Dirt to Data

- Where is your data?
- Who has access to it?
- Is it being watched?


75

Westley McDuffie

Security Evangelist
IBM X-FORCE
wpmcduff@us.ibm.com

Before the Internet: Data Has Always Been in Play

- Roman Empire – Sealed wax tablets, encrypted scrolls, guarded couriers
- WWII – Operation Mincemeat – Deception with physical data planted on a corpse


FIFTEENTH
KOLN
(COLOGNE)
XXX
XII
XIII
NINTH
XIX
XVI
VII
V
FIRST
NINTH
XXXX
FIRST
LXXXI
GDS
176
183
15
10 SS
9
340
2 SS
363
9 SS?
246
3
47
12
3
353
344
12 SS?
89
155
272
326
49?
84
102
2
29
30
104
9
83
3
5
8
78
1
7
43
Hasselt
Bilsen
Tongres
Waremme
Liége
Seraing
Herstal
Herve
Limbourg
Dison
Theux
Huy
St. Georges
Monschau
Schleiden
Euskirchen
Münstereifel
Erkelenz
Odenkirchen
Grevenbroich
Heinsberg
Hongen
Julich
Aachen
(Aix la Chapelle)
Eupen
Albert
Demer
Geer
Geleen
Vesdre
Amblève
Meuse
Peer
Bree
Mechelen
Maastricht
St. Trond


RUSSIA
BLACK SEA
GEORGIA
ARMENIA
AZERBAIJAN
CASPIAN SEA
TURKEY
MEDITERRANEAN SEA
LATUFF 2008


UKRAINE
RUSSI

Modern APTs: The New Threat Actors, Same Old Objective

- APT29 (Russia) – Targets U.S. federal & defense orgs
- APT40 (China) – Naval and supply chain espionage
- Lazarus Group (North Korea) – Financial and psychological disruption

Stand by for the next phase of operations.

QUESTIONS

CONCERNS

COMPLAINTS

OAKOC: Framing the Battlespace

- O – Obstacles
- A – Avenues of Approach
- K – Key Terrain
- O – Observation and Fields of Fire
- C – Cover and Concealment

O – Kinetic: Obstacles

- Natural: rivers, cliffs, swamps
- Man-made: mines, wire, barriers
- Obstacles shape movement, block access, or channel engagement

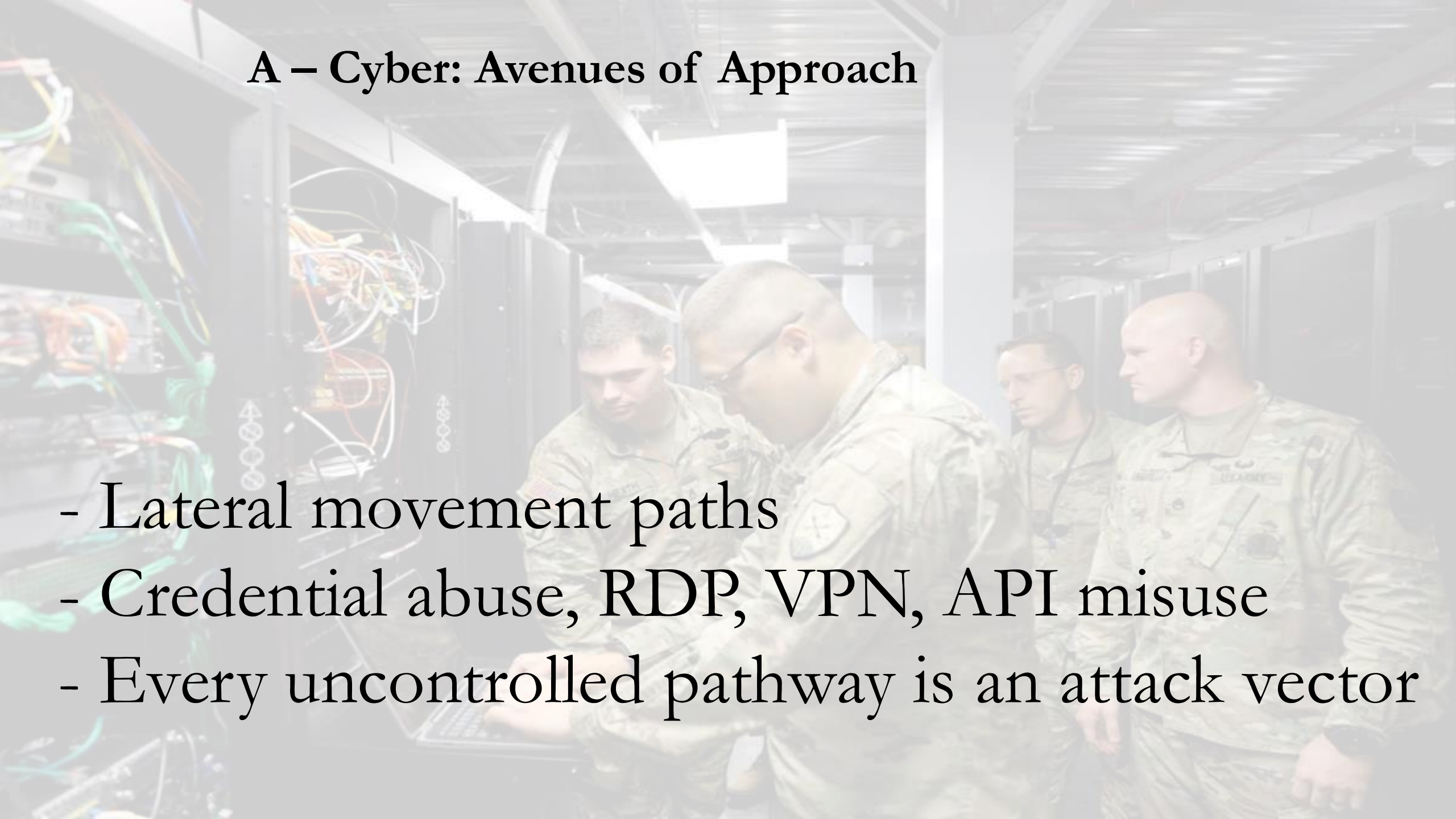
O – Cyber: Obstacles

- Firewalls, ACLs, segmentation, encryption
- Controls that limit movement or deny access
- Shape, restrict, or expose adversary maneuver inside the perimeter

A – Kinetic: Avenues of Approach

- Ground, air, sea routes for enemy/friendly movement
- Enable maneuver toward objectives
- Shape timing, surprise, and tempo

A – Cyber: Avenues of Approach

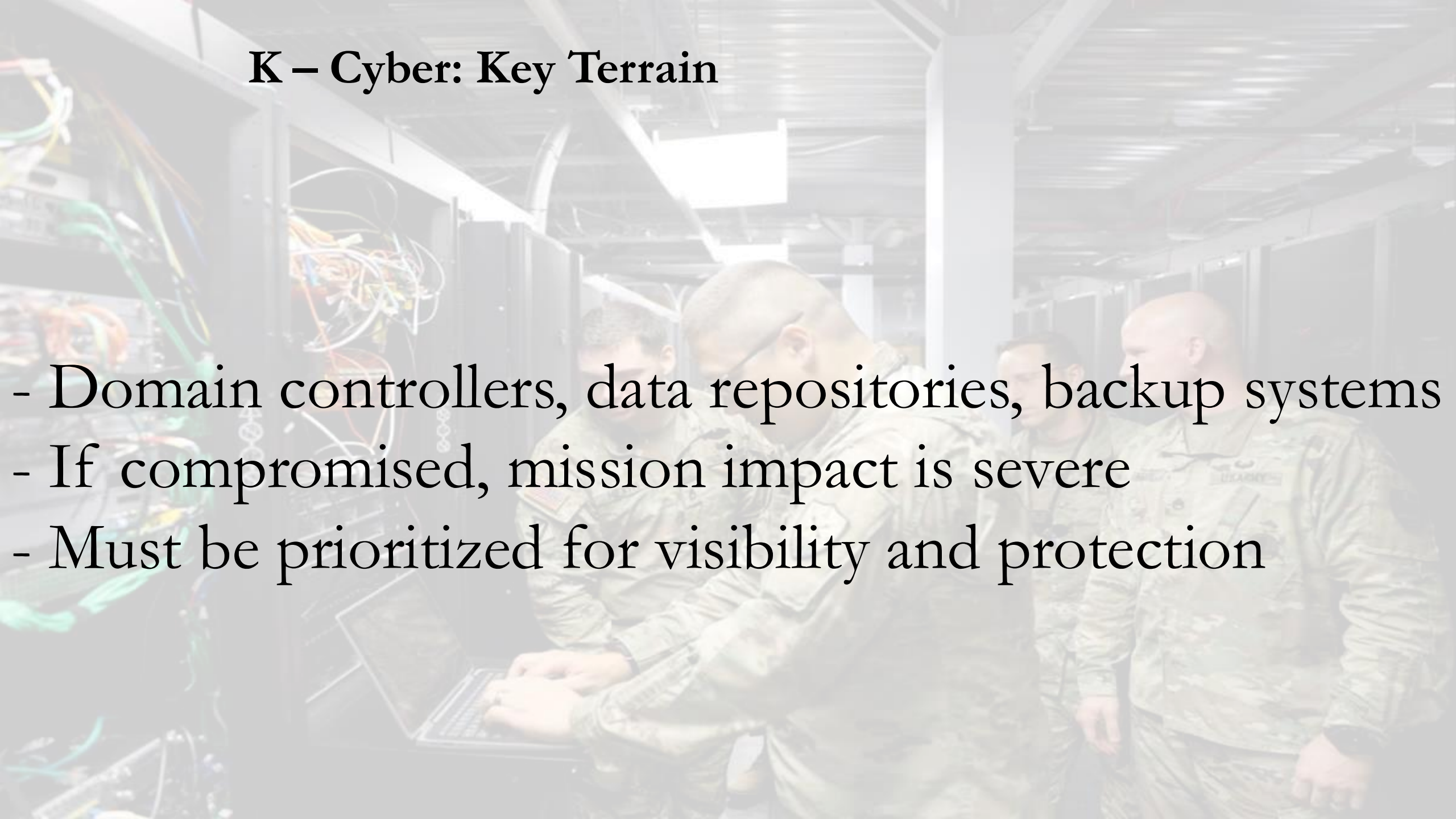


- Lateral movement paths
- Credential abuse, RDP, VPN, API misuse
- Every uncontrolled pathway is an attack vector

K – Kinetic: Key Terrain

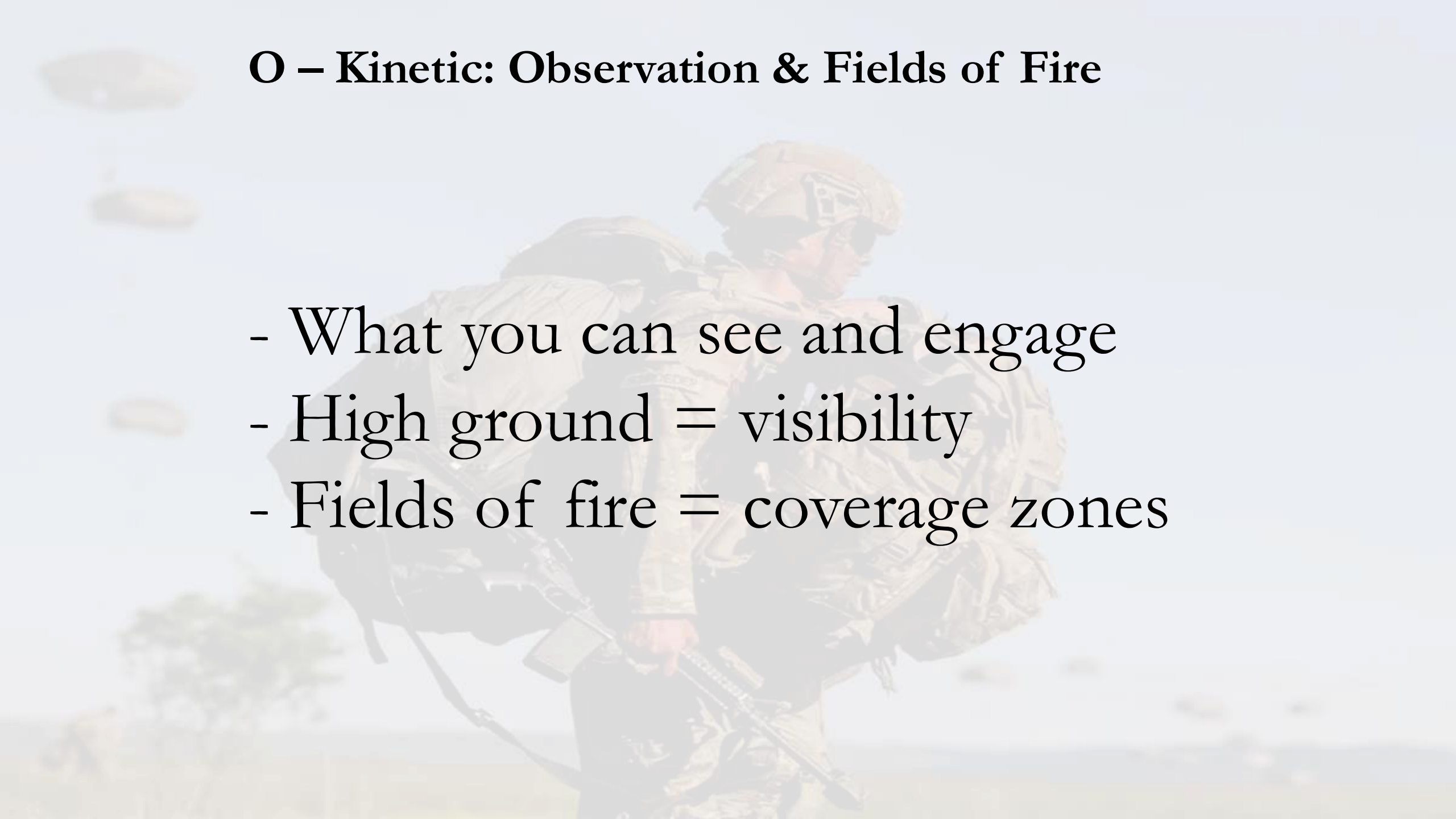
- Any position offering tactical or strategic advantage
- Control influences mission success
- Often tied to visibility, mobility, or logistics

K – Cyber: Key Terrain



- Domain controllers, data repositories, backup systems
- If compromised, mission impact is severe
- Must be prioritized for visibility and protection

O – Kinetic: Observation & Fields of Fire

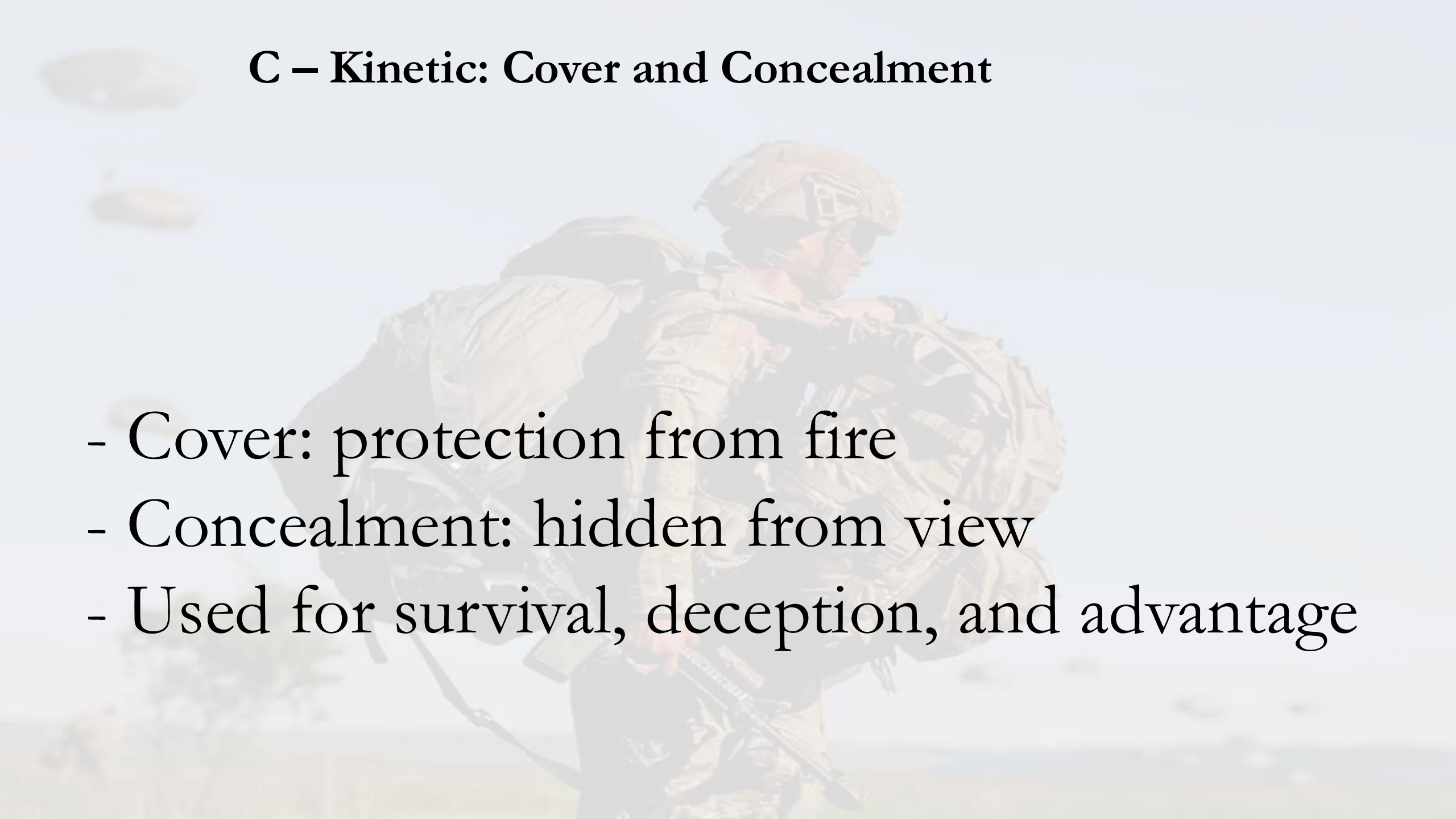


- What you can see and engage
- High ground = visibility
- Fields of fire = coverage zones

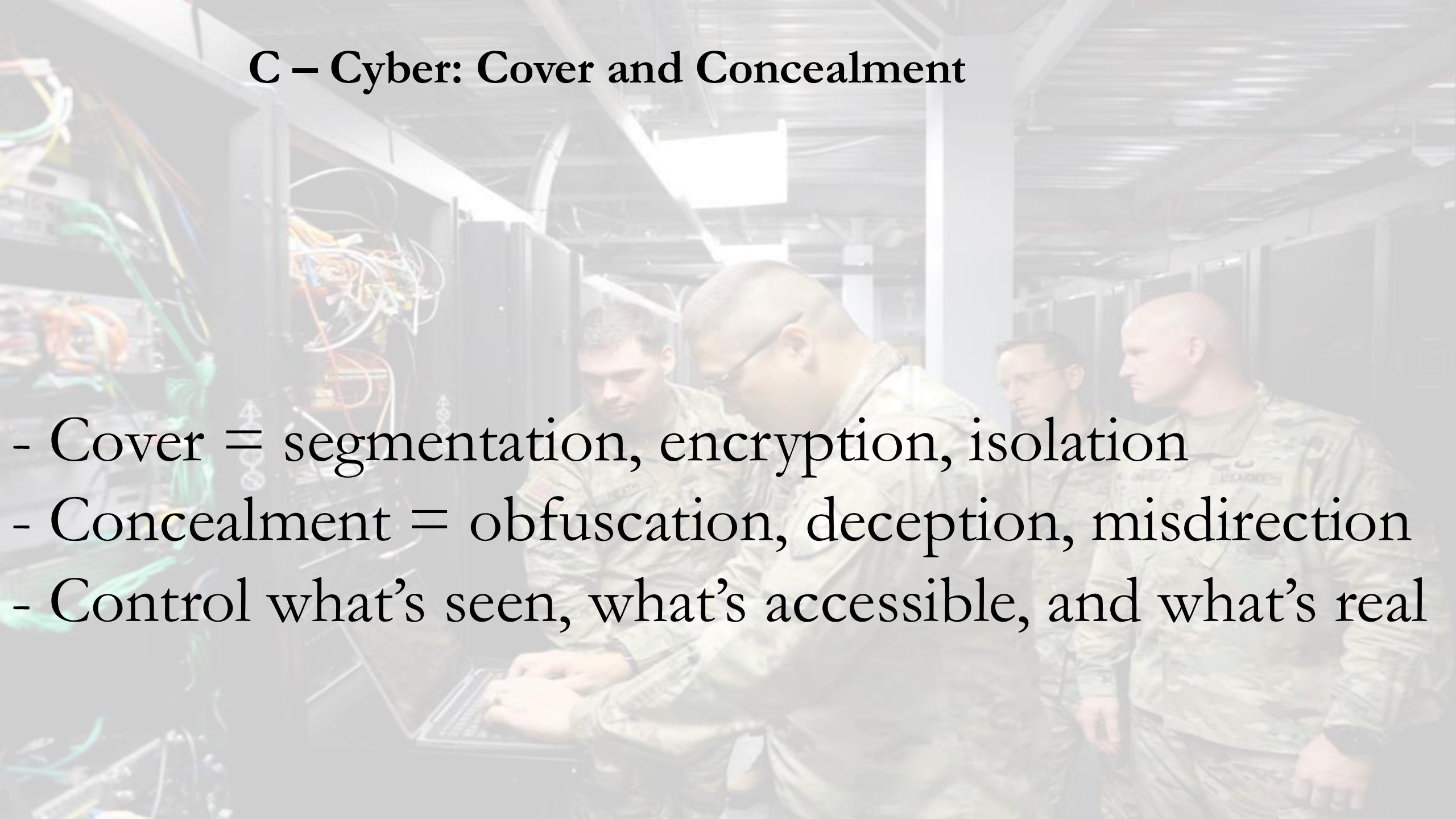
O – Cyber: Observation & Fields of Fire

- Logs, telemetry, behavioral analytics
- Visibility = observability
- Fields of fire = response capability

C – Kinetic: Cover and Concealment



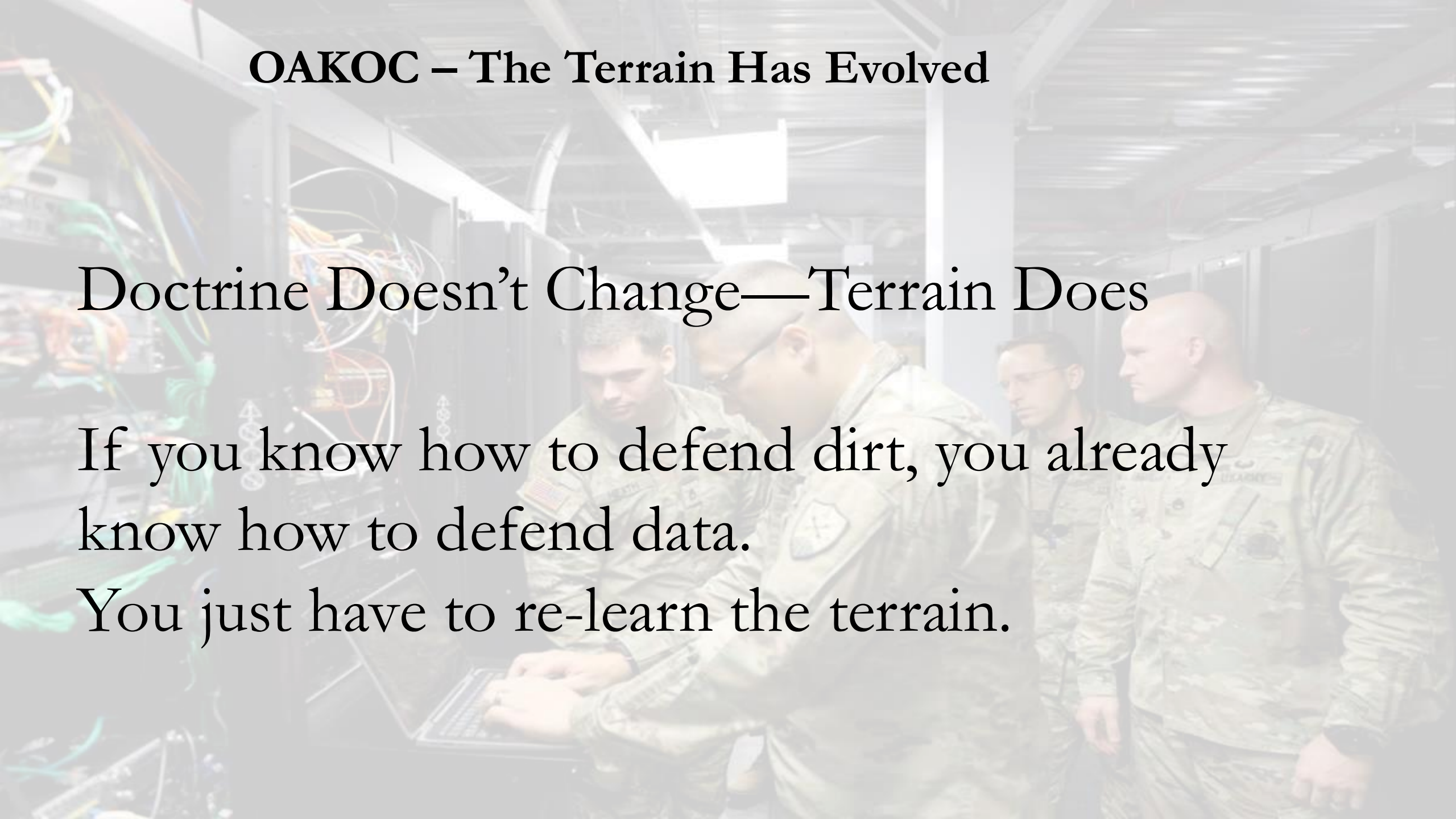
- Cover: protection from fire
- Concealment: hidden from view
- Used for survival, deception, and advantage



C – Cyber: Cover and Concealment

- Cover = segmentation, encryption, isolation
- Concealment = obfuscation, deception, misdirection
- Control what's seen, what's accessible, and what's real

OAKOC – The Terrain Has Evolved



Doctrine Doesn't Change—Terrain Does

If you know how to defend dirt, you already know how to defend data.
You just have to re-learn the terrain.

Stand by for the next phase of operations.

QUESTIONS

CONCERNS

COMPLAINTS

4.1 – Data Catalog Risk Alignment

Step 1: Map the Terrain Before You Fight On It

- Discover, catalog, and tag critical data
- Assess risk to exposure, loss, manipulation
- Establish a data baseline and track movement

4.2 – Enterprise Data Governance

Step 2: Establish Control of the Terrain

- Label and tag data for machine-enforceable policies
- Implement just-enough and just-in-time access
- Define rulesets and enforce through centralized control

4.3 – Data Labeling & Tagging

Step 3: Enable Machine-Speed Decision Making

- Enforce labels and tags based on policy
- Prioritize mission-critical assets
- Automate for scale and consistency

4.4 – Data Monitoring & Sensing

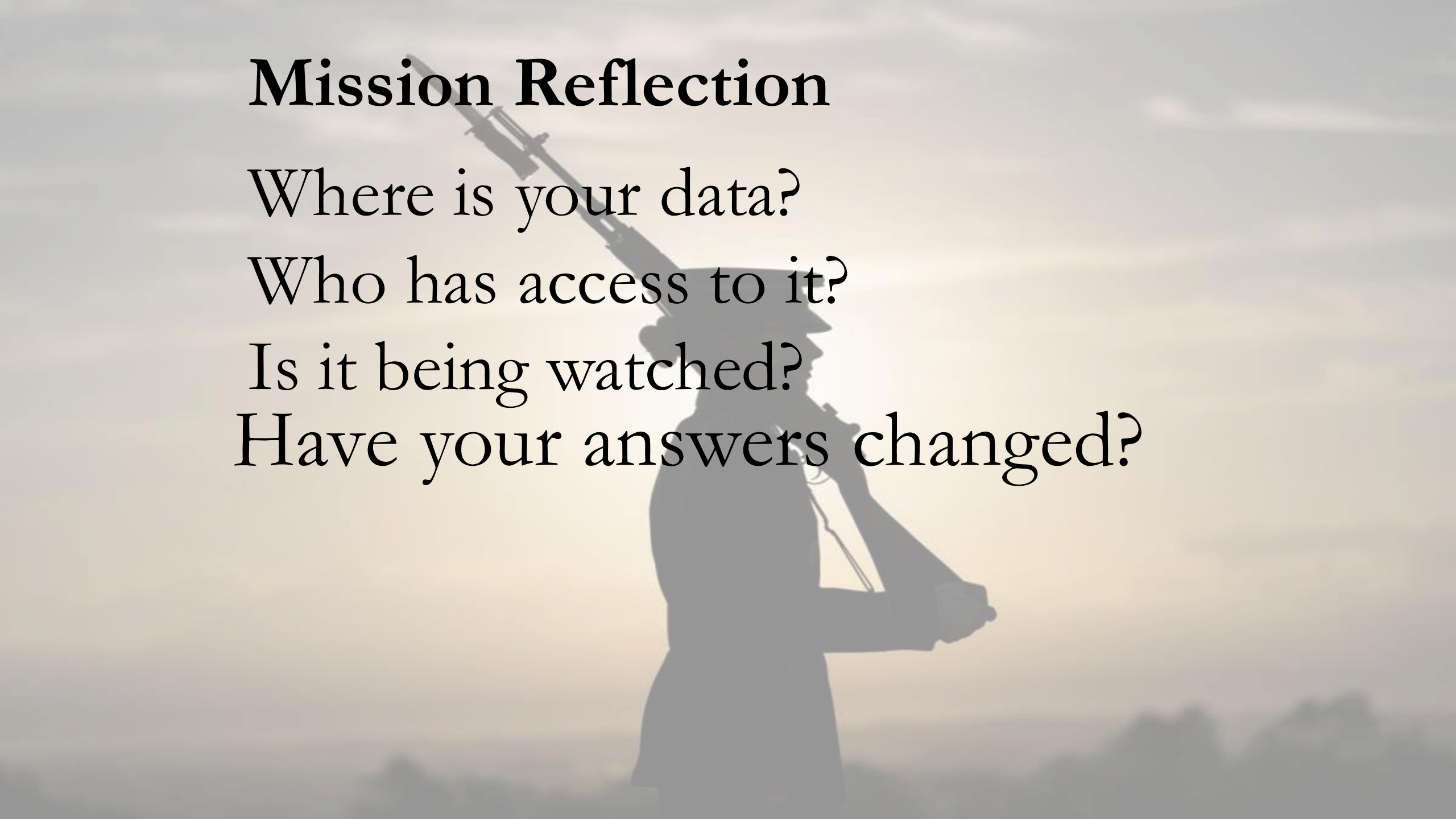
Step 4: ISR for the Data Battlespace

- Make all sensitive data observable
- Send logs to SIEM, DLP, and threat engines
- Monitor for abnormal movement, access, and use

4.5 – Data Encryption, Rights Management, & DLP

Step 5:Deny the Enemy Use of the Terrain

- Encrypt at rest and in transit
- Enforce DRM controls outside enterprise systems
- Use DLP to detect and stop exfiltration or misuse



Mission Reflection

Where is your data?

Who has access to it?

Is it being watched?

Have your answers changed?