components, compresses maintenance capacity, increases workforce burden, and therefore imposes later sustainment costs.

16.3 Maintenance Hierarchy

Table 16-2 — Maintenance Hierarchy.

Level	Scope
Field	Routine inspection, consumables, external modules, Phleboto replenishment, limited battle-damage repair.
Depot	Major component exchange, weapons/sensor calibration, limb or structural-module work, power and cooling overhaul.
Ironreach	Deep structural rebuild, hardened-core intervention, major software/security work, class reconstruction and certification.



Figure 16-2 — Ironreach maintenance environment. Strategic machines are recovered and rebuilt wherever practical.

16.4 Recovery Before Replacement

Program economics and security both favor recovery. A disabled Cybersentinel contains scarce material, controlled manufacturing knowledge, mission data, validated components, and a repairable strategic asset. Recovery teams therefore assess whether a machine can be stabilized locally, moved to a depot, or returned to Ironreach for reconstruction before replacement is authorized.

Phleboto-bots, modular external armor, compartmentalized internals, isolated power/data pathways, and replaceable mission equipment all support this doctrine. The goal is not to make the machines indestructible; it is to make useful capability difficult to destroy permanently.

16.5 Lifecycle and Replacement Policy

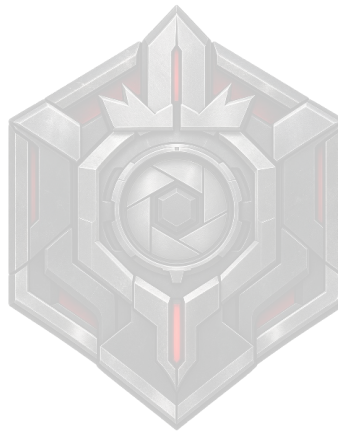
Generation IV systems are maintained through continuous component refresh rather than discarded on a short consumer-style lifecycle. Sensors, processors, communications, armor modules, weapons, software, cooling systems, and support hardware may be replaced while the controlling class architecture remains stable.

A machine is replaced when damage, structural fatigue, obsolescence, security compromise, or rebuild cost makes continued service unreasonable. Fleet growth beyond the authorized ninety-six requires a separate strategic decision; normal production is not an automatic expansion mechanism.

Recover it. Repair it. Rebuild it. Replace it only when necessary.

PART V

OPERATIONAL DOCTRINE



CROWN SECURITY RESTRICTED

CHAPTER 17

OPERATIONAL DOCTRINE

Mutual Specialization, Target Handoff & Tactical Employment

Cybersentinel doctrine begins with specialization. No production class is designed to solve every battlefield problem. Sentry, Legion, Bulwark, and Warden systems are employed according to the military effect required, with target information, protection, and response responsibilities handed between classes as the situation develops.

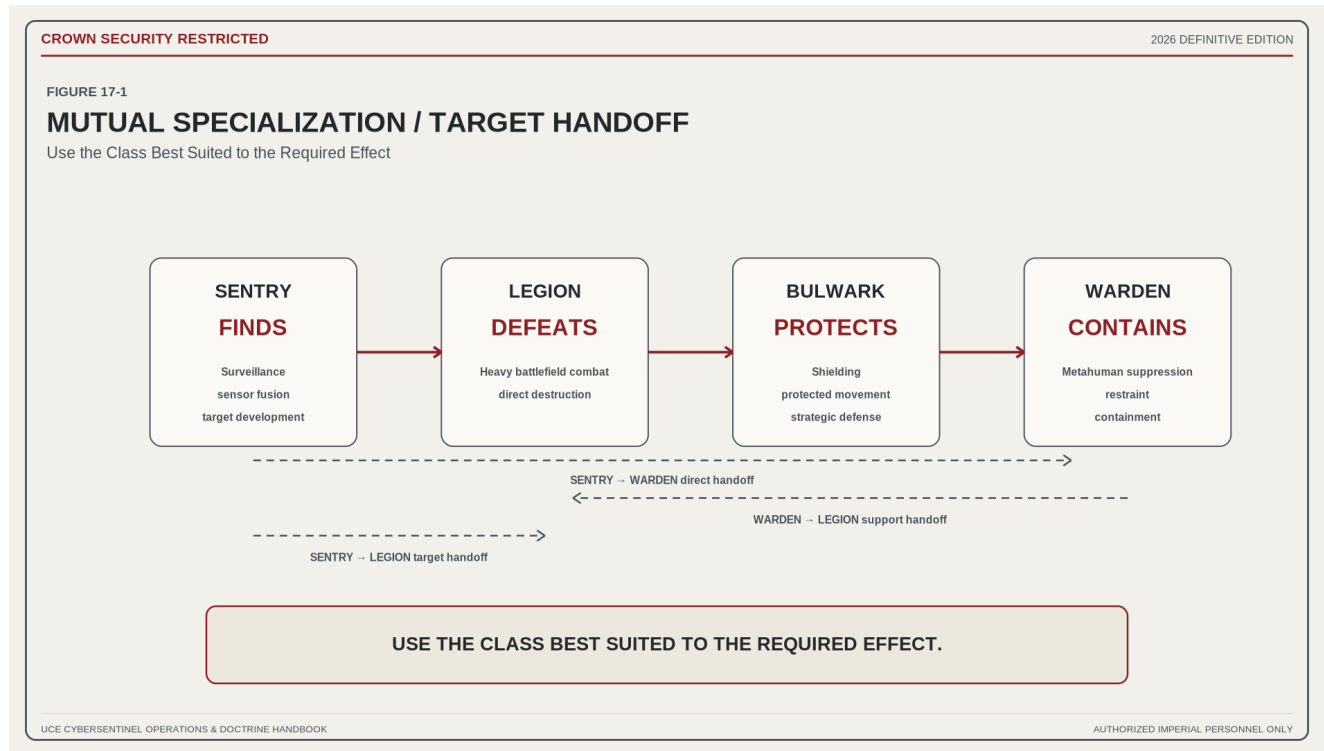


Figure 17-1 — Mutual specialization and target handoff. The sequence is doctrinal, not a rigid mandatory workflow.

17.1 Class Questions

Table 17-1 — Class Questions.

Class	Primary Operational Question
Sentry	What is happening?
Legion	What needs to be defeated?
Bulwark	What must be protected?
Warden	Which metahuman must be neutralized?
Prototype	Can this new technology work?

17.2 Target Handoff

Sentry normally develops the clearest tactical picture and passes validated tracks to the platform or conventional force best suited to act. A Legion may receive a hardened ground target; a Warden may receive a metahuman track; a Bulwark may receive threat-axis information needed to place a shield where it changes the battle.

Handoff is not always sequential. A Warden can pass a conventional threat to Legion support, a Legion can request Sentry refinement on a concealed target, and any class can provide local sensor data to another authorized node. The governing rule is effect matching, not ownership of the target.

17.3 Standard Formation Patterns

Table 17-2 — Standard Formation Patterns.

Formation	Typical Composition	Purpose
Strategic Defense	2 Sentries; optional Bulwark	Persistent detection with protected-site reinforcement.
Heavy Combat	1 Sentry + 2 Legions	Find, fix, and defeat heavy conventional threats.
Shielded Assault	1 Sentry + 2 Legions + 1 Bulwark	Heavy combat under mobile/anchored shield support.
Meta Interdiction	1 Warden + 1 Sentry; optional Legion	Track and contain a priority metahuman threat.
Meta Crisis	2 Wardens + 2 Sentries + 1–2 Legions; optional Bulwark	Multi-system response to severe powered threat.
Shield Response	1 Sentry + 1 Bulwark	Rapid protected-site or corridor defense.
Protected Transit	1 Sentry + 1 Bulwark + conventional force; optional Legion	Protect movement of strategic personnel or equipment.
Reaction	1 Sentry + 1 Legion	Compact rapid conventional response.

17.4 Concentration and Support

Cybersentinels operate with the Imperial Armed Forces rather than above them. Army maneuver units, Air Service aircraft, Maritime assets, ISOC teams, Redcoats, Enforcers, engineers, logistics personnel, and recovery forces provide capabilities that are inefficient or inappropriate to duplicate inside a Cybersentinel chassis.

The program therefore avoids using a strategic machine where a Redcoat, tank, aircraft, drone, emplacement, or conventional unit can achieve the required effect more efficiently.

DOCTRINAL PRINCIPLE: Use the class best suited to the required effect. A Cybersentinel should exist only when its presence changes the military problem.

CHAPTER 18

COMBINED-ARMS INTEGRATION

Combined-Arms Integration & Wolfe Island Defense

The defense of Wolfe Island is organized as a layered national system. Cybersentinels occupy specialized positions inside that system; they are not a separate force expected to defeat every threat independently. Detection, interception, shielding, metahuman response, and inner security are deliberately distributed among different organizations and classes.

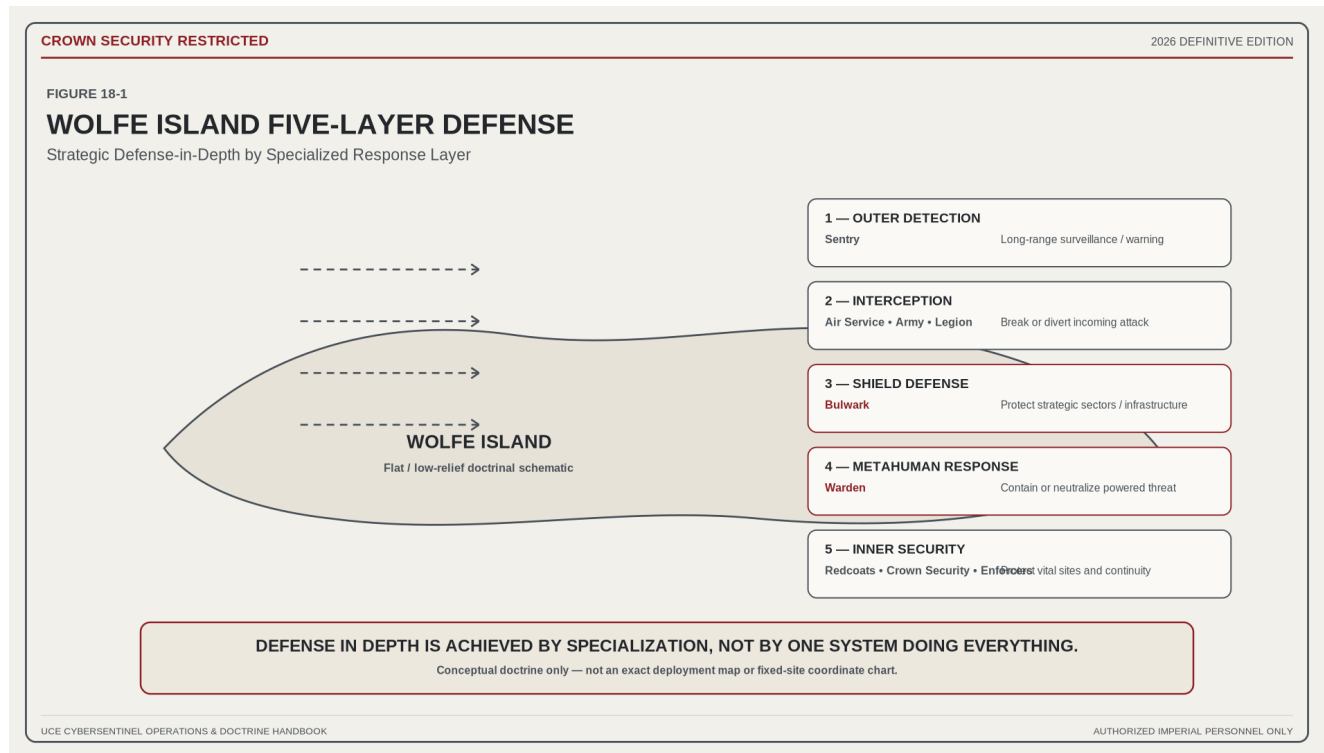


Figure 18-1 — Wolfe Island five-layer defense. Conceptual doctrine only; not an exact deployment map or fixed-site coordinate chart.

18.1 Five Defensive Layers

Table 18-1 — Five Defensive Layers.

Layer	Primary Force	Function
1 — Outer Detection	Sentry	Long-range surveillance, warning, classification, target development.
2 — Interception	Imperial Air Service / Imperial Army / Legion	Break, divert, or defeat incoming conventional attack.
3 — Shield Defense	Bulwark	Protect strategic sectors, infrastructure, formations, or evacuation corridors.
4 — Metahuman Response	Warden	Contain or neutralize priority powered threats.
5 — Inner Security	Redcoats / Crown Security / Enforcers	Protect vital sites, command continuity, restricted facilities, and recovery areas.

18.2 Defense in Depth

An attacker that penetrates one layer does not automatically defeat the next. A missed Sentry track may still be engaged by air or ground interception; a failed interception may still meet Bulwark protection; a metahuman that bypasses conventional forces may still trigger Warden response; and a penetrated external perimeter still encounters hardened inner security.

This structure also prevents the Cybersentinel program from becoming a single point of national failure. Conventional formations retain their own command, weapons, logistics, and defensive functions while Cybersentinels add strategic effects where they provide disproportionate value.

18.3 Conventional and Robotic Force Integration

Table 18-2 — Conventional and Robotic Force Integration.

Force	Integration Role
Imperial Army	Ground maneuver, fires, engineering, perimeter and recovery support.
Imperial Air Service	Air interception, reconnaissance, lift, strike, and air-defense integration.
Imperial Maritime Service	Lake approaches, transport, interdiction, and shore support.
ISOC	Low-visibility or specialist operations around high-priority threats.
Redcoats	Persistent robotic manpower, interior security, close combat, and site defense.
Enforcers / Crown Security	Restricted-site protection, command continuity, and exceptional internal-security response.

DOCTRINAL PRINCIPLE: Defense in depth is achieved by specialization, not by one system doing everything.

CHAPTER 19

LARGE-SCALE & NATIONAL MOBILIZATION

Large-Scale Mobilization, Sentinel Groups & Temporary Command

Large Cybersentinel concentrations are exceptional. The fleet is designed to protect multiple sectors, retain strategic reserve, support recovery, and survive the loss or isolation of individual formations. Mobilization doctrine therefore distinguishes national alert posture from the number of systems actually committed to a single operation.

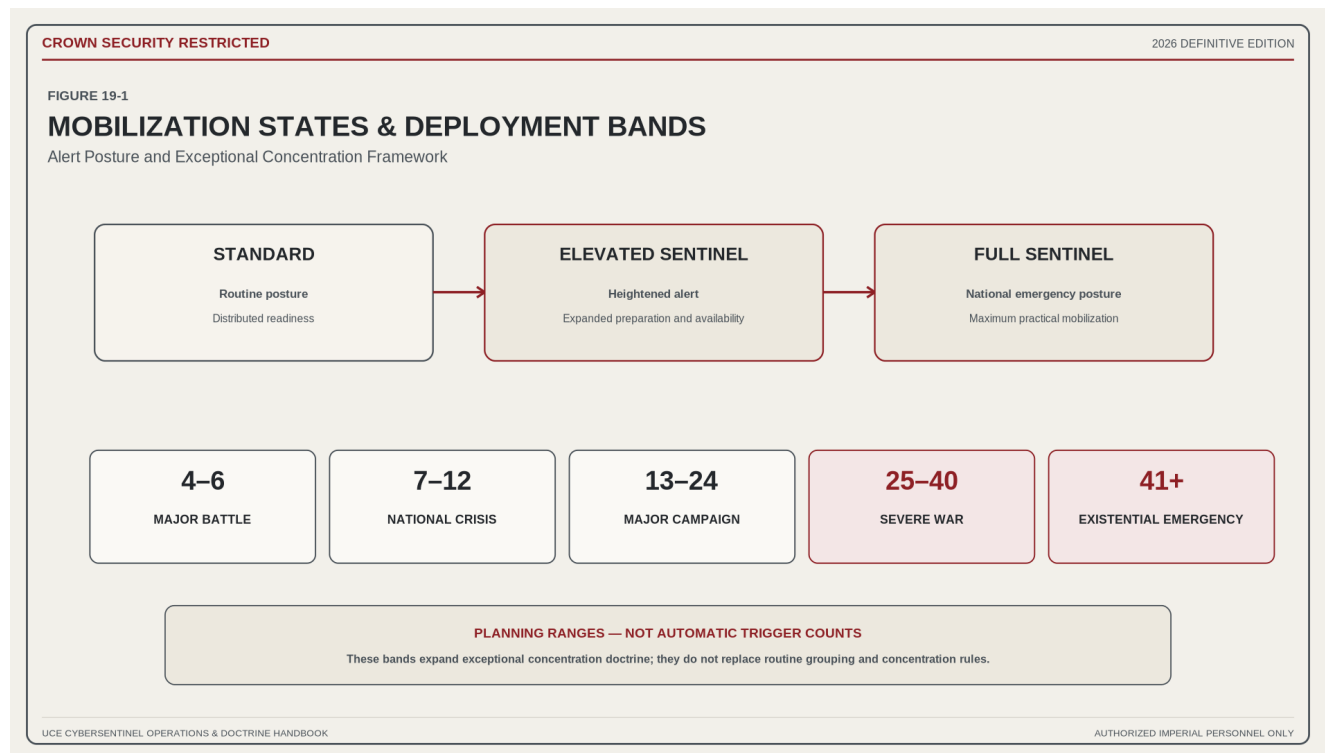


Figure 19-1 — Mobilization states and deployment bands. Ranges are planning guides, not automatic trigger counts.

19.1 National Mobilization States

Table 19-1 — National Mobilization States.

State	Meaning
Standard	Routine distributed posture; normal training, maintenance, site defense, and rotational readiness.
Elevated Sentinel	Heightened preparation, expanded availability, mission configuration, and theater reinforcement.
Full Sentinel	National emergency posture using the maximum practical combat strength consistent with continuity, maintenance, and strategic reserve needs.

19.2 Deployment Bands

Table 19-2 — Deployment Bands.

Systems Committed	Planning Context
4-6	Major battle

7–12	National crisis
13–24	Major campaign
25–40	Severe war
41+	Existential emergency

These bands extend the routine concentration framework; they do not replace it. They describe the scale of commitment that planners should associate with increasingly severe national situations, not an automatic order to deploy a particular number of machines.

19.3 Cybersentinel Operations Group (COG)

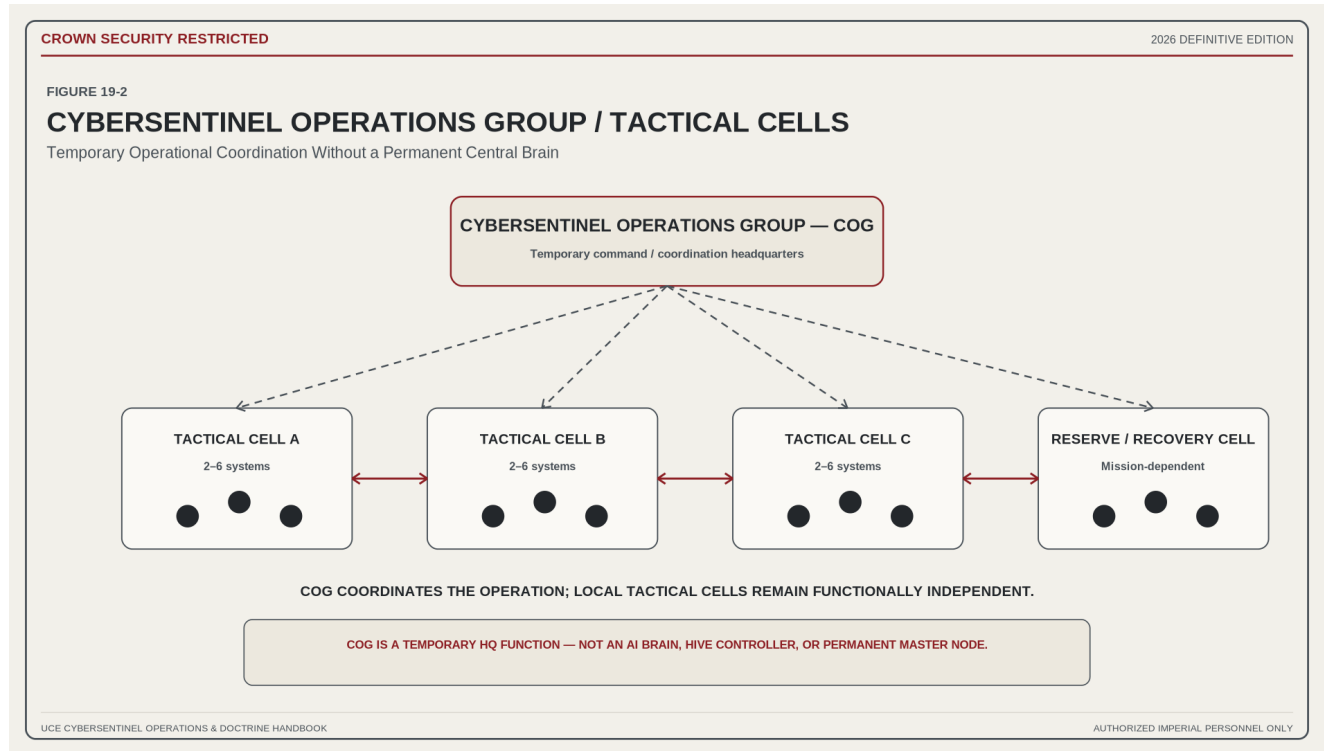


Figure 19-2 — Temporary Cybersentinel Operations Group and tactical-cell structure.

A Cybersentinel Operations Group is a temporary headquarters or coordination function established when the scale of an operation requires dedicated Cybersentinel command integration. It is not a permanent national headquarters and is not an AI brain or central controller.

COG staff coordinate mission envelopes, theater priorities, conventional-force integration, recovery, logistics, and tactical-cell boundaries. Tactical cells normally contain two to six systems and retain local ISTM coordination and bounded tactical autonomy.

19.4 Reserve and Continuity

Where practical, planners preserve approximately fifteen to twenty percent of combat-capable strength for strategic reserve, recovery coverage, maintenance margin, or emergent threats. The percentage is a planning principle rather than a rigid quota.

No ordinary doctrine contemplates committing all ninety-six authorized systems to one battle. A literal national-collapse scenario would be required before concentration at that scale could even be considered.

Disperse strategically. Concentrate tactically. Recover aggressively. Preserve command independence.

CHAPTER 20

EW, COMMUNICATIONS & DEGRADED OPERATIONS

Electronic Warfare, Communications & Degraded Operations

Cybersentinels are designed to continue useful military action when communications are damaged, jammed, partitioned, delayed, or intentionally isolated. Electronic warfare therefore degrades coordination progressively rather than creating an automatic all-or-nothing loss of platform function.

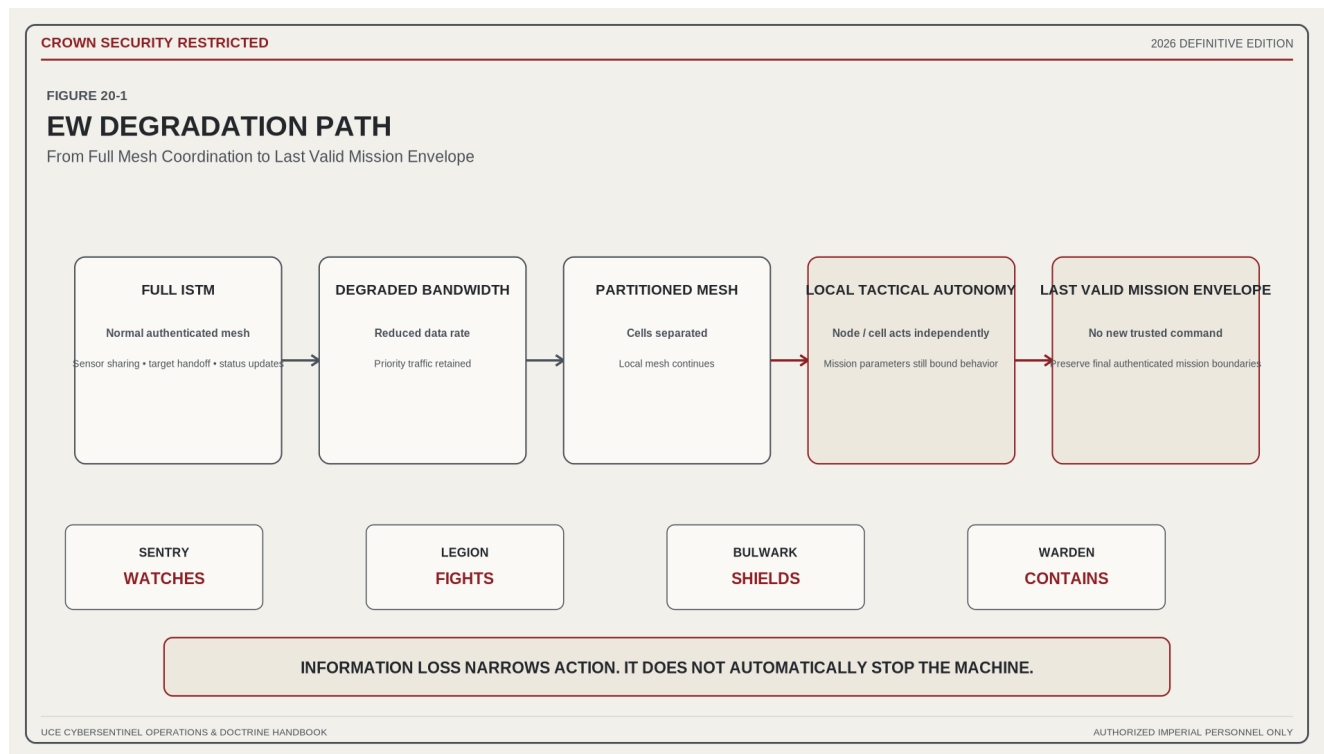


Figure 20-1 — Electronic-warfare degradation path from full ISTM coordination to the Last Valid Mission Envelope.

20.1 Degradation Path

Table 20-1 — Degradation Path.

Condition	Platform / Network Behavior
Full ISTM	Authenticated mesh with broad sensor, track, command, and status sharing.
Degraded Bandwidth	Priority command and threat data retained; lower-value traffic reduced.
Partitioned Mesh	Local cells continue while cross-cell awareness becomes incomplete.
Local Tactical Autonomy	Platform or cell acts independently inside the authorized Mission Envelope.
Last Valid Mission Envelope	No new trusted command available; final authenticated objectives, restrictions, and ROE remain controlling.

20.2 Communications Resilience

Generation IV communications use layered authentication, rotating keys, challenge-response procedures, alternate pathways, and local storage of validated mission information. No universal master code exists. Loss of one relay, command node, or communications band should not collapse the entire force.

When bandwidth narrows, the system prioritizes authenticated command, threat tracks, friendly identification, safety-critical status, and target handoff over routine diagnostic and lower-value sensor traffic.

20.3 Electronic Attack and Information Confidence

Table 20-2 — Electronic Attack and Information Confidence.

Confidence Condition	Interpretation
High confidence	Multiple trusted sensors / authenticated sources agree.
Reduced confidence	Partial data, intermittent links, or unresolved source disagreement.
Local confidence	Platform relies primarily on onboard sensors and local cell data.
Untrusted	Data path fails authentication, shows compromise indicators, or conflicts with protected security state.

20.4 Mission Continuity by Class

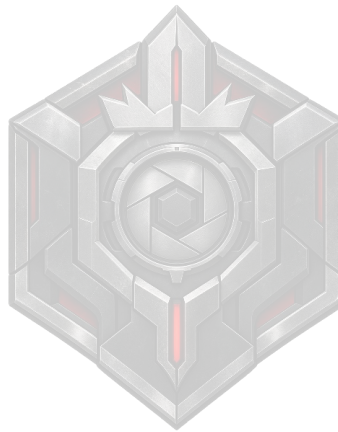
Table 20-3 — Mission Continuity by Class.

Class	Degraded-Network Priority
Sentry	Continue local watch, track development, and protected-site sensing.
Legion	Continue authorized combat within validated target and engagement constraints.
Bulwark	Continue shielding or protected-position mission as locally sustainable.
Warden	Continue containment / countermeasure action against the validated priority threat.

COMMAND NOTE: Loss of communications does not automatically order withdrawal and does not grant unlimited discretion. Information loss narrows action while the Last Valid Mission Envelope continues to bound behavior.

PART VI

DAMAGE, RECOVERY & LEARNING



CROWN SECURITY RESTRICTED

CHAPTER 21

DAMAGE STATES & BATTLEFIELD SURVIVAL

Functional Survival Under Progressive Damage

Cybersentinel survivability is built around the principle that damage should propagate poorly. A platform is not considered combat-effective merely because its armor remains intact, nor is it considered lost because a major subsystem has failed. The decisive question is whether the machine can still execute a bounded mission function without creating unacceptable risk to Imperial forces, protected infrastructure, or its own technology-security posture.

Damage-State Doctrine

Table 21-1 — Damage-State Doctrine.

State	Meaning	Command / System Response
GREEN	Nominal or minor degradation	Normal mission execution. Local repair may occur without mission interruption.
AMBER	Meaningful degradation	Mission remains viable, but weapons, mobility, sensors, power, or cooling are constrained. Re-tasking or support may be required.
RED	Severe degradation / functional defeat risk	Platform preserves essential control, attempts withdrawal or protected posture, and prioritizes recovery or denial decisions.
BLACK	Security condition, not a damage color	Technology-security state invoked when capture, compromise, hostile control, or restricted-system exposure becomes the dominant risk.

Damage Isolation

Generation IV architecture distributes control, power routing, sensors, cooling, and local subsystem logic so that a single strike is less likely to collapse the entire platform. Replaceable outer armor absorbs punishment; structural layers preserve load paths; hardened internal systems retain minimum mission control. The machine should lose capability in pieces rather than fail as one monolithic mechanism.

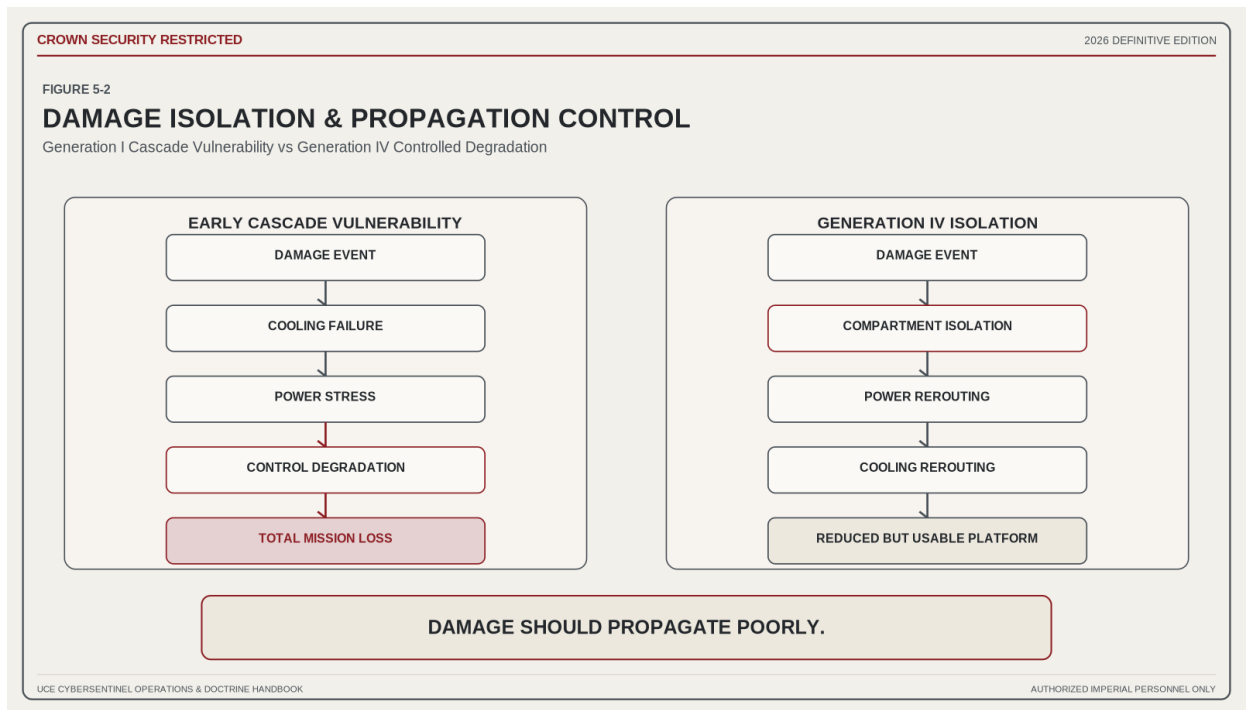


Figure 21-1 — Damage Isolation & Propagation Control

Power Loss & Load Shedding

When available generation or storage falls below demand, Cybersentinels shed low-priority loads before sacrificing essential control. Noncritical support systems are reduced first, followed by secondary combat-support loads. Mission-critical systems are preserved as long as possible; command core, safety logic, and minimum control remain last in the hierarchy.

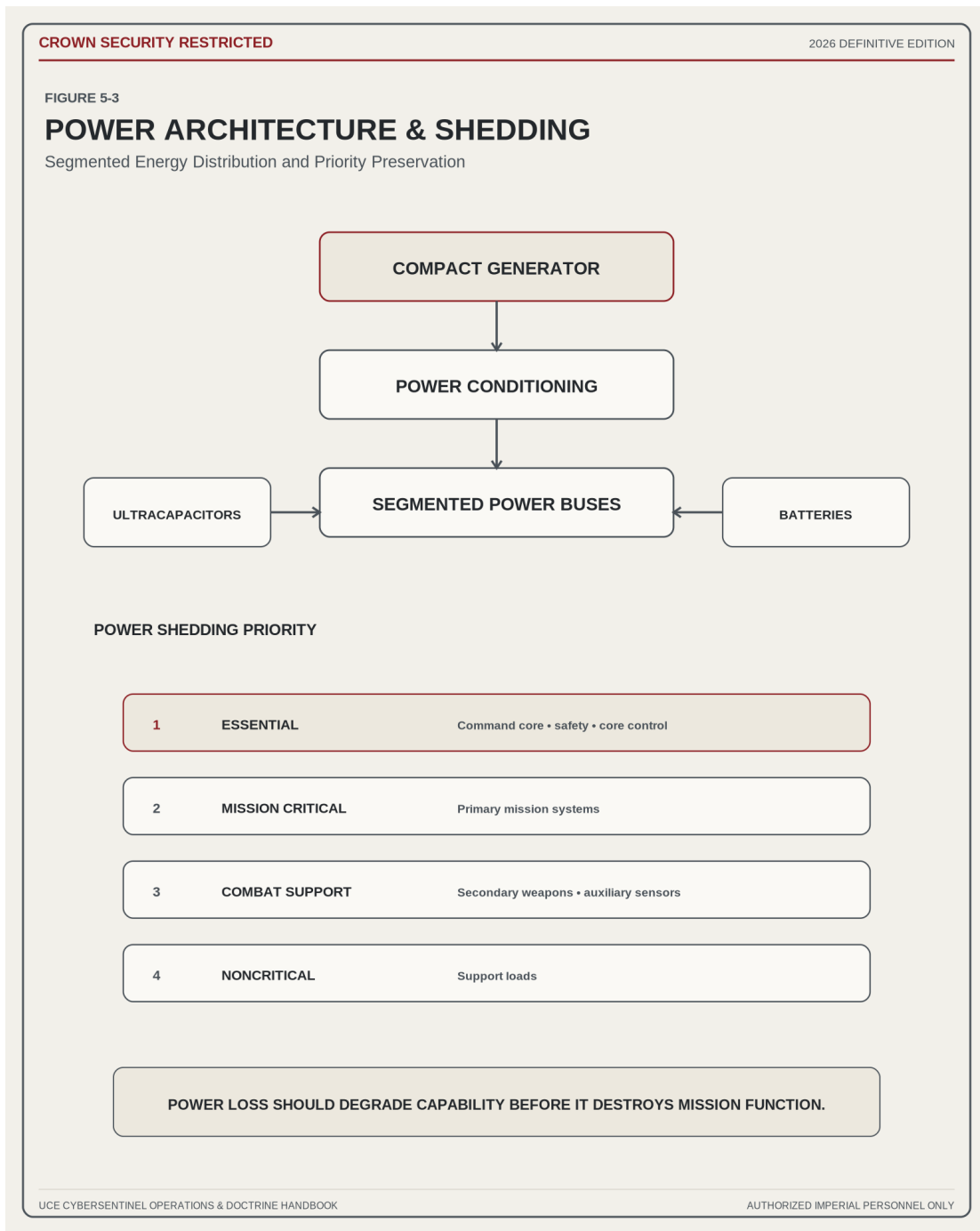


Figure 21-2 — Power Architecture & Shedding

Battlefield Survival Priorities

Table 21-2 — Battlefield Survival Priorities.

Priority	Action
1	Preserve authenticated command state and the current Mission Envelope.
2	Maintain minimum locomotion, stabilization, or protected posture appropriate to class.
3	Preserve sensors and communications sufficient to

	distinguish friendly, hostile, and prohibited targets.
4	Retain mission-critical weapons or shield function when tactically justified.
5	Initiate Phleboto-bot repair where repair time and exposure permit.
6	Transition toward recovery, protected withdrawal, or staged denial when continued combat becomes counterproductive.

Functional Defeat

A Cybersentinel may be functionally defeated without being physically destroyed. Immobilization, loss of primary sensors, loss of class-defining weapon or field capability, catastrophic cooling restrictions, or inability to authenticate command can remove the system from useful combat even when the chassis remains recoverable. Functional defeat therefore triggers recovery planning before destruction becomes inevitable.

Chapter Summary

Battlefield survival is a systems problem, not an armor contest. The Generation IV design objective is controlled degradation: preserve command, retain the class-defining mission effect where possible, repair locally when practical, and recover the machine before damage becomes irreversible.

CHAPTER 22

RECOVERY & TECHNOLOGY DENIAL

Recover the Machine. Preserve the Knowledge. Deny Only What Must Be Denied.

The Empire treats a disabled Cybersentinel as both a military asset and a concentrated body of technical knowledge. Recovery is therefore the default response. Technology denial exists to prevent hostile exploitation when recovery cannot be completed in time; it is not a routine self-destruct doctrine and is never a substitute for disciplined battlefield recovery.

Recovery Doctrine

Table 22-1 — Recovery Doctrine.

Condition	Preferred Response
Recoverable / secured	Stabilize, isolate hazards, dispatch recovery force, preserve logs and damaged components.
Recoverable / contested	Establish security bubble, suppress hostile access, conduct rapid extraction or protected field repair.
Temporarily unrecoverable	Maintain remote or local security state, preserve data, prepare staged denial if hostile capture becomes probable.
Capture imminent	Apply the lowest denial level sufficient to protect restricted technology.
Chassis unrecoverable	Preserve knowledge first; escalate denial only to the minimum irreversible level required.

Technology Denial Ladder

The denial sequence deliberately increases in irreversibility and collateral consequence. Commanders are expected to stop at the lowest level that achieves the security objective. There is no universal fleetwide kill switch and no routine catastrophic self-destruct mechanism.

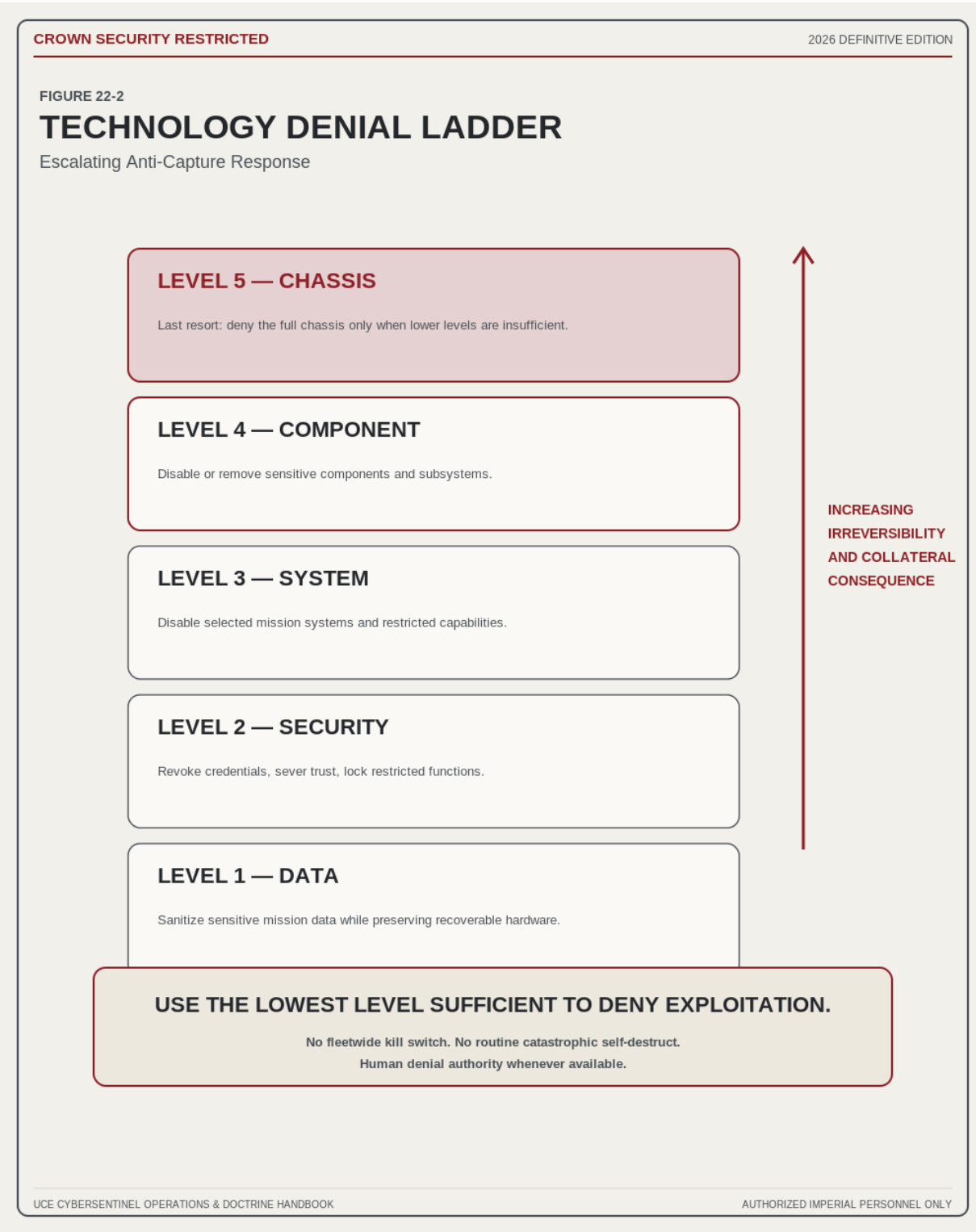


Figure 22-1 — Technology Denial Ladder

Table 22-2 — Technology Denial Ladder.

Level	Primary Effect
DATA	Purge or invalidate sensitive logs, keys, mission records, and recoverable intelligence.
SECURITY	Lock restricted interfaces, revoke credentials, isolate

	control paths, and prevent unauthorized access.
SYSTEM	Disable selected control, sensor, weapon, AI, or power-management functions.
COMPONENT	Physically or thermally destroy specific restricted modules that cannot be secured.
CHASSIS	Last-resort irreversible denial of the broader platform when capture would expose unacceptable technology.

Authority & Restraint

Denial authority is bounded by the Mission Envelope, theater command, and applicable contingency authorization. A damaged platform may autonomously protect credentials and restricted interfaces, but major irreversible denial remains a controlled security action. Anti-capture measures must not create more danger to UCE forces or protected civilians than the enemy action they are intended to prevent.

Recovery Intelligence

Every recovered loss is treated as a technical report written in metal. Damage patterns, hostile tactics, software behavior, repair performance, ammunition expenditure, cooling events, and command-link history are retained for Ironreach analysis. The objective is not simply to return the chassis to service; it is to convert the event into future survivability.

Chapter Summary

Recovery precedes denial. Denial is staged, selective, and proportional. The program protects both the machine and the knowledge inside it, while avoiding the Generation I mistake of treating destruction as the easiest form of security.

CHAPTER 23

PHLEBOTO-BOT REPAIR SYSTEMS

Distributed Micro-Repair for Field Survival and Controlled Recovery

Phleboto-bots are small host-directed repair machines carried aboard production Cybersentinels. They are not independent combat drones and do not possess flight capability. Each unit is approximately 1.5 inches in diameter, built around a brass spherical body with six limbs: four for climbing and magnetic attachment and two equipped for interchangeable repair tools.



Approved Phleboto-Bot visual reference

Physical Architecture

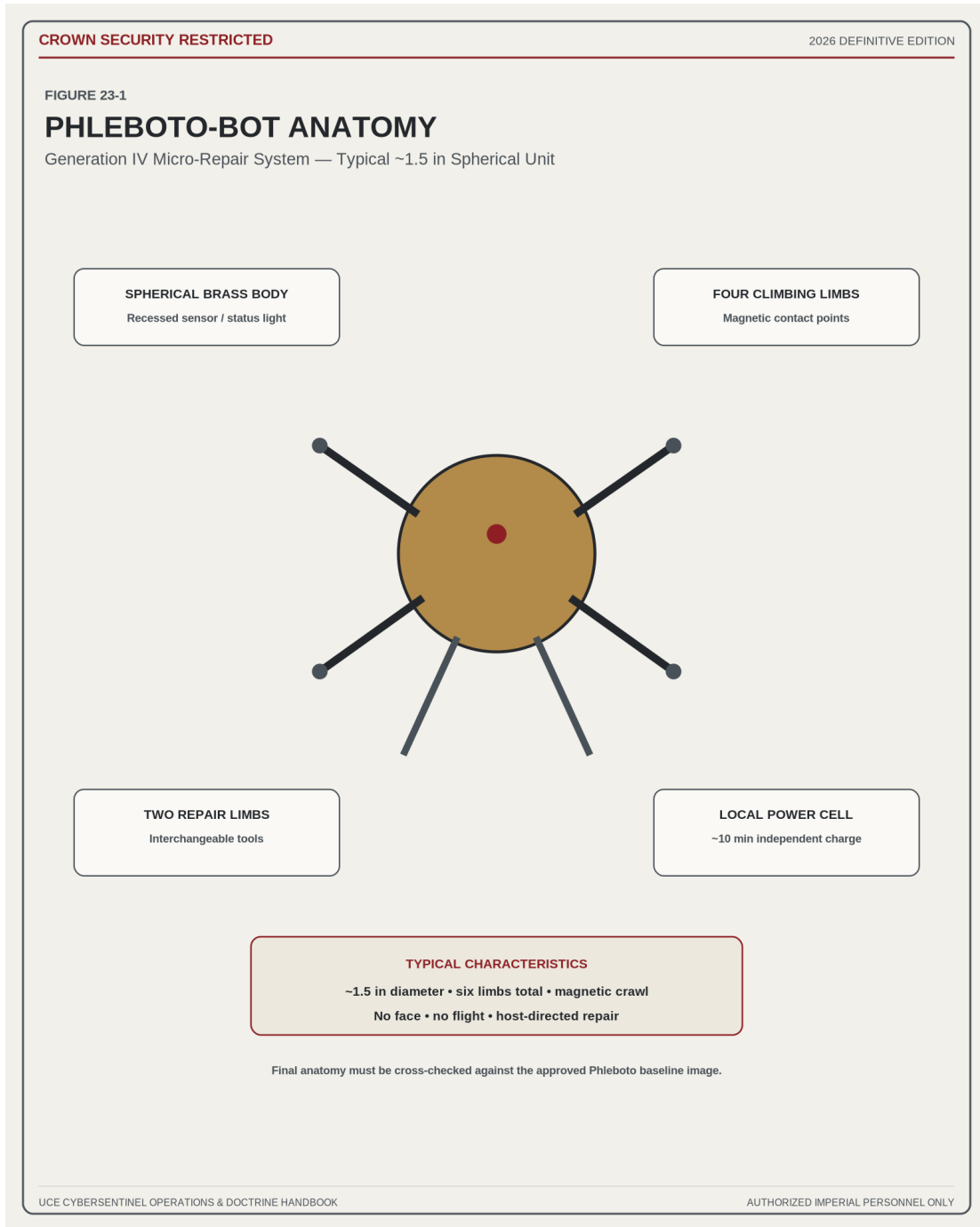


Figure 23-1 — Phleboto-Bot Anatomy

The repair system is deliberately simple at the individual-bot level. A Phleboto-bot crawls across armor and internal service pathways, attaches magnetically, inspects designated damage, and performs a narrow set of host-assigned tasks. It does not improvise a separate mission, act as an autonomous swarm, or leave the host platform to conduct combat.

Class Complement

Table 23-1 — Class Complement.

Class	Canisters	Approx. Phleboto-Bots
Sentry	6	600+
Legion	8	800+
Bulwark	12	1,200+
Warden	10	1,000+

Repair Levels

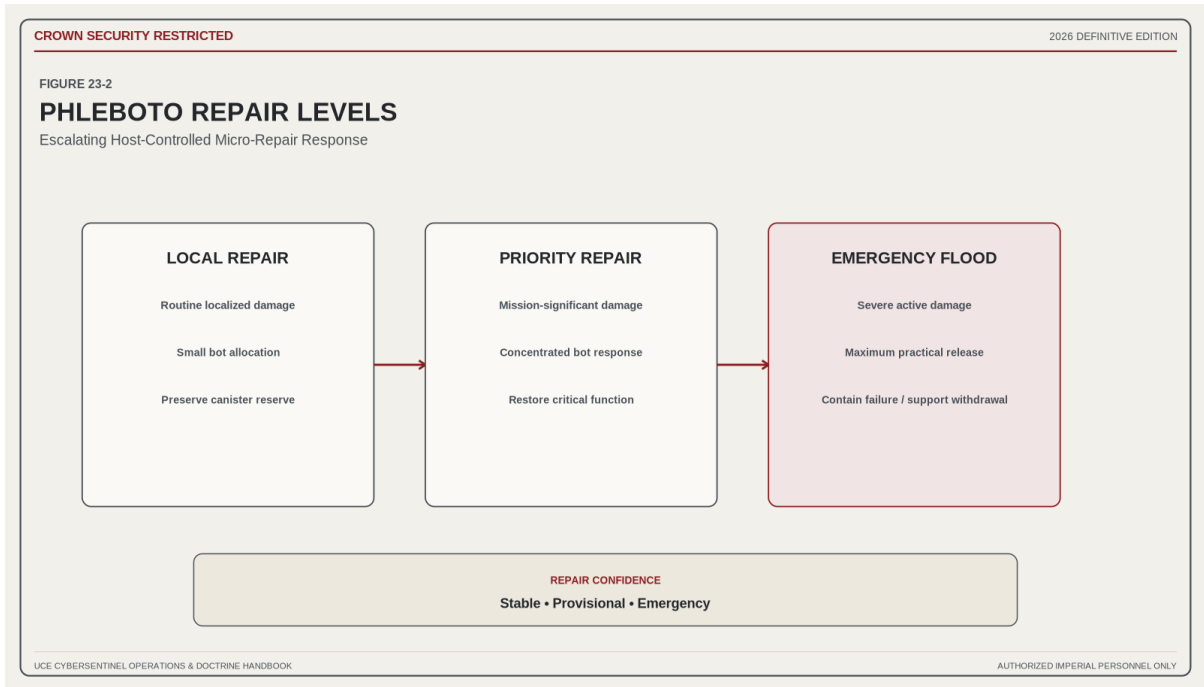


Figure 23-2 — Phleboto Repair Levels

Local Repair

Routine localized damage is addressed with a limited bot allocation. The objective is to seal, reconnect, reinforce, clear debris, restore sensor or data continuity, or stabilize small mechanical failures without consuming the reserve needed for later damage.

Priority Repair

Mission-significant failures receive concentrated repair effort. Bots may be redirected from routine maintenance to restore a class-defining function, reinforce a damaged load path, recover cooling or power routing, or stabilize a subsystem long enough to complete the Mission Envelope or withdraw.

Emergency Flood

Severe damage may justify release of the maximum practical repair allocation. Emergency Flood is not a promise of full restoration. Its purpose is to arrest cascading failure, preserve essential function, support protected withdrawal, and improve the chances of later depot or Ironreach recovery.

Repair Confidence

Table 23-2 — Repair Confidence.

Assessment	Meaning
STABLE	Repair has restored the affected function within expected

	operating margins.
PROVISIONAL	Function is available but remains restricted, monitored, or unsuitable for prolonged high-load use.
EMERGENCY	Temporary stabilization only; continued operation is justified solely by mission or survival necessity.

Limitations

Phleboto-bots cannot replace major armor modules, fabricate a destroyed limb, restore a vaporized power component, or erase the need for depot maintenance. Their value lies in distributed resilience: turning some mission-killing failures into manageable degradation and buying time for recovery.

Chapter Summary

The Phleboto system is a repair multiplier, not a miracle. Its strategic value is measured in platforms that remain controllable, recoverable, and technically intelligible after damage that would otherwise have produced a total loss.

CHAPTER 24

FIVE GAMBIT LESSONS

The Generation I Failures That Define Generation IV Doctrine

Operation: Gambit provided the Cybersentinel program with its most expensive education. Generation I machines proved that the concept could fight, but they also exposed weaknesses in centralized command, subsystem interdependence, anti-capture design, threat assumptions, and post-loss learning. Modern doctrine is built around five lessons that are treated as institutional memory, not historical trivia.

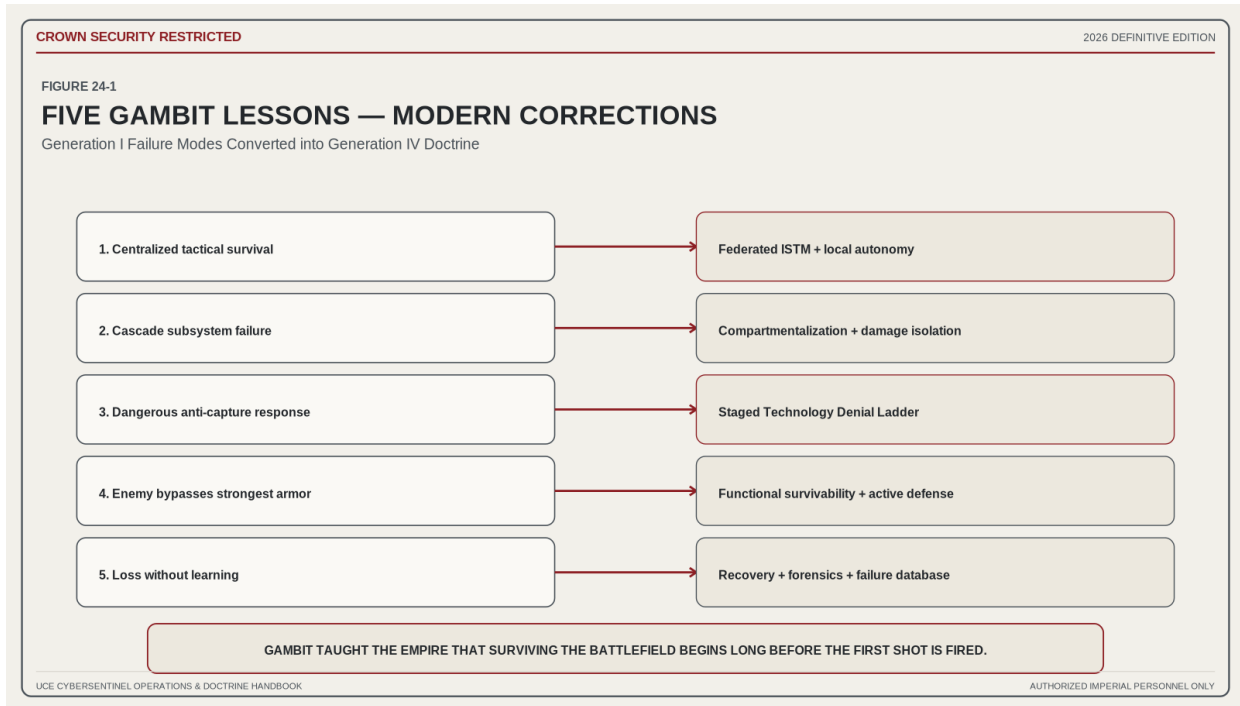


Figure 24-1 — Five Gambit Lessons / Modern Corrections

LESSON 1

Do not centralize tactical survival around one network.

Modern correction: federated ISTM, local tactical autonomy, degraded mission operation, and the Last Valid Mission Envelope allow the force to continue operating when the wider network is disrupted.

LESSON 2

Do not let one damaged subsystem destroy the whole machine.

Modern correction: compartmentalization, distributed control, segmented power, redundant routing, and physical damage isolation make capability loss progressive rather than catastrophic.

LESSON 3

Anti-capture measures must not kill more UCE forces than the enemy.

Modern correction: the Technology Denial Ladder replaces crude destructive responses with proportional data, security, system, component, and only-last-resort chassis denial.

LESSON 4

The enemy will not necessarily attack the strongest armor first.

Modern correction: survivability protects functions, not merely surfaces. Sensors, cooling, mobility, communications, exposed mechanisms, and mission-critical support systems are defended as part of the combat architecture.

LESSON 5

Recover knowledge from every loss.

Modern correction: battlefield recovery, forensics, maintenance records, damaged components, tactical logs, and failure analysis feed directly back into Ironreach engineering and doctrine.

Institutional Effect

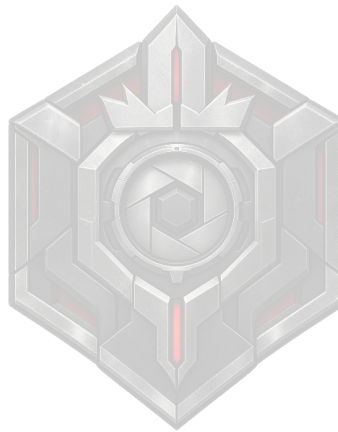
These lessons explain why Generation IV Cybersentinels are decentralized without being strategically independent, heavily armored without depending solely on armor, repairable without being disposable, and protected by denial mechanisms that are staged rather than catastrophic. They also explain why every deployment produces engineering data even when no machine is lost.

Chapter Summary

Gambit did not end the Cybersentinel concept. It forced the program to mature. The modern system exists because the Empire chose to preserve the successful idea while systematically eliminating the failure modes that nearly destroyed it.

PART VII

REFERENCE & CURRENT STATUS



CROWN SECURITY RESTRICTED

CHAPTER 25

VISUAL & IDENTIFICATION ANNEX

Definitive visual control reference for class recognition, markings, proportions, and approved identification cues.

Purpose and Controlling Standard

This annex establishes the controlling visual-identification standard for Generation IV Cybersentinels. It is intended to let Imperial personnel distinguish classes quickly, verify whether a depicted platform is consistent with the approved program family, and identify visual drift before it enters training, intelligence, engineering, or public-facing material.

Where a conflict exists between descriptive prose and an approved class baseline, the approved baseline and current dimensional tables control. Prototype systems are excluded from standardized silhouette identification because no universal Prototype chassis exists.

Generation IV Visual Family

Production Cybersentinels share a restrained industrial identity: dark gunmetal or blackened armor, brushed or worn metallic structure, limited Imperial red accents, recessed sensors, integrated weapon systems, and no human face. The family must read as defense-industry machinery rather than costume armor, heroic mecha, animal robotics, or consumer technology.



CS-S4-01 SENTRY



CS-L4-01 LEGION



CS-B4-01 BULWARK



CS-W4-01 WARDEN

Figure 25-1 — Approved Generation IV production-class baseline references.

Class Recognition Matrix

Table 25-1 — Class Recognition Matrix.

Class	Primary Form	Typical Scale	Fast Recognition Cues	Primary Role
Sentry	Low industrial quadruped	~14 ft / ~18 t	Broad low hull; four articulated legs; low sensor crown; no head	Surveillance, site defense, EW, local air defense
Legion	Broad heavy biped	~20 ft / ~38 t	Short powerful legs; wide torso; integrated heavy weapon; no head	Heavy battlefield combat
Bulwark	Low fortress / deployable tower	~12 ft travel / ~32 ft deployed / ~62 t	Rectangular armored body; hybrid mobility; telescoping shield column; no arms/head	Strategic shielding and protected movement
Warden	Tall narrow biped	~21 ft / ~34 t	Sensor-dense narrow frame; agile proportions; containment architecture; no head	Metahuman contingency and containment
Prototype	No standard form	Unrestricted	Mission-specific and experimental; silhouette not standardized	Experimental combat, defense, mobility, cognition, special systems, extreme environment

Markings and Identification

The universal program insignia is subordinate to national and branch markings. Generation IV production systems use restrained red identification elements rather than broad decorative paint. A small recessed red identification bar may be present on approved exterior surfaces. Markings must remain functional, repeatable, and compatible with field repair and panel replacement.

Class names and designations are documentary identifiers; large exterior text labels are not required for field recognition. Same-generation, same-class machines of the same production model must retain the same controlling exterior silhouette. Internal subvariants may alter equipment, software, sensor fit, or weapons without casually changing the chassis family.

Silhouette Controls

Sentry must never read as a robotic dog, wolf, animal, humanoid, or conventional tank-on-legs. Legion must not become a giant armored person, rifleman, Gundam-like machine, or heroic mech. Bulwark must remain a low armored fortress in travel configuration and a tower-like shield platform only when deployed. Warden must remain visibly taller, narrower, and more sensor-dense than Legion; it is not simply a lighter Legion.

Phleboto-Bot Identification

The standard Phleboto-bot is approximately 1.5 inches in diameter with a brass-toned spherical body, six limbs total, a tiny recessed sensor and red status light, and interchangeable repair tooling. Four limbs are optimized for climbing and magnetic attachment; two are repair manipulators. Phleboto-bots crawl and climb. They do not fly and do not possess faces.

Environmental and Geographic Visual Control

Cybersentinel imagery set on Wolfe Island or at Ironreach must preserve the established geography: flat to gently rolling terrain, Lake Ontario shoreline or low horizon where appropriate, and no mountains. Approved defense-industry interiors, yards, hangars, hardened structures, and wet-weather industrial environments are preferred to stylized science-fiction backdrops.

Chapter Summary

Generation IV recognition depends on mission-shaped architecture. Sentry is the low quadruped observer, Legion the broad heavy fighter, Bulwark the armored shield fortress, and Warden the narrow containment specialist. Consistent silhouettes, restrained markings, and realistic industrial presentation are part of the program standard—not decoration.

CHAPTER 26

QUICK-REFERENCE OPERATIONAL ANNEX

Condensed operational data for rapid command, planning, maintenance, and identification reference.

Production-Class Quick Reference

Table 26-1 — Production-Class Quick Reference.

Class	Auth.	Height	Mass	Road	Underwater	Hover / Lift	Phleboto
Sentry	48	~14 ft	~18 t	40 mph road	~150 ft	~90 sec / ~40 mph	6 / 600+
Legion	24	~20 ft	~38 t	35 mph road	~250 ft	~2 min / 45 mph	8 / 800+
Bulwark	12	~12 ft travel / ~32 ft deployed	~62 t	Mission-dependent	~100 ft	~20 sec obstacle lift / ~15 mph	12 / 1,200+
Warden	8	~21 ft	~34 t	42 mph road	~250 ft	~2 min / 45 mph	10 / 1,000+
Prototype	4	Unrestricted	Unrestricted	Concept-dependent	Concept-dependent	Concept-dependent	Concept-dependent

Fleet Strength Definitions

Table 26-2 — Fleet Strength Definitions.

Measure	2026 Value	Meaning
Authorized Fleet	96	Legally/programmatically authorized 2026 establishment.
Inventory Present	Variable	Systems physically on charge, including units in maintenance or deep service.
Available Combat Strength (ACS)	Variable	Systems currently available for combat employment after readiness, maintenance, damage, and mission restrictions are applied.

Authorized 2026 Inventory

Table 26-3 — Authorized 2026 Inventory.

Sentry	Legion	Bulwark	Warden	Prototype	TOTAL
48	24	12	8	4	96

Readiness States

Table 26-4 — Readiness States.

State	Meaning
R1 — Immediate Ready	Available for immediate tasking within established alert posture.
R2 — Mission Ready	Operational and taskable with normal mission preparation.
R3 — Maintenance Ready	Recoverable to mission-ready status through scheduled/local maintenance.
R4 — Deep Service	Major overhaul, rebuild, restricted test, or long-duration service state.

Command Priority

- 1. Crown-authorized national command
- 2. Imperial Armed Forces high command

- 3. Theater / sector commander
- 4. Authorized local battlefield commander
- 5. Mission Envelope
- 6. Independent tactical execution

Deployment Groupings

Table 26-5 — Deployment Groupings.

Grouping	Systems	Typical Use
Singleton	1	Routine site, surveillance, specialist, or contingency tasking
Element	2–3	Significant local response
Detachment	4–6	Major battle / concentrated response
Heavy Detachment	7–12	National-crisis concentration
Sentinel Group	13+	Exceptional campaign-level concentration under temporary COG coordination

National Deployment Bands

Table 26-6 — National Deployment Bands.

Band	Planning Range
Major Battle	4–6
National Crisis	7–12
Major Campaign	13–24
Severe War	25–40
Existential Emergency	41+

These are planning ranges, not automatic trigger counts. They expand the routine concentration framework rather than replacing it. Normal doctrine disperses strategically and concentrates tactically; deployment of the entire 96-system establishment is not a routine concept of operations.

Class Employment Questions

Table 26-7 — Class Employment Questions.

Class	Command Question
Sentry	What is happening?
Legion	What needs to be defeated?
Bulwark	What must be protected?
Warden	Which metahuman must be neutralized?
Prototype	Can this new technology work?

Technology Denial Ladder

DATA → SECURITY → SYSTEM → COMPONENT → CHASSIS. Use the lowest level sufficient to deny useful exploitation. There is no universal fleetwide kill switch and no routine catastrophic self-destruct doctrine.

Five Gambit Lessons

1. Do not centralize tactical survival around one network.
2. Do not let one damaged subsystem destroy the whole machine.
3. Anti-capture measures must not kill more UCE forces than the enemy.
4. The enemy will not necessarily attack the strongest armor first.
5. Recover knowledge from every loss.

Chapter Summary

This annex is a lookup aid, not a substitute for the detailed chapters. When rapid-reference data and chapter doctrine appear to differ, the detailed controlling chapter, current orders, and authenticated Mission Envelope govern.

CHAPTER 27

2026 STATUS

Current Generation IV program posture, authorized force, readiness philosophy, industrial status, and strategic limitations as of 2026.

Program Status

The Cybersentinel Program entered 2026 as a mature Generation IV strategic-weapons capability rather than an experimental force. The four production classes—Sentry, Legion, Bulwark, and Warden—have stable mission definitions, common architectural principles, decentralized tactical coordination, established recovery doctrine, and a controlled production base at Ironreach. Prototype systems remain deliberately limited and are not treated as a fifth standardized production class.

Authorized Force — 2026

Table 27-1 — Authorized Force — 2026.

Class	Authorized Systems	Share of Authorized Fleet
Sentry	48	50.0%
Legion	24	25.0%
Bulwark	12	12.5%
Warden	8	8.3%
Prototype	4	4.2%
TOTAL	96	100%

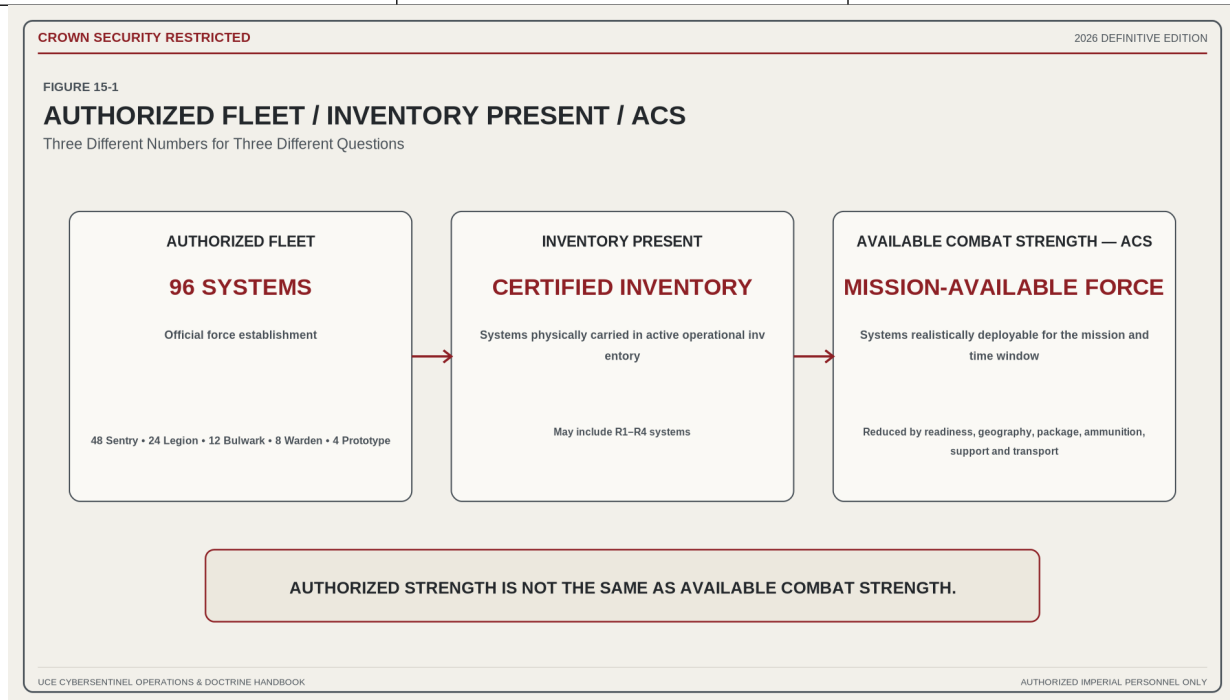


Figure 27-1 — Authorized Fleet, Inventory Present, and Available Combat Strength are related but distinct measures.

Readiness Philosophy

The program does not define combat power by raw inventory alone. Commanders distinguish the authorized establishment from systems physically present and from Available Combat Strength. R1 through R4 readiness states allow the force to preserve immediate-response capability while maintaining a deliberate overhaul and repair cycle. Where practical, doctrine seeks to retain roughly 15–20 percent of combat-capable strength outside the main committed concentration as reserve, recovery cover, or contingency capacity.

Industrial and Sustainment Status

Ironreach remains the principal center for fabrication, integration, deep service, and major rebuild. Normal production capacity is approximately 6–10 production systems per year, with a potential surge of roughly 30–50 percent at the cost of sustainment pressure, maintenance backlog, and reduced flexibility. Replacement-before-expansion remains the governing rule: new production normally restores losses toward the authorized 96-system establishment before any increase beyond that level is considered.

Typical build times remain class-dependent: Sentry approximately 6–8 months; Legion 9–12 months; Bulwark 12–16 months; Warden 14–18 months; Prototype development may require 18 months to multiple years. Common subsystem families provide roughly 30–40 percent architectural commonality without erasing mission-specific design.

Operational Maturity

Generation IV doctrine is built around Mutual Specialization and Target Handoff. Sentry detects and develops the picture; Legion delivers conventional heavy combat power; Bulwark protects forces, infrastructure, and corridors; Warden addresses metahuman contingencies; Prototype systems test capabilities that do not yet justify production-class adoption. ISTM supports coordination but does not create a hive mind, national commander, or single point of tactical survival.

Strategic Limitations

The force remains numerically finite, maintenance-intensive, and dependent on specialized industrial support. Large concentrations create opportunity costs elsewhere. Bulwark deployment trades mobility for field strength; Warden packages can degrade under multi-metahuman saturation; Legion is optimized for direct battlefield defeat rather than persistent surveillance; Sentry cannot replace heavy combat platforms; and no production class is designed to solve every tactical problem.

Metahuman uncertainty remains a permanent limitation. Warden countermeasure packages are structured around expected, plausible, and watch-list threats, but unexpected responders remain X-factors. No production system possesses universal power-nullification capability.

Strategic Expansion Control

The 96-system force is the controlling authorized 2026 establishment. Any expansion beyond 96 requires explicit future authorization and is not implied by existing production capacity. Emperor North has privately expressed an aspirational long-term concept approaching approximately 400 systems; this is not an authorization, procurement program, forecast, hidden current inventory, or approved expansion schedule. It remains a private strategic ambition only.

2026 Assessment

The defining strength of the 2026 Cybersentinel force is not scale alone. It is the combination of mission-shaped classes, human strategic authority, bounded tactical autonomy, distributed command resilience, aggressive recovery, modular

repair, and disciplined technology denial. The program is mature because it no longer depends on one machine, one network, one armor scheme, or one tactical assumption surviving contact with the enemy.

Chapter Summary

As of 2026, the United Canadian Empire maintains 96 authorized Cybersentinels across four production classes and four Prototype systems. The force is operationally mature, industrially sustainable at controlled rates, and designed to preserve knowledge and capability through damage, disruption, and loss. Future growth remains a political and strategic decision rather than an assumed continuation of current production.

GLOSSARY

Controlling terminology used throughout this handbook. Definitions are concise; detailed doctrine remains in the referenced chapters.

Table 27-2 — Chapter Summary.

TERM	DEFINITION
ACS (Available Combat Strength)	Systems realistically deployable for a given mission and time window after readiness, maintenance, recovery, crew/support, and tasking constraints are considered.
Adaptive Counter	A Warden countermeasure that improves effectiveness as the system observes and characterizes an opponent during the engagement.
AESS (Adaptive Environmental Suppression Suite)	Permanent Warden environmental-control system used to alter local conditions against environmentally dependent or vulnerable metahuman threats.
Anchored Strategic Field	Bulwark shield mode established after full anchoring and stabilization; provides the strongest protected-area field available to the class.
Authorized Fleet	The officially authorized Cybersentinel force establishment. For 2026, the controlling authorization is 96 systems.
BLACK Security State	Security condition indicating suspected or confirmed compromise of the machine, credentials, software integrity, or trusted control environment.
Bulwark	CS-B4-01 production class optimized for mobile and anchored strategic shielding.
CCA-7	Common Combat Architecture used across the Generation IV Redcoat family; distinct from Cybersentinel architecture.
Class	A production category defined by primary strategic mission and controlling architecture.
COG (Cybersentinel Operations Group)	Temporary operational headquarters used to coordinate Cybersentinel formations and tactical cells; not a permanent AI brain or master node.
Containment Grip	Warden close-control restraint function intended to hold or physically control a hostile metahuman target.
Data Confidence	Assessment of the reliability and freshness of information available to a Cybersentinel or ISTM cell.
Degraded Mission Mode	Operating condition in which communications or supporting systems are reduced but the platform continues within its authenticated Mission Envelope.
Denial Ladder	Five-level anti-exploitation sequence: Data, Security, System, Component, Chassis. The lowest sufficient level is preferred.
Detachment	Operational grouping of approximately 4–6 Cybersentinels.
Element	Operational grouping of approximately 2–3 Cybersentinels.
Emergency Flood	Highest Phleboto-bot repair response, releasing the maximum practical bot allocation to contain severe active damage or support survival/withdrawal.
Field Contraction	Bulwark shield response that reduces protected area to preserve field strength, power, or stability.
Full Sentinel	National emergency mobilization posture representing the maximum practical Cybersentinel readiness and concentration state.

Generation IV	2024–2026 mature production generation incorporating decentralized ISTM, mature survivability, recovery, denial, and mission-shaped class architectures.
Hard Counter	Countermeasure expected to directly and strongly interfere with a known threat mechanism.
Heavy Detachment	Operational grouping of approximately 7–12 Cybersentinels, normally reserved for national-crisis conditions.
IADS (Integrated Active Defense System)	Layered defensive process for detection, classification, tracking, response selection, and defeat/disruption of relevant threats.
ICCOM	Imperial Cybersentinel Command; operational authority for the Cybersentinel force.
Inventory Present	Certified systems physically carried in active inventory; distinct from authorized establishment and ACS.
Ironreach	Principal Cybersentinel fabrication, integration, test, deep-service, and major-rebuild complex.
ISTM (Imperial Sentinel Tactical Mesh)	Decentralized tactical coordination architecture allowing authenticated information sharing and federated operation without a permanent master node.
Last Valid Mission Envelope (LVME)	Most recent authenticated Mission Envelope retained for continued bounded action when trustworthy command updates are unavailable.
Legion	CS-L4-01 production class optimized for heavy conventional battlefield combat.
Localized Containment Barrier (LCB)	Permanent Warden system for creating a localized containment effect around a target or engagement area.
Mission Envelope	Human-defined bounds governing objective, area, rules of engagement, protected assets, prohibited targets, authorized weapons, duration, withdrawal, denial, and escalation.
Mission Ready (R2)	Readiness state indicating a system can deploy after normal mission preparation but is not held at immediate-launch posture.
Mobile Field	Bulwark shield mode available while the platform remains mobile or incompletely anchored; offers less strength/coverage than the anchored strategic field.
Mutual Specialization	Doctrine that assigns tasks to the Cybersentinel class best suited to produce the required military effect.
Neutralize	Render a hostile capability unable to continue the relevant threat; the term does not inherently require lethal action.
Operational	Certified and carried as part of active inventory; not synonymous with immediately available for combat.
Package Degradation	Reduction in Warden countermeasure effectiveness when target assumptions are wrong, systems are damaged, or multiple threats exceed the configured package.
Phleboto-bot	Approximately 1.5-inch brass-toned six-limbed micro-repair robot used for host-directed inspection, repair, and stabilization. It crawls/magnetically adheres and does not fly.
Preservation-Denial Mode	Operating condition emphasizing survival, recovery, and protection of sensitive technology when mission continuation is no longer practical.
Priority Response List	Warden planning framework identifying expected, plausible, and watch-list metahuman threats for mission-package selection.
Prototype	CS-X4-## experimental system or concept. Prototype is not a fifth production class and is not assumed to have a standard chassis.
R1 Immediate Ready	Highest routine readiness state; system is certified, supplied, and held

	for rapid deployment.
R3 Maintenance Ready	System remains in active inventory but requires maintenance action before deployment.
R4 Deep Service	System is undergoing major overhaul, rebuild, or deep technical service and is not part of immediate ACS.
RDA (Resonance Disruption Array)	Permanent Warden countermeasure intended to interfere with resonance-dependent hostile capabilities.
Redcoat	UCE robotic soldier family. Redcoats provide persistent manpower-scale combat presence; they are distinct from strategic Cybersentinel weapons platforms.
Replacement-Before-Expansion	Industrial doctrine under which new production normally restores losses toward the authorized 96-system establishment before any increase above that level.
Sentry	CS-S4-01 low industrial quadruped production class optimized for surveillance, warning, target development, electronic warfare, and local defense.
Sentinel Group	Exceptional operational grouping of 13 or more Cybersentinels.
Shield Burn	Bulwark emergency field behavior that accepts severe power/thermal burden to preserve a protected objective for a limited period.
Singleton	Employment of one Cybersentinel for a discrete mission.
Soft Counter	Countermeasure intended to reduce, complicate, or constrain a threat rather than directly nullify it.
SRP (Sentinel Recovery Point)	Designated recovery location or handoff point for damaged, disabled, or recoverable Cybersentinel systems.
Substitution Mode	Bulwark function allowing synchronization with fixed shield infrastructure to substitute for, reinforce, or temporarily replace a local shield-network element.
Target Handoff	Transfer of a developed threat track, engagement problem, or containment requirement to the class or force best suited to act on it.
TCN (Tactical Coordination Node)	Temporary ISTM coordination role created for a mission or network condition; not a permanent command node.
Technology Denial	Controlled destruction, disabling, or sanitization used to prevent enemy exploitation of sensitive Cybersentinel technology.
Warden	CS-W4-01 production class optimized for metahuman contingency, restraint, adaptive countermeasures, and containment.
YELLOW COMMAND	Authenticated command that appears anomalous, inconsistent, or suspicious and therefore requires secondary verification without automatically declaring the machine compromised.

ACRONYM REFERENCE

Approved acronyms and abbreviations used in this edition.

Table 27-3 — Chapter Summary.

ACRONYM	MEANING
ACS	Available Combat Strength
AESS	Adaptive Environmental Suppression Suite
CCA-7	Common Combat Architecture 7
COG	Cybersentinel Operations Group
EPS	Electronic Perception Spoofer
IADS	Integrated Active Defense System
IAF	Imperial Armed Forces
ICCOM	Imperial Cybersentinel Command
ISOC	Imperial Special Operations Command
ISTM	Imperial Sentinel Tactical Mesh
LCB	Localized Containment Barrier
LVME	Last Valid Mission Envelope
RDA	Resonance Disruption Array
SRP	Sentinel Recovery Point
TCN	Tactical Coordination Node
TMI	Tactical Machine Intelligence
UCE	United Canadian Empire

LIST OF FIGURES

Figure 2-3 — Cybersentinel Generation Evolution, 2008–2026.	16
Figure 3-1 — Cybersentinel Design Gate.	19
Figure 3-2 — Foundational distinction between Redcoat robotic soldiers and Cybersentinel strategic weapons platforms.	20
Figure 5-1 — Common Cybersentinel Core Architecture.	26
Figure 5-3 — Segmented power architecture and priority shedding.	28
Figure 5-2 — Damage isolation and propagation control.	29
Figure 6-1 — Generation IV class size and mass comparison. Final source-derived silhouettes pending substitution.	31
Figure 6-2 — Cybersentinel armor and structural protection layers.	32
Figure 7-1 — Integrated Active Defense System architecture.	35
Figure 8-1 — CS-S4-01 Sentry baseline identification image.	40
Figure 8-2 — Sentry in Watch Configuration during strategic-site surveillance.	42
Figure 8-3 — CS-S4-01 Sentry technical profile.	43
Figure 9-1 — CS-L4-01 Legion baseline identification image.	44
Figure 9-2 — Legion in heavy direct-fire employment. Braced-fire doctrine emphasizes recoil stability and target-value discipline.	46
Figure 9-3 — CS-L4-01 Legion technical profile.	47
Figure 10-1 — CS-B4-01 Bulwark in transport configuration at Ironreach. Operational artwork is used here; dimensional values are controlled by handbook text.	48
Figure 10-2 — Bulwark eight-stage deployment sequence. Final publication geometry will be source-derived from the approved chassis.	49
Figure 10-3 — Bulwark shield modes: Mobile Field, Anchored Strategic Field, and Field Contraction.	50
Figure 10-4 — Anchored Bulwark shield employment. The field is a protected-area effect, not a permanent invulnerability bubble.	51
Figure 11-1 — CS-W4-01 Warden baseline identification image.	52
Figure 11-2 — Warden 5+3 countermeasure architecture. Final publication silhouette will be derived from the approved Warden source image.	54
Figure 11-3 — Warden containment operation. The class is optimized for controlled interdiction rather than routine battlefield patrol.	56
Figure 11-4 — CS-W4-01 Warden technical profile.	57
Figure 13-1 — Command priority and Mission Envelope architecture.	63
Figure 13-2 — YELLOW COMMAND vs BLACK security-state distinction.	65
Figure 14-1 — Imperial Sentinel Tactical Mesh operational topology. Final publication nodes will use source-derived class silhouettes.	66
Figure 15-1 — Authorized Fleet, Inventory Present, and Available Combat Strength.	68
Figure 15-2 — Cybersentinel readiness cycle.	70
Figure 16-1 — Ironreach manufacturing flow from parallel subsystem construction through certification.	72

Figure 16-2 — Ironreach maintenance environment. Strategic machines are recovered and rebuilt wherever practical. 73

Figure 17-1 — Mutual specialization and target handoff. The sequence is doctrinal, not a rigid mandatory workflow. 76

Figure 18-1 — Wolfe Island five-layer defense. Conceptual doctrine only; not an exact deployment map or fixed-site coordinate chart. 78

Figure 19-1 — Mobilization states and deployment bands. Ranges are planning guides, not automatic trigger counts. 80

Figure 19-2 — Temporary Cybersentinel Operations Group and tactical-cell structure. 81

Figure 20-1 — Electronic-warfare degradation path from full ISTM coordination to the Last Valid Mission Envelope. 83

Figure 21-1 — Damage Isolation & Propagation Control 87

Figure 21-2 — Power Architecture & Shedding 88

Figure 22-1 — Technology Denial Ladder 91

Figure 23-1 — Phleboto-Bot Anatomy 94

Figure 23-2 — Phleboto Repair Levels 95

Figure 24-1 — Five Gambit Lessons / Modern Corrections 97

Figure 25-1 — Approved Generation IV production-class baseline references. 101

Figure 27-1 — Authorized Fleet, Inventory Present, and Available Combat Strength are related but distinct measures. 106

LIST OF TABLES

Table FM-1 — Revision Control. 6

Table 1-1 — Production Classes. 12

Table 4-1 — Classification by Primary Strategic Mission. 22

Table 4-2 — Prototype Categories. 23

Table 6-1 — Class Dimensions and Mass. 31

Table 6-2 — Mobility and Environmental Reference. 33

Table 7-1 — Weapon Families. 35

Table 8-1 — Physical Configuration. 41

Table 9-1 — Physical Configuration. 45

Table 9-2 — Power Allocation States. 46

Table 10-1 — Physical Configuration. 48

Table 11-1 — Physical Configuration. 52

Table 11-2 — Permanent and Configurable Countermeasure Architecture. 54

Table 11-3 — Countermeasure Performance. 55

Table 12-1 — Prototype Categories. 58

Table 12-2 — Disposition and Technology Transfer. 59

Table 13-1 — Command Priority. 64

Table 13-2 — Operating Modes. 64

Table 14-1 — Shared Data.	66
Table 14-2 — Degraded-Mesh Behavior.	67
Table 15-1 — 2026 Authorized Inventory.	68
Table 15-2 — Authorized Fleet, Inventory Present and ACS.	69
Table 15-3 — Readiness States.	69
Table 15-4 — Operational Groupings.	71
Table 16-1 — Typical Construction Time.	72
Table 16-2 — Maintenance Hierarchy.	73
Table 17-1 — Class Questions.	76
Table 17-2 — Standard Formation Patterns.	77
Table 18-1 — Five Defensive Layers.	78
Table 18-2 — Conventional and Robotic Force Integration.	79
Table 19-1 — National Mobilization States.	80
Table 19-2 — Deployment Bands.	80
Table 20-1 — Degradation Path.	83
Table 20-2 — Electronic Attack and Information Confidence.	84
Table 20-3 — Mission Continuity by Class.	84
Table 21-1 — Damage-State Doctrine.	86
Table 21-2 — Battlefield Survival Priorities.	88
Table 22-1 — Recovery Doctrine.	90
Table 22-2 — Technology Denial Ladder.	91
Table 23-1 — Class Complement.	94
Table 23-2 — Repair Confidence.	95
Table 25-1 — Class Recognition Matrix.	101
Table 26-1 — Production-Class Quick Reference.	103
Table 26-2 — Fleet Strength Definitions.	103
Table 26-3 — Authorized 2026 Inventory.	103
Table 26-4 — Readiness States.	103
Table 26-5 — Deployment Groupings.	104
Table 26-6 — National Deployment Bands.	104
Table 26-7 — Class Employment Questions.	104
Table 27-1 — Authorized Force — 2026.	106
Table 27-2 — Chapter Summary.	109
Table 27-3 — Chapter Summary.	112

INDEX

ACS 68–69, 103
 Adaptive Counter 37, 55
 AESS 36, 55
 Anchored Strategic Field 36, 49–50
 Authorized Fleet 68–69, 103, 106
 BLACK Security State 17
 Bulwark 12–13, 20–23, 27, 31, 33, 35
 COG 21, 23, 33, 56, 58, 81, 100–102, 104
 Containment Grip 53, 55
 Damage Isolation 29, 86–87, 97
 Data Confidence 37
 Denial Ladder 90–91, 98, 104
 Electronic Warfare 12, 16, 29, 35–36, 40–41, 45, 83
 Emergency Flood 95
 Field Contraction 36, 49–50
 Five Gambit Lessons 97, 104
 Full Sentinel 80
 Generation I 12–17, 22, 25, 28–29
 Generation II 16–17, 22
 Generation III 16–17, 22
 Generation IV 12–15, 17, 22, 25, 28–30
 Hard Counter 37, 55
 IADS 35
 ICCOM —
 Inventory Present 68–69, 103, 106
 Ironreach 13, 15, 48, 69, 72–73, 92, 95, 98, 102
 ISTM 17, 37, 41, 64, 66, 81, 83, 97, 107
 Last Valid Mission Envelope 17, 41, 64, 67, 83–84
 Legion 12–13, 20–23, 27, 31, 33, 35
 Mission Envelope 12–13, 17, 21, 37, 41, 57, 62–64
 Mobile Field 36, 49–50
 Mutual Specialization 21, 76, 107
 Neutralize 57, 76, 78, 104
 Phleboto-bot 16–17, 26, 30, 73, 89, 93–96
 Preservation-Denial Mode —
 Priority Response List 55
 Prototype 12–14, 20–23, 31, 33, 58
 Readiness 68–70, 80, 103, 106–107
 Recovery 13–14, 17, 21–22, 26, 30–31, 33–34
 Redcoat 12–13, 18, 20, 46, 51, 57, 77–79
 Replacement-Before-Expansion 13, 69, 107

Sentry 12–13, 20–23, 27, 31, 33, 35

Shield Burn 36, 50

SRP —

Substitution Mode 50

Target Handoff 67, 76, 84, 107

TCN 66

Technology Denial 17, 90–91, 98, 104, 108

Warden 12–13, 15, 20–23, 31, 33, 35

Wolfe Island 42, 78, 102

YELLOW COMMAND 17, 64–65



CROWN SECURITY RESTRICTED

AUTHORIZED IMPERIAL PERSONNEL ONLY

**NO CYBERSENTINEL IS IRREPLACEABLE; NO CYBERSENTINEL IS
EXPENDABLE WITHOUT PURPOSE.**