The Marine Corps Information Assurance Program

Ray A. Letteer, CISSP, NSA-IAM, ITIL
Director, IA Division; USMC SIAO; MCEN DAA
Headquarters, US Marine Corps, C4IA

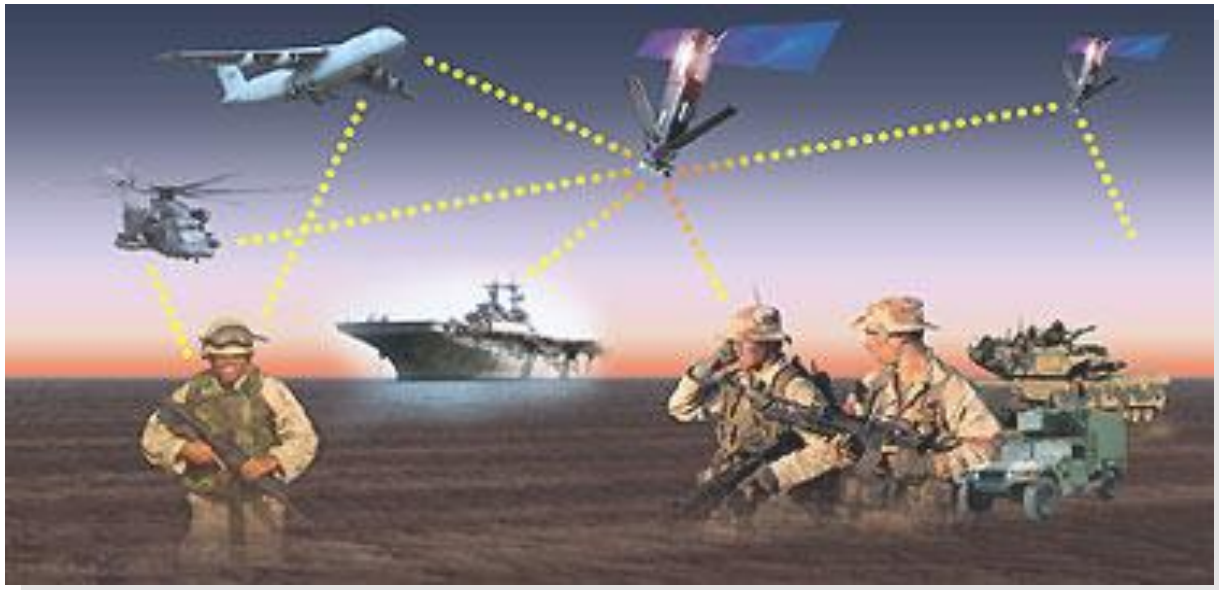
A Marine Corps fighting force armed with assured, secure, accurate, and timely information, to enhance the ability to take the fight to any enemy, any where, and win.

Historical Perspective
Bringing Civilization To Its Knees

What's Really Important

"America's Marines are fully engaged in the fight for freedom around the globe. …**I restate for emphasis: Our Marines and Sailors in combat are our number one priority in all that we do.**"

General James T. Conway, Commandant of the Marine Corps
2006 CMC Planning Guidance

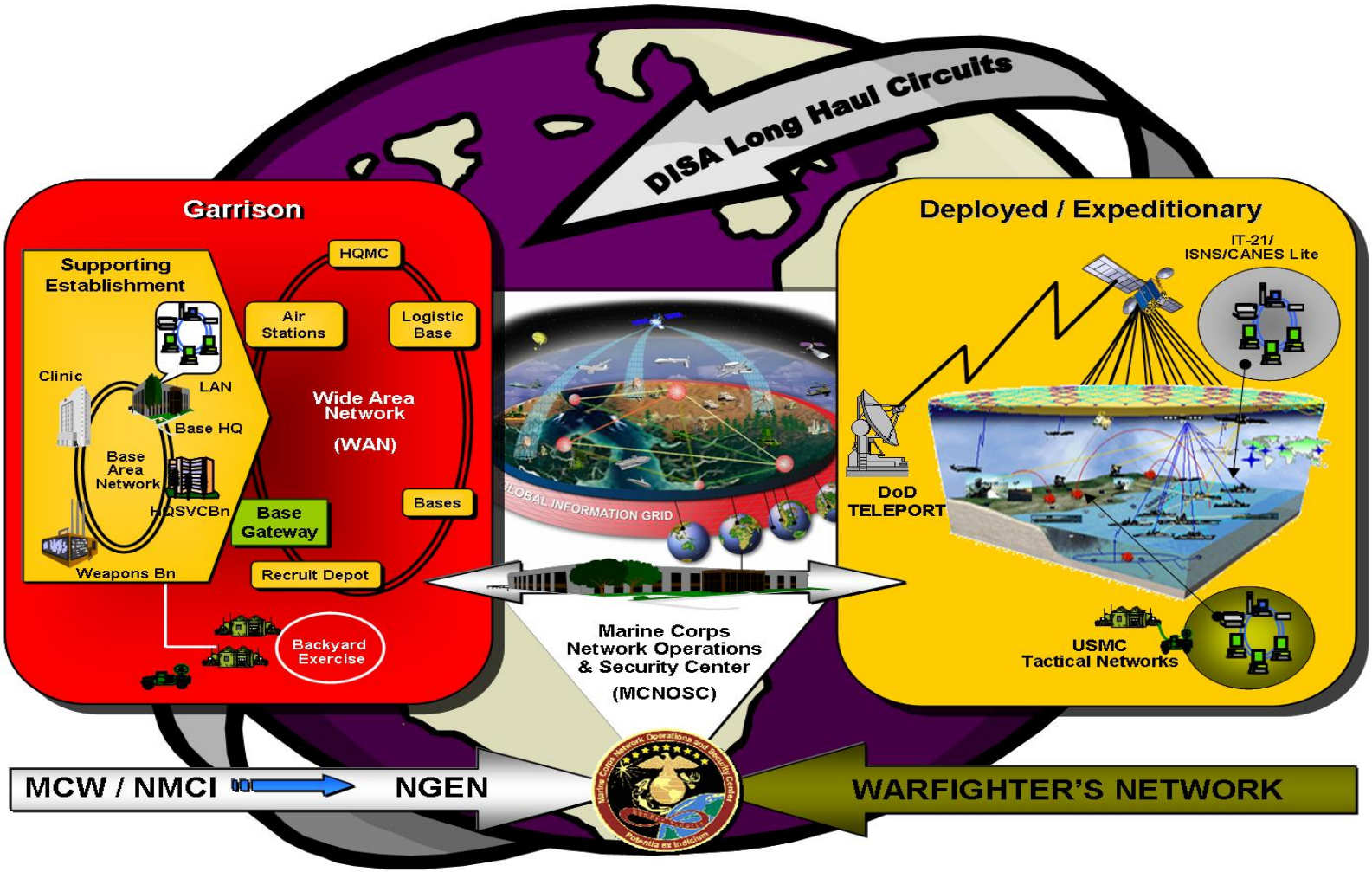


Information Assurance Pillars

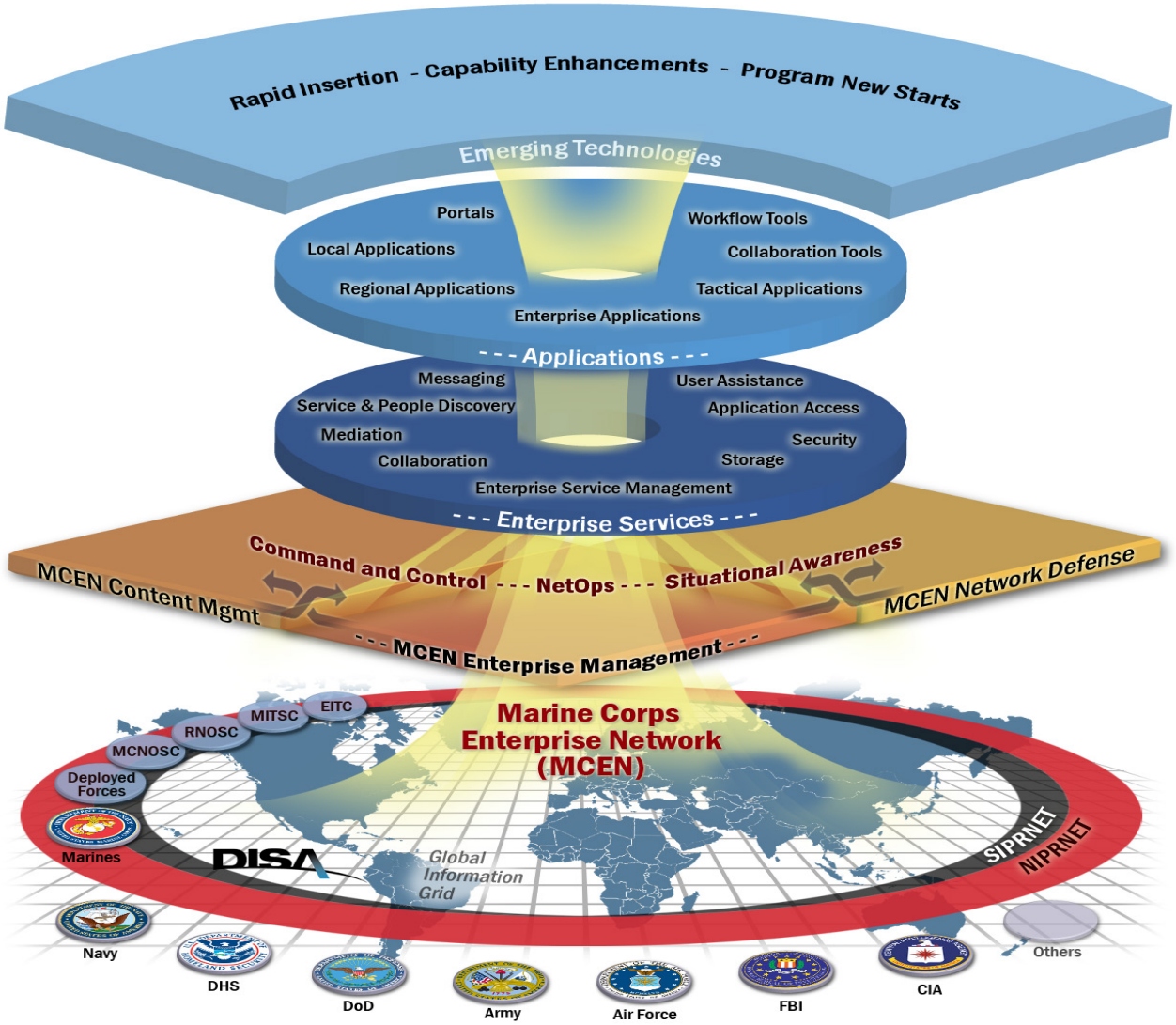
- Protect information,
- Defend systems and networks (Computer Network Defense or CND),
- Provide situational awareness & IA command and control,
- Transform & enable IA capabilities,
- Create an IA empowered workforce.

All of this is in support of the warfighter

Marine Corps Enterprise Network



Information Sharing Network



Marine Corps Cyber Security Two-Fold Mission Statement

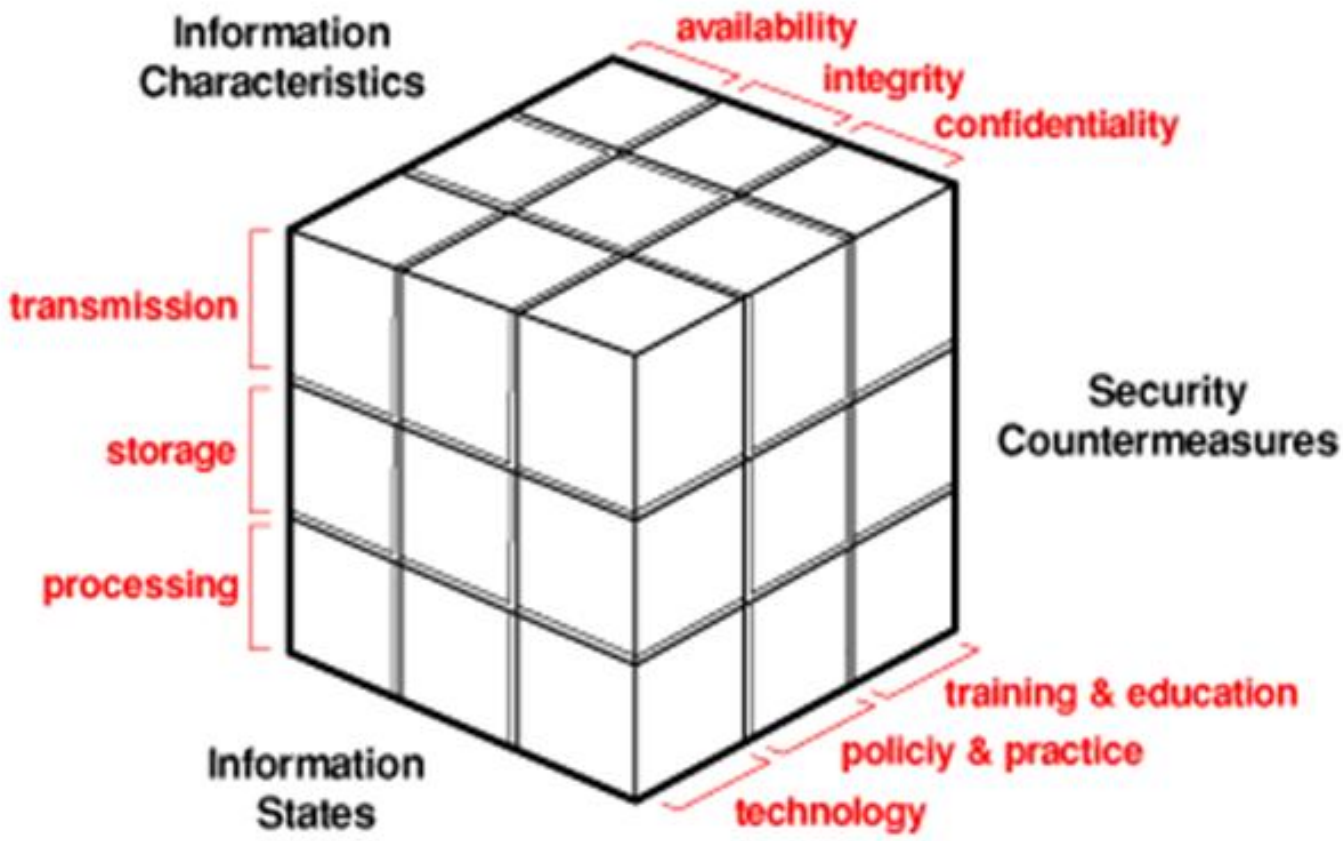
Ensure policies, procedures, standards, and methodologies are implemented within the Marine Corps to guarantee assured information delivery, data integrity, and ensured information protection.

Ensure an end-to-end capability that delivers secure information at the right time, to the right place, and in a useable format, allowing commanders to exercise command and communication, regardless of proximity to their assigned forces.

Close-up and Personal Cyber Challenges

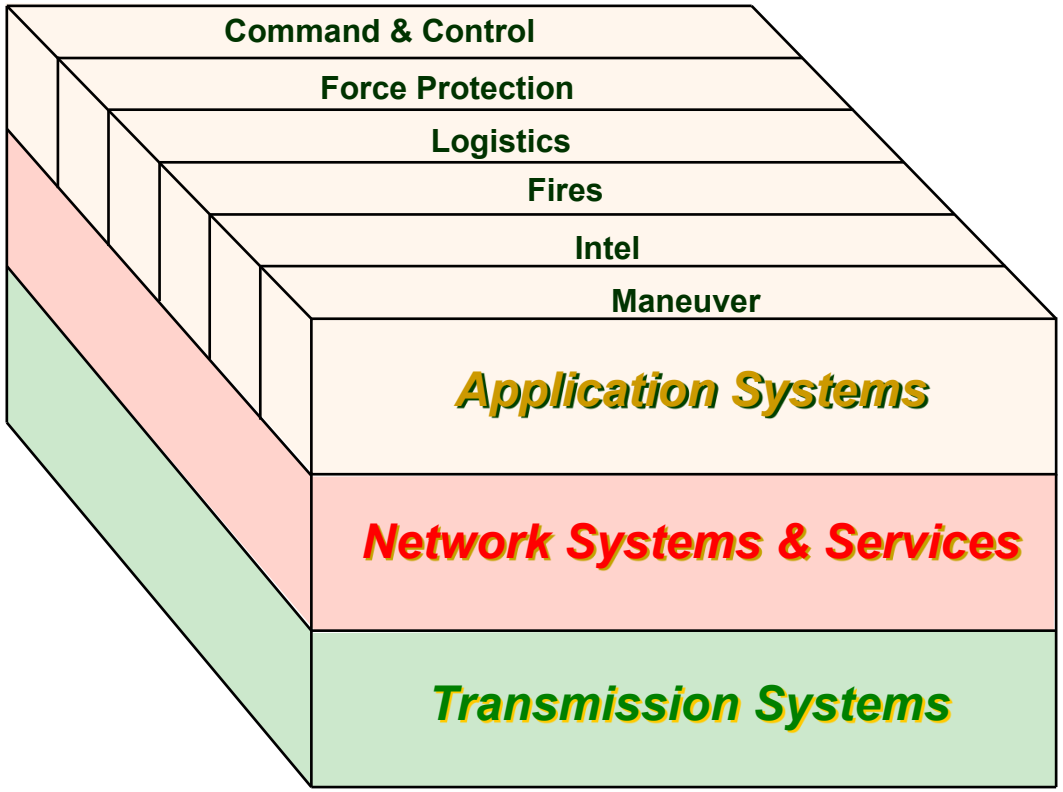
- Securing information operations in expeditionary maneuver warfare extending from the Operating Forces to the Supporting Establishment.
- Employing secure state-of-the-art technology.
- Providing cybersecurity awareness training to all users, and specialized training and education for certified Marine Corps cybersecurity professionals.
- Deploying a consistent defense in depth strategy with a robust suite of computer network defense tools, integrating the capabilities of people, sound procedures, and technology to achieve strong, effective, multi-layer and multi-dimensional protection to the Marine Corps portion of the GIG.
- Ensuring the secure development of systems and networks, including the integration of DOD, national, and allied systems that impact the Marine Corps architecture, and the use of corporate network enterprise applications.

Governance Approach



The McCumber Cube, John McCumber, 1991

Information Technology Architecture Cube



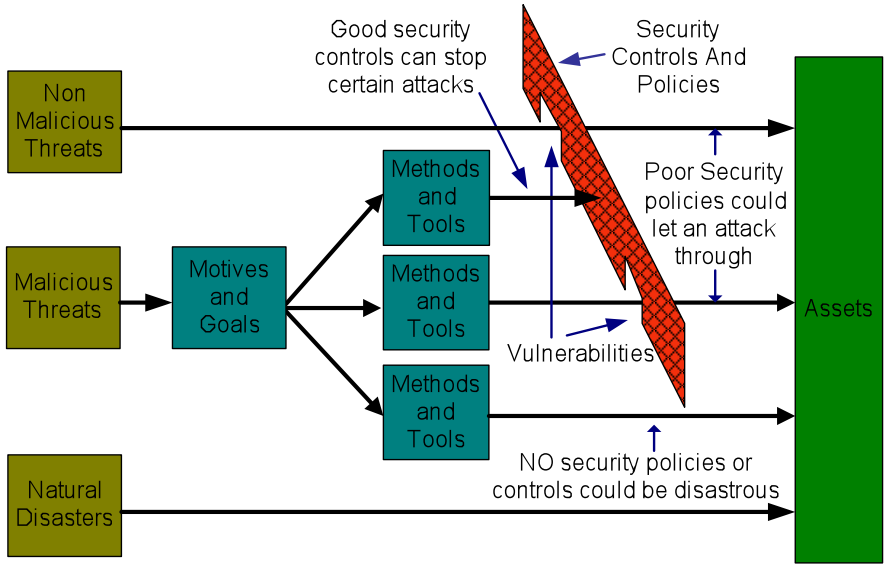
Focus of cyber security efforts

Dave Green, 2003

What keeps me up at night…

- Poor browser configurations,
- SQL misconfigurations,
- Undefined secure software supply chain,
- Poor operating system design,
- Failure to follow policy,
- Increasingly more sophisticated phishing /spear-phishing email attacks.
- Rush to unprotected social networking systems.
- Haste to push EOIP (Everything Over IP)
- Convergence onto mobile/smartphone technologies (e.g., SME-PED)

Ingredients of an Attack



Motive + Means + Opportunity = *ATTACK!*

"As the command and control system becomes increasingly complex, it likewise becomes increasingly vulnerable to disruption, monitoring, and penetration by the enemy..." MCDP 6

Possible Security Framework

- **Chain of Custody:** The confidence that each change and handoff made during the source code's lifetime is authorized, transparent and verifiable.
- **Least Privilege Access:** Personnel can access critical data with only the privileges needed to do their jobs.
- **Separation of Duties:** Personnel cannot unilaterally change data, nor unilaterally control the development process.
- **Tamper Resistance and Evidence:** Attempts to tamper are obstructed, and when they occur they are evident and reversible.
- **Persistent Protection:** Critical data is protected in ways that remain effective even if removed from the development location.
- **Compliance Management:** The success of the protections can be continually and independently confirmed.
- **Code Testing and Verification:** Methods for code inspection are applied and suspicious code is detected.

Paul Nicholas, Principal Security Strategist Manager for the Critical Infrastructure Protection group at Microsoft and Chair of SAFECode

Points to consider

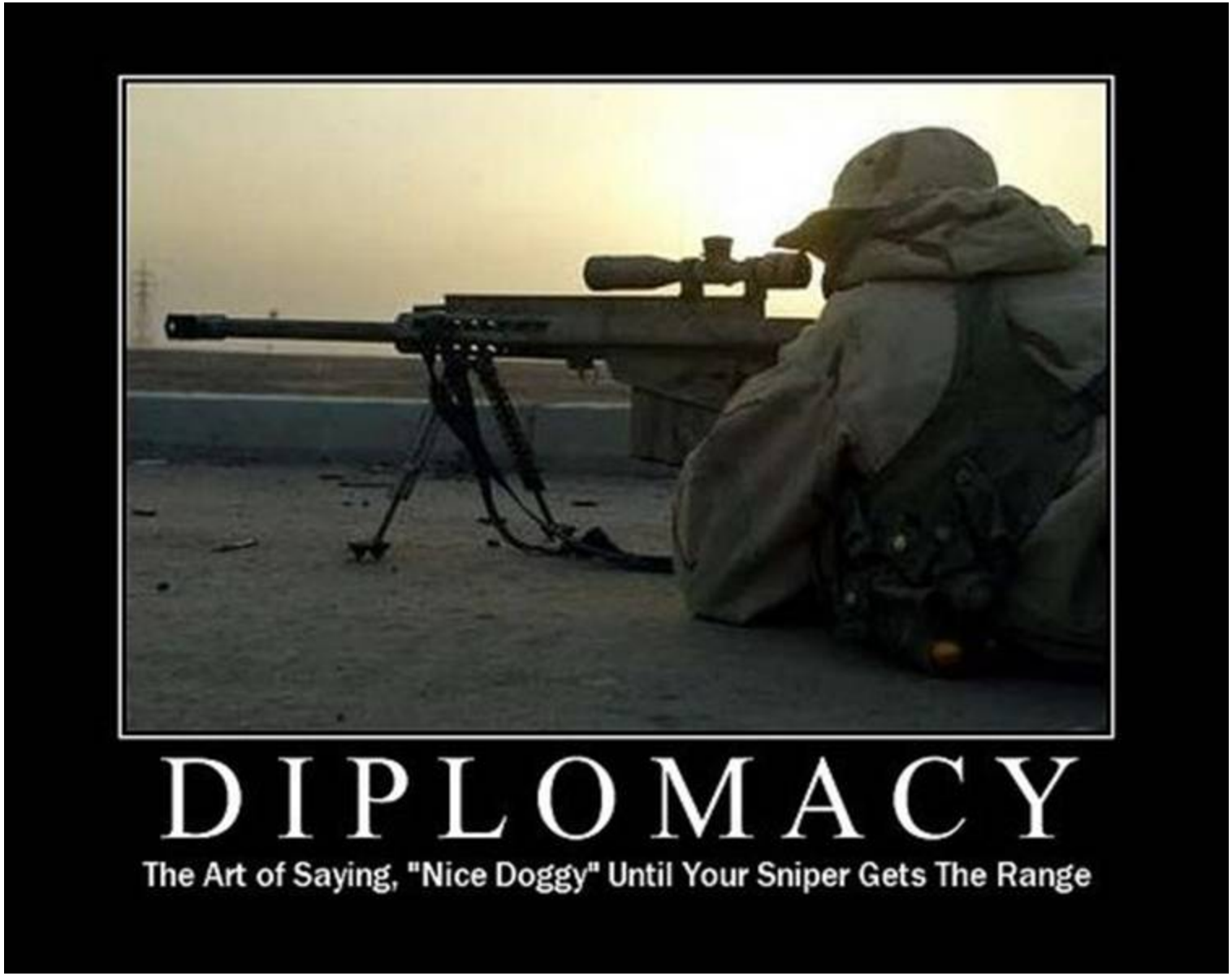
- The most technologically advanced tools, used **without enforcement** of basic IA policies, routine auditing and reporting procedures, are nothing more than "perfume on a pig".

- The implementation of IA takes more than tools and "boxes"; it takes a **trained and committed leadership and workforce**.

- Try as we might to foresee all forms of attack, compromise, and illicit activity, we are always subject to the affect of user-error in judgment – **you can't patch "stupid"**. Sometimes some form of **judicial/non-judicial** action is necessary.

The Gunny was slow to grasp the concept of "touch screen."

Questions?


DIPLOMACY
The Art of Saying, "Nice Doggy" Until Your Sniper Gets The Range