

FULL SPECTRUM SPACE CYBERSECURITY PROFESSIONAL

QUESTION SET · STUDENT EDITION

Module 01

Concept of Operations

Question set

COPYRIGHT AND LEGAL NOTICES

© 2026 D2 Team CORP, a 501(c)(3) nonprofit. All rights reserved.

TLP:AMBER. Limited disclosure. Recipients may share this document only within their own organization and its clients, on a need-to-know basis, and only to the extent necessary to act on the information.

This document is part of the Full Spectrum Space Cybersecurity Professional program. It is provided to enrolled learners and to the credentialing bodies it is submitted to. Redistribution outside the cohort and those bodies is not authorized.

Verbatim sources. Every taxonomy definition in this document is the published METEORSTORM taxonomy text, quoted exactly. Definitions are never abbreviated, paraphrased, or reworded in this publication.

Trademarks. ethicallyHackingspace (eHs)® is a brand of D2 Team CORP, not a separate legal entity. Other names appearing in this document are the property of their respective owners and are used for identification only.

No warranty. This publication is provided for education. It is not legal, regulatory, or engineering advice for any specific system.

PUBLISHER	D2 Team CORP, a 501(c)(3) nonprofit
PROGRAM	Full Spectrum Space Cybersecurity Professional
DOCUMENT	Module 01 Concept of Operations, question set, student edition
EDITION	Student edition · revised 2026-09-24
CONTACT	www.d2teamcorp.org

SCOPE AND STANDING OF THIS WORK · READ BEFORE JUDGING THE ENUMERATION

What this is. Kestrel Orbital's first application of the METEORSTORM framework, produced by three departments who had never used it before, in five working days. It is a deliberately scoped first pass over the telecommand path: the command-and-control chain from the operator console to execution on orbit.

Why that scope, and not more. The mandates chose it. Executive Order 14144 puts the command and control of an operational platform first, and the NIS2 Directive places a duty of care and a reporting clock on the ground operator. The fleet is already flying, so the first pass ran on the part that would end the mission if an adversary took it. Enumerating everything else first would have been thorough and useless.

What it is not, stated plainly. It is not an exhaustive model of the platform and does not claim to be. Elements off the telecommand path are not enumerated. Some assets group several physical units where those units share an owner, a build and a patch path. Gaps in the ordinal sequence mark elements the register tracks outside this scope. Every one of those is a recorded decision taken at the enumeration meeting, not an oversight discovered later.

How it grows. Ordinals are issued once and never renumbered, so everything enumerated here keeps its identifier as the register expands. The same eight-step procedure runs on the next scope, and the one after that. A first pass that names its boundary can be extended. One that hides its boundary has to be rebuilt.

The standard we hold ourselves to. A scope choice is stated openly. A defect is fixed, never narrated. If you find an element misnamed, a parent wrong, or a count that does not add up, that is a defect and we want to hear about it. If you find something outside the telecommand path missing, that is the scope, it was chosen deliberately, and it is on the roadmap. The two are not the same criticism, and this work is built so you can tell them apart.

Contents

- 01 QS Question Set
- 02 KEY Answer Key

QS

Question Set

Every checkpoint question for this module, 36 in all, with its options. Three are worked and marked in the classroom; the rest are yours to work on your own. Answer each one before opening the key, and if your answer differs, trace which chapter rule it breaks before reading the reason.

Context checkpoint

Q1 Context checkpoint worked in the classroom

You were hired into Kestrel Orbital to establish which new department?

- a. SCOR, Space Cybersecurity Operations and Resilience
- b. A second Security Operations Center for the space side
- c. The Satellite Operations Center, newly stood up
- d. A compliance office reporting to the regulators

Q2 Context checkpoint worked in the classroom

SCOR works across which three existing departments to drive them toward resilient cyber operations?

- a. Mission Assurance, Launch Services, and Ground Network Operations
- b. Security Operations, Satellite Operations, and Satellite Design & Engineering
- c. Flight Dynamics, Mission Planning, and Spacecraft Health Monitoring
- d. Launch Operations, Payload Engineering, and Recovery Services

Q3 Context checkpoint

What is the core problem SCOR was created to solve?

- a. The satellite hardware keeps failing on orbit without warning
- b. There are not enough detection rules written for the platform
- c. The three departments defend one platform but describe it differently
- d. The regulators require a dedicated cyber department by name

Q4 Context checkpoint

Day 1 starts by decomposing the telecommand path. Why that part of the platform first?

- a. It is the command-and-control path Executive Order 14144 and NIS2 bind
- b. It is the newest part of the platform, so it has no documentation yet
- c. It is the only part of the platform that flies on orbit
- d. It is the only path Satellite Operations does not already monitor

Q5 Context checkpoint

Which two regulatory mandates put the telecommand path in scope for Day 1?

- a. SPD-5 and the Outer Space Treaty of 1967
- b. ISO 27001 and the SOC 2 audit standard
- c. The Outer Space Treaty and the ITAR export rules
- d. Executive Order 14144 and the NIS2 Directive

Q6 Context checkpoint

How is the Space ISAC mandate scoped for SCOR?

- a. Share everything the SOC sees with Space ISAC members in real time
- b. It is scoped to the other two mandates: a detection and a redacted alert
- c. Space ISAC membership alone satisfies it, with no machine-to-machine channel
- d. It is scoped to pre-launch design reviews and nothing else

Data model checkpoint

Q7 Data model checkpoint

The data model you bring the three departments has two halves. Its taxonomy is:

- a. The controlled set of names: the shared names every element is given
- b. The rules for how the named elements relate to each other
- c. The catalogue of threats the Analytic layer records
- d. The per-instance descriptions the enumeration adds

Q8 Data model checkpoint

The second half of that model, the ontology, is:

- a. The controlled list of element names the taxonomy publishes
- b. The rules for how the named elements relate, the parent chain
- c. The enumeration procedure walked once for every element
- d. The catalogue of detection signatures the SOC will run

Q9 Data model checkpoint worked in the classroom

You decompose Kestrel Orbital's platform into elements across which four layers?

- a. TCP, IP, DNS, TLS
- b. People, Process, Technology
- c. PCE, SEG, SVC, AST
- d. Confidentiality, Integrity, Availability

Q10 Data model checkpoint

The four layers form a strict parent chain. Which layer is the root that every element you enumerate traces up to?

- a. AST (Asset), the concrete element layer
- b. SVC (Service), the delivered function layer
- c. SEG (Segment), the operational enclave layer
- d. PCE (Primary Capability Environment)

Q11 Data model checkpoint

Why does SCOR drive one shared data model across the three departments?

- a. So each department can audit the other two departments' work
- b. So each department can keep its own private naming scheme
- c. So all three departments describe the same platform the same way
- d. So the platform can be rebuilt from the model after an incident

PCE checkpoint

Q12 PCE checkpoint

What does the Primary Capability Environment (PCE) layer add that an inventory starting at the asset cannot give you?

- a. The operating environment, named as a first-class element
- b. The list of software vulnerabilities on the platform
- c. The enclaves the platform is distributed into, one per role
- d. The concrete assets that implement each named service

Q13 PCE checkpoint

Every SEG, SVC, and AST element links up to a PCE element. Why does that matter?

- a. So the environment can be patched like an asset
- b. So every downstream element inherits the same environment context automatically
- c. Because regulators require five layers
- d. So detections can fire at the environment layer instead of the asset layer

Q14 PCE checkpoint

Kestrel Orbital's Day-1 CONOPS populates how many of the five PCE environments, and which?

- a. All five
- b. One: Orbital only
- c. Two: Terrestrial and Orbital
- d. Three: Terrestrial, Aerial, and Orbital

Q15 PCE checkpoint

PCE records the environment, the where. What does it deliberately NOT name?

- a. The orbital regime the platform flies in
- b. The spacecraft and equipment operating there
- c. The atmospheric region the platform crosses
- d. The maritime domain a tracking vessel works in

Q16 PCE checkpoint

Why is contextualizing the environment a genuine innovation for space cyber defense?

- a. It reduces the number of elements you have to enumerate at all
- b. It moves detection work from the SOC to Satellite Operations
- c. The same hardware is attacked differently on the ground than on orbit
- d. Space platforms cannot be modeled at the asset layer at all

Segment checkpoint

Q17 Segment checkpoint

As you decompose the platform for the three departments, what does the Segment (SEG) layer name?

- a. The self-contained enclaves the platform is distributed into
- b. The orbital regime the platform flies in, the environment
- c. The concrete assets that implement each named service
- d. The function an enclave delivers to the wider platform

Q18 Segment checkpoint

For Kestrel Orbital's satellite-control scope, which three SEG TAGs do you enumerate (across its four SEG elements)?

- a. Launch, Aquatic, Deep Space
- b. Space, Link, Ground
- c. Space, Ground, User
- d. Launch, Link, Ground

Q19 Segment checkpoint

Every SEG element you enumerate links up to what?

- a. One or more PCE (environment) elements above it
- b. One or more SVC elements below it
- c. Nothing; SEG is the top layer
- d. The Analytic elements that reference it

Q20 Segment checkpoint

Why does naming the segment matter to the departments you are aligning?

- a. Regulators require segment names in every incident filing
- b. Adversaries pick an enclave, so naming it names what you defend
- c. It lets each department keep its own segment names locally
- d. It fixes which orbital regime the platform actually flies in

Q21 Segment checkpoint

How many segment types does the published taxonomy define, of which Kestrel's telecommand scope uses three TAGs across its 4 SEG elements?

- a. Four
- b. Six
- c. Ten
- d. Fifty-four

Service checkpoint

Q22 Service checkpoint

What does the Service (SVC) layer record for the three departments?

- a. The function an enclave delivers, what it actually does
- b. The physical hardware in a rack
- c. The orbit the platform flies in
- d. The enclave the platform is distributed into

Q23 Service checkpoint

The three SVC values you tag services with are:

- a. Hardware, Software, Firmware
- b. Control Plane, Data Plane, Hybrid
- c. Space, Link, Ground
- d. Read, Write, Execute

Q24 Service checkpoint

Command and Data Handling (C&DH) is which SVC value?

- a. Control Plane
- b. Data Plane
- c. Hybrid
- d. Signal

Q25 Service checkpoint

A service that spans more than one segment, like telecommand, is recorded how?

- a. As duplicate service elements, one per segment
- b. With DISTRIBUTED set to Y and every participating SEG listed in PARENT
- c. It anchors to the Ground segment alone as the controlling enclave
- d. With a SUBSYSTEM tag naming each segment it crosses

Q26 Service checkpoint

Why does the Security Operations Center write detection rules at the SVC layer?

- a. Because SVC elements carry the platform's IP addresses and ports
- b. So the rule fires on the function and survives a hardware refresh
- c. Because the segment layer is far too broad to alert against
- d. Because regulators require every rule to cite a named service

Asset checkpoint

Q27 Asset checkpoint

The Asset (AST) layer is where your three departments converge. What does it name?

- a. The concrete things that implement a service
- b. The operating environment the platform runs in
- c. The function an enclave delivers to the platform
- d. The enclaves the platform is distributed into

Q28 Asset checkpoint

The six AST values you tag assets with are:

- a. Control Plane, Data Plane, Hybrid, Space, Link, Ground
- b. Hardware, Firmware, Software, Data, Signal, Hybrid
- c. Read, Write, Execute, Delete, Modify, Own
- d. PCE, SEG, SVC, AST, AN, TEN

Q29 Asset checkpoint

Each AST element you enumerate links up to what?

- a. A PCE directly
- b. The Analytic elements that target it
- c. One or more SVC (service) parents
- d. Another asset

Q30 Asset checkpoint

Why is AST the layer where the work actually happens?

- a. It is the only layer the SOC can see in the telemetry feed
- b. Patching, monitoring and replacing act on assets, not on services
- c. It is the first layer the enumeration procedure visits
- d. It is the only layer that carries a description

Q31 Asset checkpoint

What optional tag can an AST element carry, and why?

- a. A DISTRIBUTED tag, because assets can span segments
- b. A PARENT tag, because PARENT is optional at this layer
- c. No optional tags are allowed at the asset layer
- d. A SUBSYSTEM tag, to group related sub-parts of one asset

Enumeration checkpoint

Q32 Enumeration checkpoint

The Day-1 deliverable is a CONOPS of how many elements, split how?

- a. 44 = 4 PCE + 4 SEG + 15 SVC + 21 AST
- b. 44 = 2 PCE + 4 SEG + 16 SVC + 22 AST
- c. 40 = 4 PCE + 4 SEG + 15 SVC + 17 AST
- d. 44 = 4 PCE + 2 SEG + 17 SVC + 21 AST

Q33 Enumeration checkpoint

An element that falls outside the scope the enumeration declared is:

- a. Enumerated with a SUBSYSTEM tag
- b. Enumerated but left without a parent
- c. Not enumerated
- d. Moved to the Analytic layer

Q34 Enumeration checkpoint

Telecommand spans the Space, Link, and Ground segments. How is that recorded on the service?

- a. Three duplicate SVC elements, one for each segment
- b. DISTRIBUTED set to Y, with every SEG listed in PARENT
- c. One SVC element anchored to the Ground segment only
- d. A SUBSYSTEM tag naming each segment it crosses

Q35 Enumeration checkpoint

Every parent chain you enumerate terminates at a PCE, because PCE is the root. What does that buy the departments?

- a. Any element named can be traced to a physical place and a jurisdiction
- b. It keeps the element count balanced across all four layers evenly
- c. It lets an asset be counted under more than one parent service
- d. It gives the Analytic layer a parent element to inherit from

Q36 Enumeration checkpoint

Which pair are both PCE elements in the Day-1 deliverable?

- a. The Reston site and the GEO regime
- b. The Ground segment and the Link segment
- c. Telecommand and C&DH
- d. The OBC and the OBDH bus

WORK EVERY QUESTION BEFORE YOU READ ON. THE ANSWERS BEGIN ON THE NEXT
PAGE.

KEY Answer Key

The answer with the reason it is the answer. If yours differs, trace which chapter rule it breaks before reading on.

Q1

a. SCOR, Space Cybersecurity Operations and Resilience You lead SCOR, Kestrel Orbital's new Space Cybersecurity Operations and Resilience department. Its mission is to evolve the existing departments toward resilient cyber operations; aligning them onto one shared data model is how it gets there.

Q2

b. Security Operations, Satellite Operations, and Satellite Design & Engineering SCOR's mission is to evolve these three departments toward resilient cyber operations. One shared description of the platform is the means: it lets enrichment cross their handoffs without re-translation.

Q3

c. The three departments defend one platform but describe it differently SCOR's mission is to evolve the three departments into one resilient cyber operation, able to anticipate, withstand, and recover from attacks together. With no centralized taxonomy, ontology, or enumeration process, each names the platform its own way, so a threat moving from the Link into the Ground segment is re-explained at every handoff and detection and recovery lag. The centralized taxonomy, ontology, and enumeration process are the means to that resilience.

Q4

a. It is the command-and-control path Executive Order 14144 and NIS2 bind The telecommand path runs from the operator console to the spacecraft. Executive Order 14144 imposes requirements Kestrel Orbital must meet on that command and control, encrypt the commands, guarantee their integrity, authenticate the source, and reject unauthorized commands, and the NIS2 Directive puts the ground-based infrastructure that carries it under mandatory risk-management and incident-reporting obligations. You decompose it first because that is where the obligations land and where you have to be able to show they are met.

Q5

d. Executive Order 14144 and the NIS2 Directive Executive Order 14144 in the United States sets requirements Kestrel Orbital must meet for protecting the command and control of the space system; the NIS2 Directive in Europe places the ground-based infrastructure that carries it under mandatory risk-management and incident-reporting obligations. Together they make the telecommand path a standing obligation, not a choice, which is why you decompose it first.

Q6

b. It is scoped to the other two mandates: a detection and a redacted alert Space ISAC sharing is not open-ended; it is scoped to serve the other two mandates. For Executive Order 14144, SCOR writes a detection for each command-and-control protection the order requires and shares a redacted alert on a confirmed attack. For the NIS2 Directive, SCOR shares incidents to the thresholds the directive sets. Sharing is targeted to the obligations, not everything the team sees.

Q7

a. The controlled set of names: the shared names every element is given The taxonomy is the words you give all three departments: one controlled set of names, so Security Operations, Satellite Operations, and Satellite Design & Engineering name the same part the same way.

Q8

b. The rules for how the named elements relate, the parent chain The ontology is the relationships: the four layers form a strict parent chain, so any element the departments name carries its full context up to the environment.

Q9

c. PCE, SEG, SVC, AST Primary Capability Environment (PCE), Segment (SEG), Service (SVC), and Asset (AST): the four layers you sort every part of the platform into.

Q10

d. PCE (Primary Capability Environment) PCE is the root; every SEG, SVC, and AST element links up to a PCE, so nothing you enumerate floats without its context.

Q11

c. So all three departments describe the same platform the same way

Adoption of one shared description is the mission. One shared data model is what lets enrichment cross the departments' handoffs without re-translation.

Q12

a. The operating environment, named as a first-class element PCE names the environment, the where, as the root of the parent chain. Most models start at the asset and never model the environment the platform operates in.

Q13

b. So every downstream element inherits the same environment context automatically

Parent anchoring means an asset resolves up through its service and segment to its environment, so every element carries its operating context for free.

Q14

c. Two: Terrestrial and Orbital The telecommand path spans the ground complex and the orbit, so Terrestrial and Orbital are enumerated, held as 4 PCE elements: Reston, Kiruna, GEO, and MEO. The other three environments stay reference.

Q15

b. The spacecraft and equipment operating there PCE names only the environment. The spacecraft and equipment that operate in it are named later at the Segment, Service, and Asset layers, keeping the where separate from the what.

Q16

c. The same hardware is attacked differently on the ground than on orbit

An element's threats, failure modes, and response options depend on where it operates. Naming the environment up front lets all three departments reason about that difference the same way.

Q17

a. The self-contained enclaves the platform is distributed into SEG names the enclaves, Space, Link, Ground, User and the rest, the parts an adversary picks to operate against and the parts your three departments defend.

Q18

b. Space, Link, Ground Kestrel's telecommand scope enumerates 4 SEG elements across three TAGs: Space (the bird), Link (the uplink and downlink), and Ground (two enclaves: the Reston command authority and the Kiruna TT&C station). The telecommand path runs Ground to Link to Space. User is a fourth segment type in the taxonomy, but the customer edge is out of scope for this platform, so it is not enumerated.

Q19

a. One or more PCE (environment) elements above it A segment is an enclave inside an environment, so each SEG names one or more PCE parents in the parent chain.

Q20

b. Adversaries pick an enclave, so naming it names what you defend Nobody attacks 'the satellite'. The Security Operations Center scopes a hunt to a segment, anything on the Link, and that shared boundary is the line all three departments defend.

Q21

c. Ten Ten segments are published (Launch, Link, Ground, User, Aquatic, Low Altitude, High Altitude, Near Space, Space, Deep Space); Kestrel's telecommand scope uses three (Space, Link, Ground) across 4 SEG elements, the Ground TAG holding the Reston and Kiruna enclaves, and teaches User as a segment type that is out of scope for this platform.

Q22

a. The function an enclave delivers, what it actually does Two enclaves tagged the same can do different jobs. SVC records the function so the departments can say what is actually at risk, not just which box is involved.

Q23

b. Control Plane, Data Plane, Hybrid Control Plane commands the platform, Data Plane moves mission product, and Hybrid does both.

Q24

c. Hybrid C&DH both commands the bus and routes mission data, so it is a Hybrid service.

Q25

b. With DISTRIBUTED set to Y and every participating SEG listed in PARENT

A cross-segment service stays one element: set DISTRIBUTED to Y and list every participating SEG in PARENT, as with the telecommand service.

Q26

b. So the rule fires on the function and survives a hardware refresh

Targeting the function, not the box, means the detection still fires after Satellite Design & Engineering swaps the hardware behind it.

Q27

a. The concrete things that implement a service AST is the concrete layer where the departments meet: the actual hardware, code, data, and signals a detection fires on and a patch lands on.

Q28

b. Hardware, Firmware, Software, Data, Signal, Hybrid Hardware, Firmware, Software, Data, Signal, and Hybrid are the six asset classes.

Q29

c. One or more SVC (service) parents An asset implements a service, so every AST names at least one SVC parent and its parent chain reads straight up through that service to the segment and the environment. Where one physical asset carries several services, it names all of them: the flight computer that runs command handling, attitude control and attack detection is one asset with three service parents, and an adversary who takes it takes all three.

Q30

b. Patching, monitoring and replacing act on assets, not on services

Satellite Design & Engineering does not patch 'the control plane'; they patch a specific firmware image on a specific box. A detection fires and a patch lands at AST resolution, where all three departments converge.

Q31

d. A SUBSYSTEM tag, to group related sub-parts of one asset An AST element takes one or more SVC parents and an optional SUBSYSTEM tag that groups related assets, like the star trackers, sun sensors, and gyros inside the ADCS sensor suite.

Q32

a. 44 = 4 PCE + 4 SEG + 15 SVC + 21 AST The telecommand-path CONOPS holds 44 elements: 4 environments, 4 segments, 15 services, and 21 assets, every parent link populated below the root.

Q33

c. Not enumerated The scope constraint is absolute: an element outside the Step 01 scope is not enumerated. The User segment type is the worked example, real in the taxonomy, out of scope on this platform.

Q34

b. DISTRIBUTED set to Y, with every SEG listed in PARENT A service that spans segments stays one element: DISTRIBUTED Y, with each participating segment listed as a parent, never duplicates.

Q35

a. Any element named can be traced to a physical place and a jurisdiction A root is what makes the parent chain terminate, and a chain that terminates somewhere physical is what lets three departments argue about the same thing. Name any asset and you can walk up to the site or the orbit regime it lives in, which is what pins the regulator, the owner and the environment to it. The other three are real ideas in the wrong place: layer counts are never balanced and are not meant to be; shared assets are a cardinality rule, not a root rule; and the Analytic layer has no parent at all, it anchors through a target field instead.

Q36

a. The Reston site and the GEO regime The four PCE elements are the Reston and Kiruna terrestrial sites plus the GEO and MEO orbital regimes; segments, services, and assets live in the lower layers.