Security Analysis of Radar System

Shai Cohen, Tomer Gluck, Yuval Elovici, Asaf Shabtai

Department of software and information system engineering
Ben-Gurion University of the Negev, Israel

CBG Cyber@ Ben-Gurion University of the Negev

Motivation

- Most studies conducted on protecting radar systems have focused on electronic warfare
- Radar systems also include a wide variety of components, such as a communications system or SCADA system
- Used the literature and testbed to create cyber security analysis for the radar

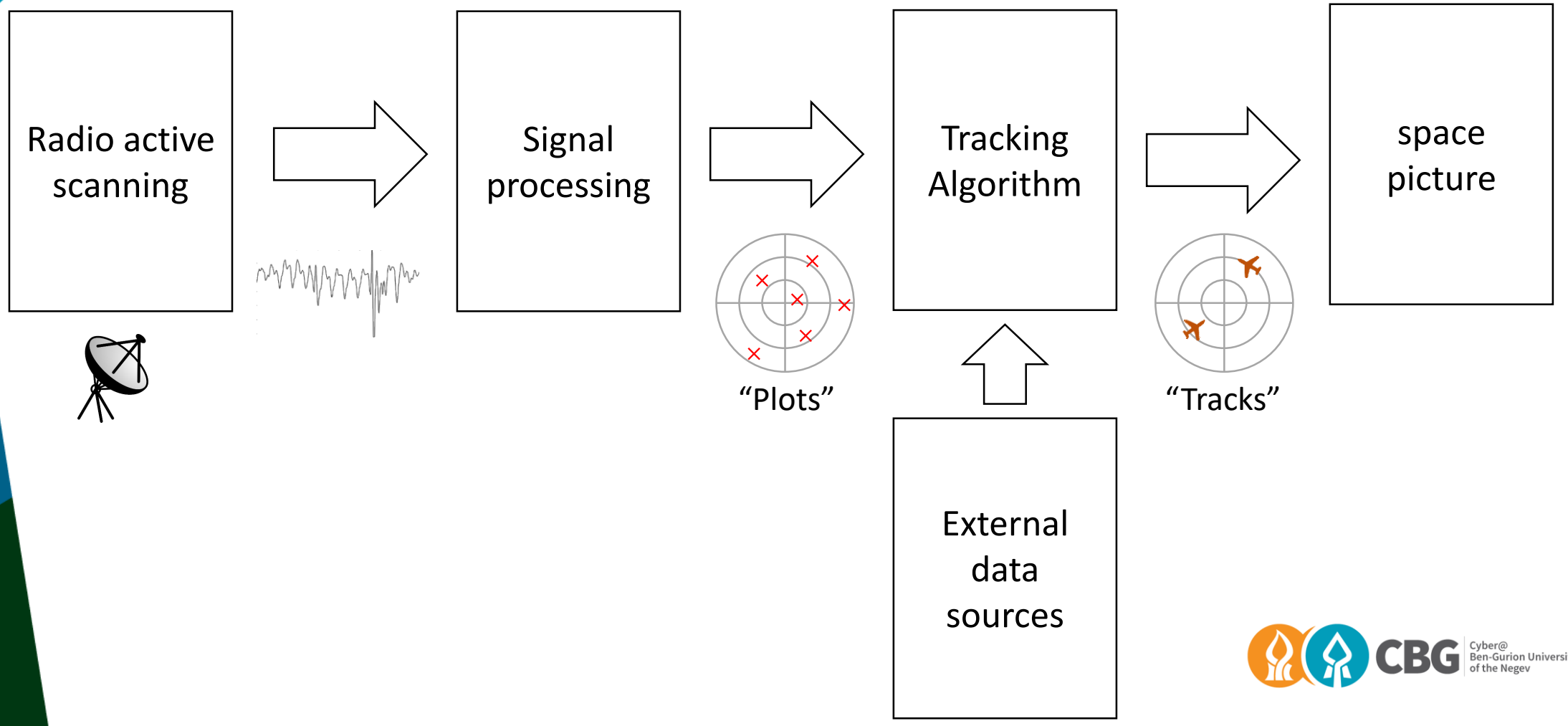
Overview

- Radar structure
- Testbed
- Taxonomy
- Demonstrated attack
- Conclusions

Definition

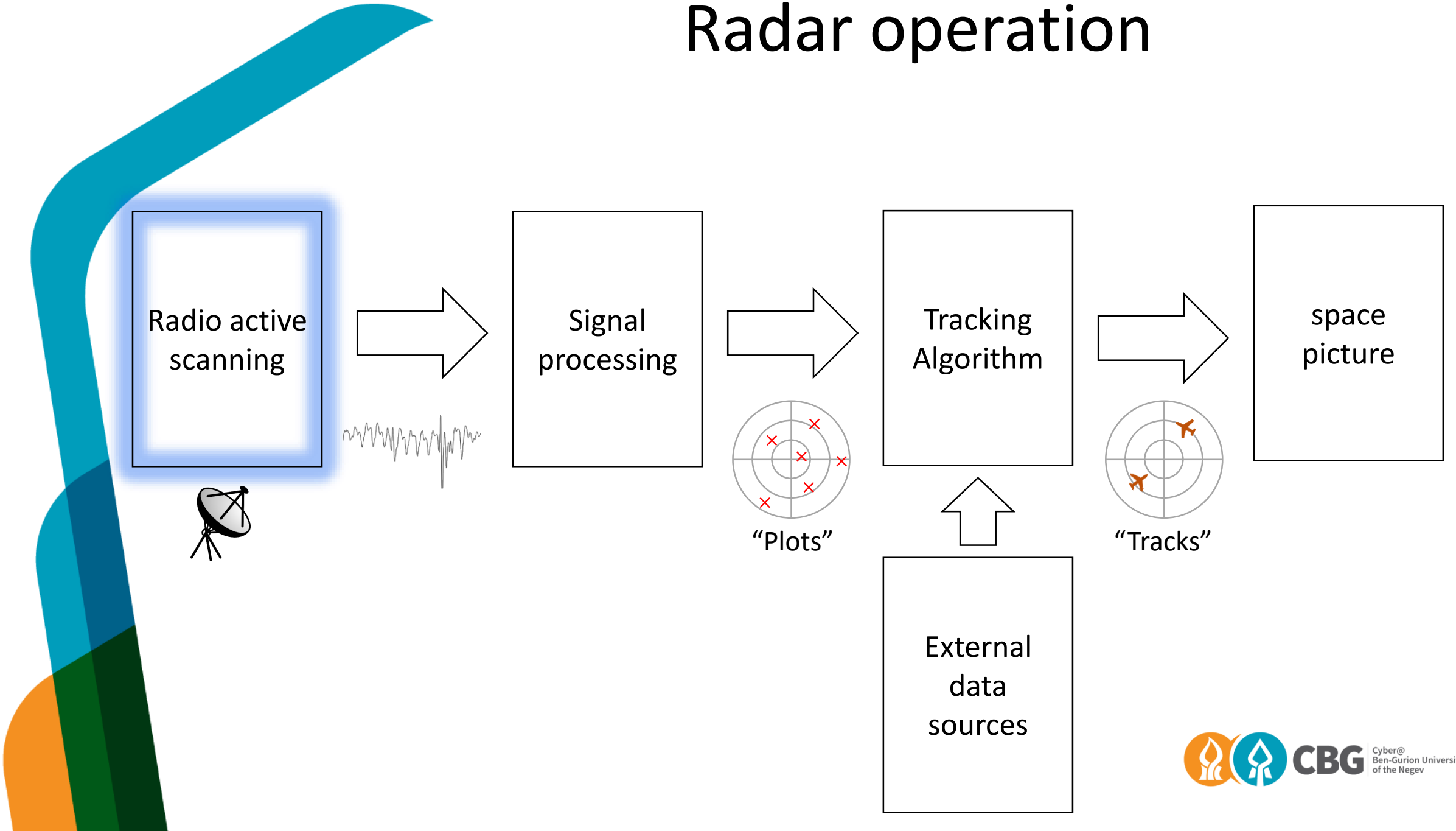
- Radar – Radio Detecting And Ranging
- Detect and monitor objects in space using electromagnetic waves
- Can detect aircrafts, ships, missiles, etc.

Radar operation



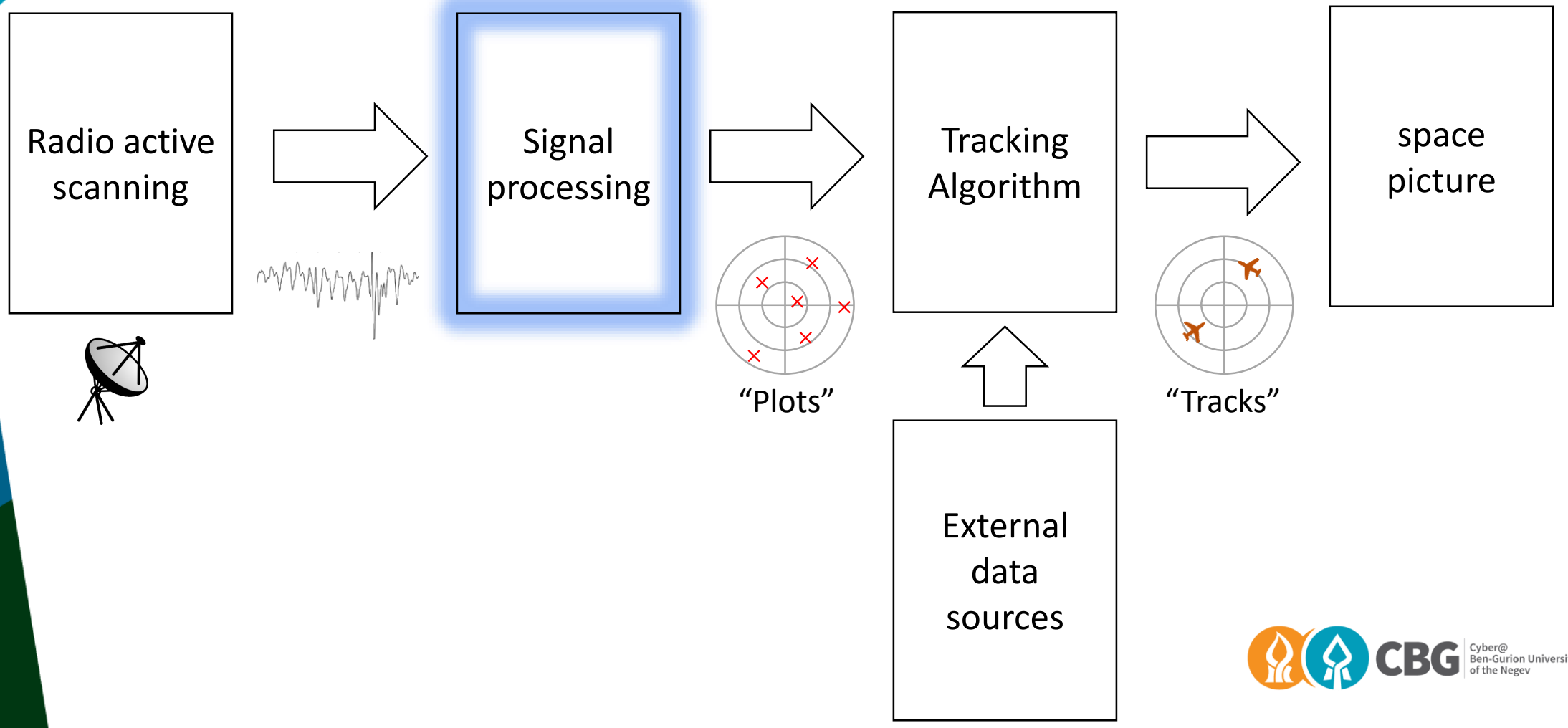
CBG Cyber@ Ben-Gurion University of the Negev

Radar operation



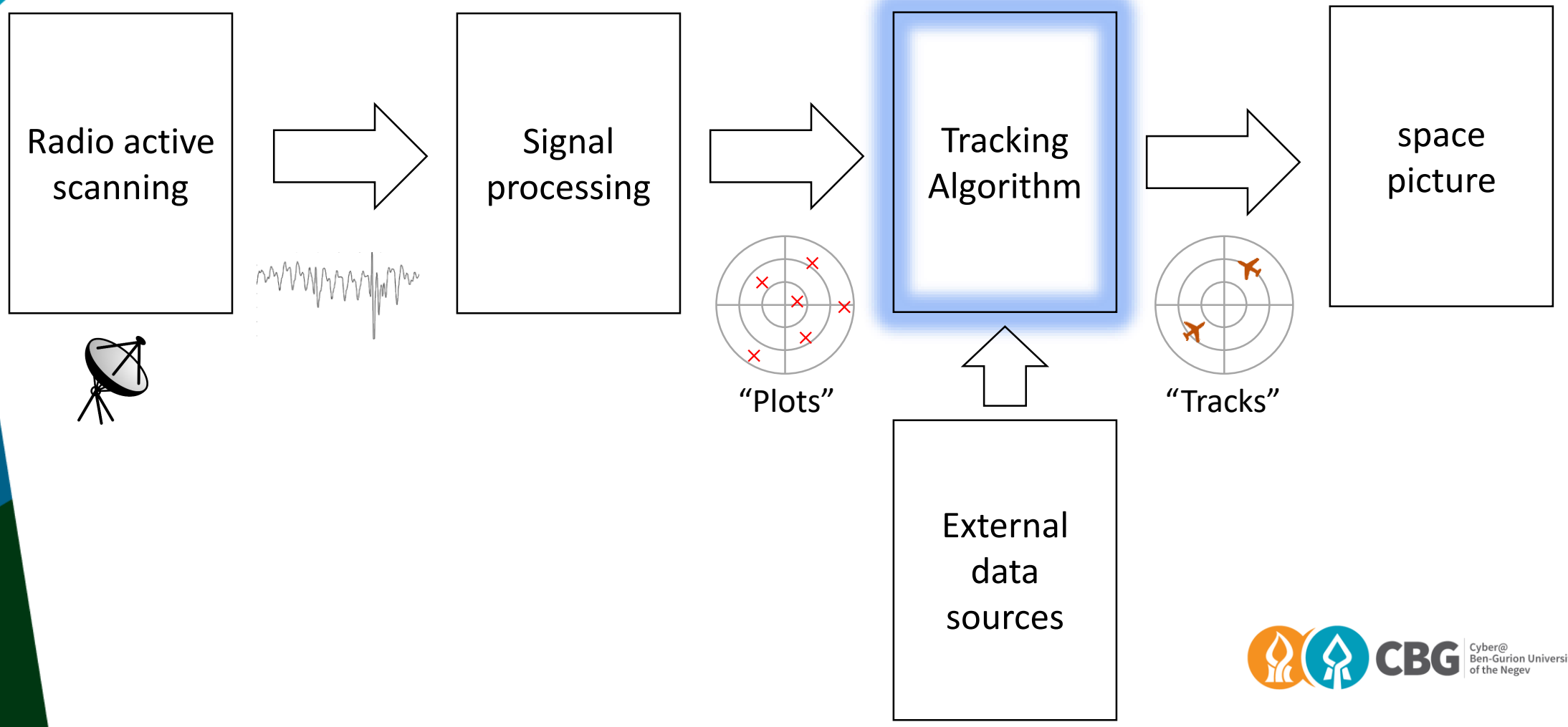
CBG Cyber@ Ben-Gurion University of the Negev

Radar operation



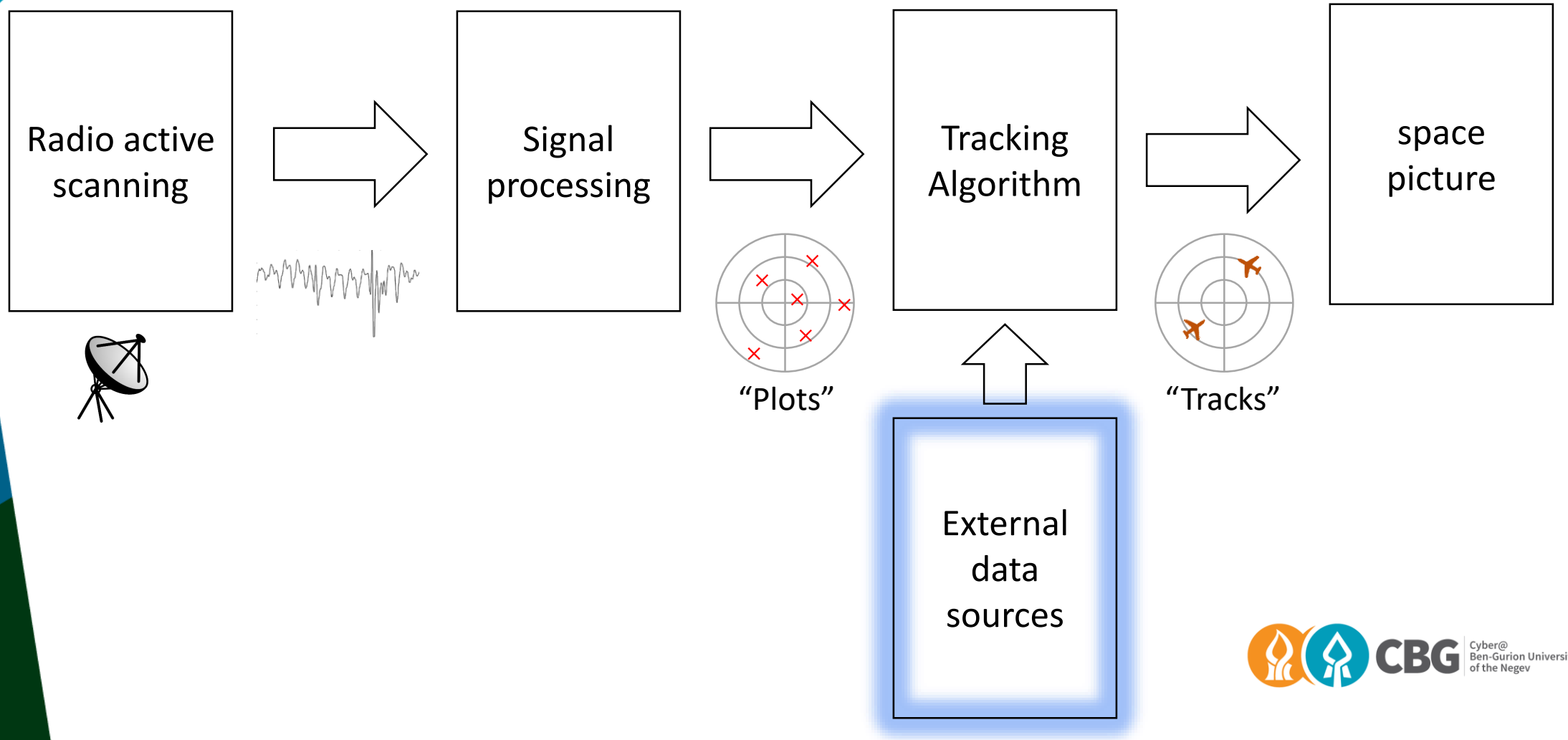
CBG Cyber@ Ben-Gurion University of the Negev

Radar operation



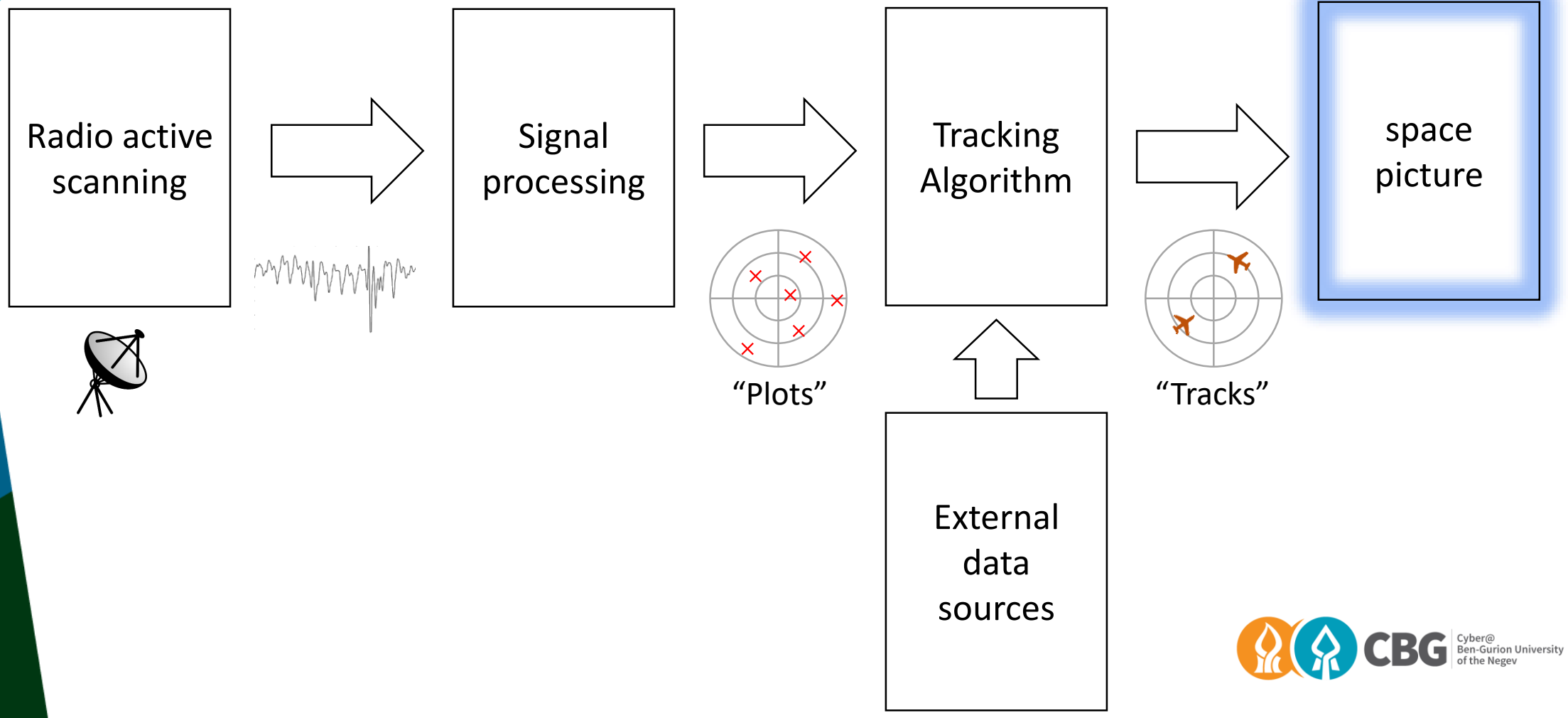
CBG Cyber@ Ben-Gurion University of the Negev

Radar operation



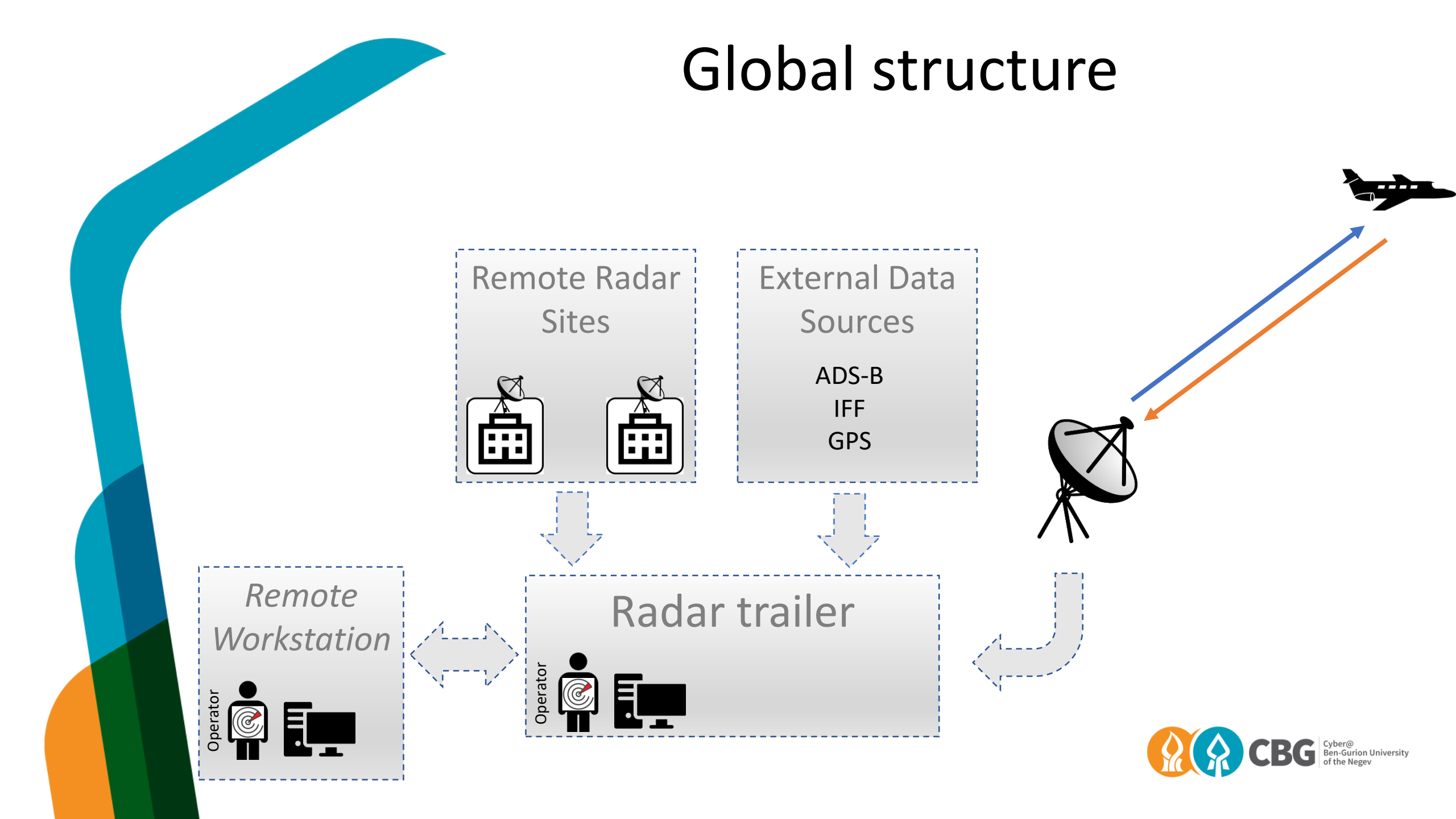
CBG Cyber@ Ben-Gurion University of the Negev

Radar operation



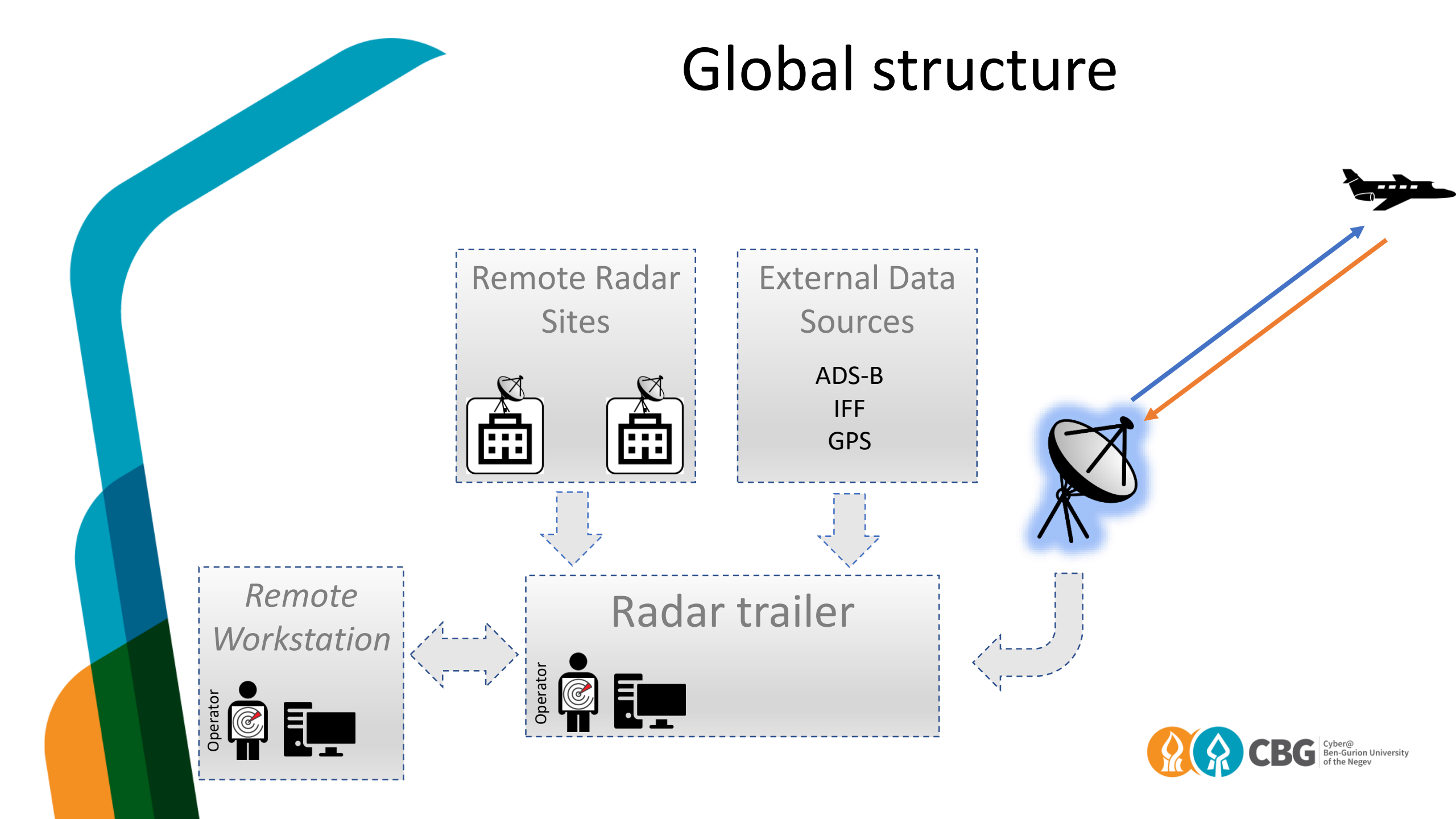
CBG Cyber@ Ben-Gurion University of the Negev

Global structure



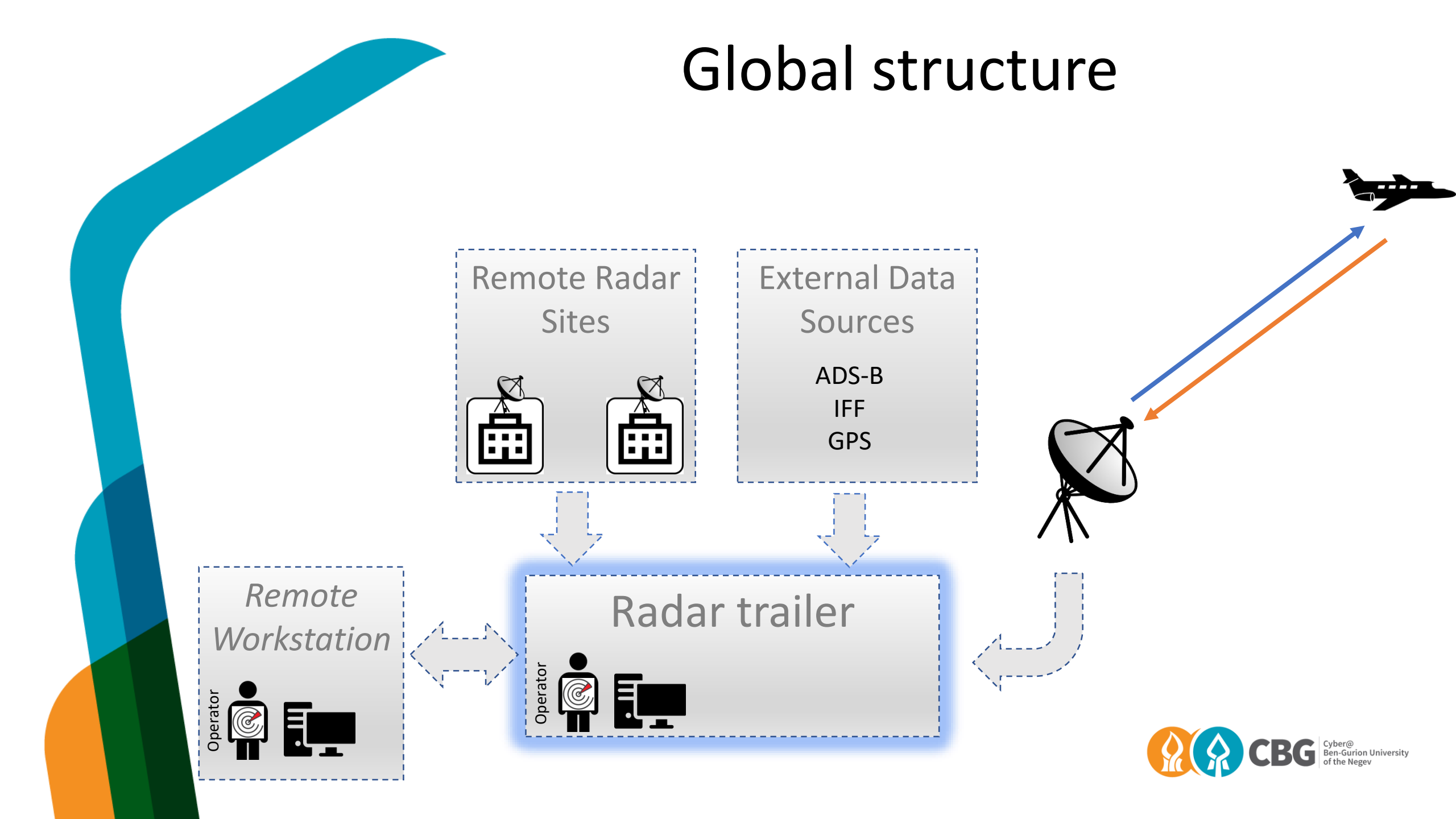
CBG Cyber@ Ben-Gurion University of the Negev

Global structure



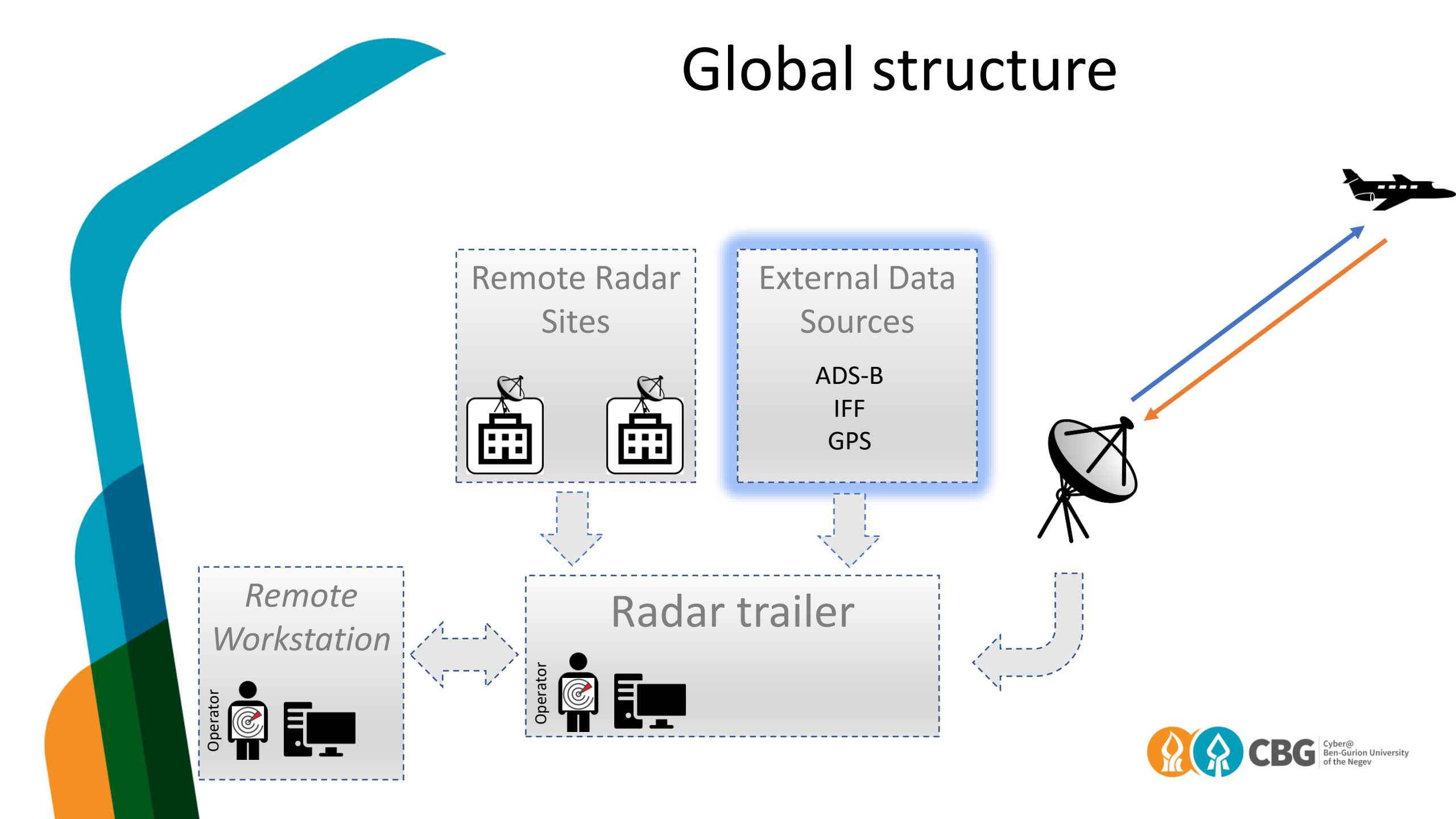
CBG Cyber@ Ben-Gurion University of the Negev

Global structure



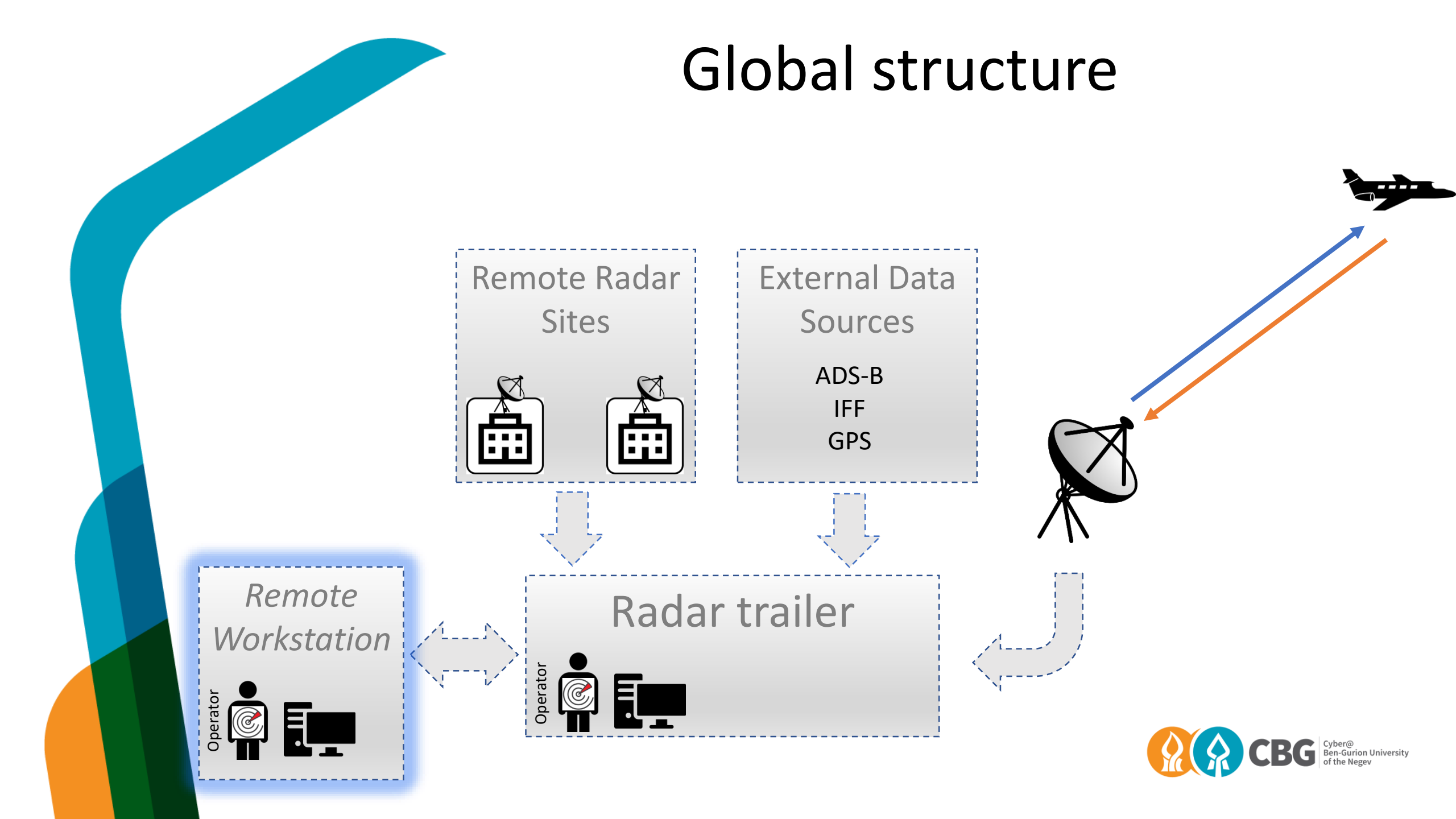
CBG Cyber@ Ben-Gurion University of the Negev

Global structure



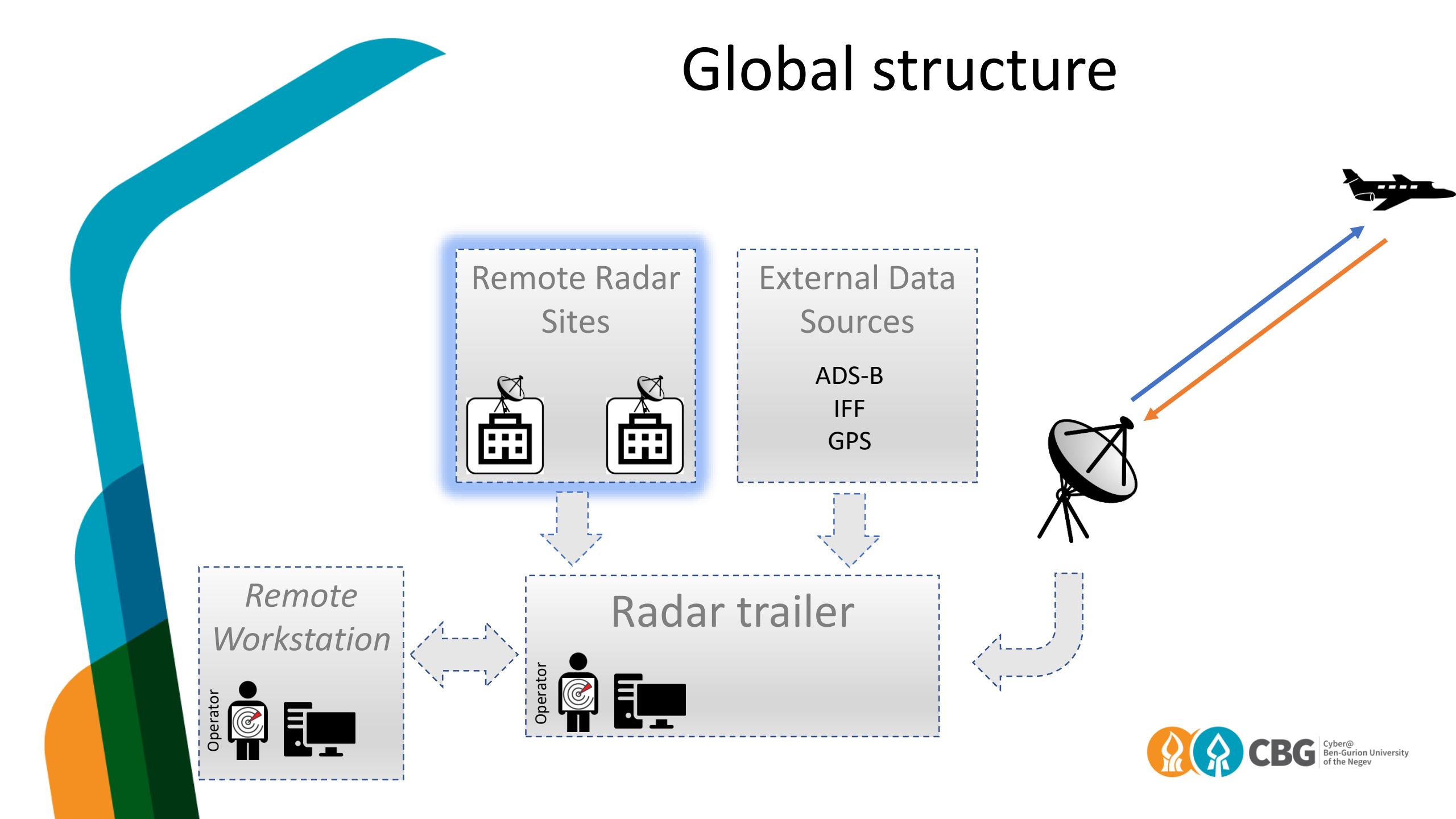
CBG Cyber@ Ben-Gurion University of the Negev

Global structure



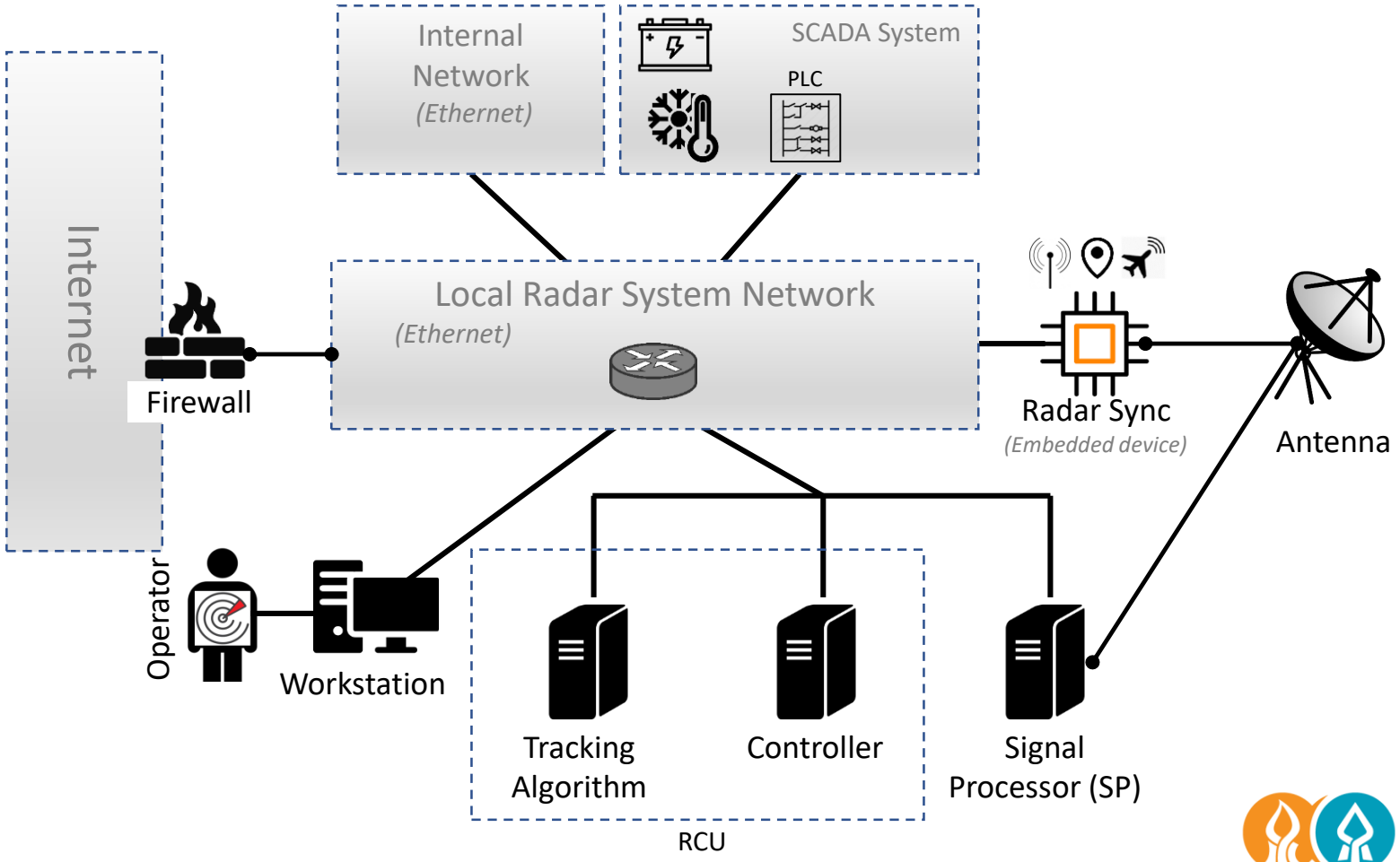
CBG Cyber@ Ben-Gurion University of the Negev

Global structure



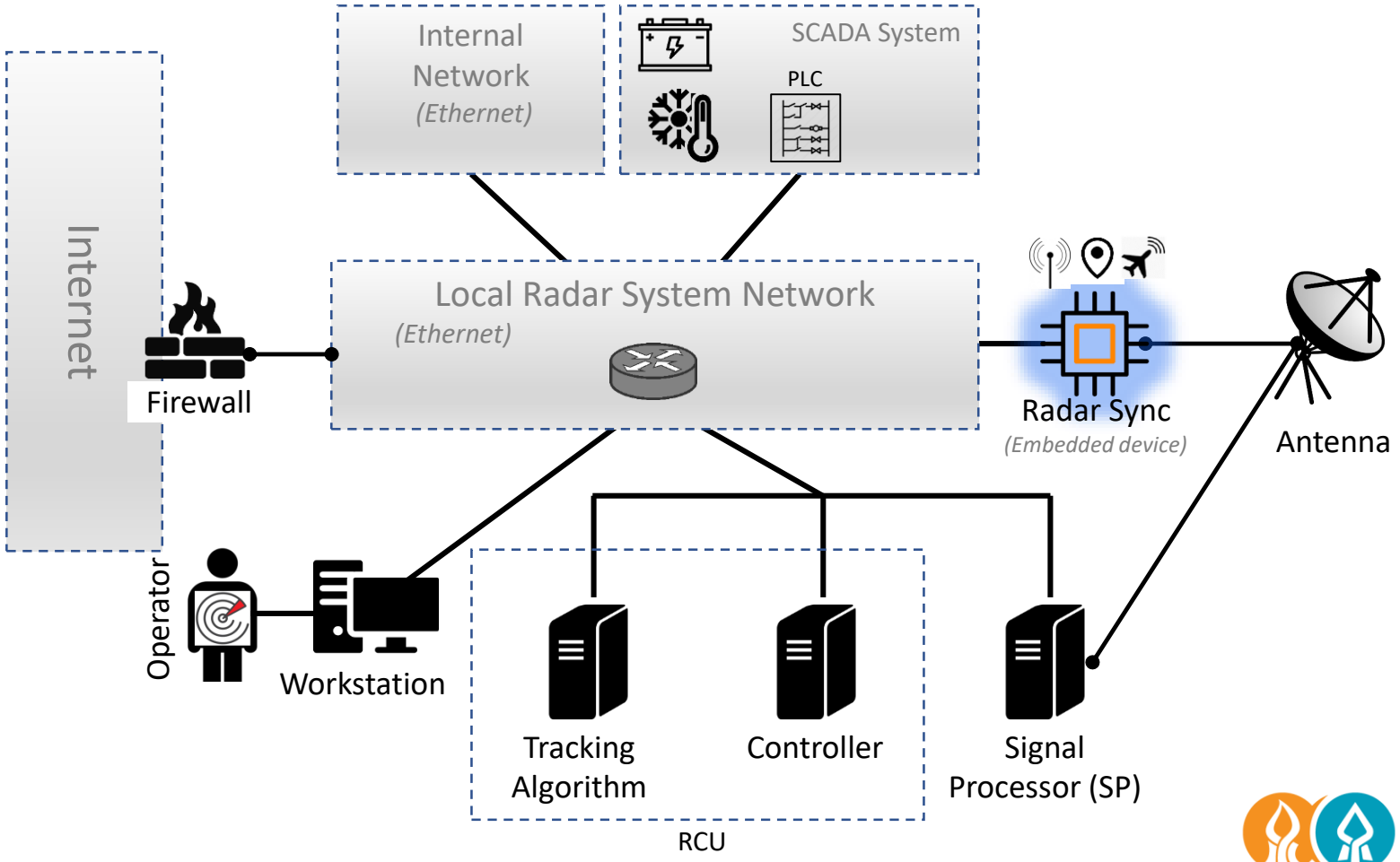
CBG Cyber@ Ben-Gurion University of the Negev

Radar trailer



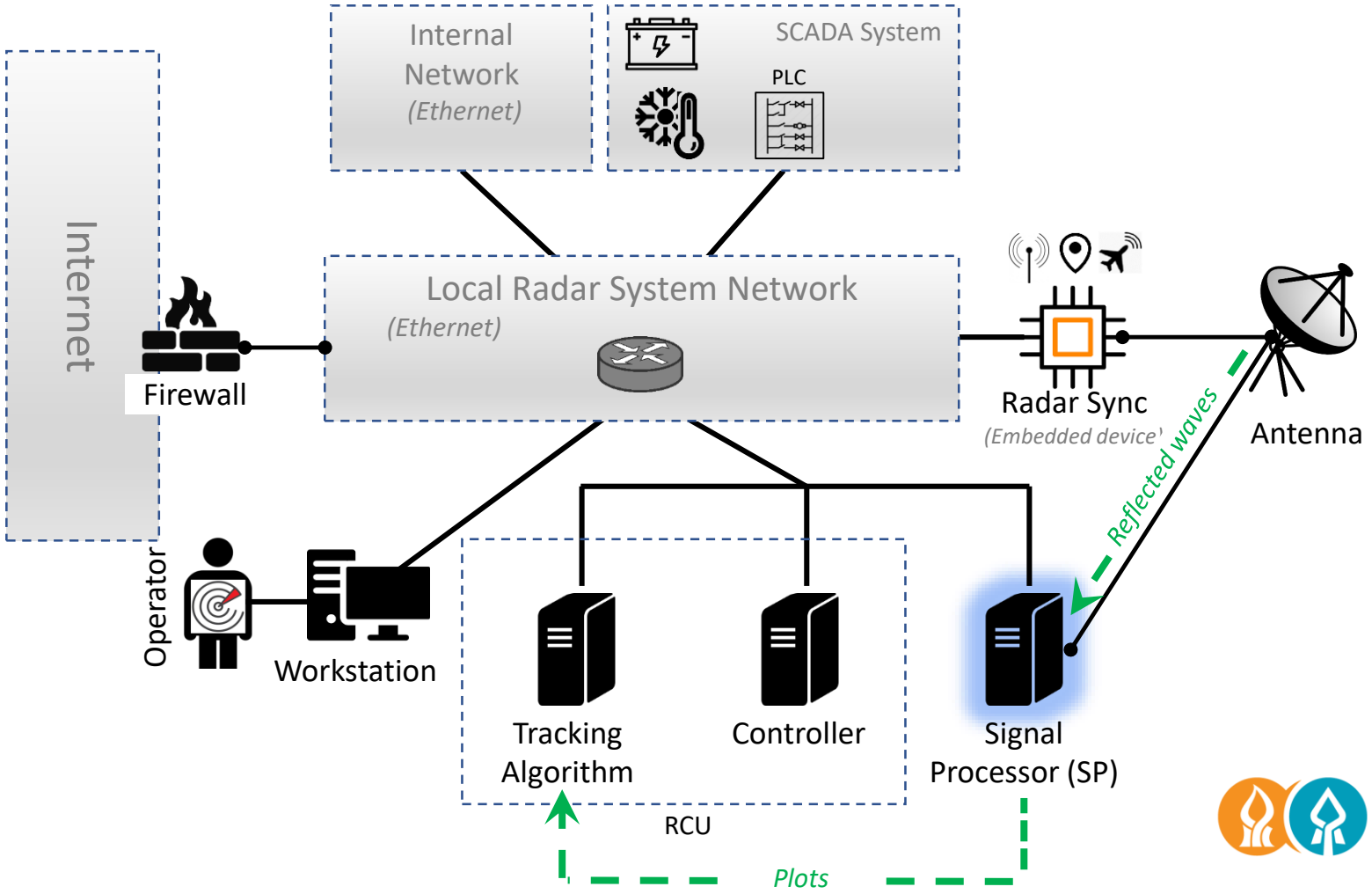
CBG Cyber@ Ben-Gurion University of the Negev

Radar trailer



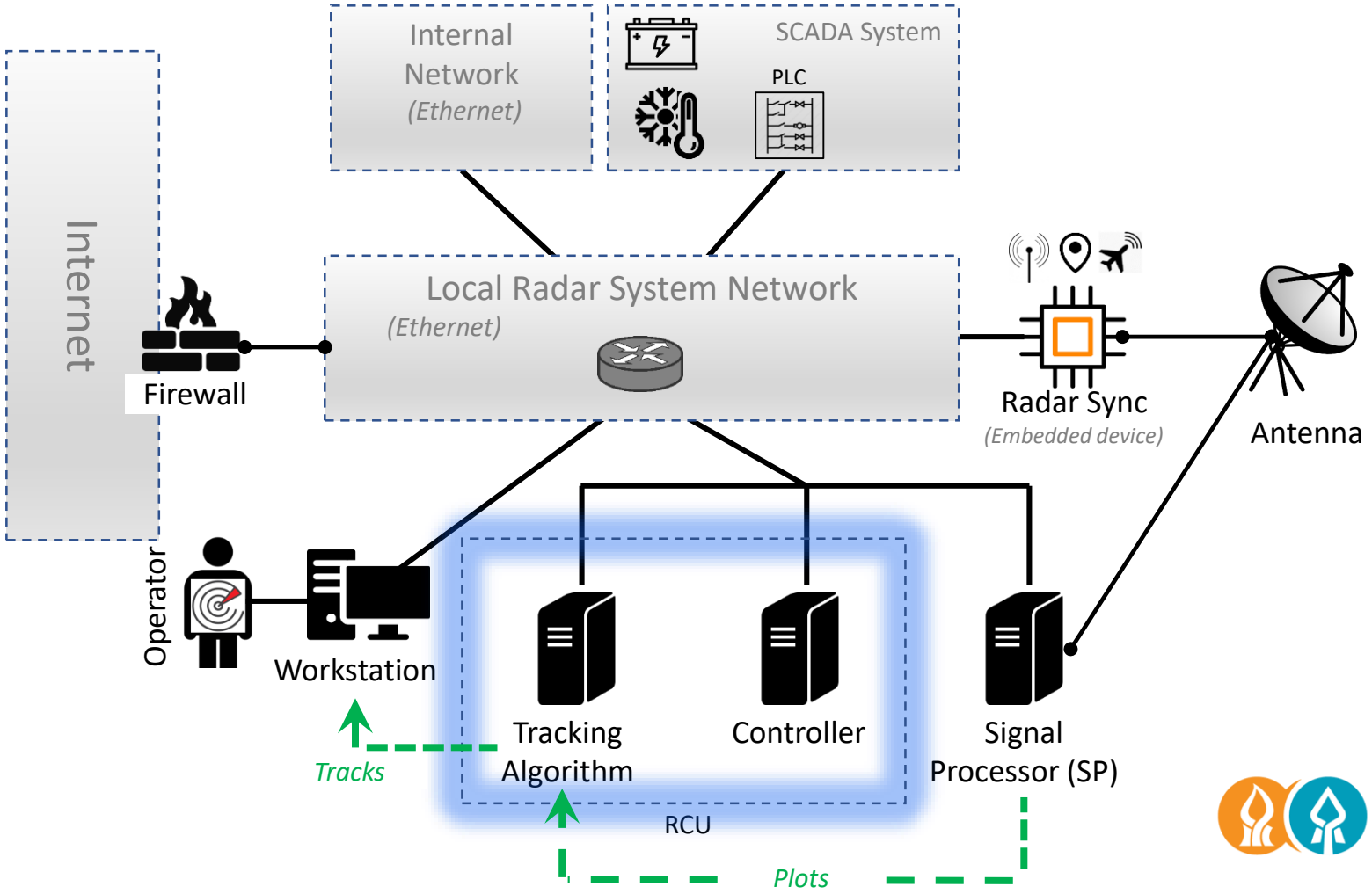
CBG Cyber@ Ben-Gurion University of the Negev

Radar trailer



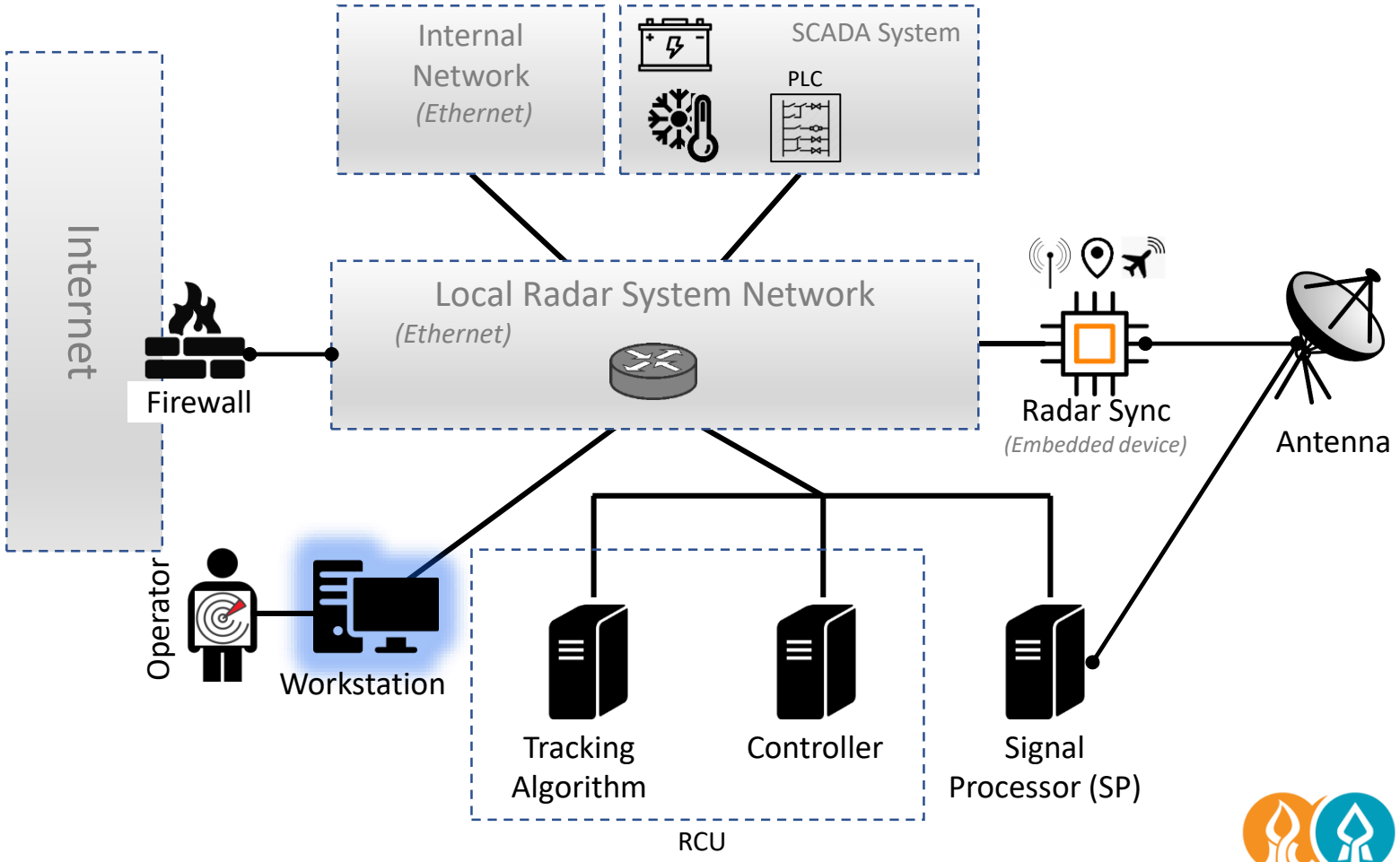
CBG Cyber@ Ben-Gurion University of the Negev

Radar trailer



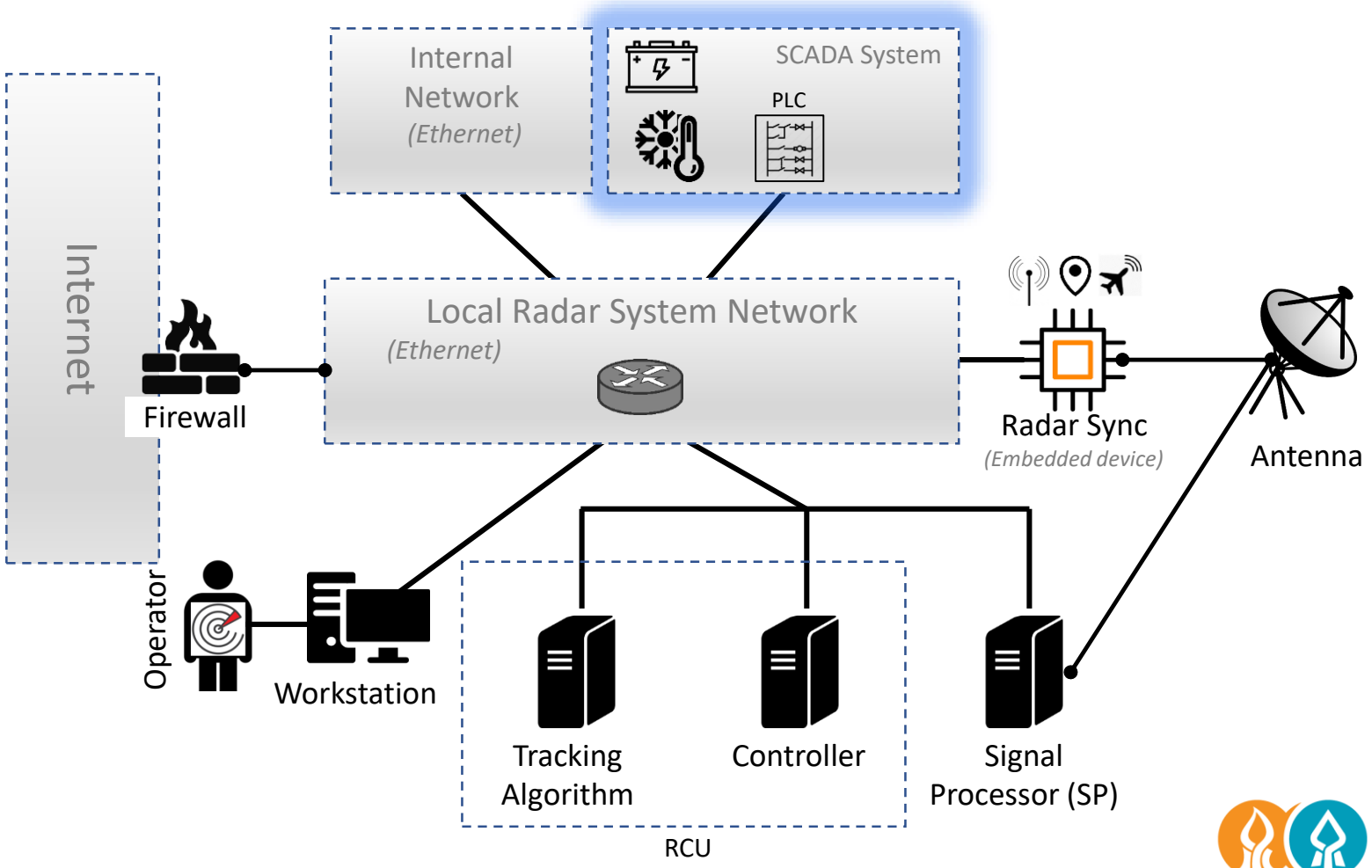
CBG Cyber@ Ben-Gurion University of the Negev

Radar trailer



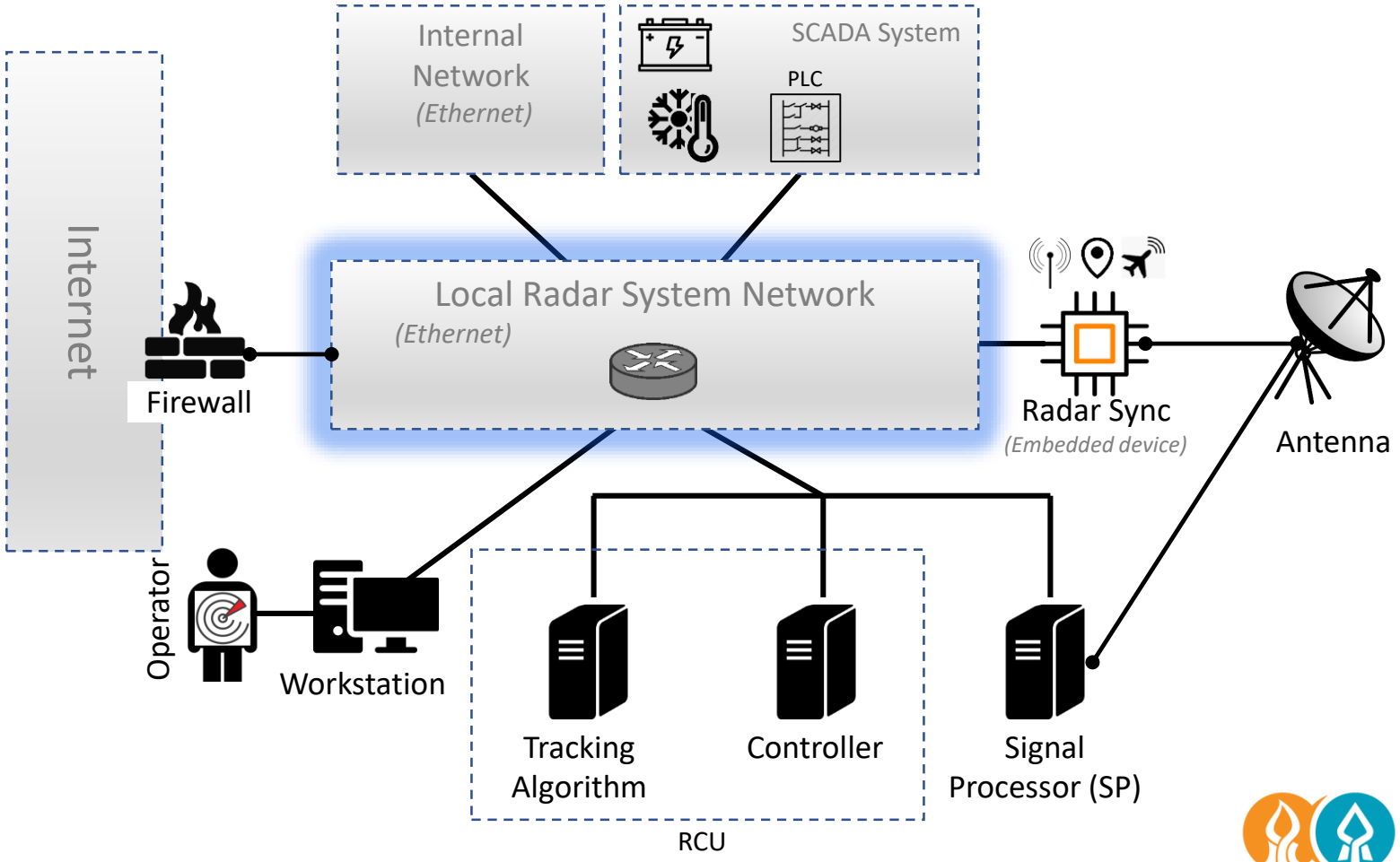
CBG Cyber@ Ben-Gurion University of the Negev

Radar trailer



CBG Cyber@ Ben-Gurion University of the Negev

Radar trailer



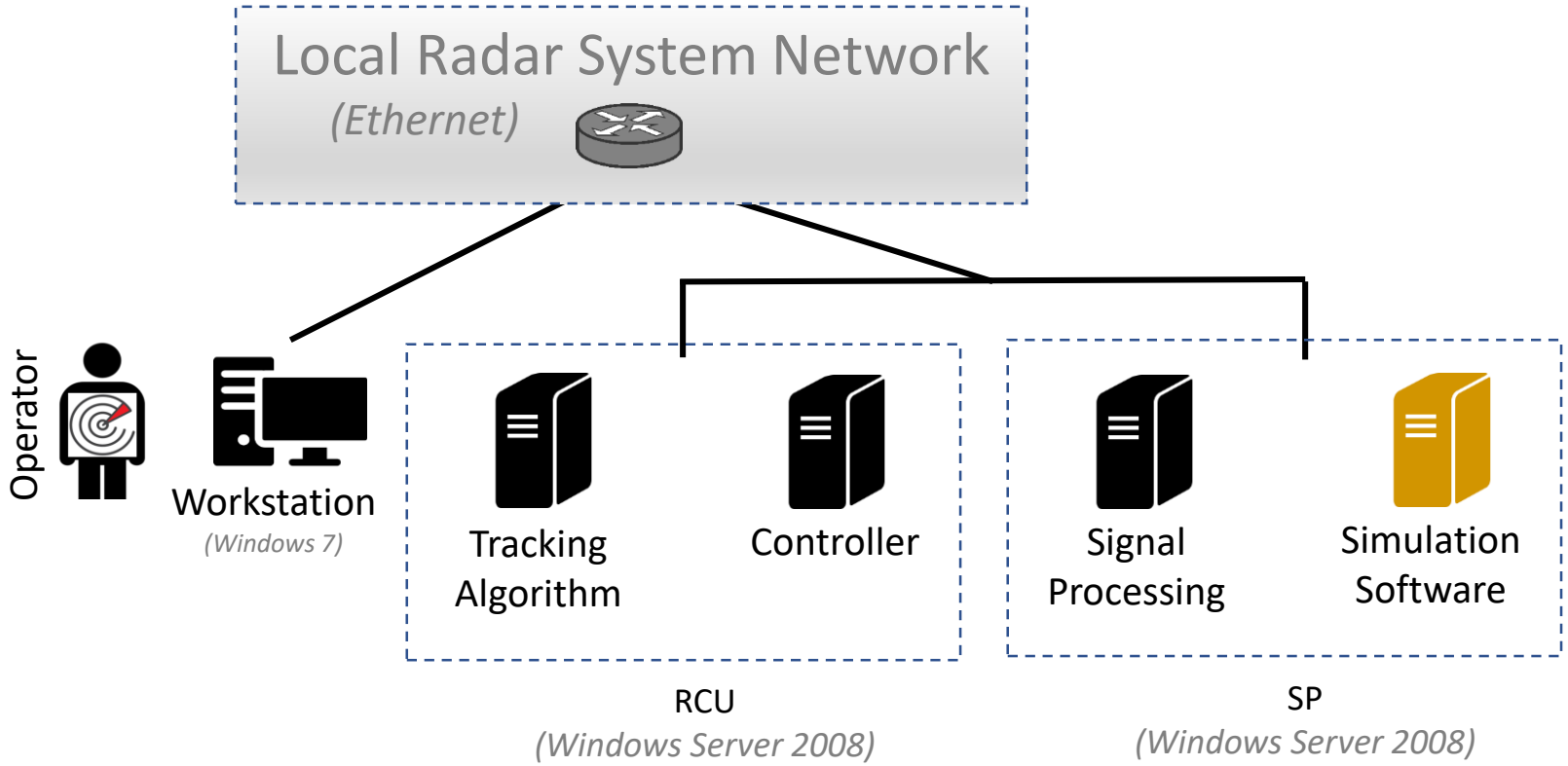
CBG Cyber@ Ben-Gurion University of the Negev

Testbed

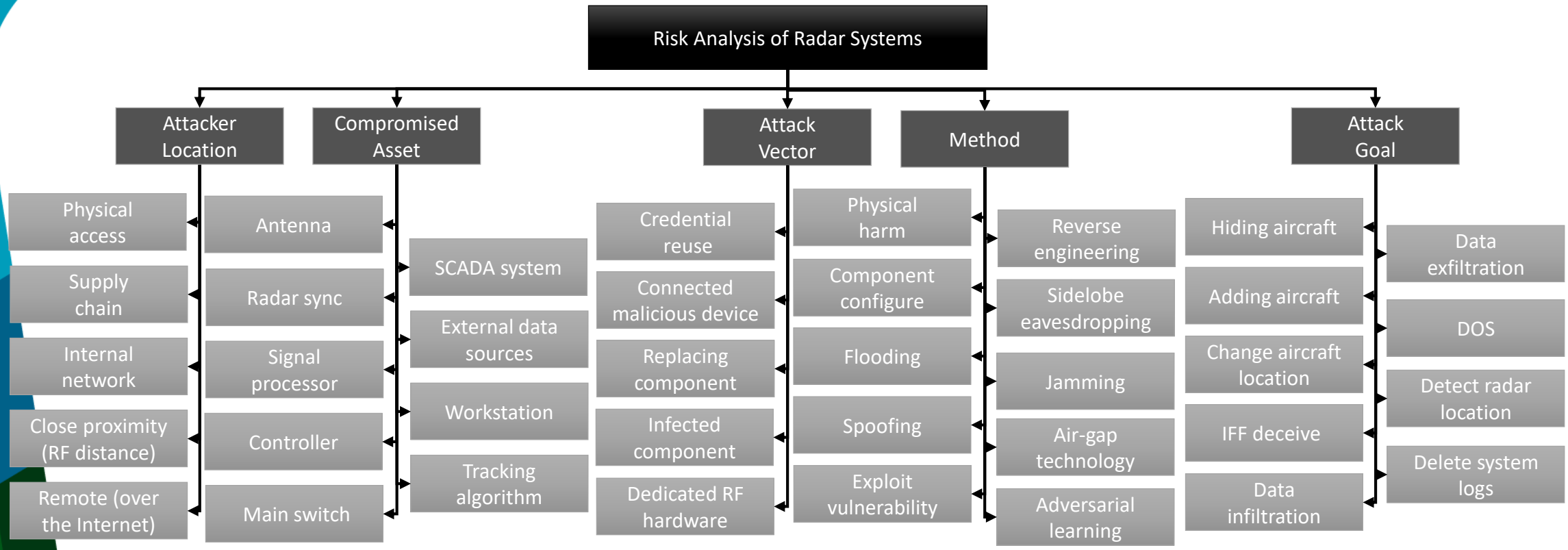
Description

- Subset of the components used in a real radar system created for this task.
- Based on monostatic radar and has detection, interrogation, decoding, and tracking capabilities.

Structure

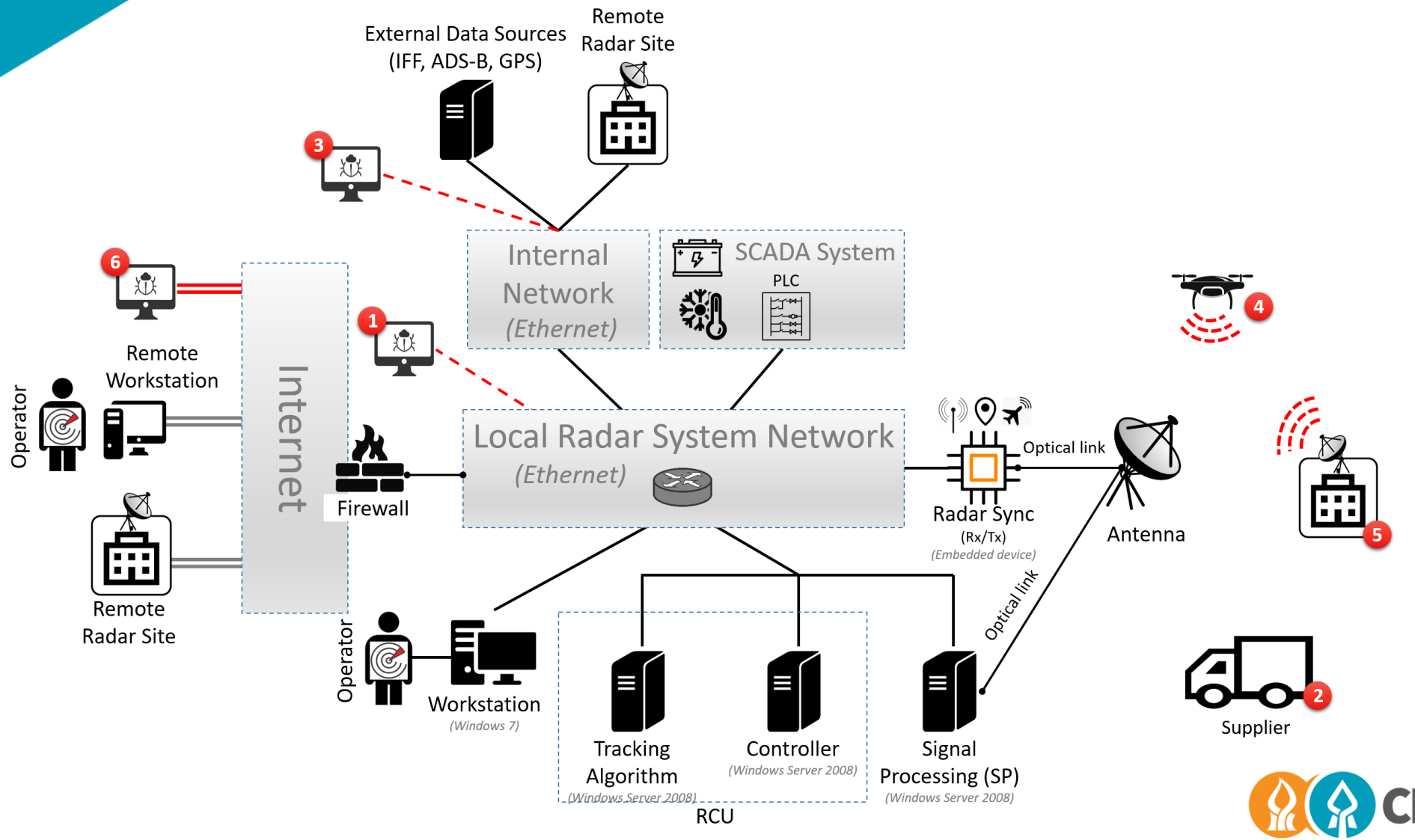


Taxonomy



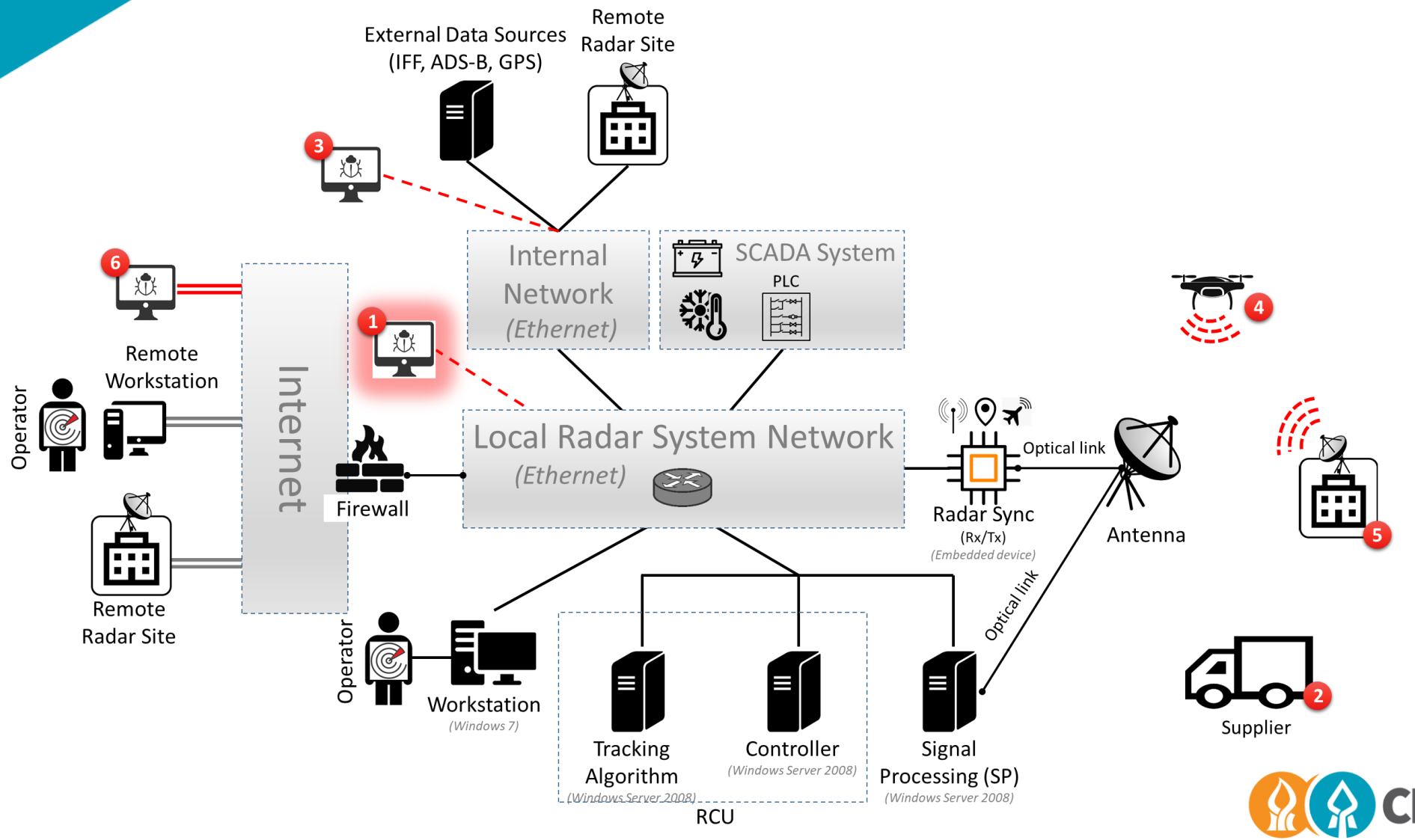
CBG Cyber@ Ben-Gurion University of the Negev

Attacker location



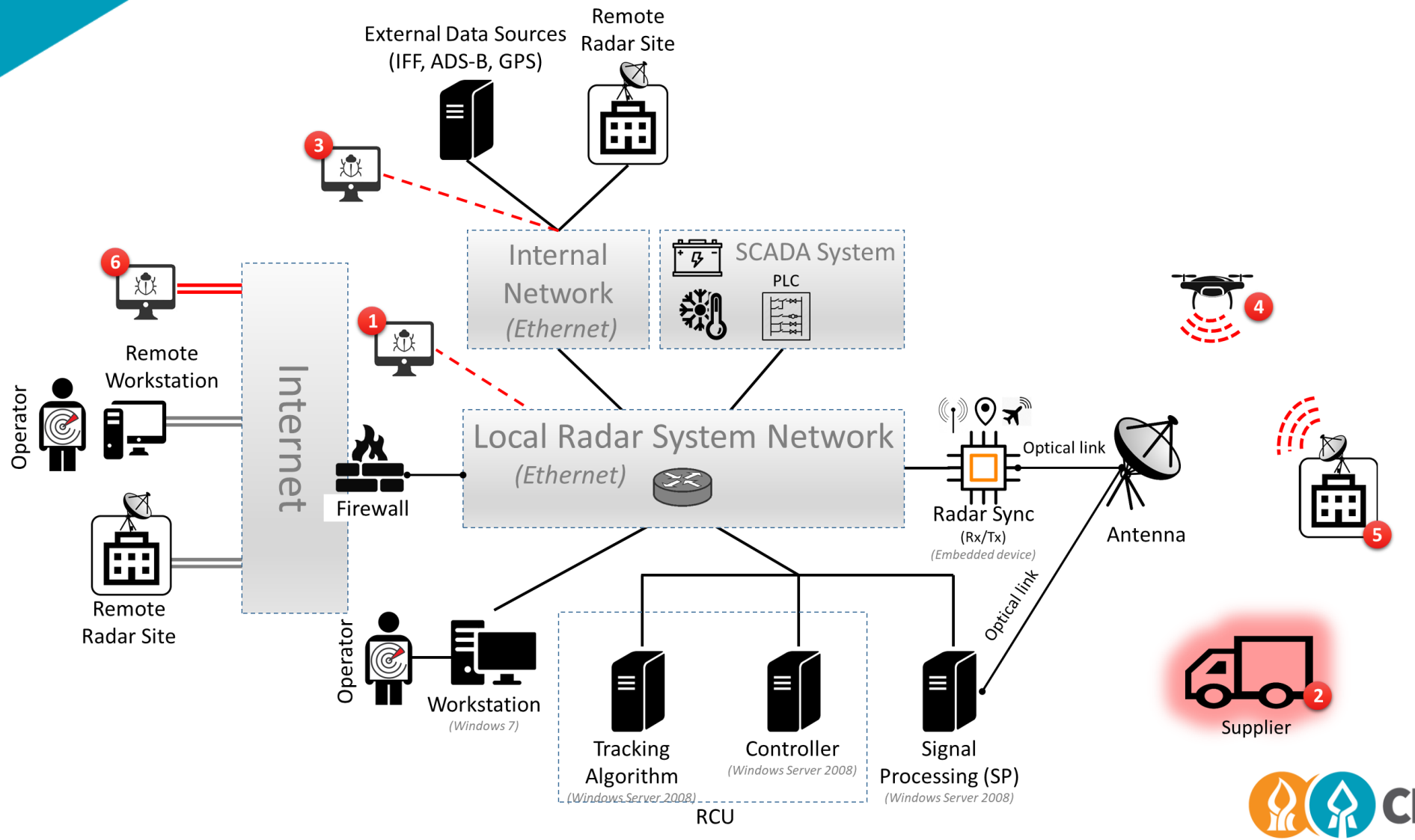
CBG Cyber@ Ben-Gurion University of the Negev

Attacker location



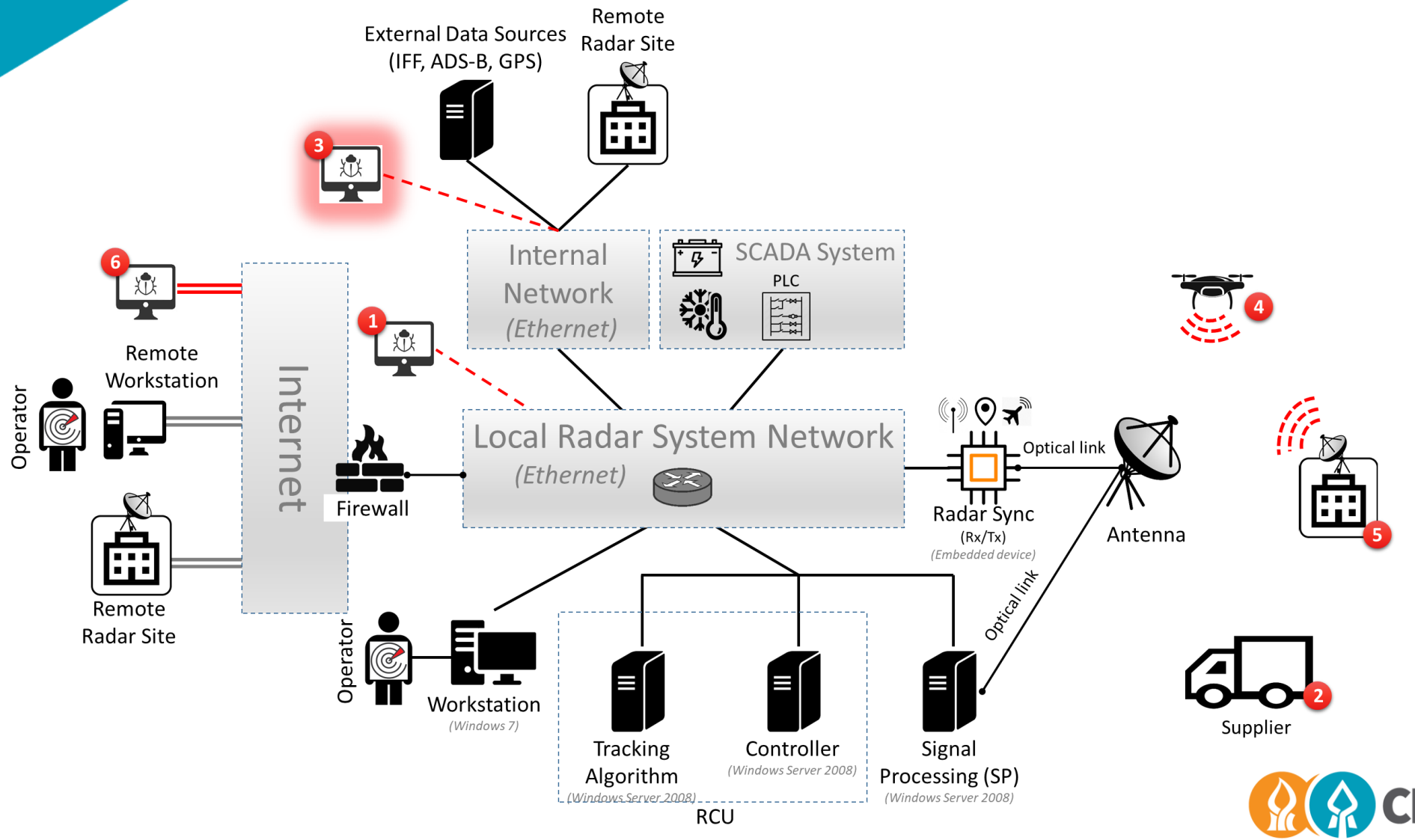
CBG Cyber@ Ben-Gurion University of the Negev

Attacker location



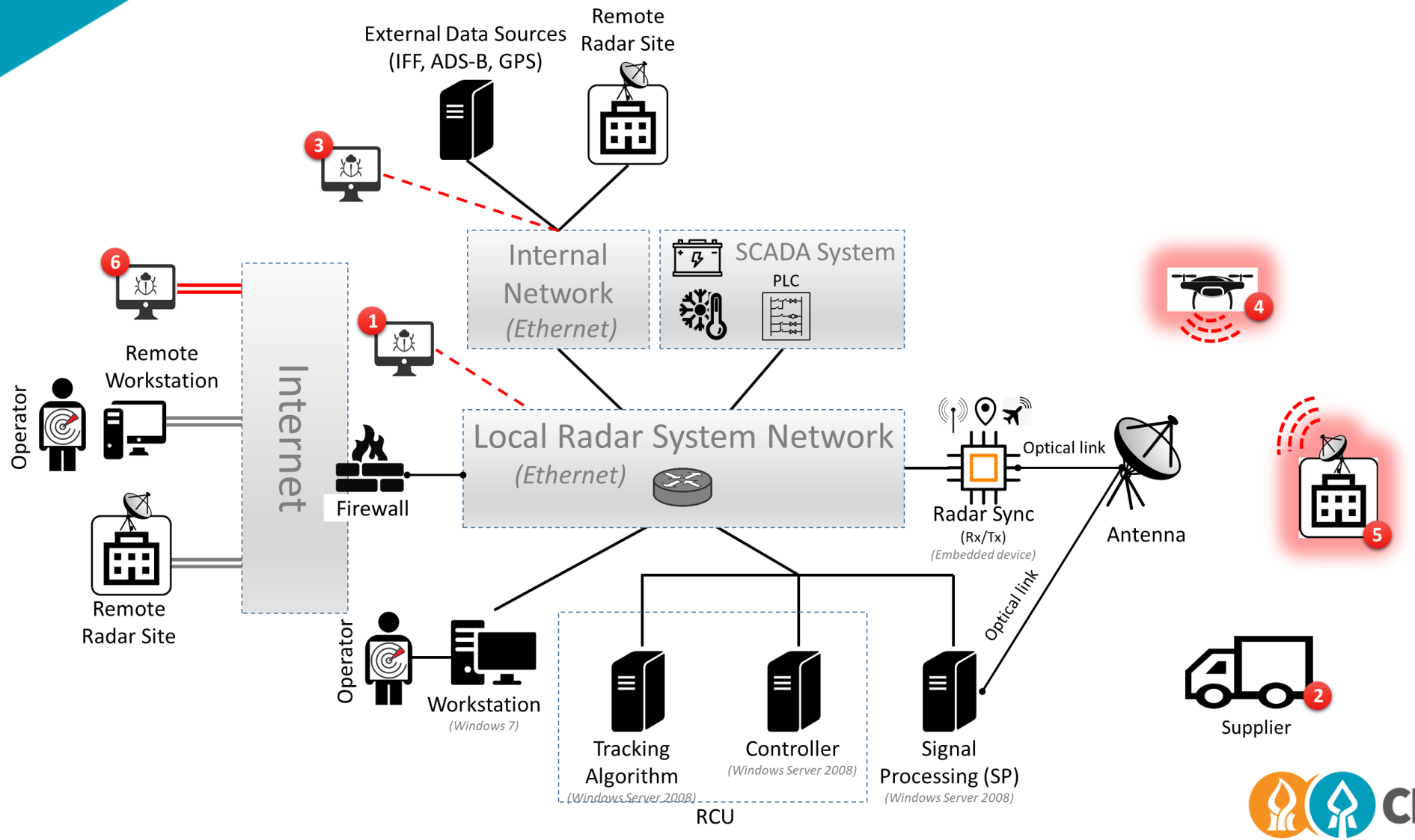
CBG Cyber@ Ben-Gurion University of the Negev

Attacker location



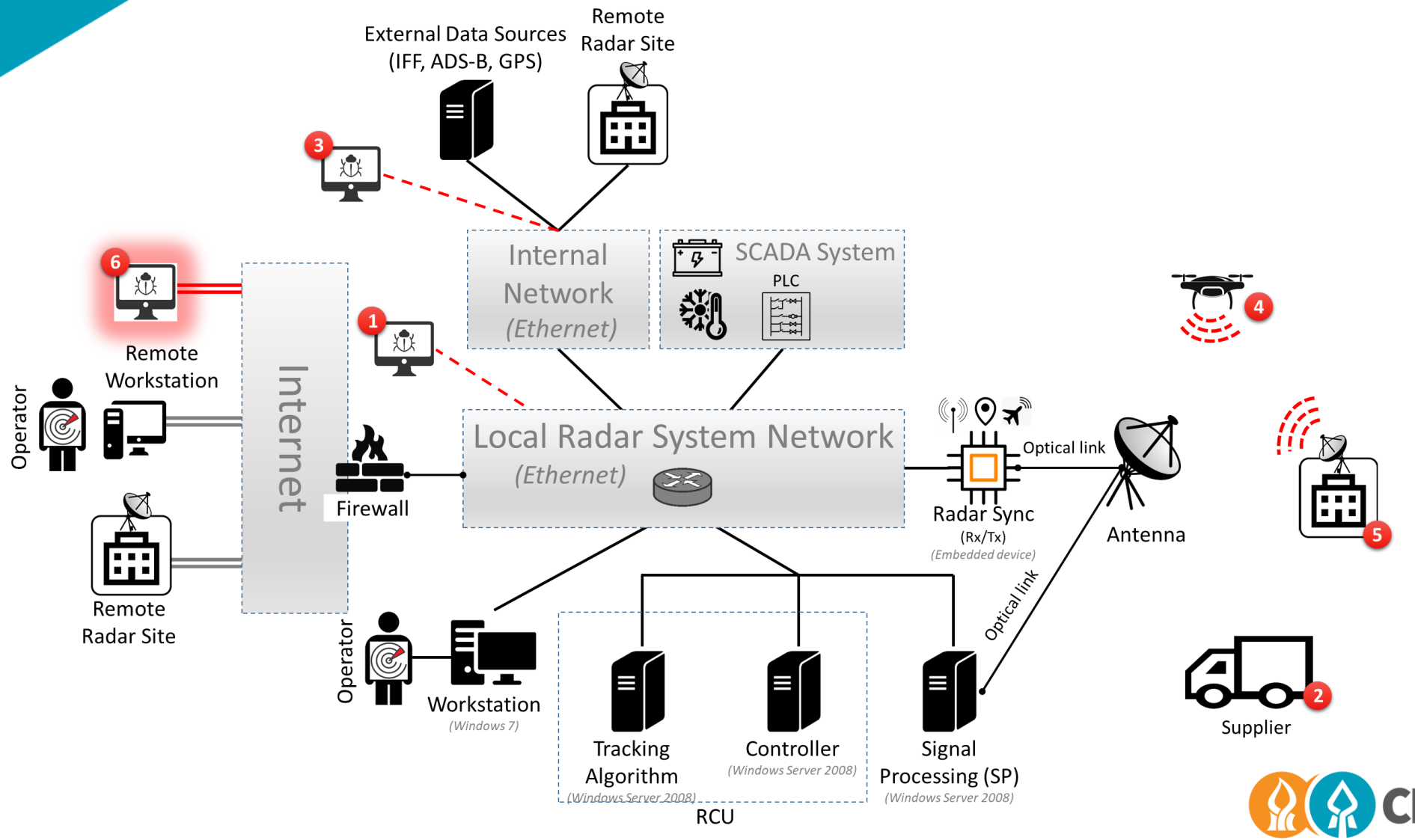
CBG Cyber@ Ben-Gurion University of the Negev

Attacker location



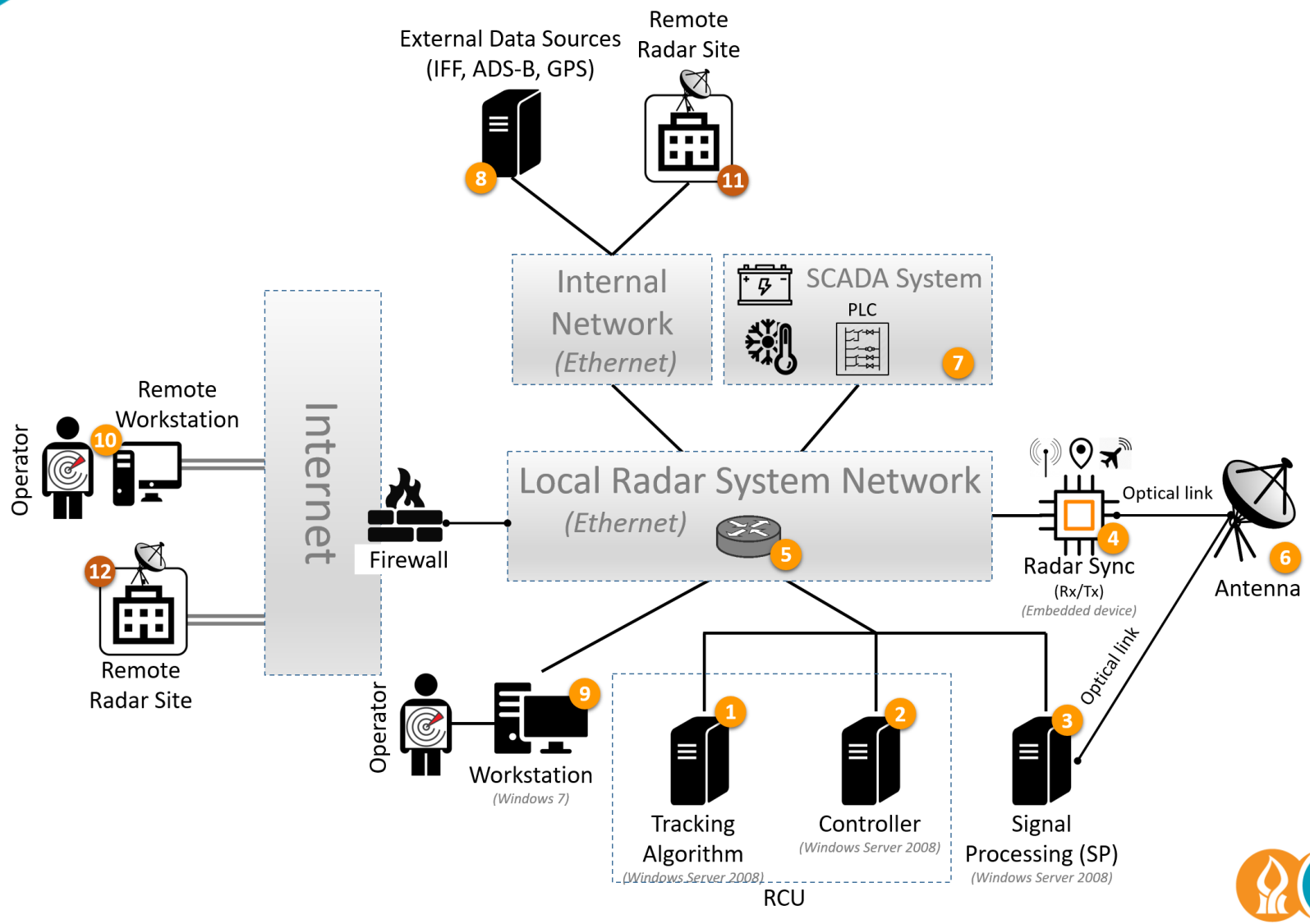
CBG Cyber@ Ben-Gurion University of the Negev

Attacker location



CBG Cyber@ Ben-Gurion University of the Negev

Compromised asset



CBG Cyber@ Ben-Gurion University of the Negev

Attack vector

- This is the action the attacker performs in order to initiate the attack. Possible attack vectors:
  - Credential reuse
  - Connected malicious device
  - Replacing component
  - Supply chain infected component
  - Dedicated hardware – Using any hardware with RF capability that is in a close range to the radar antenna

Attack Goal

- Hiding aircraft
- Adding aircraft
- Change aircraft location
- IFF deceive

Integrity

- Data exfiltration
- Data infiltration
- Detect radar location

Confidentiality

- DOS
- Delete system logs

Availability

Method

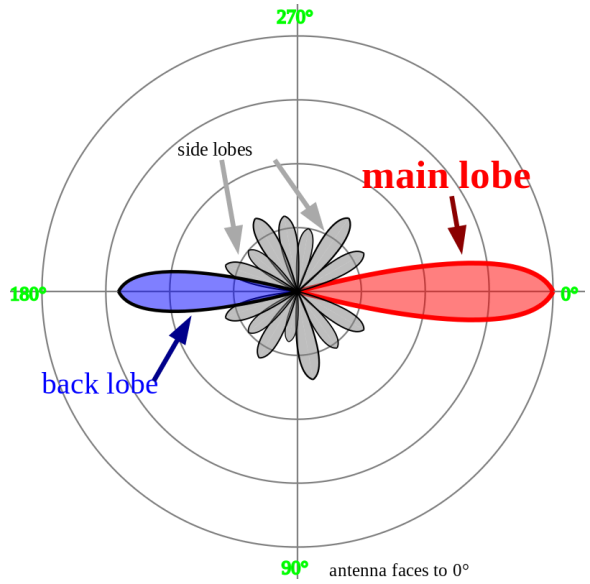
- The additional technology or techniques the attacker uses in order to implement the attack and achieve his/her goals The relevant methods we identify in our system are:

  - Physical harm
  - Component configure
  - Flooding – overload radar network components
  - Spoofing (e.g., ARP poisoning, IP spoofing)
  - Signal jamming - use of electromagnetic energy in order to confuse the system
  - Exploit vulnerability
  - Air-gap technology
  - Reverse engineering

Method

Sidelobe eavesdropping

Radar antenna radiates energy to other directions besides the main direction, thereby creating sidelobes.
These sidelobes could contain valuable information for the attacker, and by analyzing them, the attacker can figure out the antenna's direction or determine some of the antenna's classified parameters.



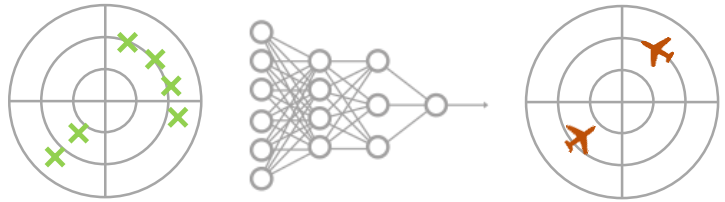
CBG Cyber@ Ben-Gurion University of the Negev

Method

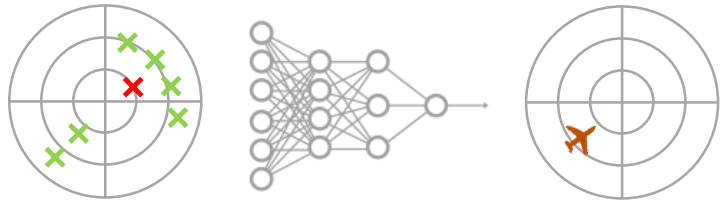
Adversarial learning (AL)

Machine learning (ML) domain, dealing with the manipulation of ML models

An attacker can use AL techniques in order to manipulate the radar's object detection or classification models, as well as jamming detectors.



Regular data



Adversarial learning attack

CBG Cyber@ Ben-Gurion University of the Negev

Method

Adversarial learning - example

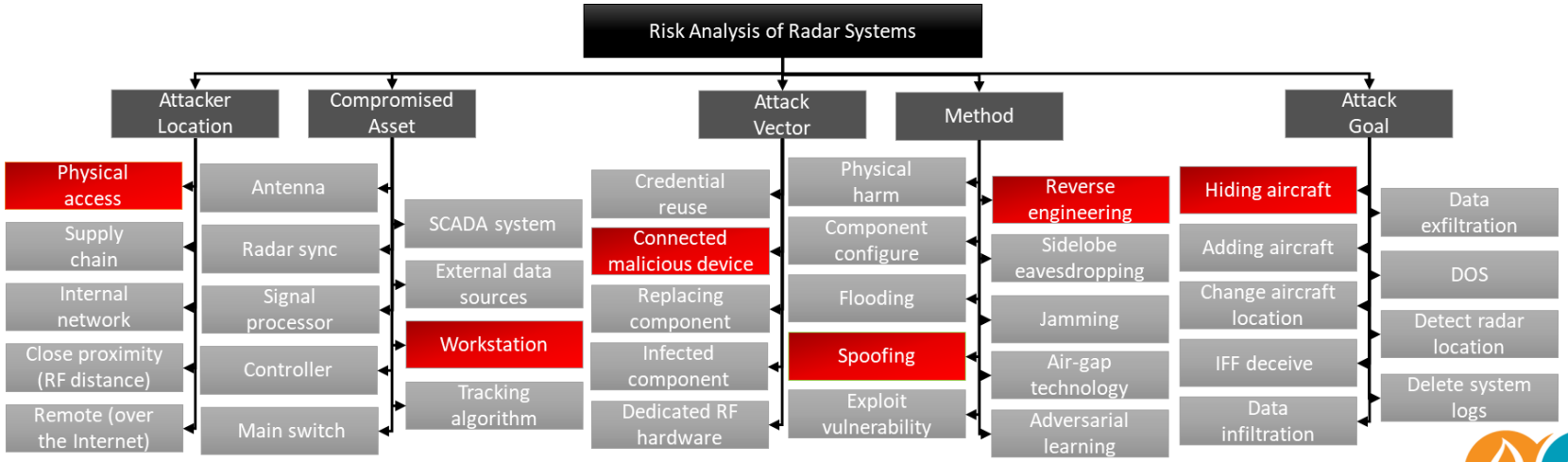
- LiDAR (Light Detection and Ranging) used laser beams to measure the target location
- The LiDAR technology is very similar to Radar
- Some examples of adversarial attacks on LiDAR technology as successfully shown at:
  - Cao, Yulong, et al. "Adversarial objects against lidar-based autonomous driving systems." *arXiv preprint arXiv:1907.05418* (2019).
  - Cao, Yulong, et al. "Adversarial sensor attack on lidar-based perception in autonomous driving." *arXiv preprint arXiv:1907.06826* (2019).

Attack POC

Attack Description

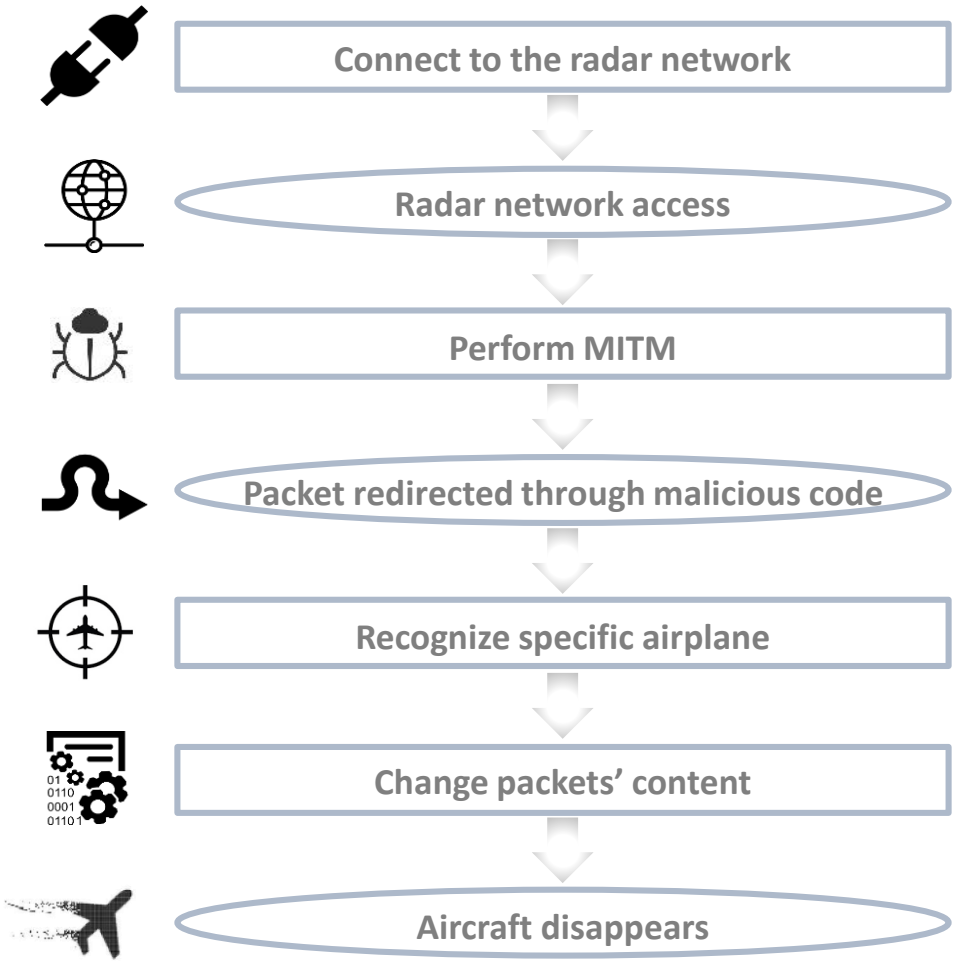
We choose to provide POC for the chosen scenario:

- Attacker location – physical access
- Attack goal – hiding a specific aircraft
- Attack vector – connected malicious device
- Attack method – reverse engineer the radar then change packet content (i.e. spoofing)



CBG Cyber@ Ben-Gurion University of the Negev

Attack flow



CBG Cyber@ Ben-Gurion University of the Negev

POC Goal

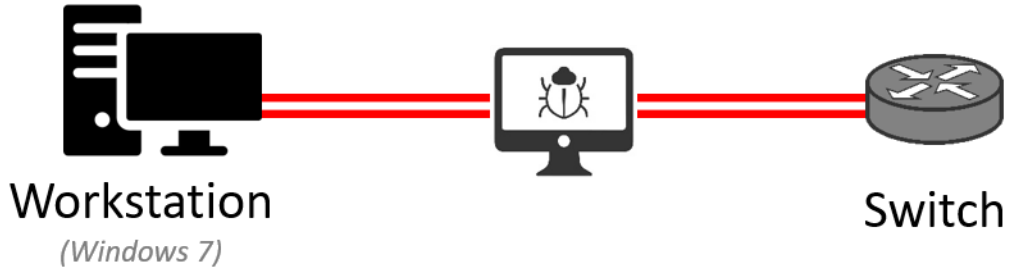
Prove the ability of a malicious actor to reverse engineer the radar and hide a specific aircraft from the system operator

POC implementation stages

- Connect the malicious device
- Reverse engineer the radar networking protocols
- Write and execute the attack code

POC setup

The first laptop network card was connected to the switch, and the other one was connected to the workstation

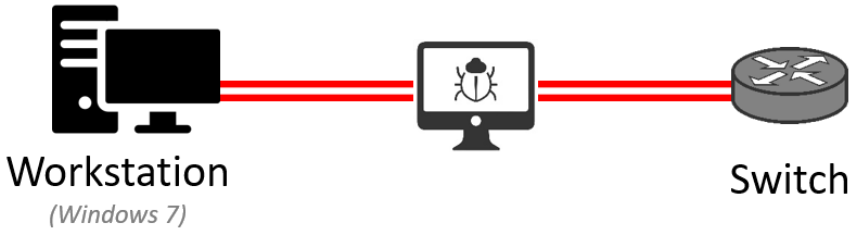


POC reverse engineering Application layer

- Object properties has defined using 32 bytes of data, only four of them are used to describe the object's location
- The object's location has defined with Polar coordinate, two bytes described the radius and two bytes described the angular location of the object

POC attack code

- Open TCP sockets with workstation and with the other radar components
- Route the radar packets between the radar components and the workstation
- Recognize object within the packets and delete them
- Create a new moving object at the workstation screen



POC results

- Object data were manipulated by the attack code, such that:
  - No object appeared on the workstation screen
  - We create a new moving object at the workstation screen
  - No alarm has appeared at the workstation screen

Conclusion

- Radar systems may be vulnerable to cyber attack
- This research emphasizes the need for additional research in the area of radar and cyber security

Additional research – adversarial learning

- Investigate both the ability of a malicious actor to attack and compromise the machine learning algorithms used by the radar (Classification models, Jamming models, etc.)

Additional research – Data infiltration

- identifying covert channel infiltration methods such as:
  - Flight patterns
  - ADS-B
  - Firewall logs
  - Side-channel DoS
- developing detection/prevention methods.

Additional research – sidelobes eavesdropping

- Evaluate the use of sidelobes as a means of extracting valuable information about the radar such as:
  - Radar location
  - Radar parameters

- developing detection/prevention methods.

Questions?