Mindset Over Mayhem:



Battlefield Psychology for Cyber Leaders

Translate the emotional reality of combat into the psychological and operational reality of a cyber breach - without theatrics, without exaggeration, but with precision.

The audience doesn't need to feel like soldiers; they need to recognise that pressure behaves the same way in every domain, and that disciplined thinking is transferable.



1. Set the Context: "Different Battlefield, Same Brain"

Purpose:
Establish psychological equivalence between combat stress and cybercrisis stress.

Key moves:
Explain that while the environments differ, the human stress response is identical: adrenaline spikes, cognitive narrowing, emotional reactivity, and time pressure distort judgment.

Draw a parallel between:
Incoming fire > incoming threat intelligence
Fog of war > fog of incomplete data during a breach
Collateral risk > business continuity, customer trust, regulatory exposure

Position the talk as a translation exercise: ***"What we learned under fire becomes a tool kit for when your network is under attack."***

2. Introduce the Stress Response and Self Regulation Techniques

Purpose:
Give the audience practical tools to stabilise themselves before they stabilise the situation.

Combat example:
Moments from the helmet cam footage where breathing, micro pauses, or cognitive resets prevented panic.

Cyber equivalent:
A CISO or crisis team receiving alerts of a live breach-pressure spikes, decisions accelerate, and the temptation is to act before thinking.

Techniques to teach:
Physiological control: Tactical breathing, grounding, and micro pauses to widen cognitive bandwidth.

Cognitive re-framing:
Shifting from “catastrophe” to “controllables.”

Emotional detachment:
Separating identity from outcome to reduce ego driven decisions.

Tempo management:
Knowing when to slow down to speed up.

These become the foundation for decision making under cyber pressure.



3. Apply the National Decision Model (NDM) to Cyber Incidents

Purpose:
Show that the NDM is not a military tool-it's a universal decision logic.
Structure the section around the NDM's core elements:

1. Code of Ethics / Values
In combat: protection of life, mission integrity, proportionality.
In cyber: protect customers, maintain trust, uphold transparency, minimise harm.

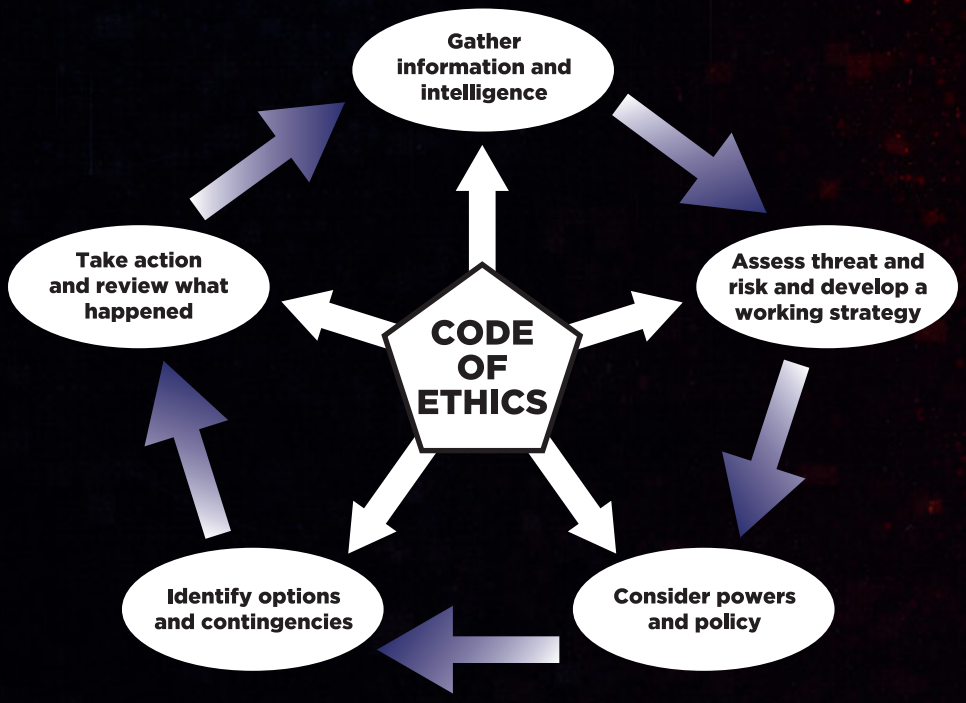
2. Gather Information & Intelligence
Combat: terrain, enemy movement, friendly positions.
Cyber: threat indicators, system logs, attack vectors, business impact.

3. Assess Threat & Risk
Combat: enemy capability vs. intent.
Cyber: attacker sophistication, lateral movement, data exposure.

4. Consider Powers & Policy
Combat: rules of engagement.
Cyber: regulatory obligations, incident response play books, legal constraints.

5. Identify Options & Contingencies
Combat: manoeuvre, withdraw, call support.
Cyber: isolate systems, shut down access, communicate internally, engage external experts.

6. Take Action & Review
Combat: execute, adapt, reassess.
Cyber: implement containment, monitor, adjust, post incident review.



Message:
"The NDM gives you a calm, values anchored structure when the situation tries to drag you into chaos."

4. Use the Helmet Cam Footage as a Mirror, Not a Movie

Purpose:
Make the footage a metaphor for cyber leadership, not a spectacle.

How to frame it:
Highlight moments where the team had incomplete information, conflicting priorities, or rapidly evolving threats.

After each clip, ask: ***"What is the cyber equivalent of this moment?"***

Draw out themes such as:

Rapid threat escalation

Communication under pressure

Trust in training and process

Maintaining situational awareness

Avoiding tunnel vision

This creates emotional resonance without forcing a false equivalence.





Battle Front Helmet Cam Footage







5. Translate Battlefield Leadership Behaviours into Cyber Crisis Behaviours

Purpose:
Give the audience a behavioural model they can adopt immediately.

Battlefield Behaviours	>	Cyber Crisis Behaviours
Distributed decision authority		Empower SMEs, avoid bottlenecks
Situational awareness		Real-time dashboards, threat intel, cross team updates
Prioritisation under fire		Protect crown jewel assets first
Calm command presence		Emotional contagion works both ways
Debrief culture		Blameless post incident reviews

6. Build a “Cyber Crisis Mindset”

Purpose:
Shift the audience from reactive to proactive thinking.

Key principles:

Assume breach the way soldiers assume contact.

Train for chaos so the first time you experience it isn’t the real thing.

Rehearse decision making, not just technical response.

Normalise stress - it’s not a failure of professionalism; it’s biology.

Use values as your compass when information is incomplete.



7. Close with a Transferable Tool kit

Purpose:
Leave the audience with a practical, memorable set of tools.

Suggested tool kit:
A 3 step self regulation drill for the first 60 seconds of a crisis.

A NDM based cyber decision card (values > info > risk > options > action).

A battlefield inspired communication protocol (short, clear, factual).

A post incident reflection model based on military debriefs.









Stuart Barker

Stuart graduated from the University of Oxford and attended the Royal Military Academy Sandhurst where he was commissioned as an Infantry Officer.

During a thirty-year career he worked within the military and intelligence sectors delivering operational outcomes in senior leadership roles.

As a soldier, Stuart has commanded soldiers on operations across the world. Operational service during The Gulf War and in Afghanistan developed his leadership and experience in delivering outcomes in high-intensity environments. As a trained mentor, he frequently worked overseas where he led teams that mentored and deployed alongside allied partners on operations. Within the intelligence community Stuart worked primarily within the covert operations arena where he has planned and commanded high-risk covert missions across the globe.

Having retired from public service Stuart now works as a director of a logistics company where he is responsible for all operational activities. He is also the founder and Director of Dark Blue Consultancy Limited which specialises in providing leadership training to senior managers working in the intelligence and security sectors.







SPEAKER OF THE YEAR 2025

My Sherpa
IN GREAT COMPANY
Manger Programme