Lockheed Martin RQ-170 Drone Story

By Milad Kahsari Alhadi

Telegram: @MiladKahsariAlhadi

RQ-170 Story – What am I going to cover?

Contents:

- What is a drone?
- What is RQ-170 Drone?
- What is the whole story of this drone about?

  - Introduction to Drone Hacking
  - How did Iran hack it?
  - Signal Jamming

Prerequisites:

- Physics
- Electronics
- Mathematics

Introduction to the stroy

Introduction – What is a Drone?

- An Unmanned Aerial Vehicle (UAV) commonly known as a drone.
- UAVs are aircraft without a human pilot aboard.
- UAVs are a component of an Unmanned Aircraft System (UAS) which include

  a UAV,
  a ground-based controller,
  and a system of communications between the two.

- The flight of UAVs may operate with various degrees of autonomy:

  either under remote control by a human operator
  or autonomously by onboard computers.

Introduction – What is a RQ Drone?

RQ-170 Sentinel is an UAV developed by Lockheed Martin:

- It's operated by the United States Air Force for the Central Intelligence Agency (CIA).
- It is a stealth aircraft fitted with aerial reconnaissance equipment.
- It is a tailless flying wing aircraft, with pods, presumably for sensors or SATCOMs, built into the upper surface of each wing.
- It is a tactical, operations-oriented platform and not a strategic intelligence-gathering design.

Specifications (RQ-170) [edit]

Data from[citation needed]

General characteristics

- **Crew:** 3 on ground
- **Length:** 14 ft 9 in (4.5 m)
- **Wingspan:** 65 ft 7 in (19.99 m)
- **Height:** 6 ft (1.8 m) estimated
- **Powerplant:** 1 × Garrett TFE731 or General Electric TF34[11] turbofan

Performance

- **Service ceiling:** 50,000 ft (15,000 m) (estimated)[37]

RQ Captured by Iranian EW Unit

Iran Captured RQ – lol, How is it Possible?!

- Iran intiated its EW by jamming the communications frequencies, forcing RQ into auto-pilot.
- How can We do that?

> We can putting noise on the communications and force the uav into autopilot.
> Then we can use spoofing -- sending a false signal for the purposes of obfuscation or other gain.

- Signal in the questions was the GPS feed, which the drone commonly acquires from several satellites.

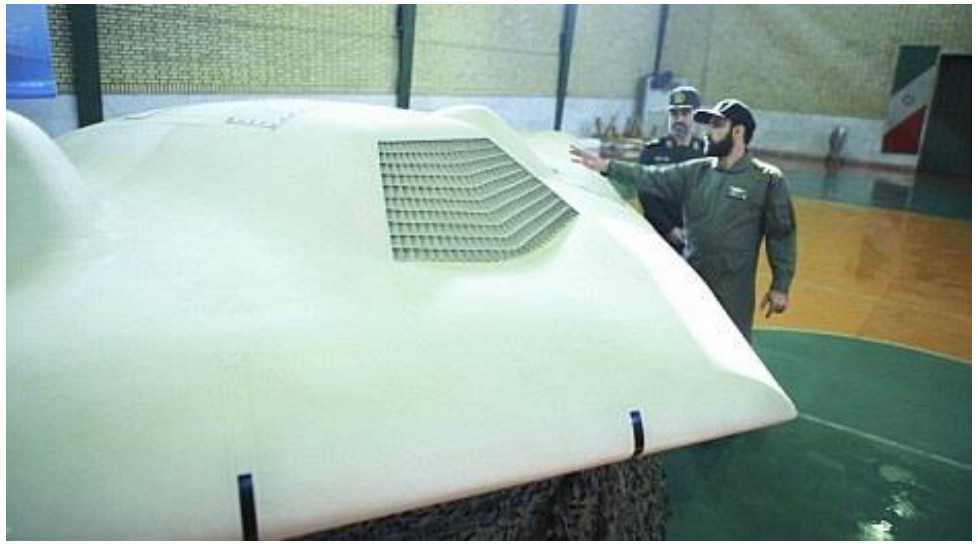
> By spoofing the GPS feed, We were able to convince it that it was in Afghanistan, close to its home base.
> At that point the drone's autopilot functionality kicked in and triggered the landing.

- Spoofing the GPS is a clever method, as it allows hackers to land on its own where we wanted it to, without having to crack the encrypted remote-control signals and communications.

Iran EW Story – Why is it interesting for Iran?!

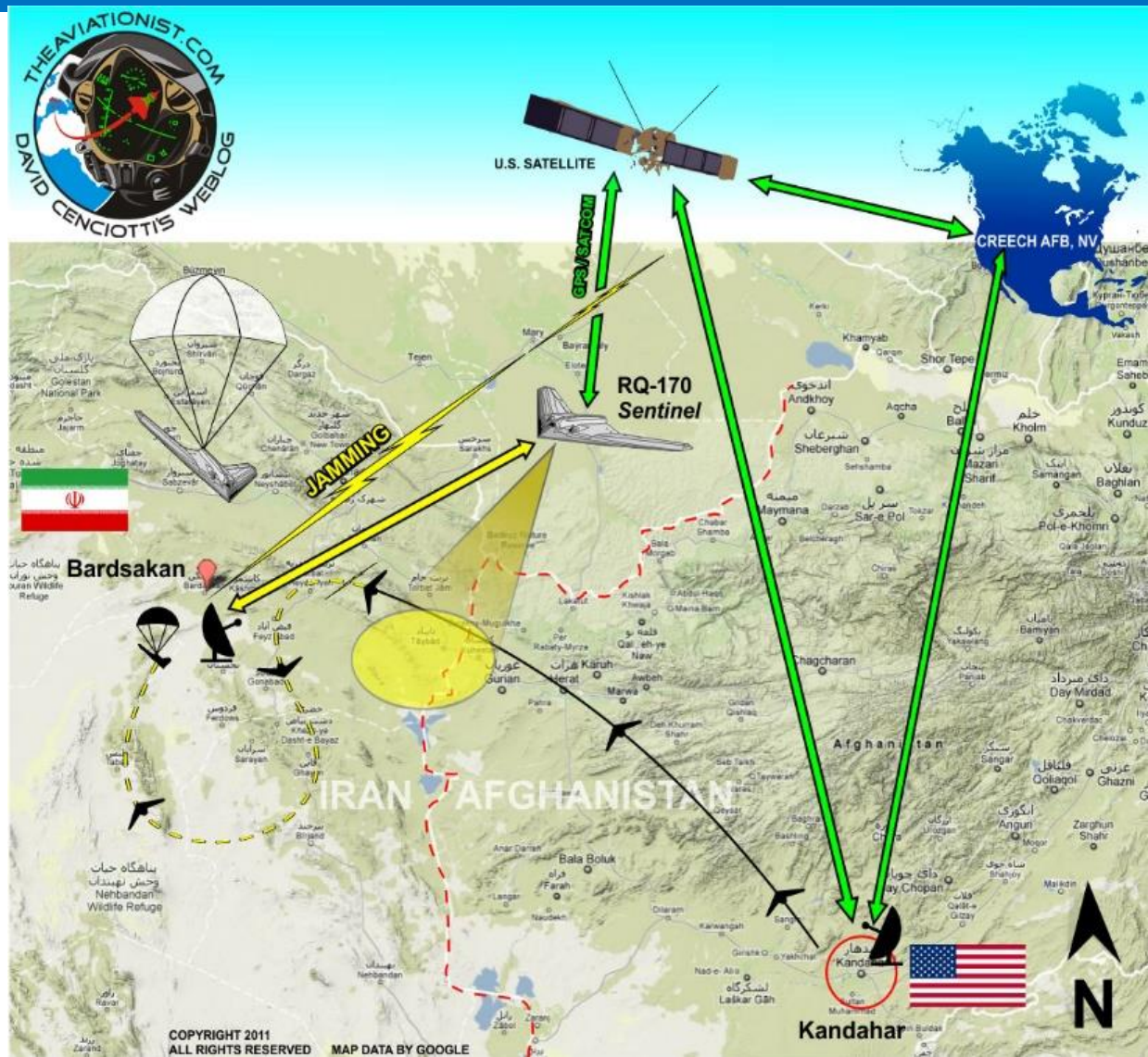
Why RQ of Lockheed Martin is interesting?

- It has stealthy characteristics.
- It has Cutting-edge technology
- The UAV that provided support in Operation Neptune Spear



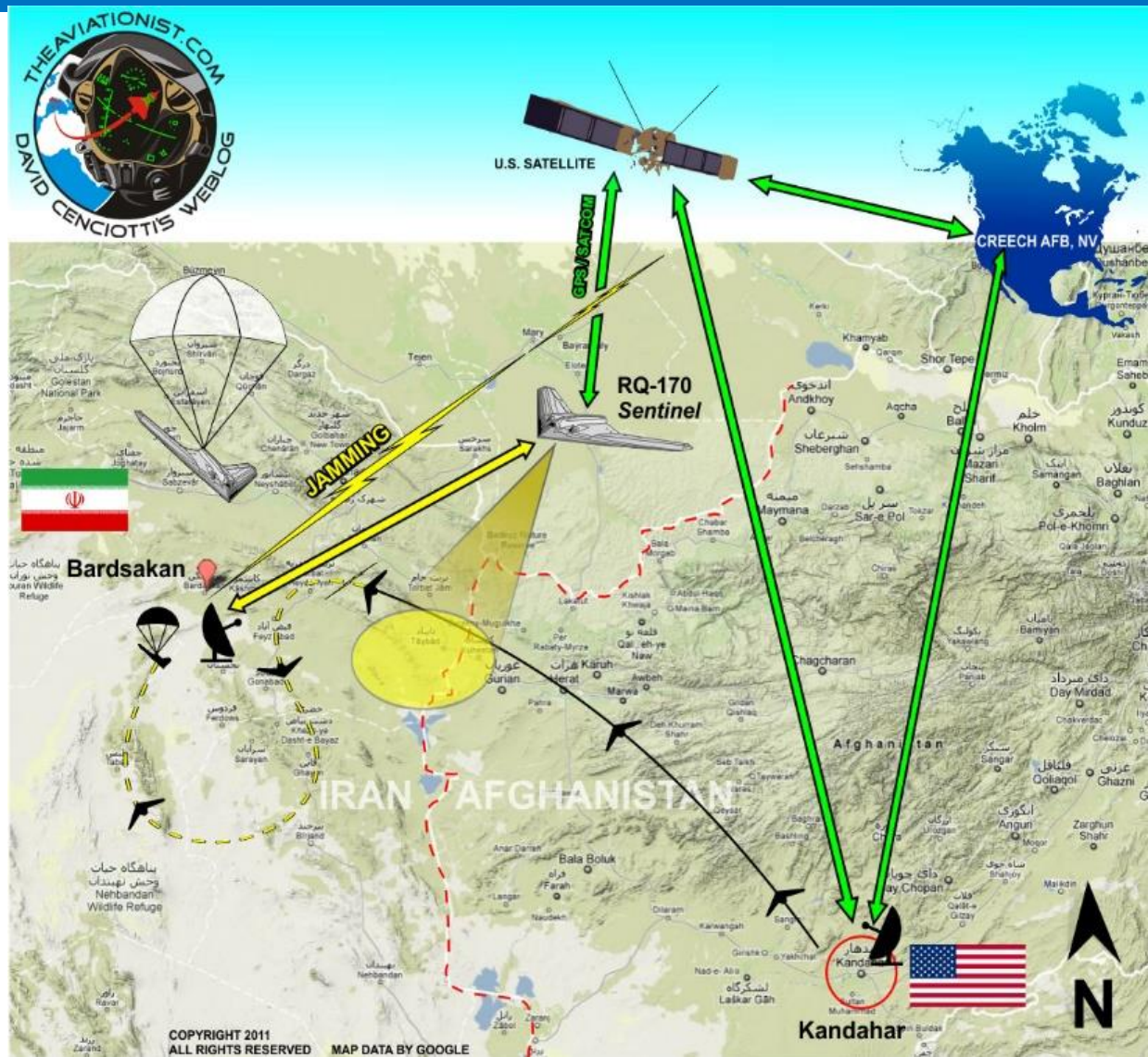
Iran EW Story – Communication Jamming:

- Loss of communication with ground station forces most drones into back-to-base mode
- Iranian Army's Electronic Warfare Unit capitalized on this by utilizing radio jamming.
- **Radio Jamming:**
  - Radio jamming is the deliberate jamming, blocking or interference with authorized wireless communications.



Iran EW Story – Communication Jamming:

- A transmitter tuned to the same frequency as the opponents‘ receiving equipment and with the same type of modulation can, with enough power, override any signal at the receiver
- Makes receiver think that actual signal is just background noise by reducing signal-to-noise ratio
- Most decent receivers know when they're being jammed due to spike in amplitude of signal and will not accept the new signal as valid



Iran EW Story – Global Positioning System:

- GPS satellites send information to unit which then determine location (courtesy of Einstein's relativity and time dilation)
- Iranian Army's Electronic Warfare Unit spoofed the GPS feed making the plane think it was close to Kandahar
- Iranian's couldn't find "perfect" match for landing strip so they made the UAV land at a slightly higher altitude (and caused damage)

While the technique did not require sophistication from a cryptography perspective, it was not entirely trivial, either, as it required precise calculations to be made to give the drone the proper forged distance.

— It was not a simple and straighforward thing for EW engineers.

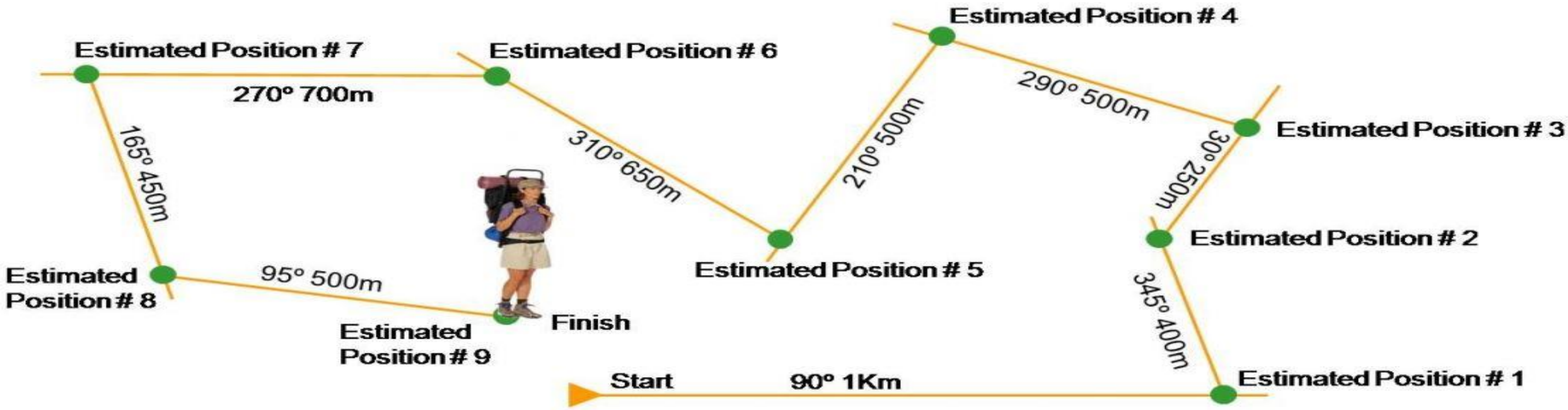
Iran EW Story – Mitigation Things:

However, Sanity Check and also Dead Reckoning can makes things more secure than before against these kinda of attacks.

- Verify that change in location is possible

  For example, the aircraft didn't just travel 1000 miles in less than a second.

- Store the path that the UAV took and if it gets jammed use that route to go back to base



Everything that has a beginning has an end.

— The Matrix Revolution