Tactical Leadership

Capt Jeremy Sparks

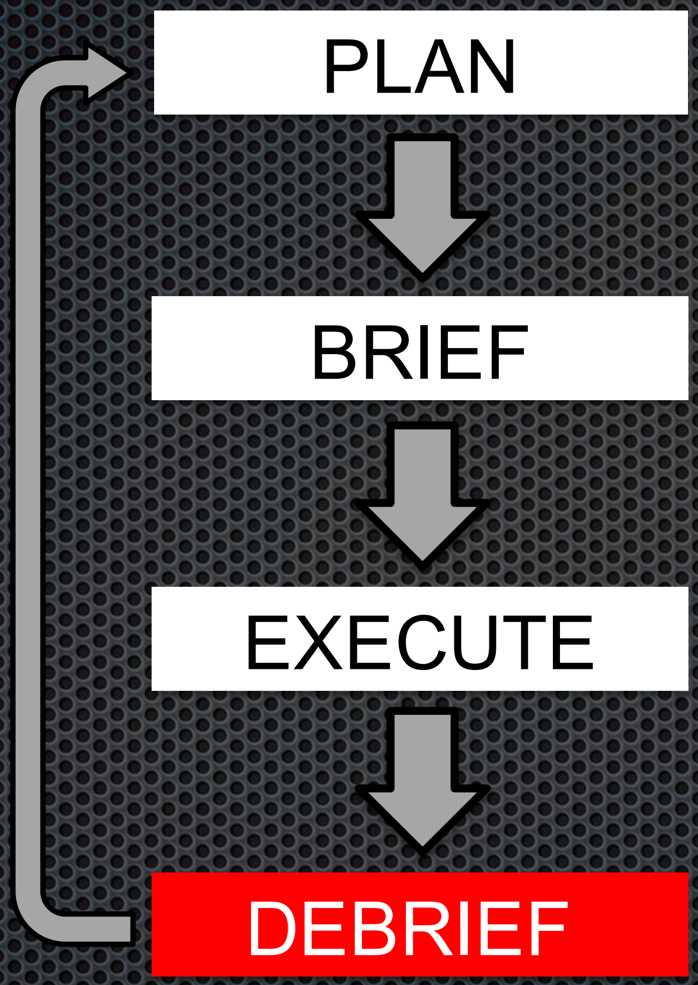
Intro

- A Buckeye
- Six years in the OANG
- Work Experiences
    - APT intrusions
    - Insiders
    - DDoS
    - Outages (Network & Weather)
    - IT upgrades
- USAFWS

Problem Statement

- Scale of network & threats plus:
    - Lack of focused CWO leadership training
    - **Critical** self-analysis missing in our community
    - **NO** IT silver bullets and **NO** new resources…
- Scope of the solution
    - Not my idea… by operators for operators
- Solution and Results
    - ORBs/Misfires/OODA

The Basic Principle



PLAN

BRIEF

EXECUTE

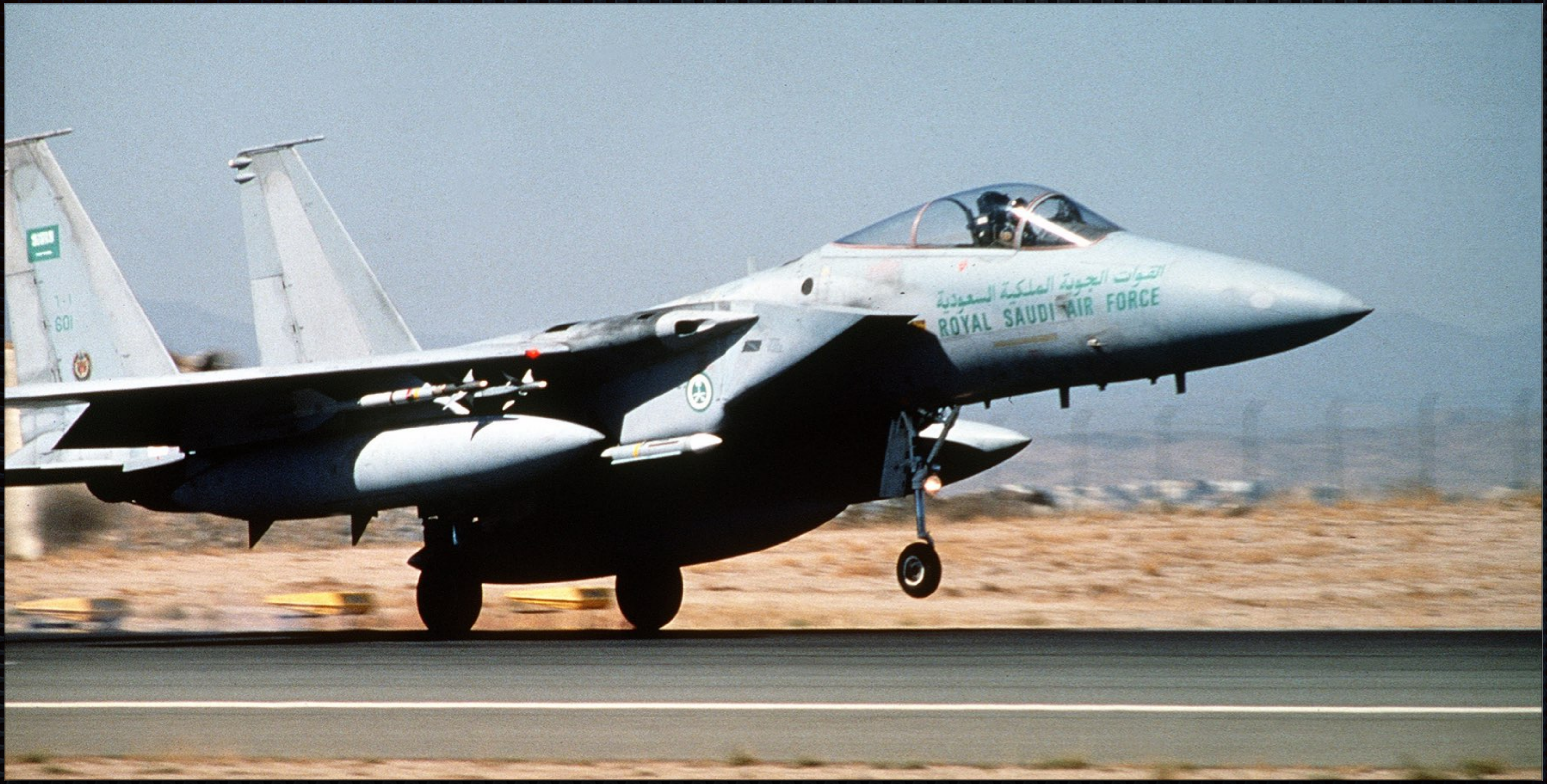
DEBRIEF

Endstate
Outline of the effort / mission

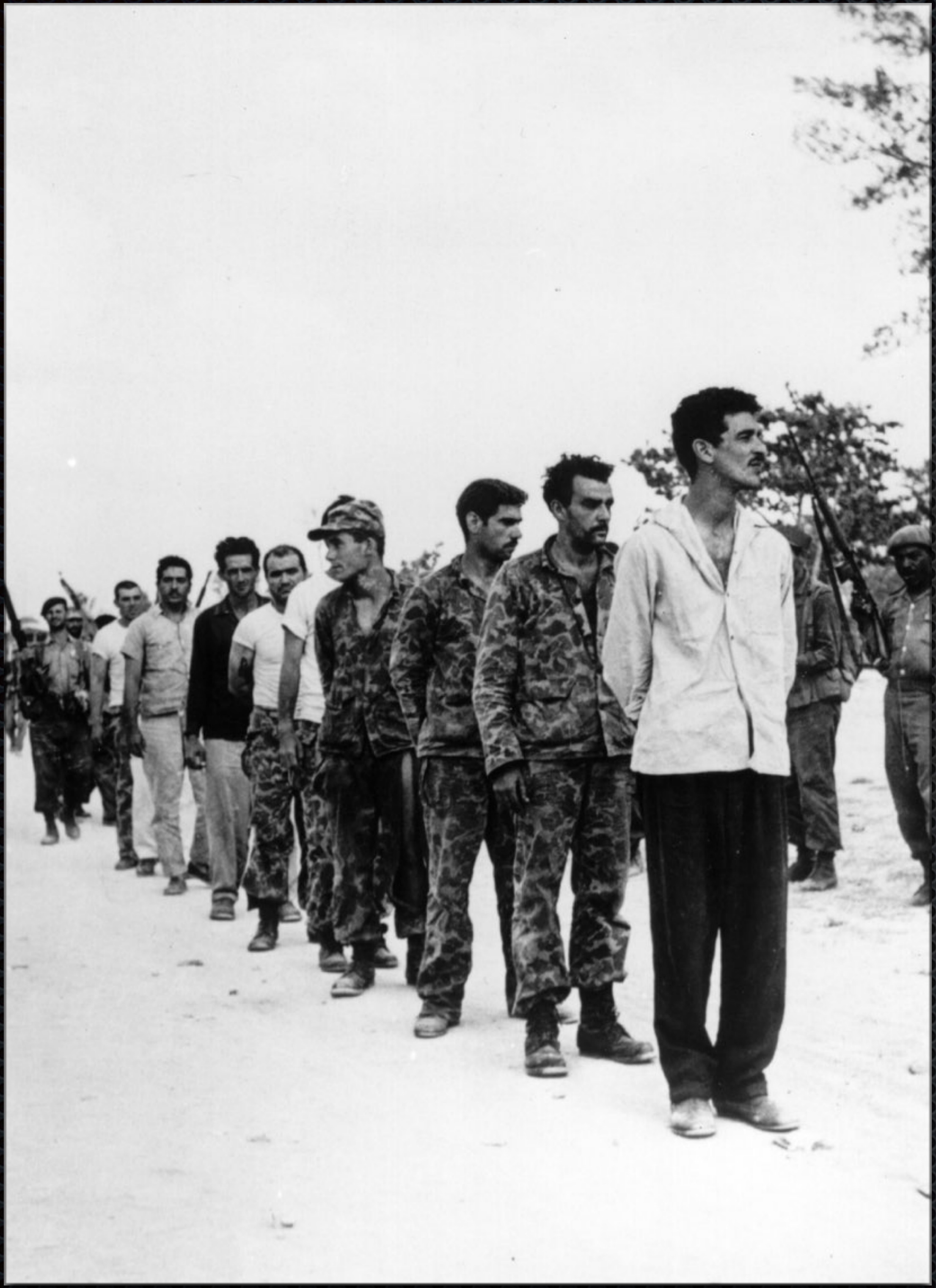
Endstate
All team members understand the plan

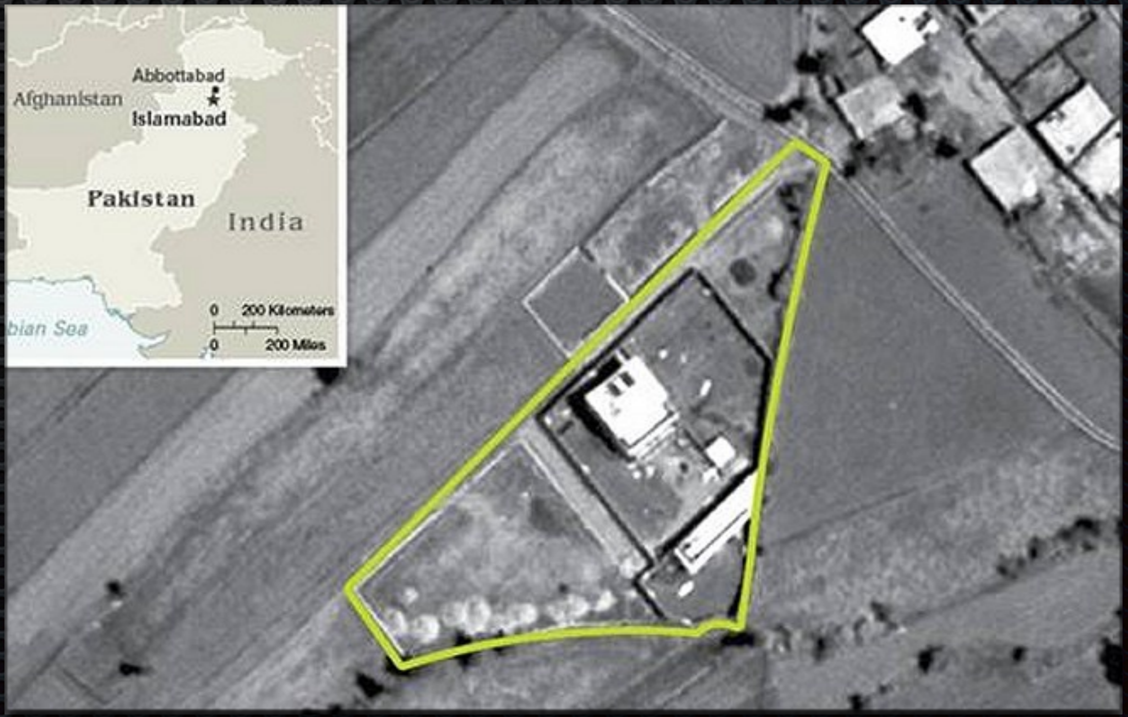
Endstate
All expected tasks completed

Endstate
Lesson Learned / Best Practices identified



Recognize this Fourth Gen Fighter?





Successful Missions are Debriefed Too!

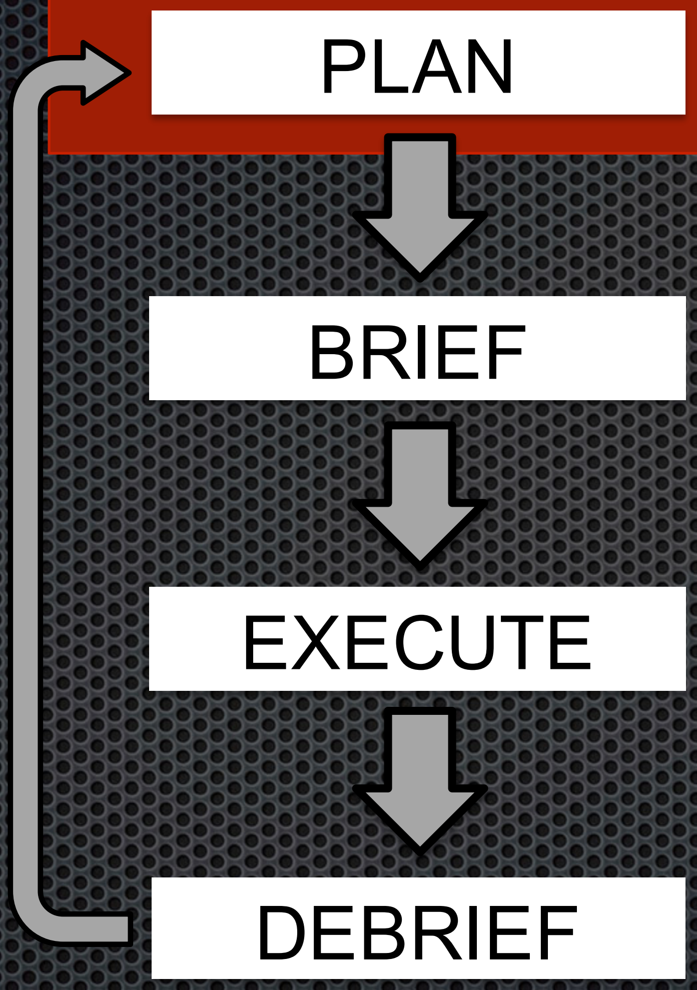
Mission

NASA

Formula 1

GE

<u>Plan</u>, Brief, Execute, Debrief



PLAN

<u>Endstate</u>
Outline of the effort / mission

BRIEF

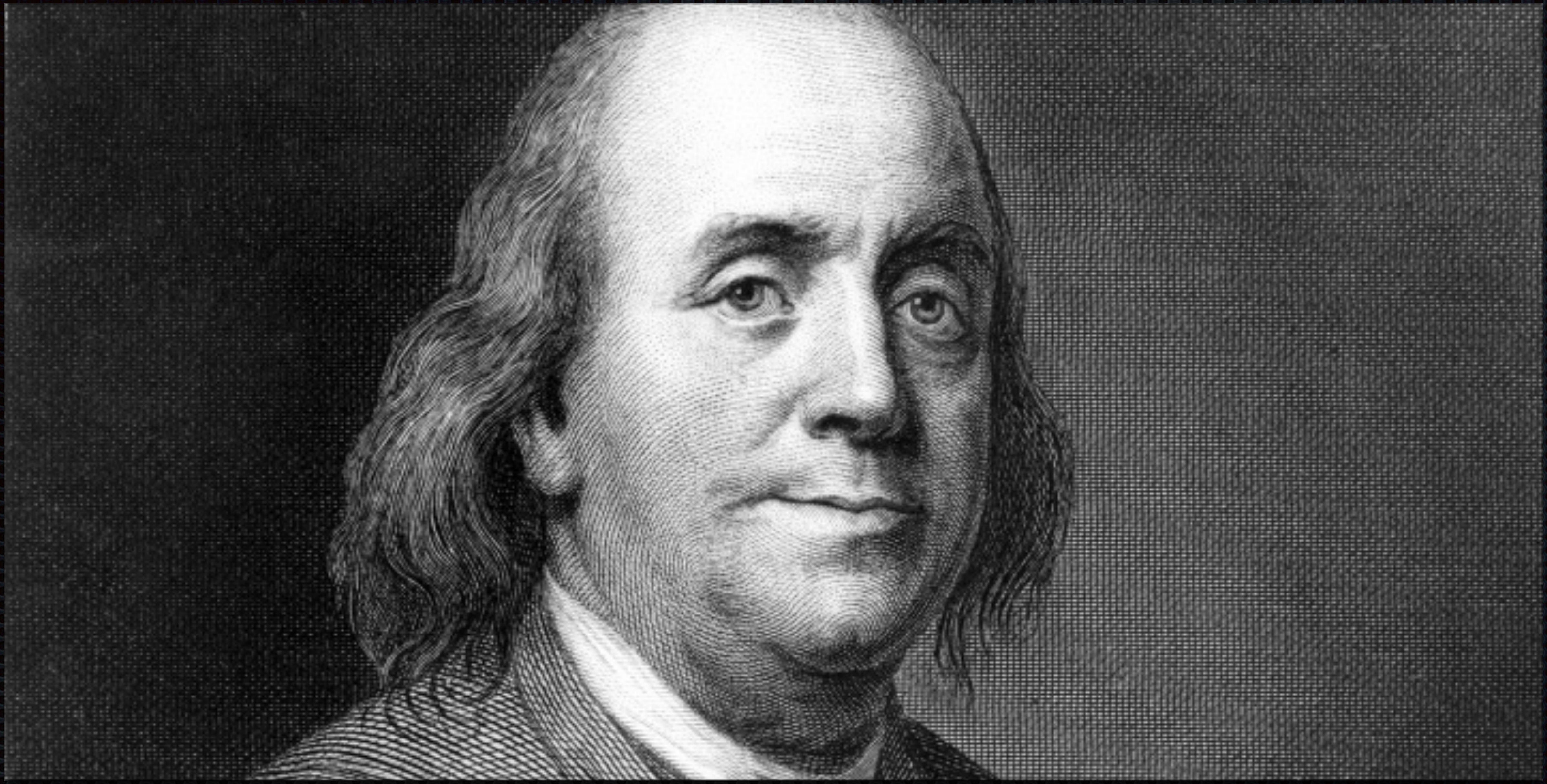
<u>Endstate</u>
All team members understand the plan

EXECUTE

<u>Endstate</u>
All expected tasks completed

DEBRIEF

<u>Endstate</u>
Lesson Learned / Best Practices identified

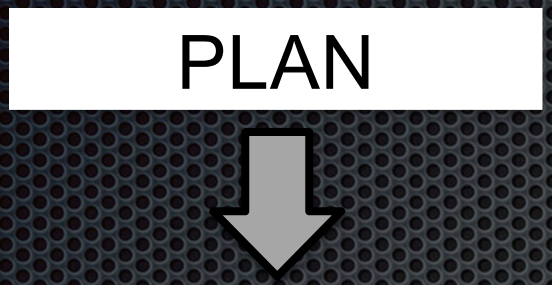


“If you fail to plan, you are planning to fail.”
Benjamin Franklin

Planning

- Good leaders are good planners
- Problem: Most people feel very uncomfortable as planners
- We discovered that it is best to have a structured planning format
  - Keeps it standardized
  - Becomes muscle memory
- SUCCESS = Everyone on your team is comfortable with planning
- Military method

Lead the planning effort/team



PLAN

Endstate

Complete Outline of the effort / mission

- Mission
- Enemy
- Environment
- Effects
- Capabilities
- Plans / Phases
- Contingencies
- Communications

If the plan sucks, you can only blame yourself

Example Plan

Spoiler Alert

MPC Objectives

Specified Objectives

- Develop SCAR mission plan for network X against enemy Y

Implied Objectives

- Develop Coord card
- Coord with NOS
- Coord with 624 OC

Mission Objectives

Specified Objectives

- Mission Assurance of compromised network
- F2T2EA Enemy Activity

Implied Objectives

- Limit network impact
- Limit kinetic mission impact

MPC Timeline

1800L - Initial Order Breakout
1830L - Prior to Initial Coord
2000L - Initial Coord Meeting
2100L - Comm Plan Dev
2200L - Contract Dev
0000L - Contingency Dev
0300L - Coord Card Dev
0345L - ROC Drill Script Dev
0400L - Brief Dev
0500L - MPC stop

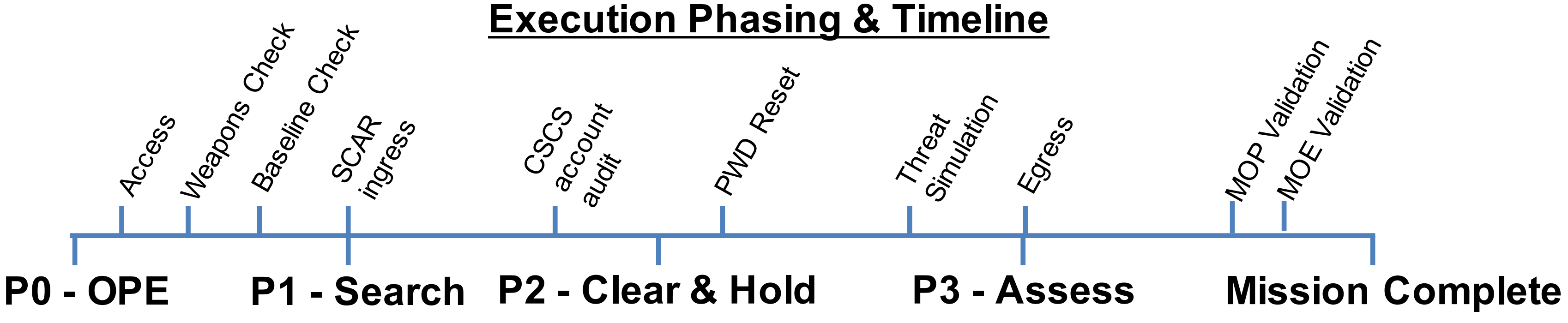
MPC Milestones

- □ Order Breakout
- □ ME3C-(PC)^2 Tactical Plan
- □ Coord Card
- □ ROC Drill Script
- □ Group Review
- □ Develop Mass Brief

Leadership Positions

MPCC: Capt Smith
MSN/CC: Capt Smith
DMPCC: N/A
Time-Keeper: SSgt Black
Scribe: Lt McDaniel
Intel Support: SrA Dundee

Execution Phasing & Timeline



Planning Workspace

Mission

Intent: Protect AF network and enable CSAR mission

Tactical End-state: AF network resources available for warfighting and free of APT

Facts: Enemy

Assumptions: Enemy intends to create a CDO environment

Constraints (must do): Notify CCO of compromises

Restraints (must not do): Take server X offline before or during CSAR mission

Environment

Targets: APT IPs & known IOCs

Terrain: AF subnet X & enclave Y

Impact Concerns

- Mission impact

Enemy

Actor: ROCKSTAR BUCKEYE

MD: ROCKSTAR BUCKEYE uses known capes IOT disrupt recovery mission

ML: FIS Espionage

Intel Gaps: Enemy intent

Enemy Ops Rhythm: Unknown

Effects

Deny lateral movement
Remove APT presence
MOE: CSAR mission
MOE: APT re-attempts access
MOE: Threat Emulation failure
MOP: 100% uptime for required net
MOP: 100% of known IOCs serviced

Capabilities

Operational Rhythm:

- SOC to perform continuous monitoring
- CERT to perform IR
- Hunt Team to pro-actively look for adversary IOCs
- IT Dept. to audit & reset passwords

Capes/Lims: Standard Corporate Toolset

Dependencies: Access

Plan

Execution Battle Rhythm

- **Phase 0: OPE**
  - Actions
    - Accesses enabled / confirmed
    - Weapon System / Cape checks
    - Confirm Known Baselines
  - Triggers
    - WS Checks & Baselines MC
- **Phase 1: Search**
  - Actions
    - SCAR forces execute SCAR plan
    - CSCS audit all accounts
  - Triggers
    - APT Detected
- **Phase 2: Clear & Hold**
  - Actions
    - Strike actions
    - Perform initial assessment
  - Triggers
    - Strike and initial assessment actions complete
- **Phase 3: Assessment / Egress**
  - Actions
    - MOPs & MOEs validated

Contingencies

Failed Assumptions
Major event failures (access, lock-outs)

Classification

Brief:
Facility:

RFI's

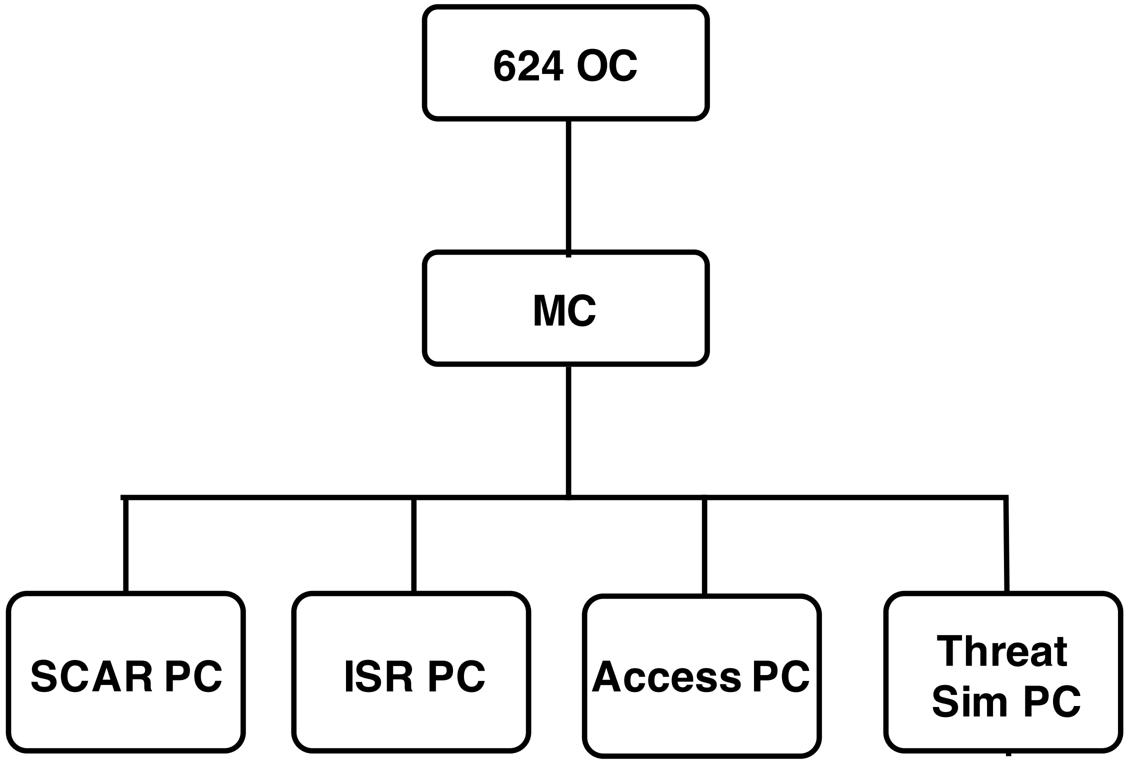
- Red order of battle
- Available mission partners
- Typical server utilization?
- CSAR comm minimize plan?
- Attribution
- Min services required for CSAR mission?
- What ports does the CSAR chat server use?
- LE/CI POC info?

Parking Lot

ROC DRILL Timeline

- Access granted
- APT detected
- Compromised account ID’d
- Password reset initiated
- Access lost
- Services drop
- mIRC Server Crash
- Weapons System “BENT”/”SICK”
- Threat Sim success/failure
- CSAR mission ROLEX

C2



Specific / Anticipated Communications

# Criteria	Authority	Communications	Action
1. Comp PWD	Access PC	“PWD X locked out”	IOC added
2. Access RQ’d	SCAR PC	“Access - IP X”	Access PC confirms
3.			
4.			

Comm Plan

Pri/Sec/Ter Comms

- Trigger points & procedures to transition to backup Comms

Brevity

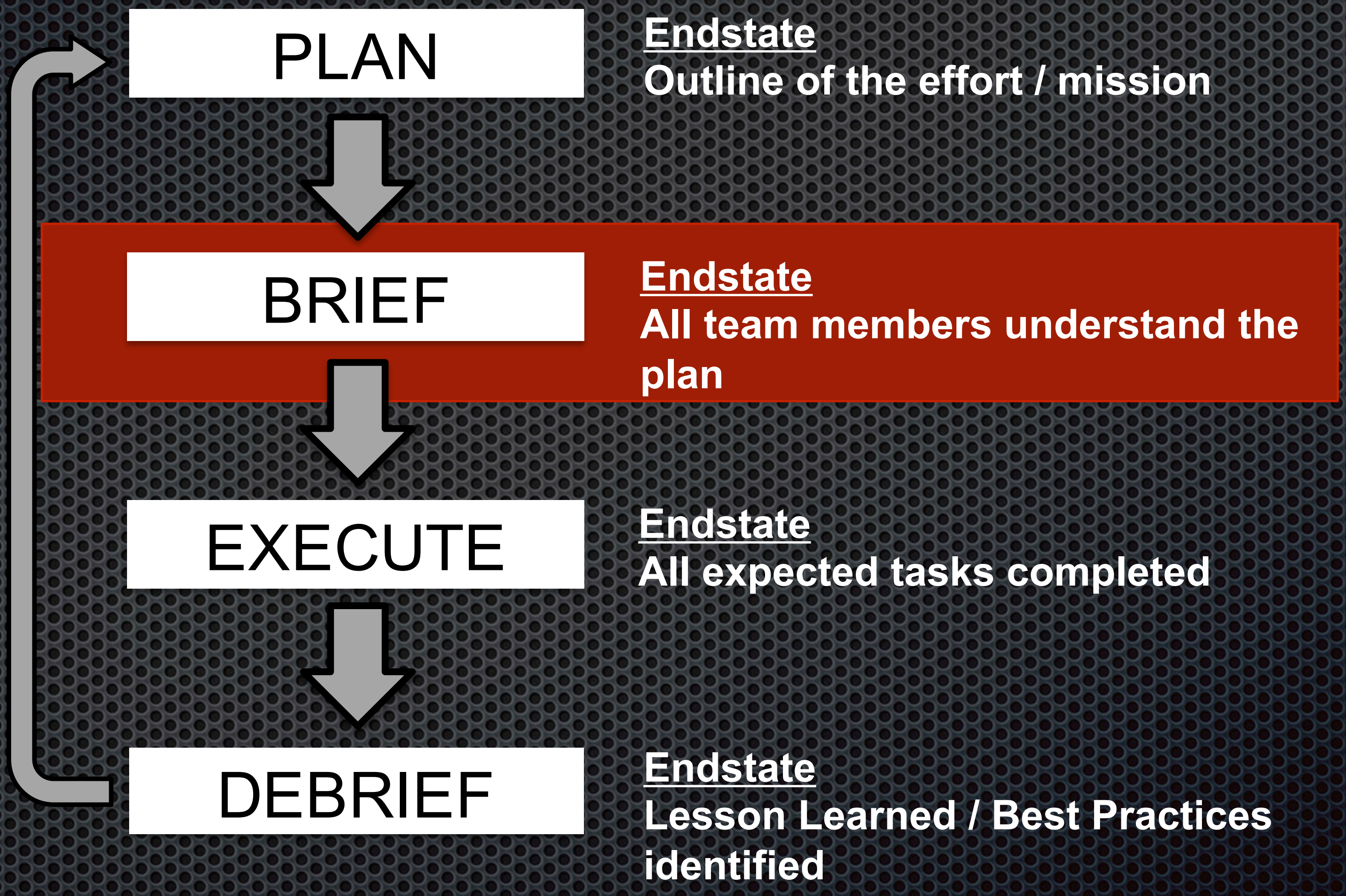
Call Signs

Collaboration (VTC, mIRC, DCS, SharePoint)

Deliverables produced during/after Execution

- Format
- Suspense

Plan, **Brief**, Execute, Debrief



PLAN

Endstate
Outline of the effort / mission

BRIEF

Endstate
All team members understand the plan

EXECUTE

Endstate
All expected tasks completed

DEBRIEF

Endstate
Lesson Learned / Best Practices identified

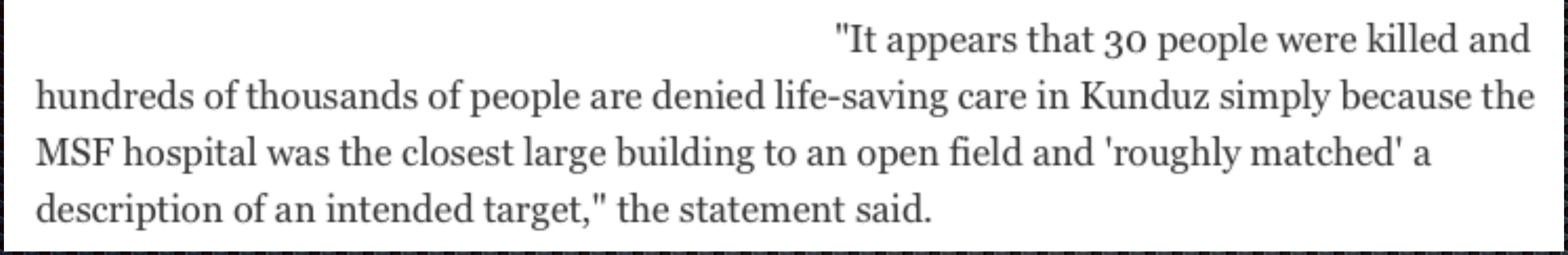
“Death and life are in the power of the tongue…”

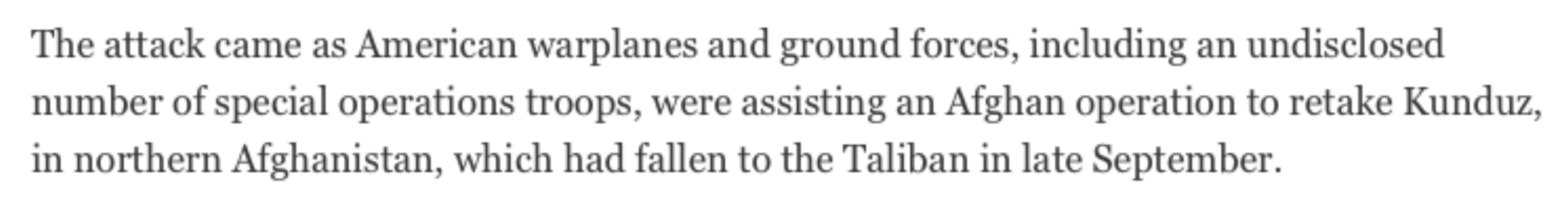
King Solomon - Proverbs 18:21

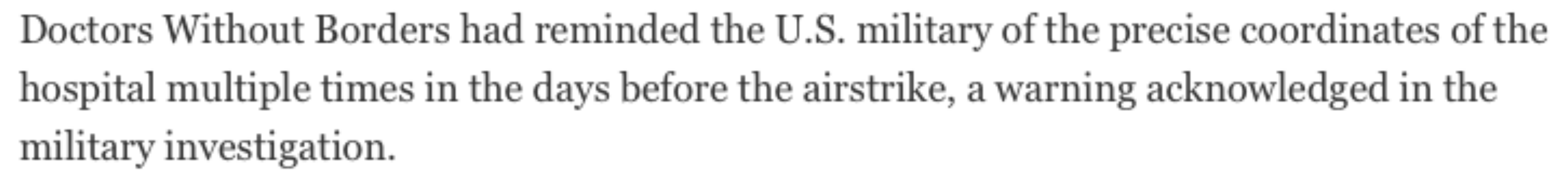
Oct. 3 strike on a Doctors Without Borders hospital, killing 30 civilians and left 37 others wounded, was ‘tragic, but avoidable.’

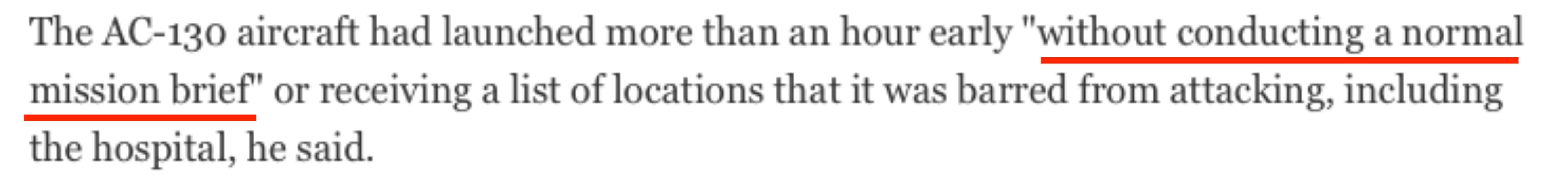
General John Francis Campbell

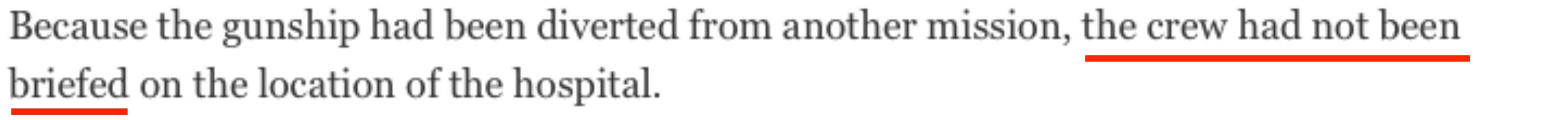
Los Angeles Times


"It appears that 30 people were killed and hundreds of thousands of people are denied life-saving care in Kunduz simply because the MSF hospital was the closest large building to an open field and 'roughly matched' a description of an intended target," the statement said.

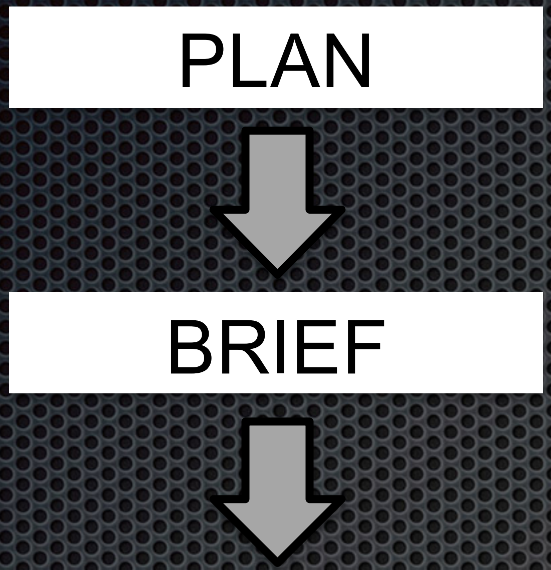

The attack came as American warplanes and ground forces, including an undisclosed number of special operations troops, were assisting an Afghan operation to retake Kunduz, in northern Afghanistan, which had fallen to the Taliban in late September.


Doctors Without Borders had reminded the U.S. military of the precise coordinates of the hospital multiple times in the days before the airstrike, a warning acknowledged in the military investigation.


The AC-130 aircraft had launched more than an hour early "without conducting a normal mission brief" or receiving a list of locations that it was barred from attacking, including the hospital, he said.


Because the gunship had been diverted from another mission, the crew had not been briefed on the location of the hospital.

Lead by briefing the team


PLAN

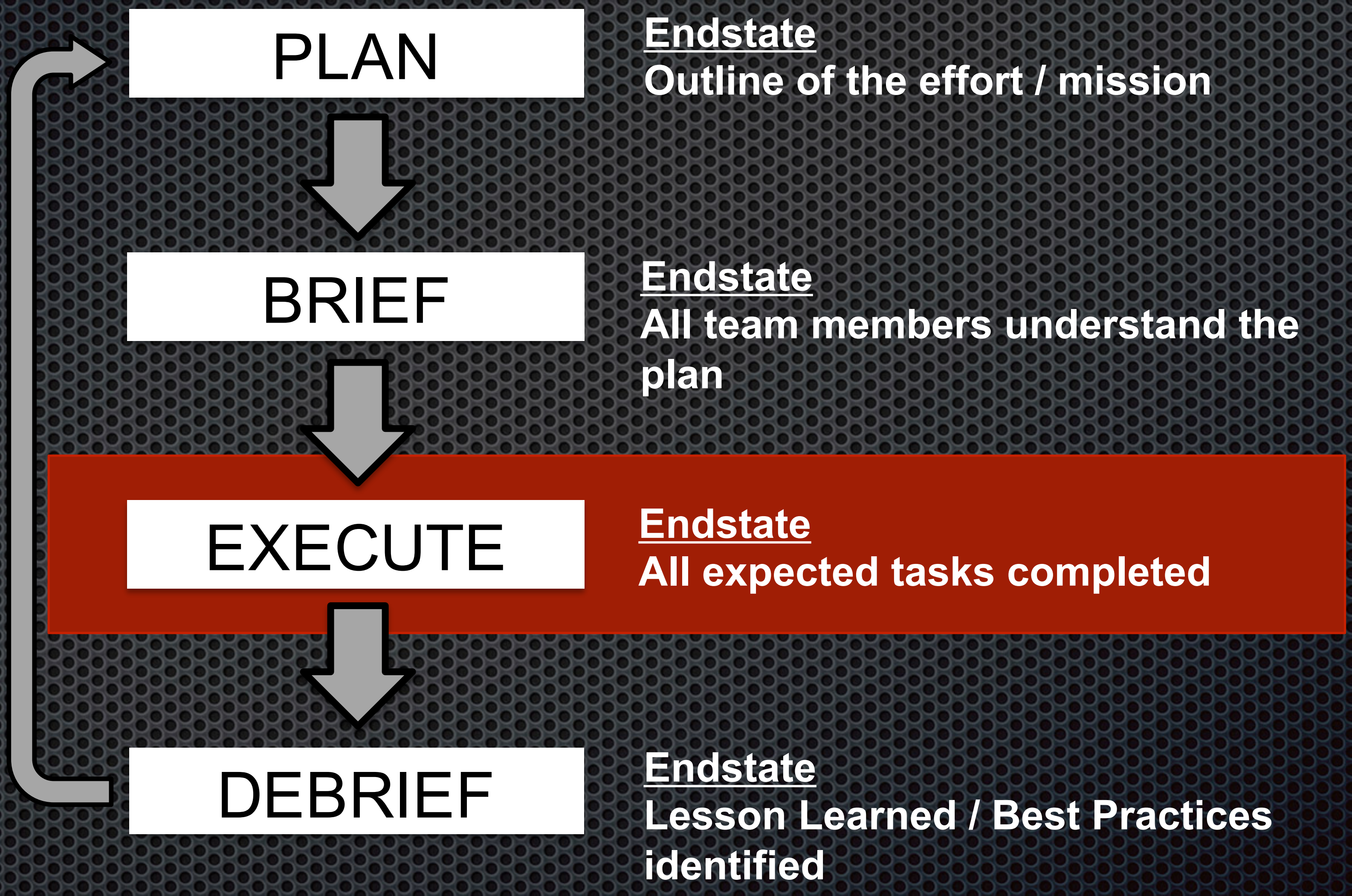
BRIEF

Endstate
All team members understand the plan

- Mission Leader Conveys Plan
  - Cover the whole mission
  - Opportunity for team to ask questions/weigh-in on planning
- Brief includes:
  - Team objectives, tasks & expectations
  - Assessment plan
  - Visual timeline of events
  - Roles/Responsibilities/Resources
  - Assumptions and Contingencies

The brief sets the tone for the whole effort

Plan, Brief, **Execute**, Debrief



PLAN

Endstate
Outline of the effort / mission

BRIEF

Endstate
All team members understand the plan

EXECUTE

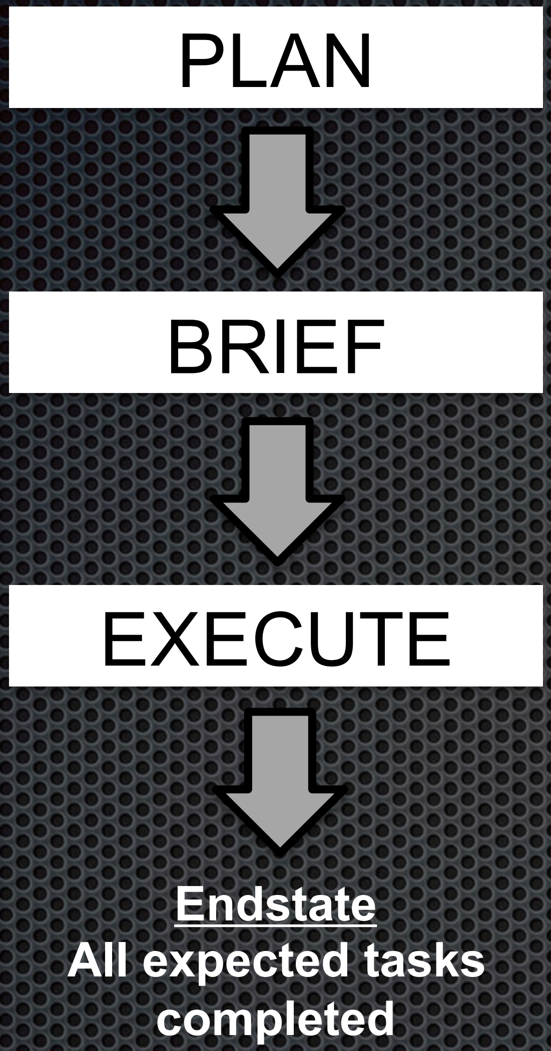
Endstate
All expected tasks completed

DEBRIEF

Endstate
Lesson Learned / Best Practices identified

Execution is the easy part

Lead during execution



PLAN

BRIEF

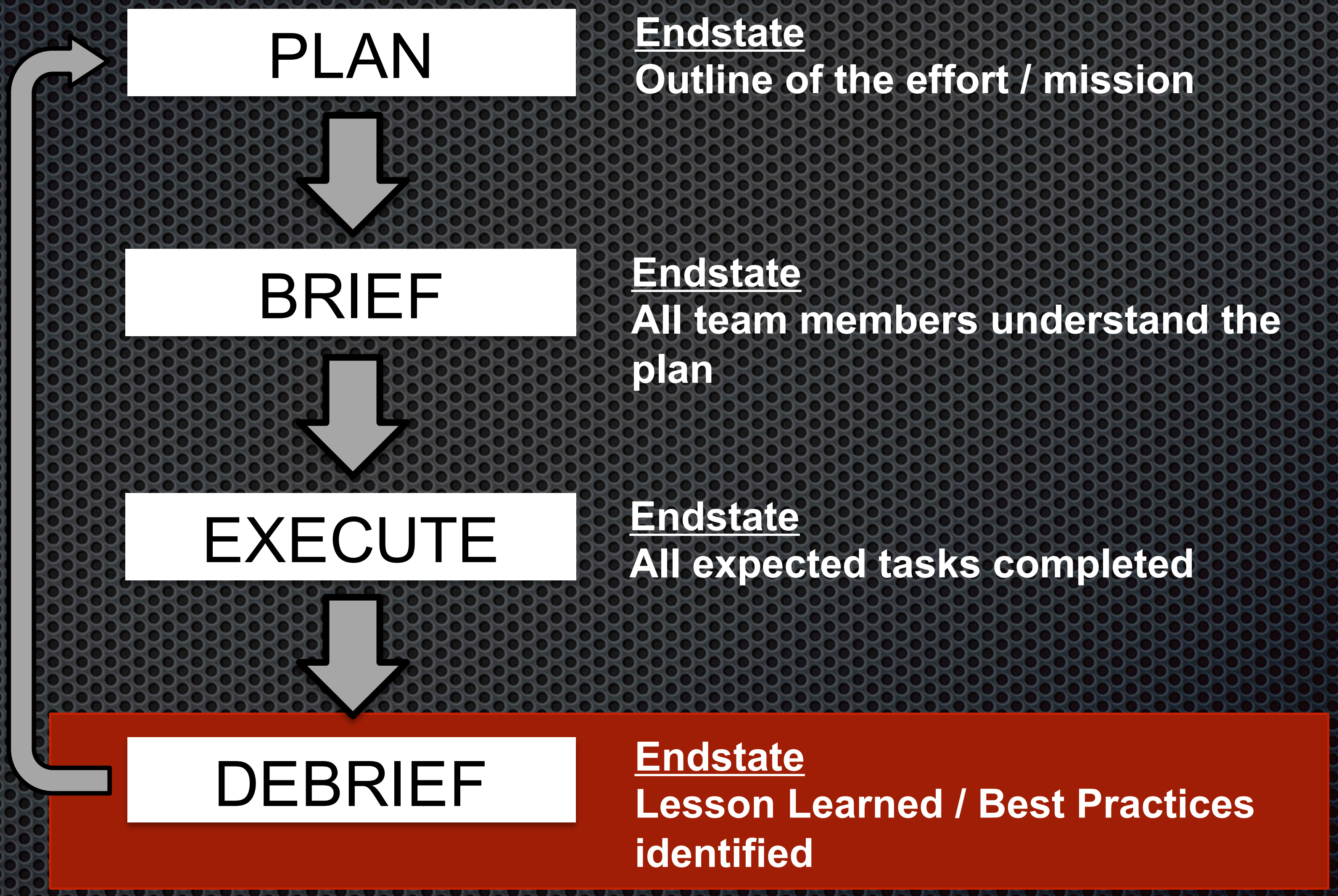
EXECUTE

Endstate
All expected tasks completed

- Execute in accordance with established guidelines & procedures
  - Directive Guidance
  - Checklists
  - Company policies
- Everyone should be noting observations throughout
  - Driven by assessment planning
  - Leader can assign focus areas to individuals

Deviations OK, but should be debriefed

Plan, Brief, Execute, **Debrief**



PLAN

Endstate
Outline of the effort / mission

BRIEF

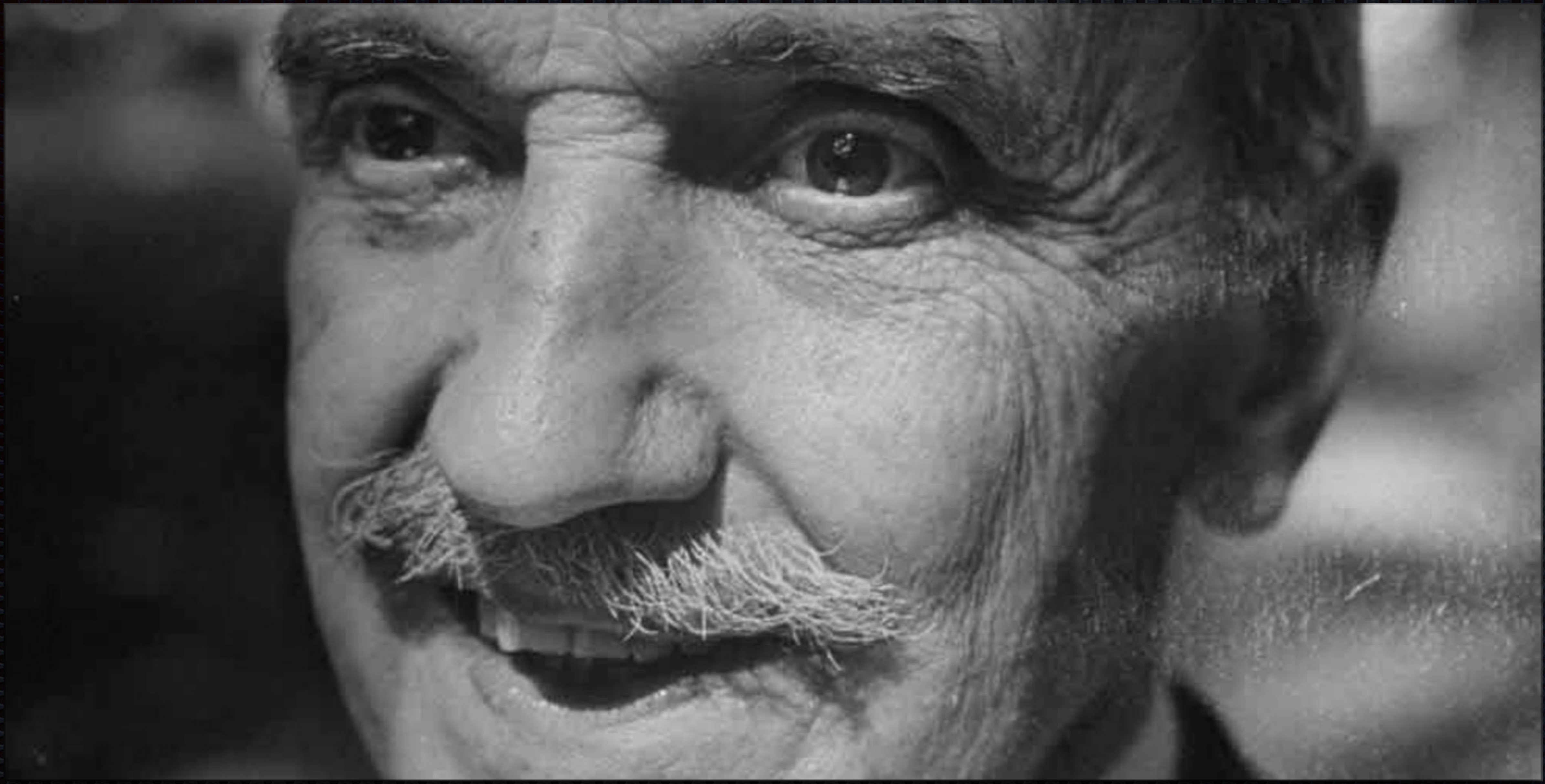
Endstate
All team members understand the plan

EXECUTE

Endstate
All expected tasks completed

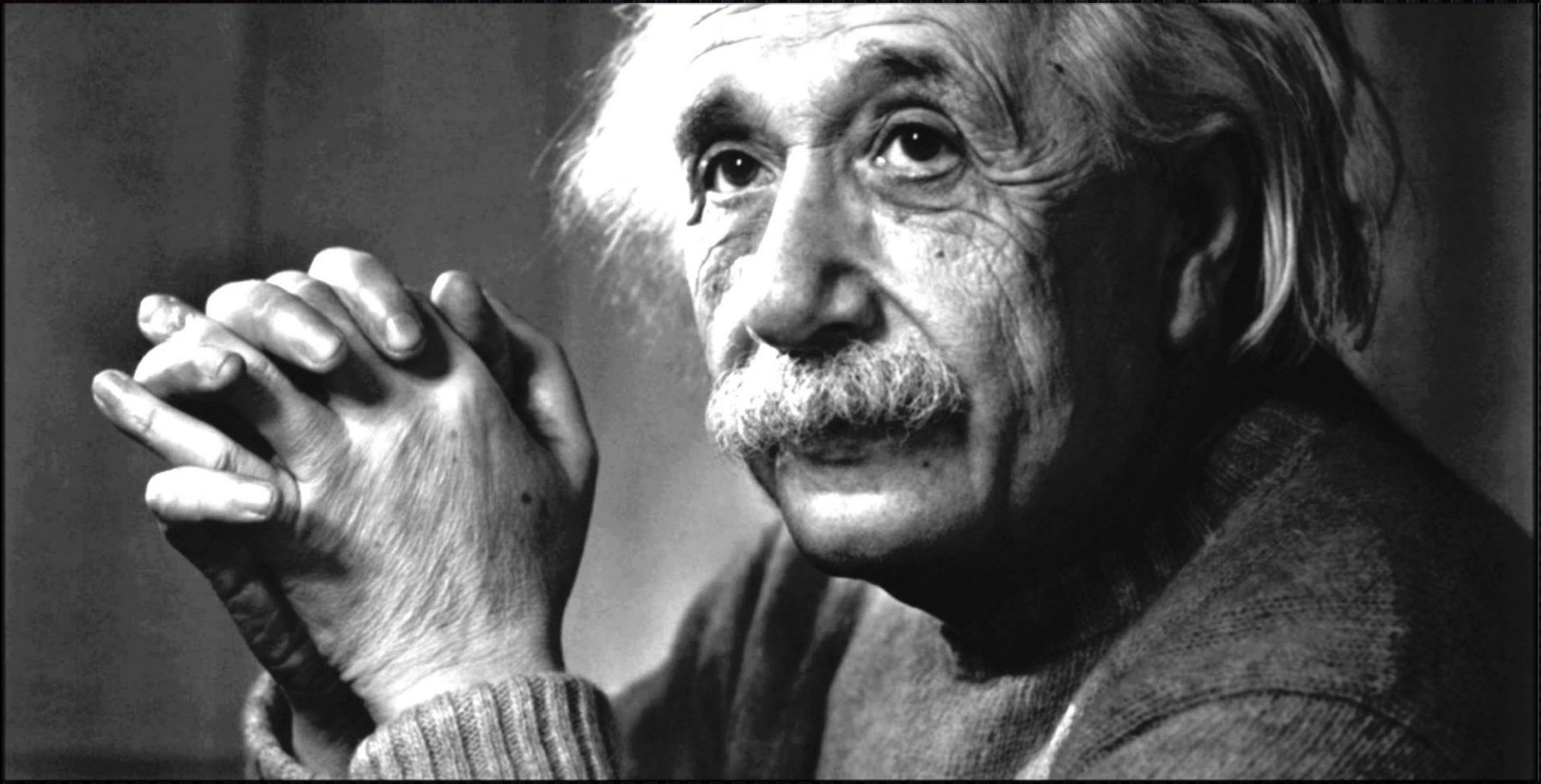
DEBRIEF

Endstate
Lesson Learned / Best Practices identified



“Those who cannot remember their mistakes are condemned to repeat them.”

George Santayana



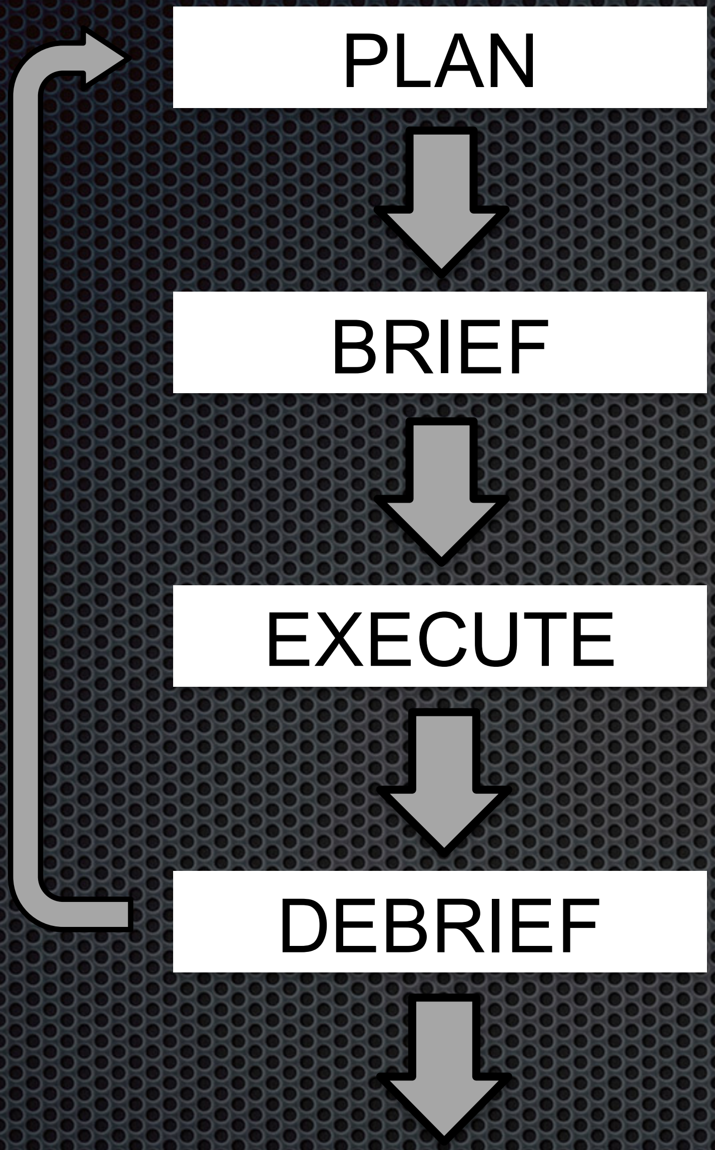
“Insanity is doing the same thing over and over again expecting different results”

Albert Einstein

“If you do what you’ve always done, you’ll get what you always got.”

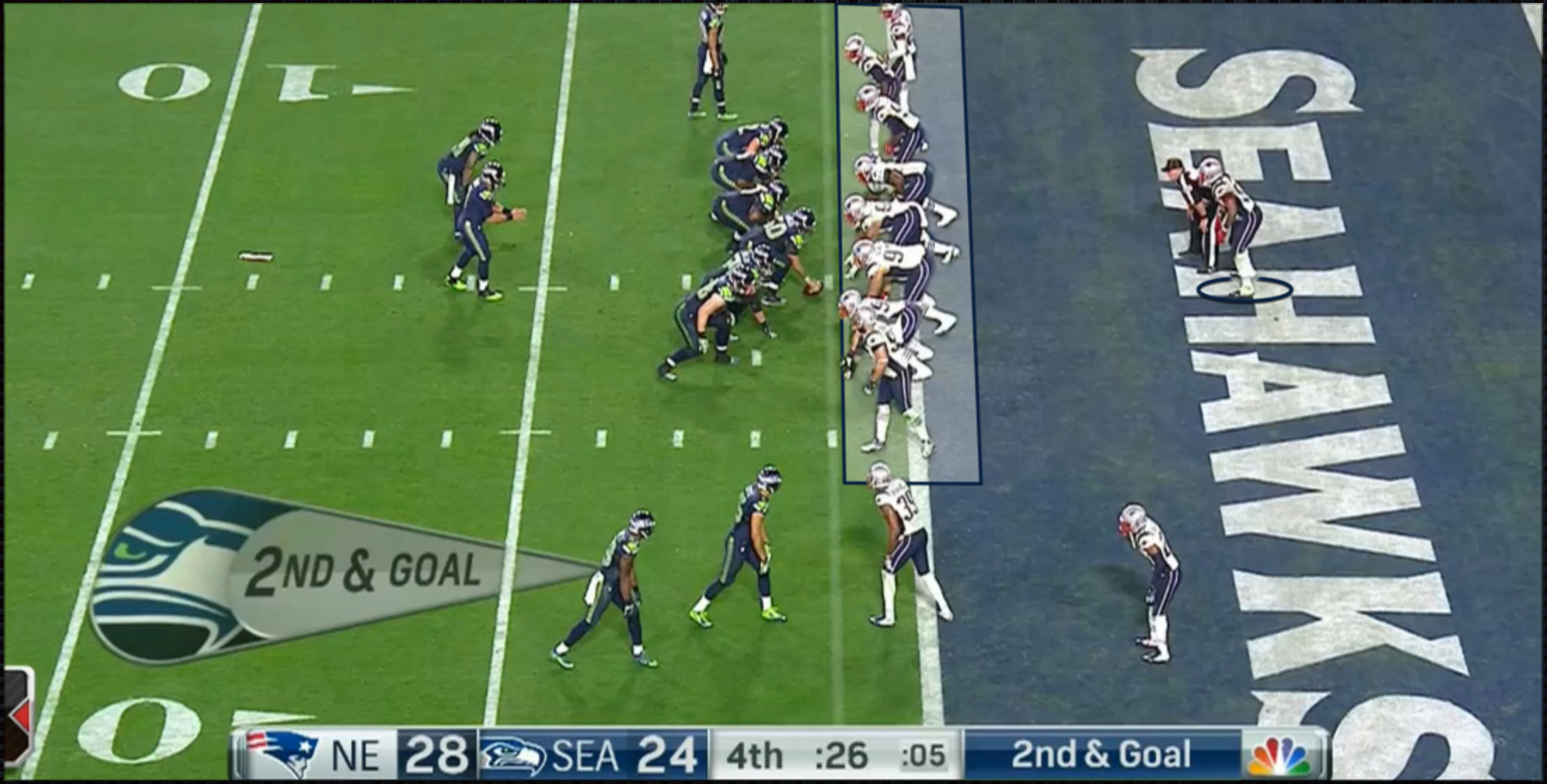
Some redneck my dad knows

Lead the Debrief



<u>Endstate</u>
Best Practices ID’d

- Reconstructing / analyzing an event to avoid repeat mistakes & clone success
- Led by leader; entire team participates & Rank is a non-factor!
- Tied to overall plan/objectives
  - What was the plan?
  - Did we stick to the plan?
  - Was the plan sufficient?
- Structured Flow
  - Repeatable
  - Aids in avoiding pitfalls/bad habits



What was the plan?

Did we stick to the plan?

Was the plan sufficient?

Debrief Basics

- A.K.A. a Hotwash or AAR
  - Institutional learning
- Must be **internally** focused
  - Bathtub Faucet
  - Busbahnhof vs. Postbahnhof
  - Salad Gate 2011

Debrief Terminology

- Observation: Actual events that occurred and any factual piece of information
- Reconstruction: Process of looking at the mission and determining the facts
- Debrief Focal Point (DFP): Aspects of the event which impeded achievement of the mission
- Root Cause (RC): The core reason the problem occurred
- Fix Action (FA): The “what” and “how” to address the root cause
- Lesson Learned (LL): Narrative statement that combines the DFP, RC, and IF
- Contributing Factors (CF): Stimuli that may have contributed to the conditions of the event

Crafting a L2

L2 ‘Equation’ =
When <activity>, 1/**RC** by **FA** so that not **DFP**

- **DFP:** Why did it take 2 days for CERT team members to locate computer X?
- **RC:** I failed to get positive contact information for the owner / admin of the asset after initial triage
- **FA:** Add step to IR checklist that requires positive contact information

Lesson Learned

When performing IR, I will ensure that I have accurate contact information for the compromised system’s owner by updating the IR checklist with a step that requires current POC information so that our team can track down compromised systems quickly.

- **DFP:** Why did the data migration event get 37 minutes off schedule?
- **RC:** I failed to ensure administrators had credentials to all of the servers requiring migration
- **FA:** Add reminder to migration crew brief that reminds administrators to double check access / credentials.

Lesson Learned

When executing a migration event, network admins will have all necessary credentials by reminding the team to verify access during the mission brief so that the data migration stays on time.

Common Debrief Mistakes

- Not internally focused
- Jumping to Fix Action before identifying the Root Cause
  - Avoid: “I already know what went wrong…Here’s simply what we do”
  - You can have suspicions, but always run through the process
- Not owning up to mistakes
  - Leave your ego and self preservation at the door!

Throwing a Dinner Party

Debrief Example

Dinner Party Example

- Objectives
  - 1) Feed guests delicious meal
  - 2) All guests leave happy/have good time
  - 3) Doesn't interfere with baby's routine
- Specified Tasks
  - Make dinner
  - Provide entertainment
  - Clean the house
- Implied Tasks
  - Decide what recipes to use
  - Go to the grocery store
  - Create dinner music playlist
  - Gather party games
- Constraints & Restraints
  - Has to end before baby's bath time
  - Can't serve alcohol to minors
- Assumptions
  - All guests will be omnivores
  - Guests do not have food allergies
- Assessment Criteria
  - Guests plates are cleaned
  - Guests joking and laughing
  - Guests are sad when it's babies bath time and they have to leave

Dinner Party Debrief

Reconstruction

- 0800 – woke up
- 1200 – ate lunch
- 1300 – wife and I begin cleaning
- 1345 – note: cleaning taking too long
- 1400 – baby is fussy
- 1400 – I start taking care of baby
- 1445 – baby falls asleep (finally)
- 1500 – left for the grocery store
- 1600 – return from store/start cooking
- 1645 – noticed missing key ingredients
- 1650 – used soy sauce for beef bouillon
- 1715 – set table/prepare entertainment
- 1730 – guests begin arriving
- 1830 – dinner served
- 1845 – guests hardly touched food
- 1850 – subject of food quickly deflected
- 1930 – guests only mingling/party dead
- 1945 – guests leave earlier than plan'd

- DFP: Why did the guests dislike the food? (Obj 1 & 2)
  - ~~The guests' tastes are subjective~~
  - I failed to feed them delicious food
    - I failed to prepare the food in accordance with the recipe
      - I did not have all of the ingredients
        - I failed to purchase all needed ingredients
          - I didn't know better

RC →

FA: create grocery list with required ingredients

Lesson Learned: When preparing for a dinner party, I will remember to buy all of the required ingredients by creating a grocery list to remind me of what ingredients are needed so that the guests will like the food.

Dinner Party Debrief

<u>Reconstruction</u>

- 0800 – woke up
- 1200 – ate lunch
- 1300 – wife and I begin cleaning
- 1345 – note: cleaning taking too long
- 1400 – baby is fussy
- 1400 – I start taking care of baby
- 1445 – baby falls asleep (finally)
- 1500 – left for the grocery store
- 1600 – return from store/start cooking
- 1645 – noticed missing key ingredients
- 1650 – used soy sauce for beef bouillon
- 1715 – set table/prepare entertainment
- 1730 – guests begin arriving
- 1830 – dinner served
- 1845 – guests hardly touched food
- 1850 – subject of food quickly deflected
- 1930 – guests only mingling/party dead
- 1945 – guests leave earlier than plan'd

- DFP: Why did the guests dislike the food? (Obj 1 & 2)
  - ~~The guests' tastes are subjective~~
  - I failed to feed them delicious food
    - I failed to prepare the food in accordance with the recipe
      - I did not have all of the ingredients
        - I failed to purchase all needed ingredients
          - I didn't know better

RC →

FA: create grocery list with required ingredients

LL: <u>When</u> preparing for a dinner party, I will remember to buy all of the required ingredients <u>by</u> creating a grocery list to remind me of what ingredients are needed <u>so that</u> the guests will like the food.

Dinner Party 2.0

- Objectives
  - 1) Feed guests delicious meal
  - 2) All guests leave happy/have good time
  - 3) Doesn't interfere with baby's routine
- Specified Tasks
  - Make dinner
  - Provide entertainment
  - Clean the house
- Implied Tasks
  - Decide what recipes to use
  - Make a grocery list
  - Go to the grocery store
  - Create dinner music playlist
  - Gather party games
- Constraints & Restraints
  - Has to end before baby's bath time
  - Can't serve alcohol to minors
- Assumptions
  - All guests will be omnivores
  - Guests do not have food allergies
- Assessment Criteria
  - Guests plates are cleaned
  - Guests joking and laughing
  - Guests are sad when it's babies bath time and they have to leave

Dinner Party 2.0 Debrief

Reconstruction

- 0800 – woke up
- 0900 – made ingredient/grocery list
- 1200 – ate lunch
- 1300 – wife and I begin cleaning
- 1500 – left for the grocery store
- 1600 – return from store/start cooking
- 1715 – set table/prepare entertainment
- 1730 – guests begin arriving
- 1830 – dinner served
- 1845 – conversation is lively/jovial
- 1900 – most guests plates empty
- 1900 – guests A, C, & D asks for seconds
- 1900 – guest B has only eaten salad
- 1900 – guest B looks frustrated
- 1915 – all guests enjoying party games
- 1930 – guest B snacking heavily - veggies
- 2045 – guests have to be kicked out
- 2100 – baby put to bed

- DFP: Why did guest B dislike the food? (Obj 1 & 2)
    - ~~Because she is a vegetarian~~
    - I failed to prepare food to her liking
        - RC → I failed to give the guests food options
            - I assumed all guests were omnivores
                - I didn't know better

FA: make a contingency plan for guests that may want/need other food options

LL: When planning dinner parties, I will be able to offer multiple meal options by having a contingency plan in place for people who may want/need other food options (e.g. vegetarian) so that every guest enjoys the dinner.

Dinner Party 3.0

- Objectives
  - 1) Feed guests delicious meal
  - 2) All guests leave happy/have good time
  - 3) Doesn't interfere with baby's routine

- Specified Tasks
  - Make dinner
  - Provide entertainment
  - Clean the house

- Implied Tasks
  - Decide what recipes to use
    - Include vegetarian recipe
  - Make a grocery list
  - Go to the grocery store
  - Create dinner music playlist
  - Gather party games

- Constraints & Restraints
  - Has to end before baby's bath time
  - Can't serve alcohol to minors

- Assumptions & Contingencies
  - All guests will be omnivores
    - Have vegetarian option

- Assessment Criteria
  - Guests plates are cleaned
  - Guests joking and laughing
  - Guests are sad when it's babies bath time and have to leave

Dinner Party 40.0

- Objectives
  - 1) Feed guests delicious meal
  - 2) All guests leave happy/have good time
  - 3) Doesn't interfere with baby's routine
- Specified Tasks
  - Make dinner
  - Provide entertainment
  - Clean the house
- Implied Tasks
  - Decide what recipes to use
  - Make a grocery list
  - Go to the grocery store
  - Create dinner music playlist
  - Gather party games

- Objectives have not changed
- Plan now accounts for:
  - Vegetarian guests
  - Gluten Free guests
  - Bad weather
  - Guests that arrive late
  - Lack of parking
  - Unexpected Guests
  - Allergic reactions
  - Medical emergencies
  - Entertainment options
  - Cable outages
  - Power outages
  - Guests with car trouble
  - Guests who overstay their welcome
  - Sick guests
  - MONEY $AVER$

Debriefing = Continuous Process Improvement

Challenges

- Corporate anti-bodies to change
- Lack of qualified planners
- Egotism in the debrief

Takeaways

- PBED may seem daunting at first, but you will get better over time
- Don’t fight the process… embrace/trust in it
- If you repeat a problem even with implementing an FA, then:
  - You did not find the true root cause or FA was not sufficient
- Archive your previous executions & previous LLs
- It’s an operational rhythm… more importantly, it’s a lifestyle / culture
- The magic is in the debrief

Questions?