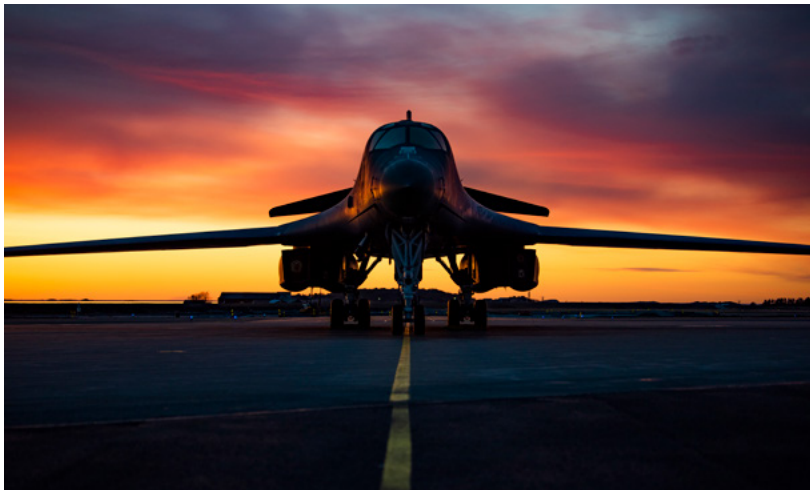
CYBER:\CASE

AIR UNIVERSITY | AIR FORCE CYBER COLLEGE

Fly, Patch, and Don't Lose[1]

Kevin L. Parker, Air Force Cyber College

Location and Organization



You are stationed overseas and assigned to the air component headquarters for the geographic combatant command. Your base, in the allied country of Sageland, hosts the air operations center that integrates air, space, cyber, and information operations in the theater and provides commanders with command and control of joint operations through detailed joint planning, target development, weaponeering, sortie allocation, air tasking order production, mission execution management, and operational-level assessment functions.

Redland, a near-peer competitor nation within this theater, is called out specifically in the National Defense Strategy. The strategy identified competition with Redland and one other country as a principal priority for the Department of Defense due to "the magnitude of the threats they pose to US security and prosperity today, and the potential for those threats to increase in the future."[2] Sageland also has ideological differences with Redland. They were on opposite sides of a war decades ago. They are major trading partners despite persistent tensions.

Communications Hub

Your base is also a communication hub connecting many functions within and outside the military. A few significant linkages that expand beyond the base include:

- Classified computer network for bases and US embassies in theater
- Unclassified computer network for bases in theater
- Weather sensors and analysis for the theater
- Missile defense warning systems—sensors and communications links to allies and national command authorities

(Redundant capabilities are considered in communications planning. However, for the simplicity of this case study, assume there are no redundant communication capabilities beyond your base.)

[1] This case study scenario is fictitious but realistically plausible. The views presented are those of the speaker or author and do not necessarily represent the views of DoD or its components.
[2] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2018), 4.

Cyber Vulnerability

A specific cyber vulnerability was recently discovered in a widely used software package. The vulnerability leaves systems susceptible to an attack in which hackers can access the system and gain root privileges. This gives hackers full control of targeted computers, the ability to exfiltrate, alter, or delete all stored data and communications, and the ability to lock legitimate users out of the system. Reports indicate that hackers have already exploited this vulnerability to gain access to other US government agency networks, locking agency employees out of their systems and erasing data. Experts say this vulnerability is very similar to the Solar Winds hack discovered in 2020, which affected the US Departments of Homeland Security, State, Energy, Commerce and Treasury through malicious code embedded in a software update.

There have been no reports of impacts to classified networks, but the extent to which the vulnerability has been exploited is unknown. Experts say the vulnerability has likely been in place for several weeks, but it is currently unknown exactly how long or if Air Force computers in this theater have been actively attacked. The list of attacked businesses and government systems grows daily. Initial reports indicate the exploitation code may have originated from within Redland.

A software patch is now available and carries a recommendation to install it immediately on all unclassified and classified systems. Installing the software patch across the entire base network will take several days, but the top tier of priority computers can be patched within four hours. This only provides partial protection for computers performing the most critical functions and leaves the majority of the computers on base and the network vulnerable to exploitation. If hackers attack lower tier computers and gain administrative privileges to the network, with more effort, it would be possible for them to access the top tier computers. The patch triggers a forced re-start for every updated computer.

Pending Bomber Operations

Bomber aircraft are on a scheduled short-duration deployment to your theater. Capable of carrying nuclear and conventional munitions, the bomber task force is part of infrequent but recurring efforts to deter potential adversaries and reassure allies in the geographic theater. Previous, similar deployments included publicized strategic messaging. The command announced on social media, “The 29-hour sortie demonstrates continued US commitment to allies and partners by showcasing their ability to deliver lethal, ready, long-range strike options to the geographic combatant commanders anytime, anywhere.”

The bombers in the task force just arrived in theater and are due to launch in one hour. They only plan to fly one mission. On the six-hour sortie, the bombers will rendezvous with fighter jets from a nearby allied country, Blueland, to fly a training mission. Securing Blueland’s participation took considerable diplomatic effort due to historical and recent tension with Redland. Blueland wanted to avoid any provocative actions toward Redland and was eventually persuaded to participate after high-level US engagement. The US government deemed it worth the effort to avoid the appearance of a unilateral action and to show solidarity within the alliance.

Questions? Contact Us at
AWC.CyberCollege.Org@us.af.mil

The bomber task force mission is on a tight timeline. Because scheduling Blueland aircraft took detailed planning and coordination, requiring the efforts of both embassies, any change in the flight time would not be able to be coordinated in time to keep the allied aircraft in the mission. Using another crew, the bomber task force is due to launch to return to CONUS in sixteen hours to meet a higher priority USSTRATCOM tasking with a hard timeline. For simplicity of this case study, assume the time to turn the bombers (landing to takeoff) is negligible. The bomber task force mission is scheduled to launch in one hour. Due to crew rest limitations, any mission delay could not exceed 12 hours.

The flight path will remain in international airspace but goes near Redland's airspace into an area where flights are often intercepted by Redland's fighter aircraft. Previous intercepts have never flared into conflict but have often resulted in both sides claiming hostile or dangerous acts by the other. Worst-case scenarios that risk immediate conflict escalation include an in-air collision with Redland intercept aircraft and navigational error that results in an actual violation of Redland airspace. To mitigate potential flare-ups and miscues in signaling intentions, the mission, along with its timing, location, and duration details have already been released to the press and widely shared. And, there are no other significant US flying operations (only local, single-ship training missions) scheduled while the bomber task force is in theater. In response to US announcements on the bomber task force mission, Redland's defense minister declared, "We take the defense of our sovereign airspace very seriously and will act to defend ourselves against any provocation. Meddling powers should remember we are armed sufficiently to make it rain missiles on the nations who willingly enable aggressive act."

Uninterruptible Power Supply

The uninterruptible power supply (UPS) that provides a limited supply of back-up power to the servers hosting the air operations center network has reached the end of its design service life. The manufacturer recommends replacing the UPS. Following this recommendation, your unit has contracted for its replacement. The contract is in place and allows for execution with six-hour notice. The replacement requires totally powering down the network and disconnecting the back-up power, since the UPS connects to both the main and back-up power supply. The contract gives the contractor up to six hours to perform the work once on site. (The time to shut down each program and system on the network can be significant, but for simplicity of this case study, assume the shut-down time to be negligible. Apply the same for re-starting each system.) The existing UPS installation does not have a by-pass option (allows the power to flow around the UPS) or battery banks that allow for partial replacements, but the new one will.

Decision Pending

You are the air component commander in this area of operations and also the commander responsible for the communications assets involved. It is your decision on what actions to take. What do you do?