**OPSEC Awareness Month Case Study 1: USS Cole**

**I. The Story: A Port Call Turns Tragic**

On October 12, 2000, the USS Cole was refueling in the port of Aden, Yemen, when a small boat approached and detonated explosives alongside the ship. The blast, estimated to have been caused by approximately 500-700 pounds of explosives, tore a massive hole in COLE's hull, killing 17 sailors and injuring another 39. The attack severely damaged the destroyer, which required extensive repairs and highlighted the vulnerability of U.S. Navy ships to small boat attacks.

Al-Qaeda ultimately claimed responsibility for the bombing. The attack underscored the growing threat of international terrorism and its ability to target U.S. interests abroad. The Cole bombing prompted increased security measures for Navy vessels, particularly during port visits, and contributed to the U.S. government's focus on counterterrorism efforts in the years that followed.

**II. Security Failures: A Cascade of Errors**

The attack on the USS Cole exposed several critical OPSEC failures. While the Navy had general security measures in place, the specific circumstances in Aden harbor revealed vulnerabilities. The perceived low threat level in the port led to a relaxed security posture. Insufficient force protection measures, such as a lack of aggressive patrol boats and limited security perimeter around COLE, allowed the small, explosive-laden boat to approach undeterred. Furthermore, the harbor's routine operations and COLE's predictable refueling schedule provided an easily exploitable opportunity for the attackers.

The most glaring OPSEC failure was the unauthorized sharing of ship schedule information by a sailor to their spouse. The contents of the sailor’s email regarding the upcoming port call in Yemen became available on a publicly accessible website. This seemingly innocuous act provided Al-Qaeda terrorists with a specific timeframe for their attack. This highlights the importance of both sailors and their families’ requirement to be aware of the information they share online. Seemingly harmless details, collected in aggregate, can be pieced together by hostile actors and acted upon.

**III. Response and Aftermath**

The attack on the USS Cole served as a harsh wake-up call, forcing the Navy to re-evaluate and overhaul OPSEC practices. It highlighted that OPSEC is not just about the protection unclassified information, but also about understanding how seemingly harmless pieces of information can be exploited by adversaries. The immediate aftermath saw increased physical security measures for ships in port, including more aggressive patrol boat tactics, stricter control of access to harbors, and enhanced physical security onboard vessels.

Long term OPSEC restructuring places greater emphasis on personal responsibility for protecting critical information, especially online. The USS Cole attack ultimately began a cultural shift within the Navy that prioritized a more proactive and vigilant approach to OPSEC integration across all operations.