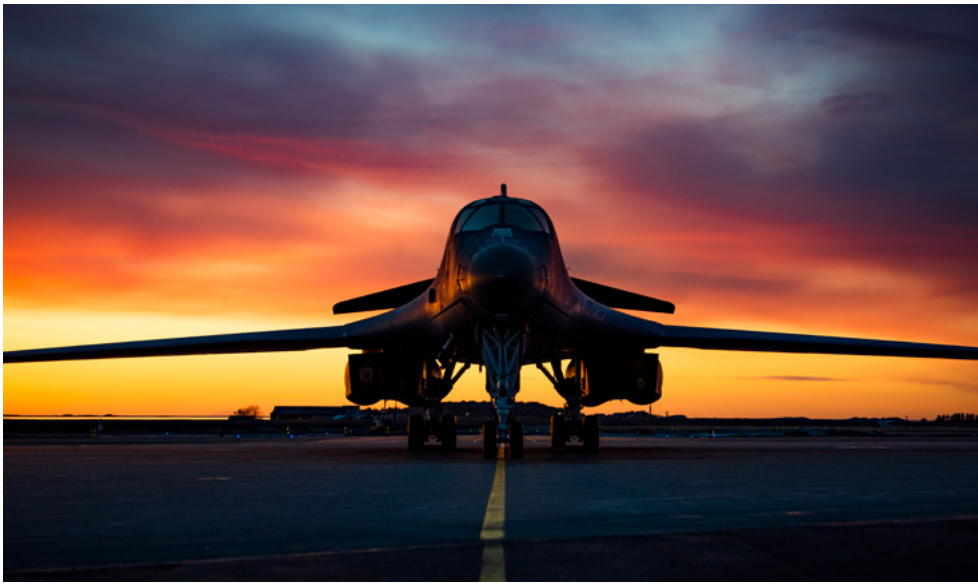
AIR UNIVERSITY | AIR FORCE CYBER COLLEGE

CASE #F01-2107R0
TEACHING NOTES

Fly, Patch, and Don't Lose



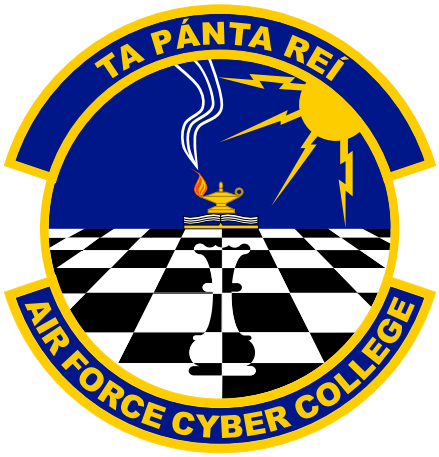
Kevin L. Parker
Air Force Cyber College

CYBER COLLEGE CASE STUDY SERIES

Air Force Cyber College

Col David B. Bosko, USAF, Commandant

Dr. Karen Guttieri, Academic Dean



Please send inquiries or comments to:

Ms. Kay Adams
Air Force Cyber College
60 W. Shumacher Ave., Bldg 803
Maxwell AFB AL 36112

Tel: (334) 953-5591
E-mail: lillian.adams.1@au.af.edu

Fly, Patch and Don't Lose

ABSTRACT

The scenario involves important air operations in a forward theater that are potentially impacted by computer system down time required to install a patch to close a known cybersecurity vulnerability. Multiple considerations are introduced, including US strategy, cybersecurity risks, host nation interests, allied nation interests, deterrence, conflict escalation, and the perception of US actions.

TARGET AUDIENCE

Primary: Military and civil servant students attending intermediate or senior developmental education programs.

Secondary: Operations personnel in the military, public, or private sectors with reliance on cyber capabilities, cybersecurity specialists—technical, management, and policy-focused—with impact on operations, policy and international relations students.

LEARNING OBJECTIVES

1. Identify how cybersecurity and system reliability are important to operations.
2. Describe the tension between operational requirements and actions necessary to maintain cybersecurity.
3. Distinguish between different viewpoints of various stakeholders and evaluate the importance of discipline expertise.
4. Prioritize competing interests in developing decision-making criteria.
5. Assess risks with various courses of action.

DISCUSSION

The following section presents questions instructors could ask in class to spark discussion.

1. What obvious options are immediately available?

Major options for the pending decision are provided, but instructors are encouraged to "tease out" the options in discussion if not arrived at naturally by students. The most basic options are to a) fly as planned and delay the patch until later, b) disrupt the flight plans (delay or cancel) to install the patch immediately, and c) fly while the computer systems are down for the patch

installation. Options involving the UPS upgrade just alter the timelines of those basic plans.

2. What is at stake? Considering some of the basic options, what could go wrong?

For options a, b, c listed above:

a) If the patch is delayed, the computer systems could be exploited. Adversaries could lock the computers and systems. Data could be altered and or stolen.

b) Disrupted flight plans risk losing participation of the allied nation Blueland, making the operation appear as a unilateral action by the United States. Not being able to execute the mission as planned would be noticed in the press and could signal questionable US force readiness. This would be detrimental to deterrence and reassurance of allies.

c) Flying with the computer systems down—either planned or due to a cyberattack—would mean limited real-time communication with aircrew. If Redland intercepted the flight and tensions flared, US response could not be immediate. If a worst-case scenario occurred and prompted an adversary reaction of launching missiles at US or allied interests (Blueland, Sageland, or others), the missile detection system would not be available to provide advanced warning.

For all options:

- Time to patch or replace the UPS is based on estimates. These estimates could be wrong and take longer than planned, causing further delays.
- Delaying the patch or UPS replacement to another day would still require a scheduled outage with a gap in service that could potentially impact other operations. Circumstances at a later time are unpredictable and may not necessarily be better than now.

3. What is the likelihood that any of the worst-case scenarios would actually happen in any given option?

Depending on student background, probabilities offered by students may be relatively uninformed based on limited information given by the scenario. The point is to recognize varying levels of probability based on available inputs—not to create perfectly accurate predictions.

4. How might Sageland (allied country host government) view the situation?

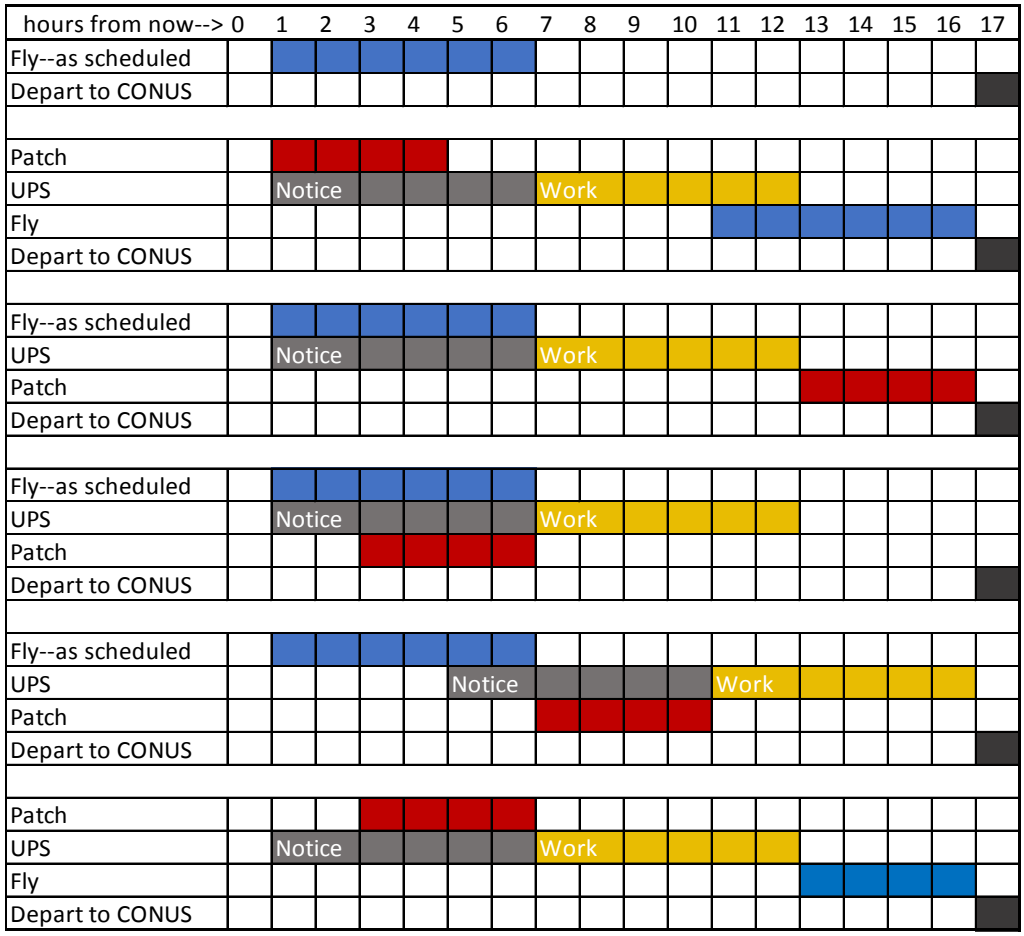
Depending on student background, input may be relatively uninformed based on limited information given by the scenario. The point is to recognize the allies may have different viewpoints.

5. Discuss the situation as a group and come up with a decision. (Can be done in groups with an outbrief explaining each group's decision logic).

Potential timing and sequencing major options (not exhaustive)

Students may develop a chart (similar to below) to explore timing in developing courses of action. If a major course of action is being missed, instructors should prompt students to chart the timing. The chart below may also be used as a handout depending on desired objectives.

Timing and Sequencing of Major Options (not exhaustive)



CASE PROGRESSION (if preferred and as time allows)

Opportunity for Questions to Subject Matter Experts?

Many of the experts involved in all aspects of the above issues are assembled. What questions do you have to make an informed decision? Please specify who you are asking the question to.

Question responses:

UPS representative. Before answering, I need to make it clear that we cannot predict the timing of the UPS failure. The manufacturer defines its service life and the equipment is expected to function throughout that service life. However, the only information or recommendation from the manufacturer after the end of the useful service life is that it should be replaced. The only thing we can guarantee is that it will fail at some point. When that point will come is not known. And, it's always better to have a planned outage than an unscheduled outage. Unscheduled outages tend to happen at the worst time. The last time we had an outage, the UPS worked, but that was 2 years ago. We'd like to test it every six months, but we can never get a scheduled outage, so we keep deferring the test.

Power representative. (Public works or civil engineering) Our commercial power to the base is very reliable. I don't have the exact numbers, but it's probably in the range of 98-99% reliable. We have a back-up generator on the building in case commercial power goes down. Of all the generators on base, when we do have a power outage, there are typically only one or two, at most, that don't start like they should. We perform monthly maintenance to make sure they are ready to go.

Cybersecurity representative. We don't know for sure yet who originated this exploitation. Initial reports say it possibly came from within Redland, but that has not been confirmed. Much like the Solar Winds hack, over the last several weeks new business and government agencies have been added daily to the list of attack victims from this vulnerability. The vulnerability in our system has been there throughout that time, but there is no way to know for sure right now if or when we will be targeted for exploitation. The first indication is when your computer suddenly stops responding and freezes up. We can run the patch on the top tier of priority systems in four hours, but that only protects those systems and leaves the majority of the computers on base and the network vulnerable to exploitation. Higher headquarters has mandated installation of the patch as soon as possible. The term "as soon as possible" is always left to the discretion of the local commander. The only thing that is completely clear is that the sooner we install the patch and close the vulnerability, the better off we will be.

Public Affairs representative. We have to ensure we don't take actions that send mixed signals to our allies and or Redland. We've released a lot of detailed operational information about this mission. There is a group of reporters that we've let on base to interview crew, maintainers, and leadership before filming the takeoff. Even though they have agreed not to file their stories until after the mission is complete, those news crews are processing through the gate to get on base already. One of the purposes of this task force was to communicate how we can effectively conduct operations like this on a moment's notice. No matter how legitimate the reason may be, any delay in flight time will be very public and will strongly detract from our intended message of readiness.

Political Advisor representative. Tensions between the United States and Redland at this moment are not at their worst. However, in the current era of great power competition, Redland takes every opportunity to take jabs or discredit the US in the press. These bomber task force missions are a big deal for reassurance of our allies, especially with the reduction of the number of troops permanently stationed in theater over the last few decades. Getting Blueland's participation in the mission was a sensitive issue, even with our allies, because they did not want to act too provocatively since their entire country is within range of Redland's missiles. Having Blueland on board is a boon, because it mitigates Redland's consistent narrative that the United States is unilaterally meddling far away from home.

Host nation representative from Sageland. We support the mission that was planned. We also understand the risk associated with this cyber vulnerability, because we are dealing with it too. Parts of our own government have been attacked. As for the flying mission, we are always wary of any provocative actions that would risk war, especially with Redland. We don't think what you have planned is provocative, but Redland can sometimes be unpredictable. Remember, the history books recount the horror of the war that took place here. This is our home. We trust your judgment will be prudent and reasonable, so we will support your decision.

Blueland allied nation representative. We have a strict schedule with limited aircraft and crews, so we are restricted operationally. We are also constrained politically. Our participation in this mission was approved with great hesitancy at the highest level of our government. We're not going to be able to participate if the mission doesn't fly as panned.

Intelligence representative. We assess that it is possible the recent cybersecurity exploits originated from within Redland. We assess that Redland will react as they usually do to the planned bomber task force flying operations. They usually intercept these types of flights with fighter aircraft. They typically do not fly in an extremely reckless manner, but they do position their jets very close to ours. They call over the radio saying our jets are violating their

airspace, even when they are not, and demand our jets land immediately in their territory. General political conditions and tensions with Redland are similar to the last time we flew a similar mission. It's not a tinderbox, but we are in constant competition on many fronts, and their leader is an opportunist.

Post-decision point questions

1. How did various inputs from others (members in the group and/or expert representatives) shape your decision compared to your initial, individual thoughts?

2. Were any members of your group experts in any aspects of the scenario? If so, how did that influence the discussion and decision?

3. Was there anyone else you would like to consult to make the decision?

4. How did the urgency of time influence your decision making process?

5. How did the probability and consequence of potential negative outcomes impact your decision?

6. How did the probability and consequence of potential positive outcomes impact your decision? Was loss aversion influenced by the case study title words "don't lose?"

7. Did you use any visuals aids to assist with decision making? If so, describe them and their impact?

8. Are there any notifications you would like to make personally before the decision is released publicly? (Emphasize partnerships and trust within your team and with allies.)

8. Even though the scenario was fictitious, did any of you feel the weight of the decision? In your hands were the lives of the aircrew, the security of information and national secrets, international partnerships, missile defense for a region with millions of people, and the potential to spark WWIII. Did any of that impact you personally as you worked through the decision?

VARIANTS

Depending on student make-up and learning objectives, other variants could use the same case.

- Policy recommendation group. Assign students responsibility as part of a working group that must present the commander a decision brief with a recommended course of action. The principal receiving the briefing can also be altered. For example, the political affairs student could be asked to brief the ambassador before making a phone call to consult with and advise the commander.

- Assigned representatives. Assign students a specific role and arm them with the expert representative responses as a basis for their role play. One student is assigned the role of commander.
- Theater-specific. Choose actual nations to replace Redland, Blueland, and Sageland. Representative viewpoints can be tailored to represent actual views. Students can also be assigned to develop a brief or write a short paper on their assigned nations' position for the scenario.
- Individual exercise followed by group exercise. For courses in leadership and decision-making, students with their first exposure to the case could record their own individual thoughts and decision as a formative benchmark. As lessons are taught throughout the course, the case can be revisited and played out in a group setting for application of the course material.

PREPARATORY READINGS

Depending on student background and familiarity with issues in the case, additional background information can be assigned as a preparatory assignment. Additional information on air operations centers, bomber task forces (including a short video), the National Defense Strategy, and the Solar Winds hack may be helpful.

"613th Air Operations Center Welcomes New Commander" and "618th Air Operations Center Welcomes New Commander" offer information on the mission of and functions performed within an air operations center.

> Kline, Staff Sgt. Mikaley. "613th Air Operations Center Welcomes New Commander." Pacific Air Forces Public Affairs, 2 July 2020. https://www.pacaf.af.mil/News/Article-Display/Article/2246662/613th-air-operations-center-welcomes-new-commander/.
>
> 618th Air Operations Center. "618th Air Operations Center Welcomes New Commander." 16 June 2020. https://www.mcchord.af.mil/News/Article-Display/Article/2222080/618th-air-operations-center-welcomes-new-commander/.

Summary of the 2018 National Defense Strategy of the United States of America provides context to students to help them better understand US national security interests and long-term strategic competition.

> Department of Defense. Summary of the *2018 National Defense Strategy of the United States of America*. Washington, DC: Department of Defense, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

The Vlamis article describes the nature and pervasive impacts of the Solar Winds hack.

Vlamis, Kelsey. "Here's a List of the US Agencies and Companies That Were Reportedly Hacked in the Suspected Russian Cyberattack." Business Insider, 19 Dec 2020, https://www.businessinsider.com/list-of-the-agencies-companies-hacked-in-solarwinds-russian-cyberattack-2020-12/.

Two articles from Pacific Air Forces and US Air Forces in Europe have information related to previous bomber task forces; the latter includes a short video with a crew member discussing the purpose and mission of the task force.

Pacific Air Forces Public Affairs. "B2 Spirit Stealth Bombers Deploy to Diego Garcia, Supports Bomber Task Force." 13 August 2020. https://www.afcent.af.mil/News/Article/2312261/b2-spirit-stealth-bombers-deploy-to-diego-garcia-supports-bomber-task-force/.

USAFE Public Affairs. "US Air Force B-2s Deploy to Europe." US Air Forces in Europe, 27 August 2019. https://www.whiteman.af.mil/News/Article/1945054/us-air-force-b-2s-deploy-to-europe/.

BIBLIOGRAPHY

Department of Defense. Summary of the *2018 National Defense Strategy of the United States of America*. Washington, DC: Department of Defense, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

—

Please send inquiries or comments to:

Ms. Kay Adams
Air Force Cyber College
60 W. Shumacher Ave., Bldg 803
Maxwell AFB AL 36112

Tel: (334) 953-5591
E-mail: lillian.adams.1@au.af.edu