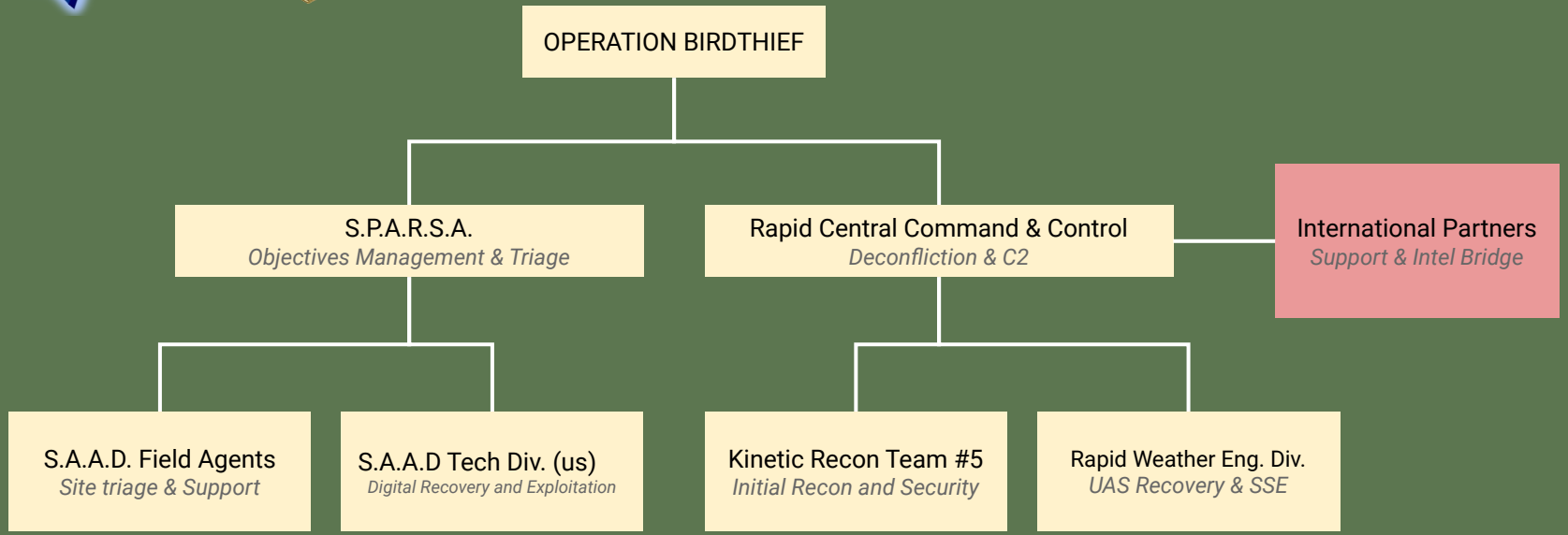
SPecial Aerial Recovery/Space Alliance

Special Aerial Acquisitions Department

OPERATION BIRDTHIEF

Enemy Drone Acquisition/Recovery

Operation Partners

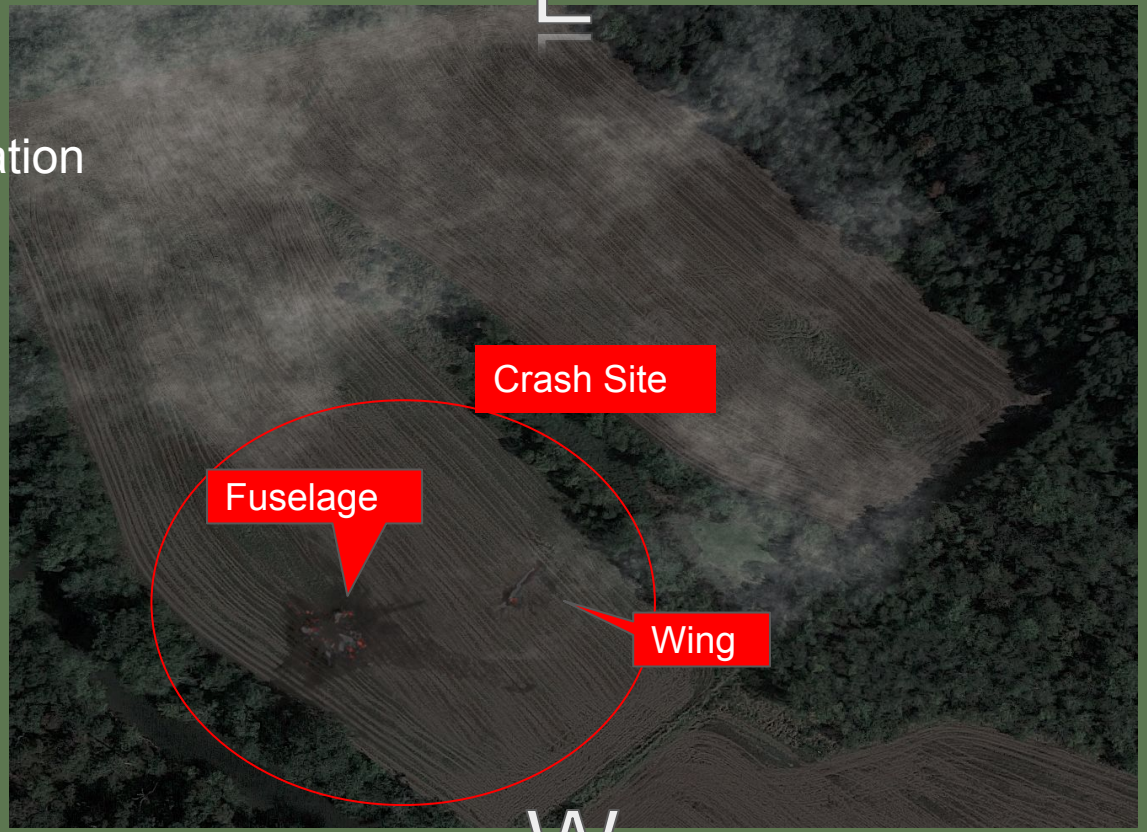


Initial Crash

- January 5th 0245
- Friendly Low-alt. RADAR systems detected a rapidly descending aircraft
- Assets confirmed crash by 0430
- KRT #5 and S.A.A.D. field agents deployed
- 25 km outside of [redacted]

Special Aerial Acquisitions Department

0500 - Initial Sat. Verification



Enemy contact

From 0600-1000 ground forces defended forward to secure the crash site

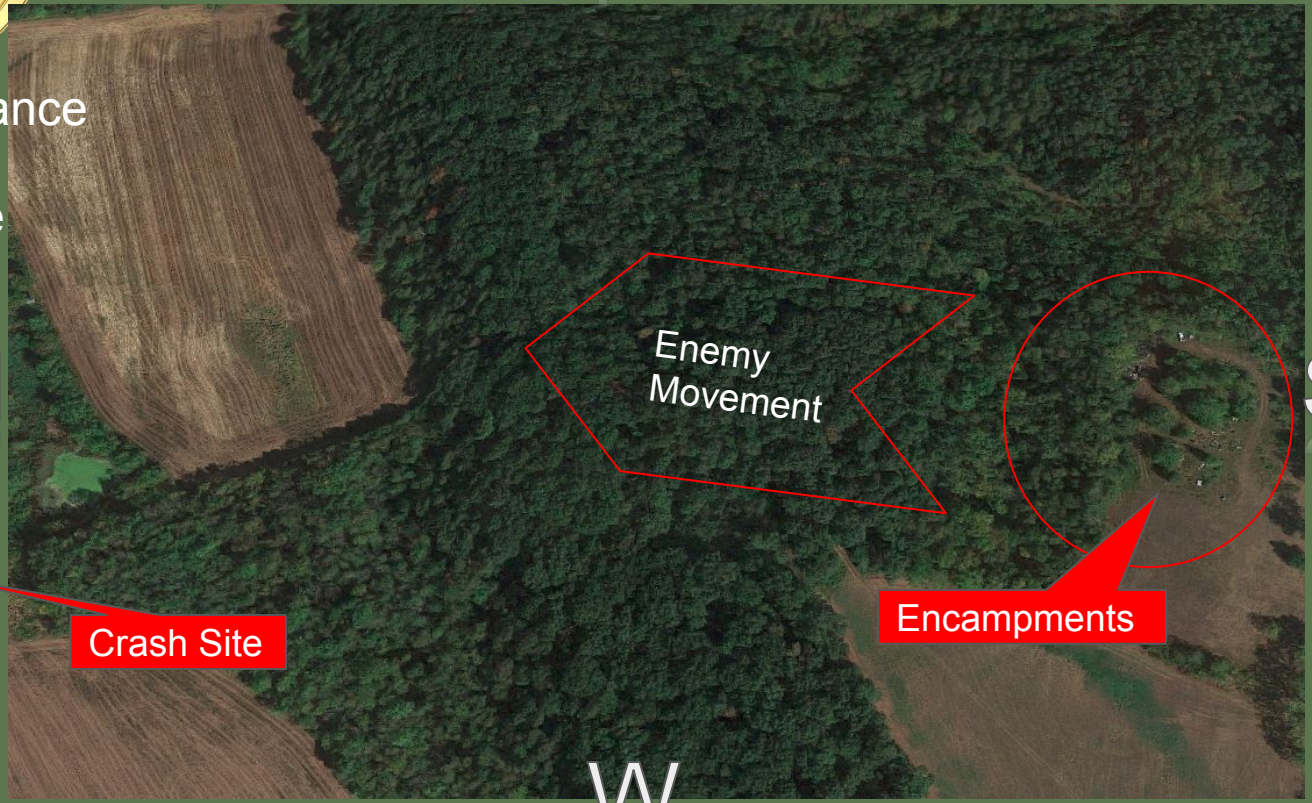
After initial destabilization attempts from the enemy, ground forces secured the area

1 casualty from the initial recon team

Special Aerial Acquisitions Department

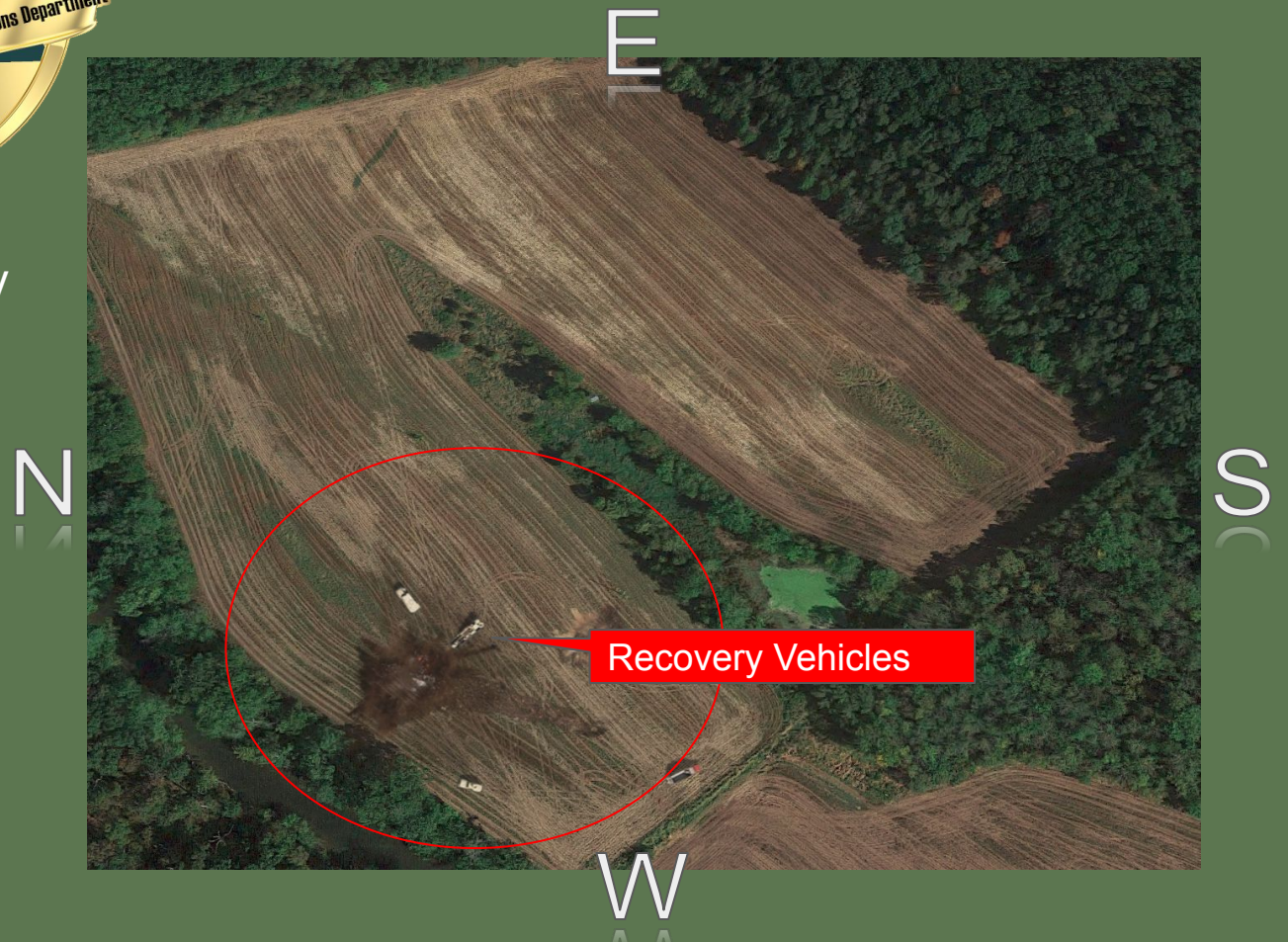
0600 - Enemy Resistance

500m from Crash Site



Special Aerial Acquisitions Department

1645 - Recovery Mostly Complete



Site Exploitation Efforts

Objective #1: FYSA

Get informed

Make sure you FULLY familiarize yourself with the briefing and slide deck.

Get as much information out of it as possible.

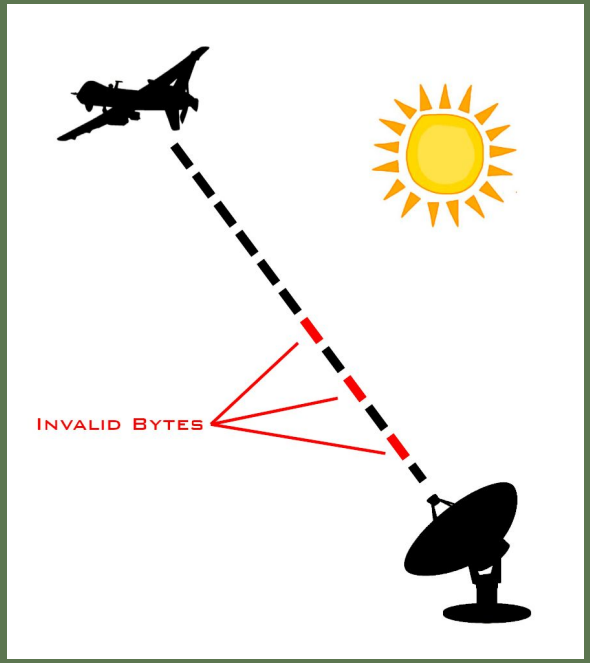
Objective #2: Downlink

Decode the Communications

We are getting a stream of data from the drone, but it seems to be heavily corrupted.

Must be the solar flares…

If only there was a way to check which bytes are corrupt..



Objective #3: Interception

Background

It turns out that our international partners have been doing a little bit of digging on the enemy UAS systems

They have located several live drones and ground controls stations

Primary Objectives

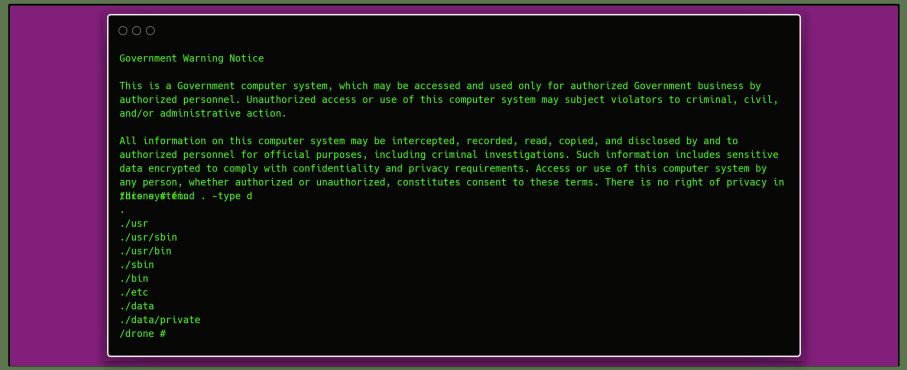
Figure out how the operator connected to the drone

Find out as much information as possible about the connection between the drone and the ground station

Partner Efforts

The partners have managed to infiltrate and exfil a PCAP from a ground control station

They claim that the ground control operator was attempting to login to a backdoor in a similar UAS system

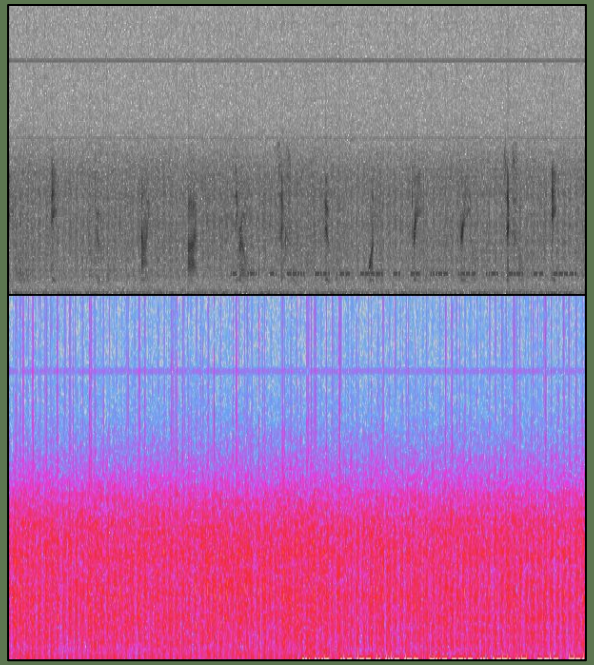


Objective #4: Number Station

Decode the Numbers

This recording was captured on the enemy drone. We aren't sure where it came from.

What do all these numbers mean? We need to figure out what the enemy knows about us right now!



Objective #5: Blackbox

Initial Efforts

Forensics acquisition recovered partial logical image

Many individual files carved from data

S.A.A.D passed the data upstream for us to analyze

Primary Objectives

Analyze the black box image (possible encryption)

Figure out all possible information about this drone

Ongoing Efforts

Repair and full recovery efforts underway

Standby for further objectives

Mission Critical Efforts

Lots of groups are trying to break this one. We *must* be the first to get the intel

Report back with findings ASAP

Objective #6: Defending Forward

Debriefing

Officially we don’t have authorization right now to take offensive action against the threats.

So ***DO NOT*** attack or exploit the ground station located at `http://bravo21-monitor.ritsec.club:5743` in any way

Objective #7: In Scope

Debriefing

The S.A.A.D. Division of S.P.A.R.S.A has brought forward new evidence in the form of an audio capture intercepted near the drone. Our techs looked at the recording, but came to no conclusions. We need you to *scope* out the meaning of this transmission.