CCS

Cyber Conflict Simulator

Military Case Study

Bridging the IT Knowledge Gap in Cyber Conflict Preparedness

The Challenge

Military technical experts have in-depth knowledge of IT systems but often lack an understanding of command-level decision-making and strategic considerations. Conversely, command-level personnel are well-versed in military operational procedures and strategic planning but lack hands-on technical expertise, particularly in the realm of information systems and cybersecurity. The gap between technical and command levels is particularly evident in modern multi-domain military operations, where IT systems and real-time information exchange serve as the foundation for agile and informed decision-making.

From a military perspective, command levels can be categorized as follows:

- **National Strategic Level** – Responsible for long-term decision-making, shaping national security policies, and aligning military objectives with broader diplomatic, informational, military, and economic (DIME) strategies.
- **Military-Strategic Level** – Responsible for defining specific military objectives required to achieve national goals.
- **Operational Level** – Designs military campaigns and defines concrete objectives required to fulfill strategic goals while ensuring synchronized execution across various domains.
- **Tactical and Technical Levels** – Execute operations and manage technical implementations.

Effective communication and collaboration between these levels is essential for effective cyber operations and strategic decision-making in the modern battlefield.

The Solution: Cyber Conflict Simulator (CCS)

To address these challenges, the Cyber Conflict Simulator (CCS) was deployed as a key training platform, designed to enhance cyber readiness and inter-level coordination. The **CCS** was used to create a simulated military network environment with Internet access. Although not a full replication of a real-world military network, it effectively highlighted one of the military's key IT challenges: **spatial network dispersion**.

Military networks are distributed across multiple locations, often with several units operating under distinct command structures within the same physical site (e.g., barracks). Despite physical proximity, these units maintain entirely separate and logically segmented network solutions. Additionally, a single unit might span geographically distant locations but still function as part of the same IT network segment. The responsibility for maintaining this intricate system was assigned to a specialized military IT support unit.

To test real-world scenarios, **CCS simulated multiple simultaneous cyber incidents** across various locations. The IT maintenance unit was unable to unilaterally prioritize responses, requiring guidance from higher command levels. The exercise demonstrated that resolving cyber incidents demands close cooperation between technical experts and senior military leadership. The incident response team included intelligence, operational, and cyber specialists who coordinated efforts with field teams while maintaining constant communication with higher command levels.

Through this simulation, the importance of integrated cybersecurity strategy in modern military operations would be underscored, reinforcing the necessity for proactive and coordinated defense mechanisms.

Key Insights and Outcomes

Enhanced Understanding Across Command Levels

- **Higher command levels** gained a clearer perspective on the capabilities and limitations of their subordinates, allowing for more informed decision-making during cyber incidents.
- **Technical personnel** developed a stronger appreciation for strategic decision-making processes and how their expertise aligns with broader military objectives.

Addressing the Unique Challenges of Cyber Operations

- Unlike traditional warfare, cyber conflicts unfold in real time, eliminating the possibility of deploying reinforcements. This underscores the necessity of proactive defense strategies, swift decision-making and continuous operational readiness.
- The exercise underscored the importance of **precise planning, inter-level coordination, and adaptive strategies** tailored to the fluid nature of cyber threats.

Improved Decision-Making at Management Levels

- By abstracting technical complexities, **CCS enabled senior leadership to engage in meaningful decision-making**, a capability often lacking in traditional cyber exercises where tactical teams dominate the decision space.

CCS as a Highly Effective Training Tool

- Traditional military training methods (e.g., tabletop scenarios and simulation-based exercises) often focus on either technical drills or high-level strategy without fully integrating both.
- In contrast, **CCS facilitated a hybrid approach -** similar to **computer-assisted exercises (CAX) and computer-assisted wargames (CAWG)** - where leadership could actively participate in decision-making while the system autonomously handled technical calculations and scenario outcomes.
- The **rapid setup and controlled environment** allowed military personnel to safely test decision-making processes and operational plans with immediate feedback.

Conclusion

The Cyber Conflict Simulator (CCS) provided a **unique and invaluable training experience**, bridging the knowledge gap between technical and command levels in the military. By simulating real-time cyber incidents and decision-making processes, CCS enabled military leaders to develop the skills necessary to manage cyber conflicts effectively. This exercise emphasized the indispensable role of cross-domain collaboration, strategic foresight, and adaptive decision-making in navigating the ever-evolving complexities of cyber warfare.