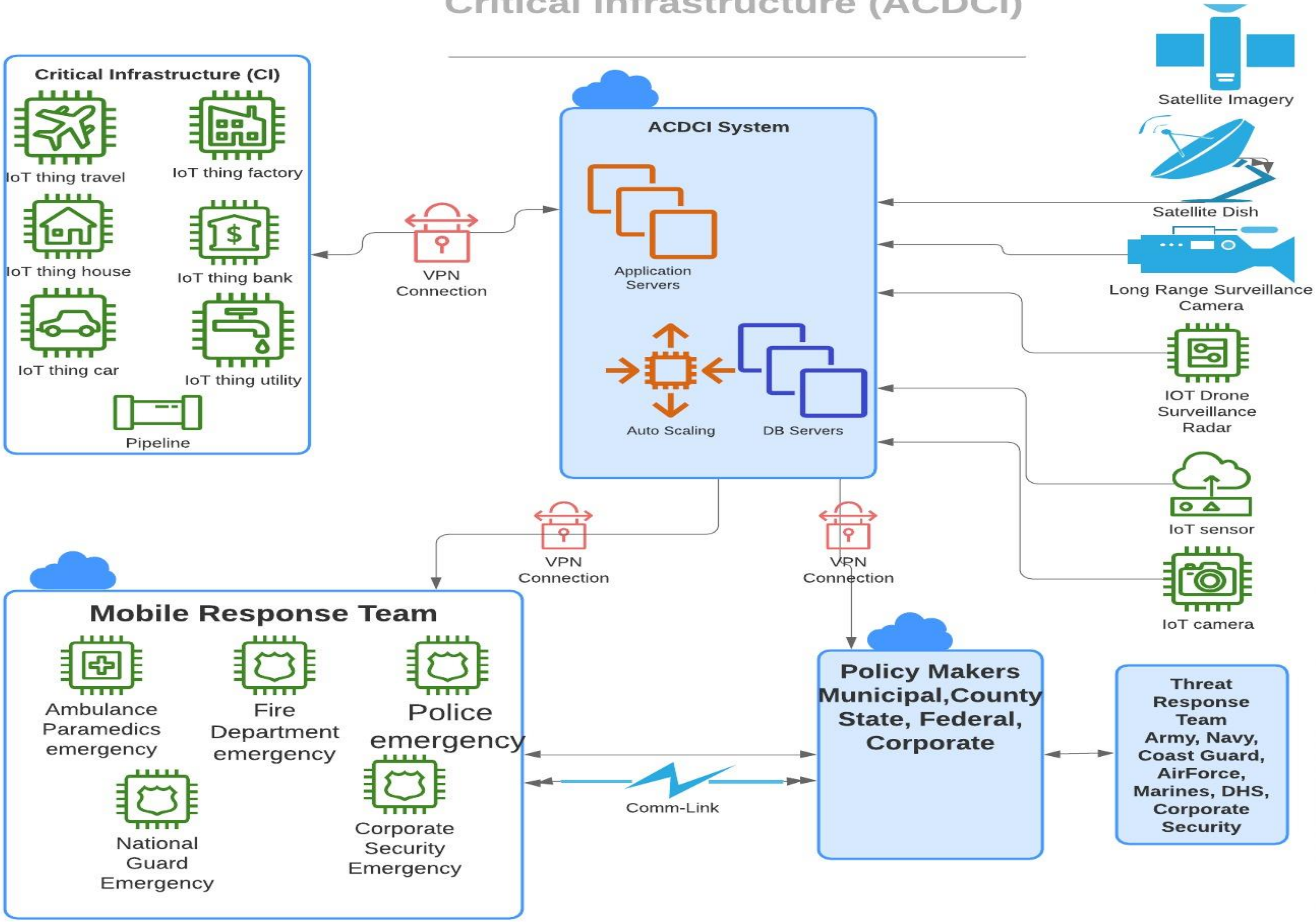
OPENC2 Active Cyber Defense of Critical Infrastructure (ACDCI) Use Case

OPENC2 Active Cyber Defense of Critical Infrastructure (ACDCI)



Critical Infrastructure (CI)

IoT thing travel

IoT thing factory

IoT thing house

IoT thing bank

IoT thing car

IoT thing utility

Pipeline

VPN Connection

ACDCI System

Application Servers

Auto Scaling

DB Servers

Satellite Imagery

Satellite Dish

Long Range Surveillance Camera

IOT Drone Surveillance Radar

IoT sensor

IoT camera

VPN Connection

VPN Connection

Mobile Response Team

Ambulance Paramedics emergency

Fire Department emergency

Police emergency

National Guard Emergency

Corporate Security Emergency

Comm-Link

Policy Makers Municipal,County State, Federal, Corporate

Threat Response Team Army, Navy, Coast Guard, AirForce, Marines, DHS, Corporate Security

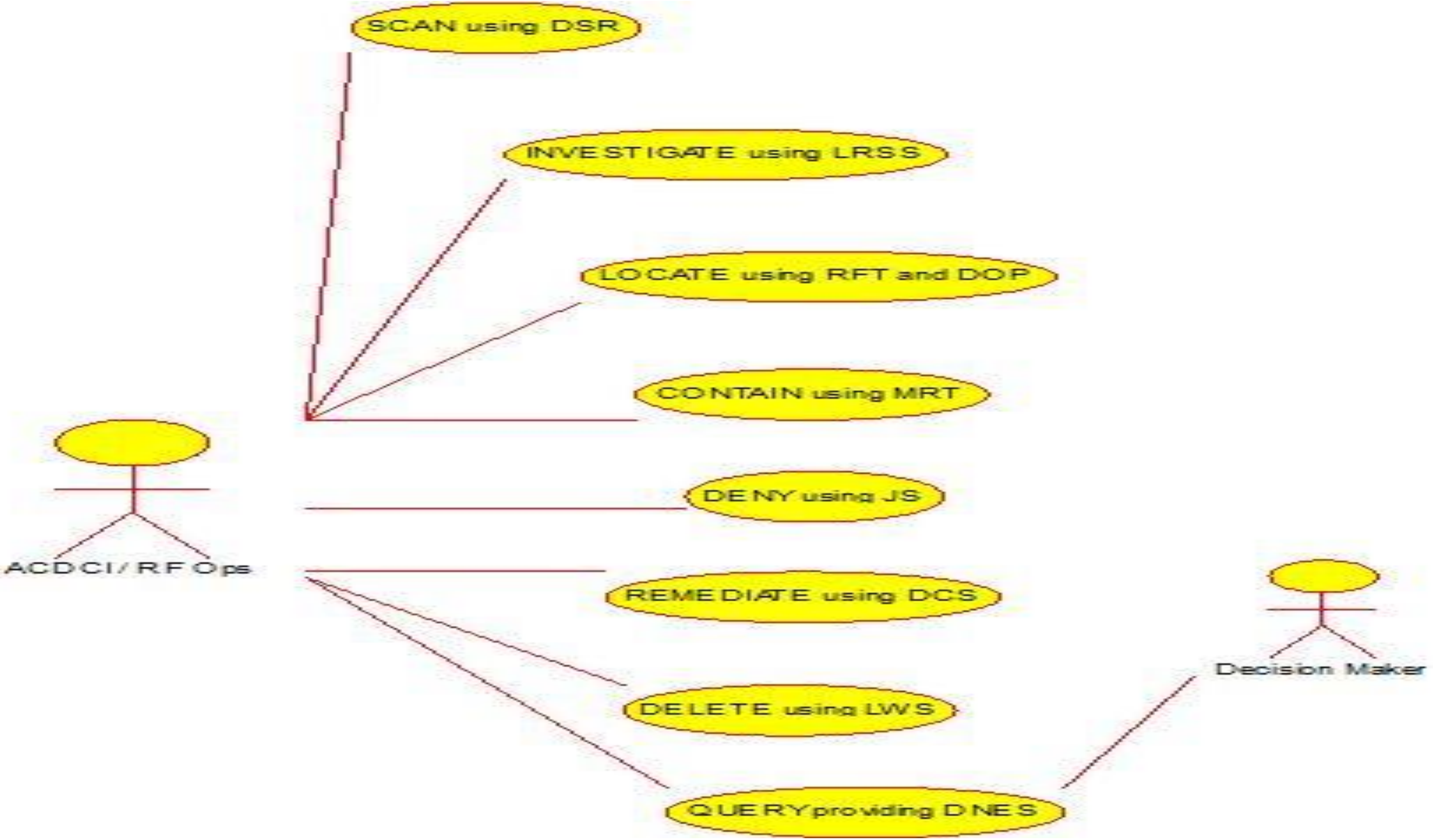
Drone Threat

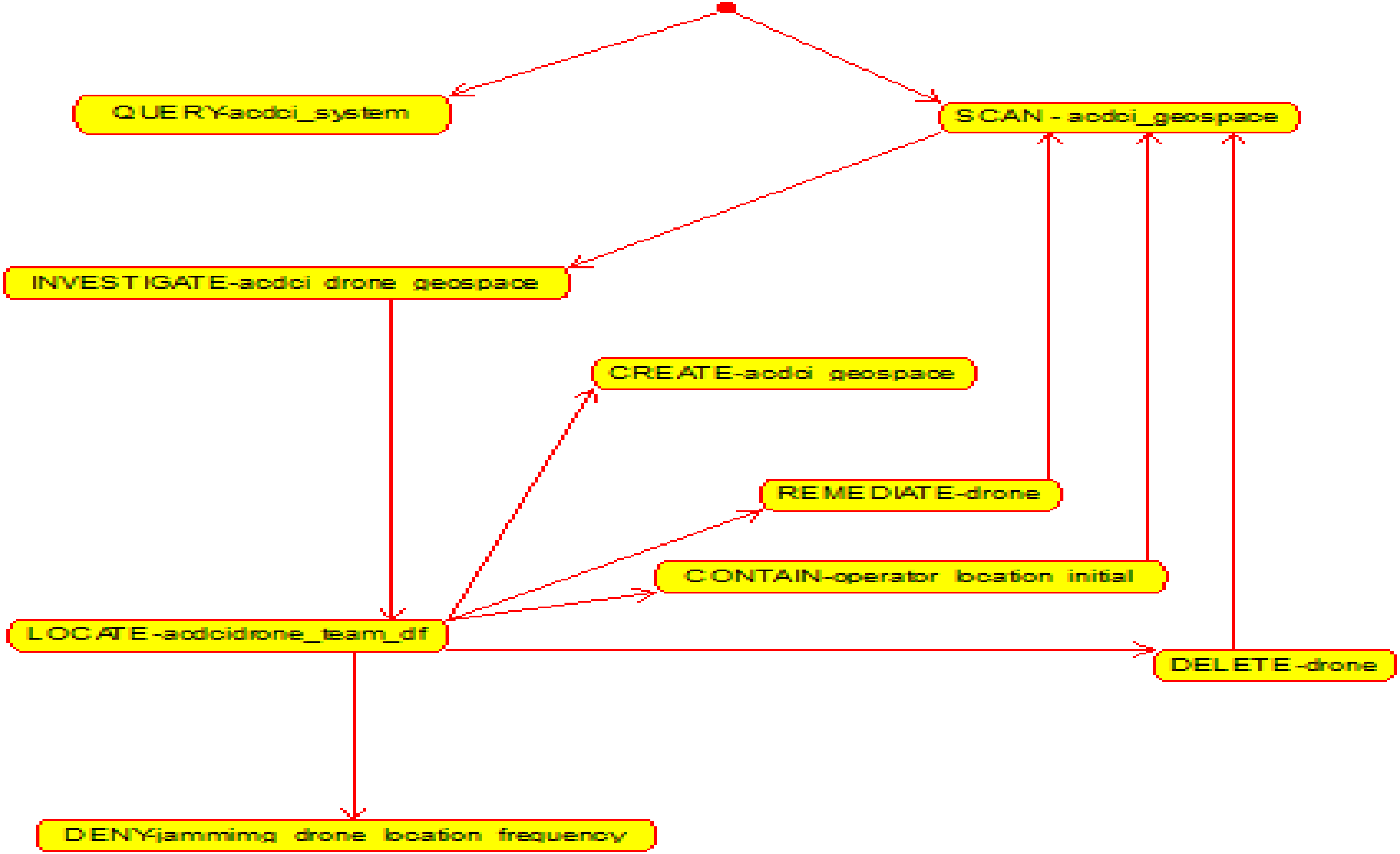
Terrestrial Robot Threat

Underwater Drone Threat

Tsunami,

Earthquake, Cyclone, Tornado, Volcanic Eruption, Hurricane Threat


SCAN using DSR
INVESTIGATE using LRSS
LOCATE using RFT and DOP
CONTAIN using MRT
DENY using JS
REMEDIATE using DCS
DELETE using LWS
QUERY providing DNES
ACDCI / RF Ops
Decision Maker


QUERY-acdci_system
SCAN - acdci_geospace
INVESTIGATE-acdci drone geospace
CREATE-acdci geospace
REMEDIATE-drone
CONTAIN-operator location initial
LOCATE-acdcidrone_team_df
DELETE-drone
DENY-jammimg drone location frequency

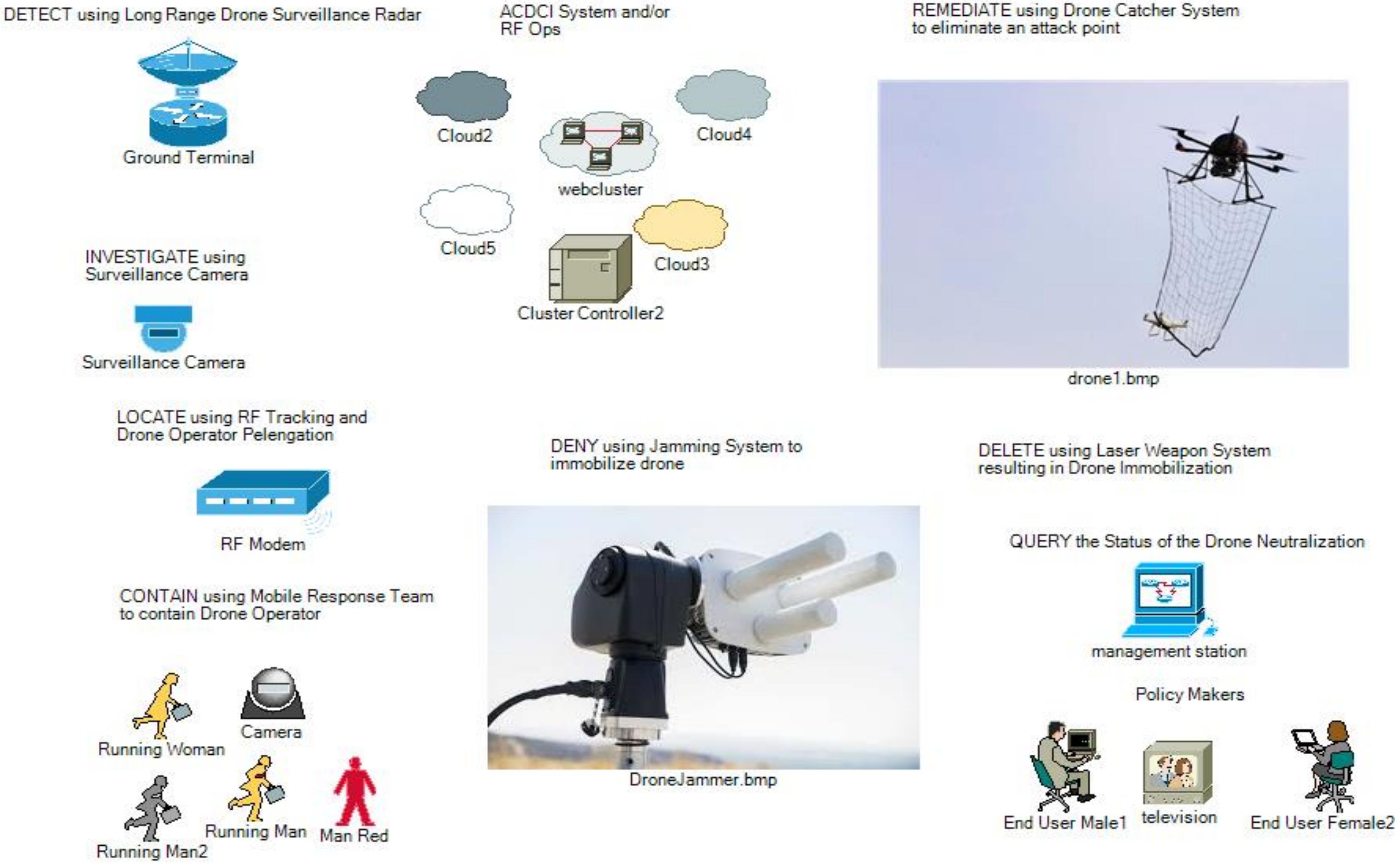
OpenC2 Orchestrator to Actuators Diagram

The GKE cluster master acts as the OpenC2 orchestrator communicating to eight GKE nodes providing the functionality for eight OpenC2 actuators■

- ACDCI/RF Ops – OpenC2 Orchestrator
- Active Cyber Defense of Critical Infrastructure (ACDCI) /Radio Frequency (RF) Ops will be hosted within the GKE cluster master.
- This is the OpenC2 Orchestrator aka Producer
- Decision Makers functionality will be hosted within the GKE cluster master.

- 8 OpenC2 Commands sent to Actuators aka Consumers
- 1. SCAN using Drone Surveillance Radar (DSR)
- 2. INVESTIGATE using Long Range Surveillance System (LSRS)
- 3. LOCATE using Radio Frequency Tracking (RFT) and Drone Operator Pelengation (DOP)
- 4. CONTAIN Drone Operator
- 5. DENY using Jamming System (JS)
- 6. REMEDIATE using Drone Catcher System (DCS)
- 7. DELETE using Laser Weapon System (LWS) Optional
- 8. QUERY to obtain Drone Neutralization Effort Status (DNES)

Active Cyber Defense of Critical Infrastructure (ACDCI) Use Case



DETECT using Long Range Drone Surveillance Radar

INVESTIGATE using Surveillance Camera

LOCATE using RF Tracking and Drone Operator Pelengation

CONTAIN using Mobile Response Team to contain Drone Operator

ACDCI System and/or RF Ops

DENY using Jamming System to immobilize drone

DroneJammer.bmp

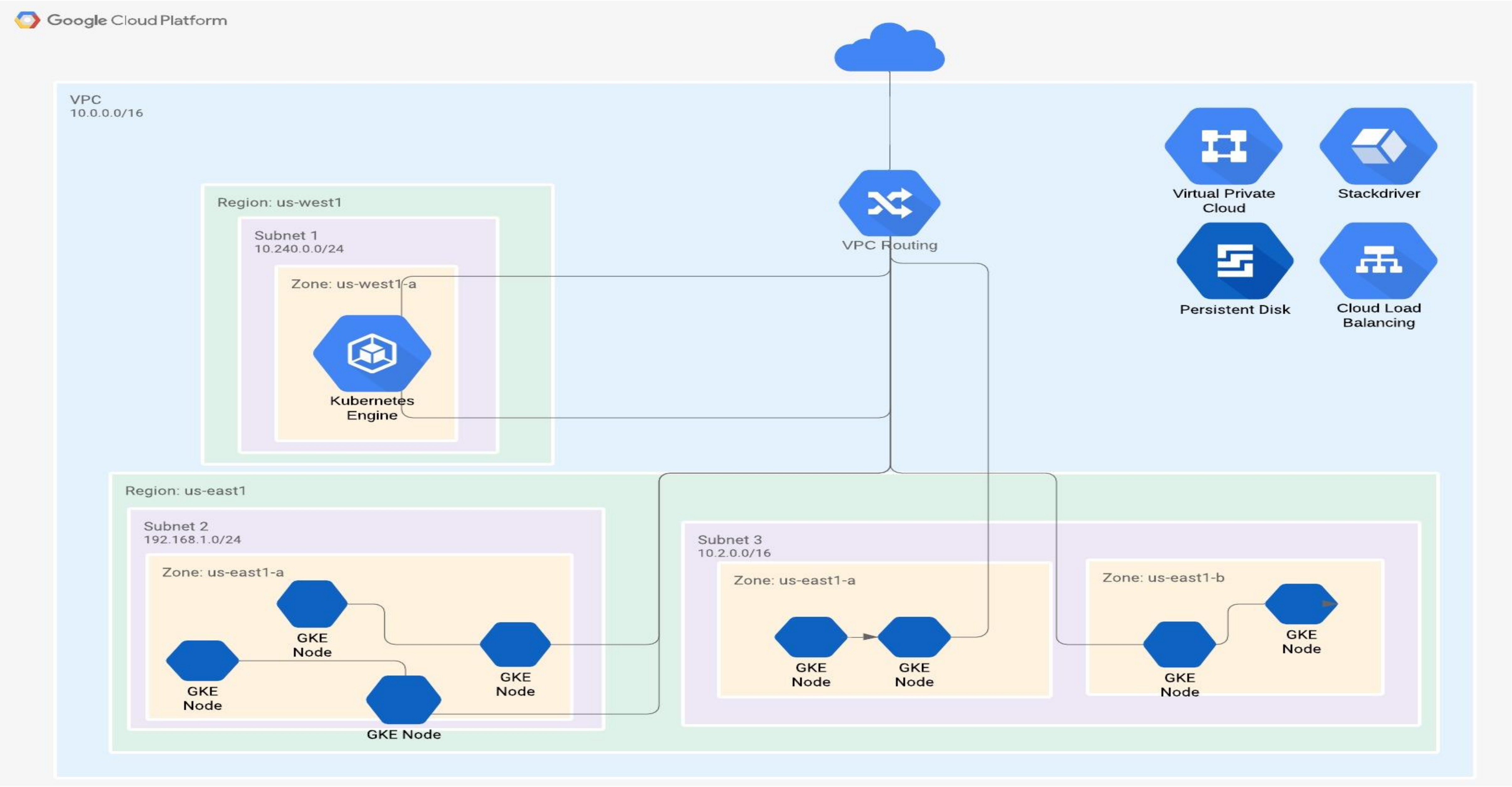
REMEDIATE using Drone Catcher System to eliminate an attack point

drone1.bmp

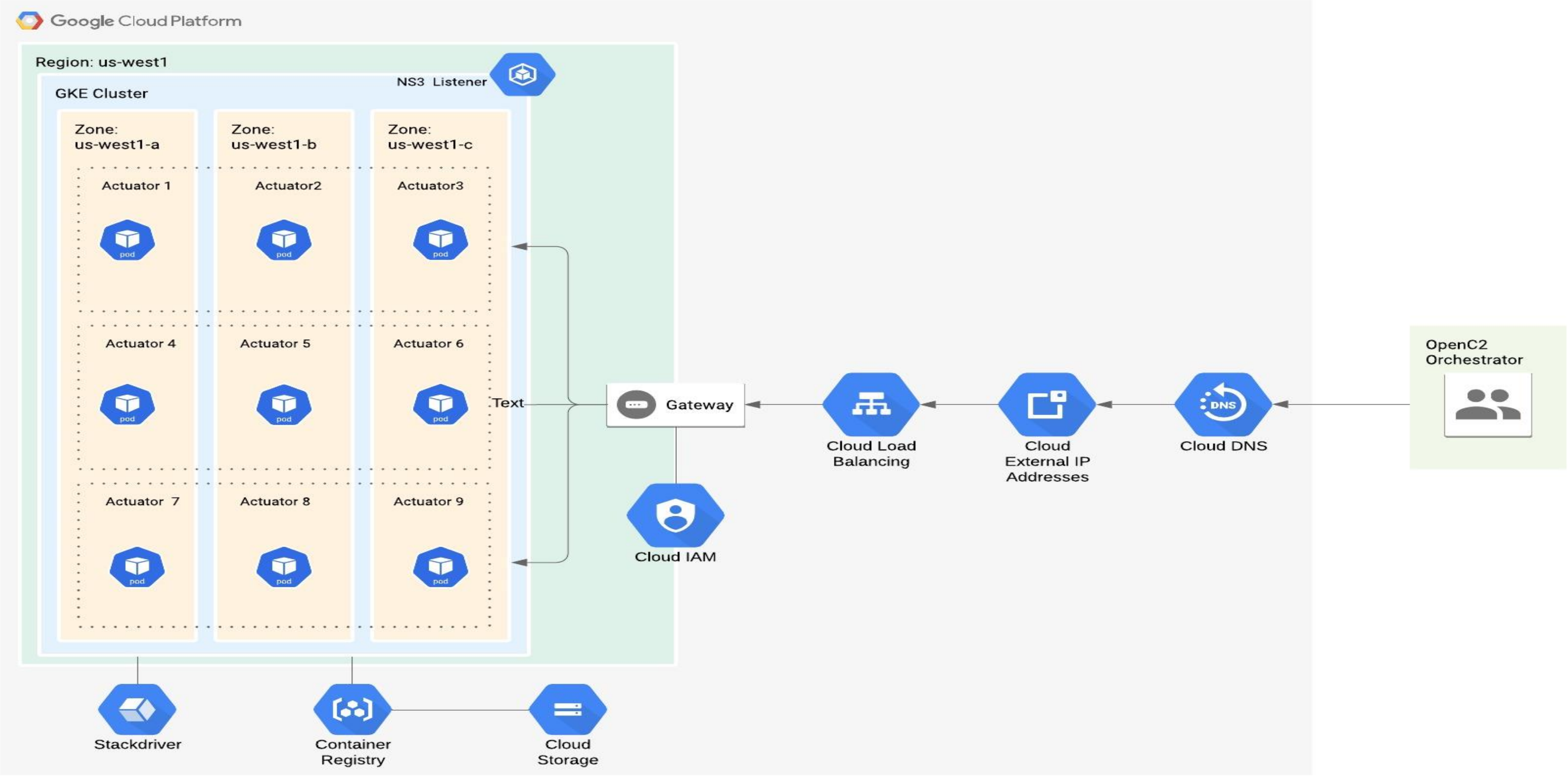
DELETE using Laser Weapon System resulting in Drone Immobilization

QUERY the Status of the Drone Neutralization

ACDCI Use case using Google Kubernetes Engine (GKE)



GCP Kubernetes Nodes with GKE for NS3 Simulator



Connected Google Cloud Platform (GCP) Services

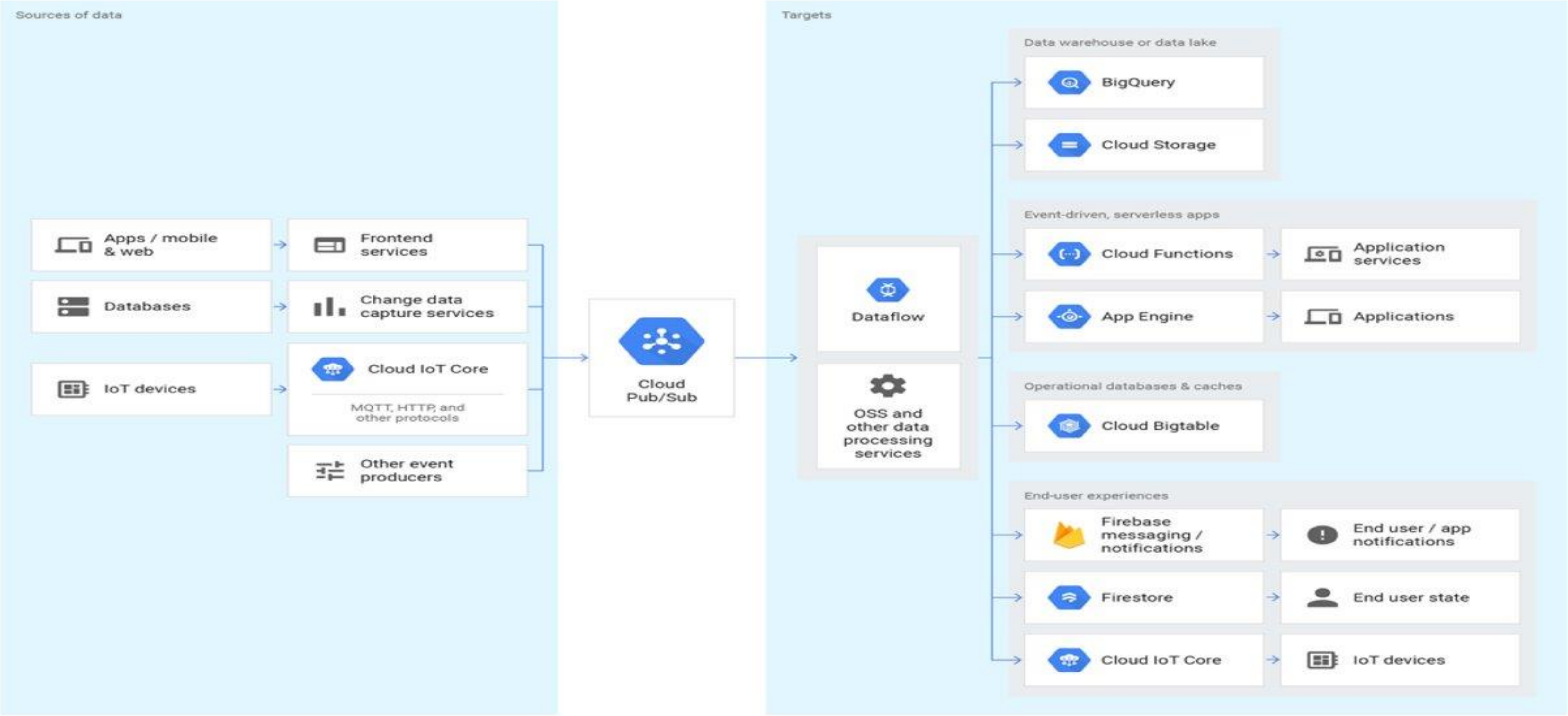
- Virtual Private Cloud(VPC) provides VPC networks that are a global resource that provide a list of regional subnetworks (subnets) in data centers connected by a global wide area network. The VPC networks are logically isolated from each other in the GCP.
- Stackdriver is a utility that enables monitoring of the hosted application in the GCP. This utility will enable one to filter, search and view logs from your VPC. This utility will provide uptime monitoring and error reporting.
- Persistent Disk (PD) provides the ability to resize the storage capacity while in use. PD provides automatic encryption of data.
- Cloud Load Balancing reacts instantaneously to changes in the numbers of users, traffic, network, backend health and other related conditions. It provides cross region load balancing with automatic multi-region failover.

Architecture using Cloud Pub/Sub

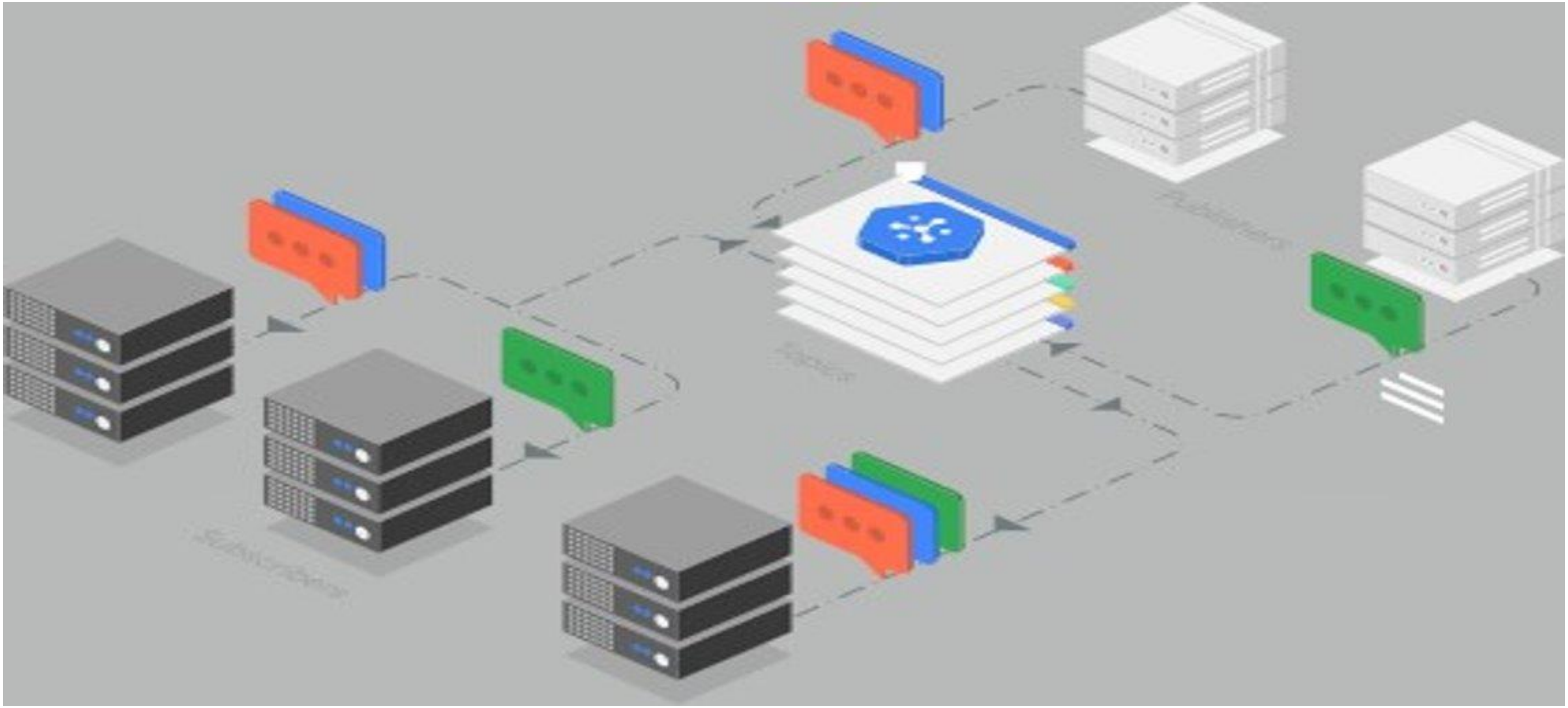
The Google Cloud Pub/Sub provides global messaging and event ingestion. The Pub/Sub is an event manager.

- Cloud Pub/Sub can scale without provisioning, partitioning, or load isolation worries, and expand applications and pipelines to new regions simply with global topics.
- Pull subscriptions make it available to more complex stateful services running in Google Kubernetes Engine.
- Multi-region environments operate seamlessly because of Cloud Pub/Sub’s global nature.
- Cloud Pub/Sub includes end-to-end encryption, Identity and Access Management (IAM), and audit logging, as well as NoOps (no operations), fully automated scaling and provisioning with virtually unlimited throughput. It also provides extreme data durability and availability with synchronous cross-zone replication.
- Publish from anywhere in the world and consume from anywhere, with consistent latency.

Cloud Pub/Sub for global messaging and event



Cloud Pub/Sub using Publishers and Subscribers


Publishers
Topic
Subscribers