**OPSEC Awareness Month Case Study 2: POOR OPSEC PRACTICE WITH PERSONAL ELECTRONIC DEVICES (PEDs) ONBOARD USS MANCHESTER**

In 2019, USS Manchester inadvertently revealed the use of unauthorized Starlink internet terminals onboard during a routine photo exercise. Images released publicly showed a Starlink dish antenna mounted on the ship, indicating the crew had bypassed existing communication systems and established an independent connection to the Starlink satellite network. This unauthorized use raised immediate concerns about potential security vulnerabilities and violations of established communication protocols within the Navy.

The incident highlighted the allure of readily available commercial technology like Starlink, offering faster and more reliable internet access compared to traditional military networks. However, it also exposed the risks associated with integrating untested and potentially unsecure systems into sensitive military environments. The incident prompted an internal investigation and underscored the need for clearer policies and procedures regarding the use of commercial technologies, particularly concerning cybersecurity and adherence to established communication protocols designed to protect OPSEC.

The incident involving unauthorized Starlink use on USS Manchester highlights several important OPSEC lessons, particularly concerning new technologies and their integration into existing security protocols:

* **Addressing the challenge of Personal Electronic Devices (PEDs) in military settings:** The incident underscores the growing challenge of PEDs in maintaining military OPSEC. Clear policies and procedures for managing personal devices and their connection to secure networks are essential. This may involve restricting access, implementing mobile device management (MDM) solutions, or prohibiting personal devices altogether in sensitive areas.
* **Adapting OPSEC to address evolving technological threats:** Command level OPSEC training and documentation must keep pace with the rapid advancement of technology. Personnel need to be educated about the specific risks associated with new technologies, especially advancements in PED capabilities (such as cellphone satellite connectivity), including potential vulnerabilities to preservation of mission.
* **Vetting new technologies thoroughly before deployment:** While new technologies offer advantages, security implications within a military context need thorough examination *before* being deployed on a naval vessel. Understanding potential vulnerabilities and attack vectors is crucial. This includes assessing the manufacturer's security practices and the technology's susceptibility to jamming, spoofing, or interception.
* **Clear communication and enforcement of policies regarding unauthorized technology:** The incident suggests a gap in communication and enforcement of existing policies regarding the use of unauthorized devices and networks. Clear guidelines and training are essential to ensure personnel understand the risks and adhere to security protocols. Regular inspections and audits can help enforce compliance.

The USS Manchester incident serves as a valuable lesson in the importance of adapting OPSEC practices to the evolving technological landscape and the need for continuous vigilance in protecting sensitive information. New technologies offer significant advantages, but they also introduce new risks that must be carefully managed.