Cybersecurity

Ray A. Letteer, DSc IA, CISSP, C|CISO
Deputy, Compliance Branch/Cybersecurity
Headquarters, US Marine Corps
Deputy Commandant for Information

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.

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 cyber security awareness training to all users, and specialized training and education for certified Marine Corps cyber security 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 DODIN.
- 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 where applicable.

Cybersecurity Program Principles

- A comprehensive cyber security program is not just mounds of paperwork; artifacts must link to verifiable action. "Walking the walk" is more important than "talking the talk", …so:

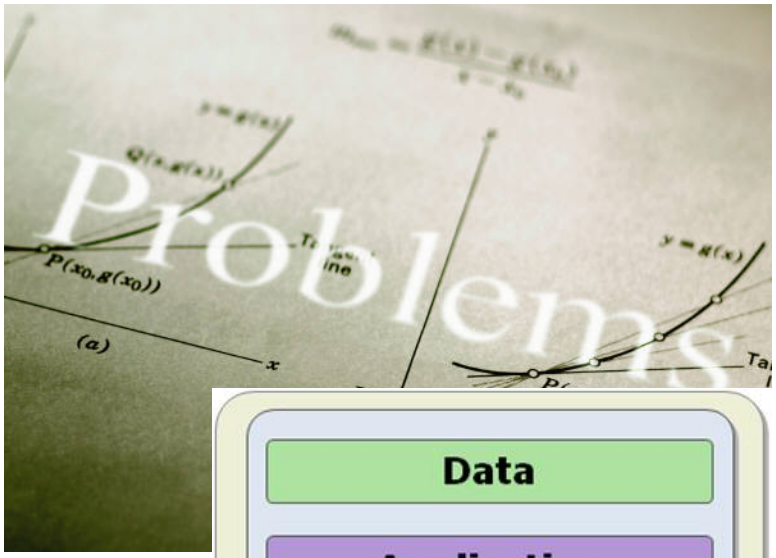
1. Find a way to say "yes", but fight "stupid.
2. Do what is right, and let the consequence follow.
3. Risk Balance vice Risk Avoidance or Risk Ignorance.
4. Remember Napoleon's corporal.

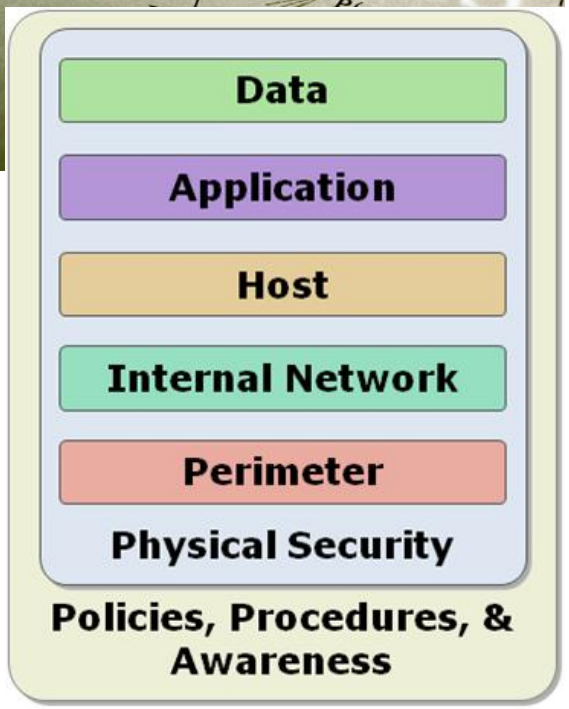
Discovered Truths

- The implementation of cyber security takes more than tools and "boxes"; it takes a **trained and committed leadership and workforce**.
- The attempt to reduce all risks to "zero" is not possible nor realistic. There is always some threat, either external or internal, maliciously planned or accidental, with which to contend. Resiliency is key, not a "perfect defense".
- The most technologically advanced tools, used **without enforcement** of basic cyber security policies, confirmed through routine auditing/testing, are nothing more than "perfume on a pig".
- 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 just can't patch "stupid"** and sometimes some form of **judicial/non-judicial** action is necessary.

Current Focus Areas

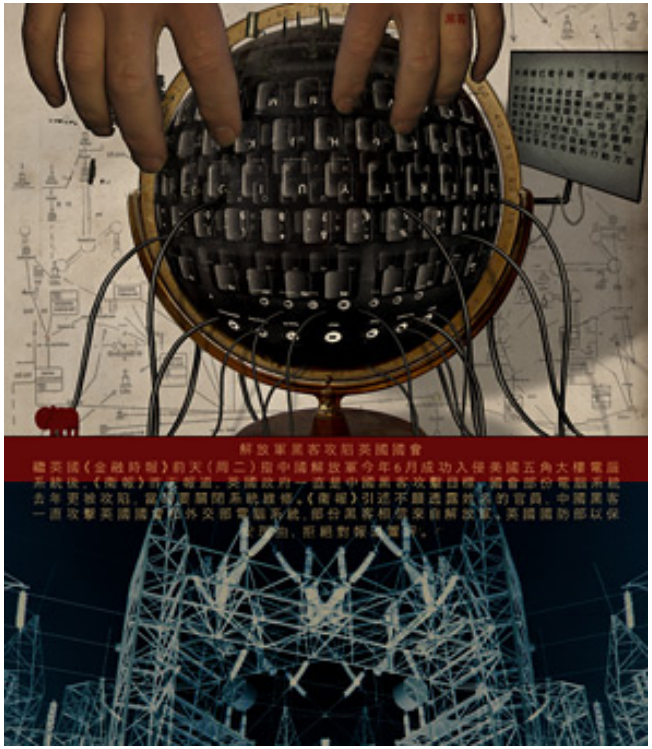
- DEVSECOPS/Software Development Foundries
- Comply-to-Connect
- FRCS/IoT
- Supply Chain Risk Management
- FedRAMP/RMF





What still keeps me up at night…

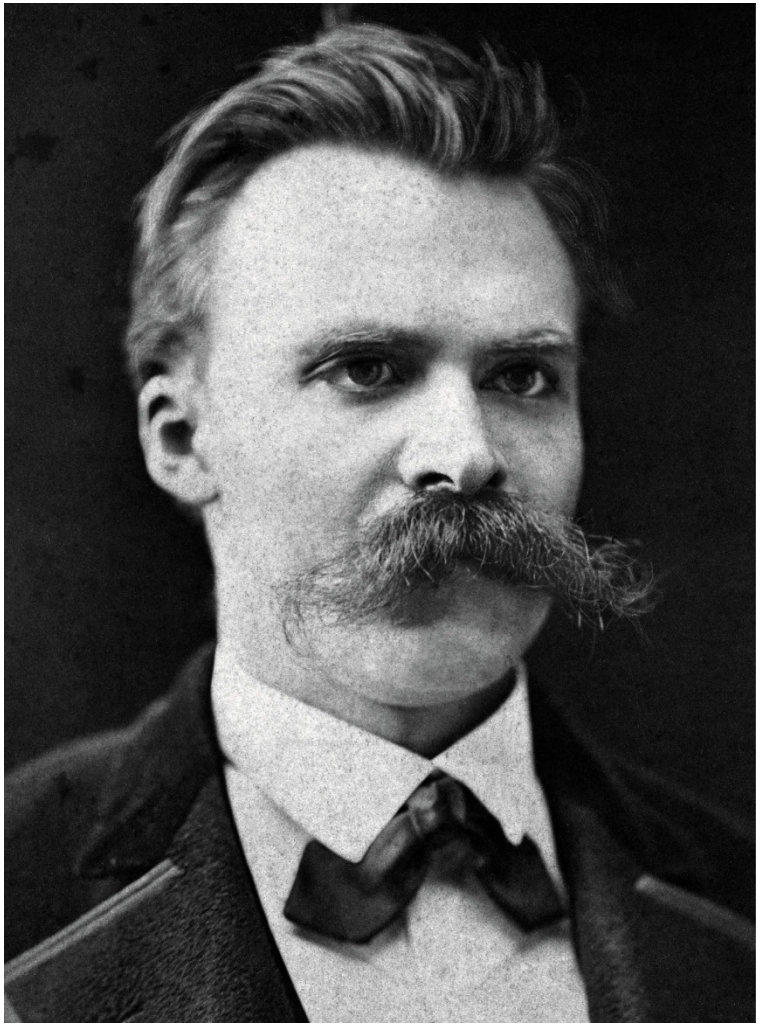
- Poorly designed applications, with no measurable or consistent security control implementation
- Lack of clear security controls for AI software
- Failure to follow policy, including **"shiny object syndrome"**.
- Lack of asset visibility…all endpoints, not just end-user devices.
- Phishing/spear-phishing email attacks increasing and becoming more sophisticated…getting linked to ransom-ware,
- Lack of clear supply chain security metrics and processes.
- Leadership & accountability



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*

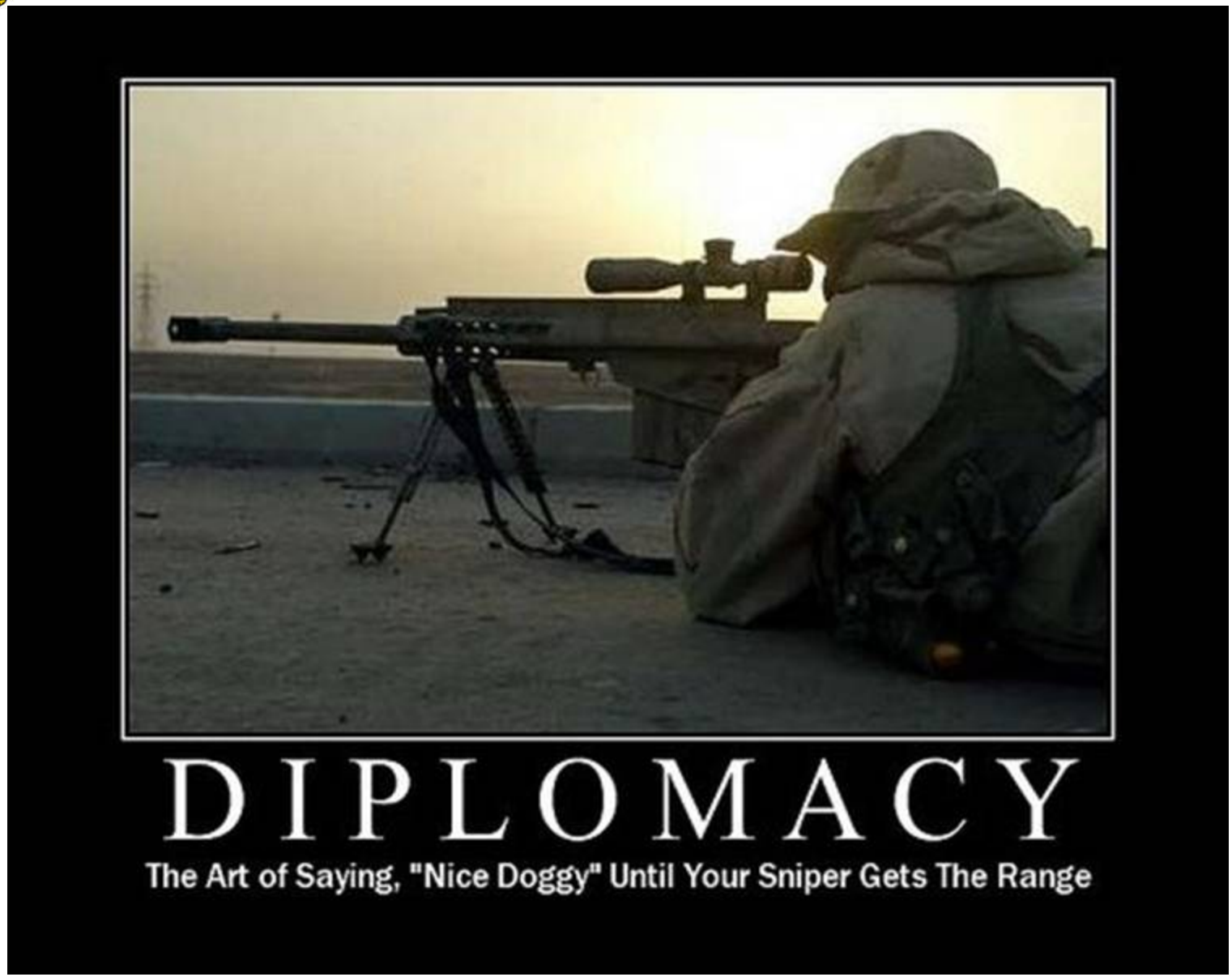
Final Thought



"If you know the ***why***, you can live any ***how***."

Friedrich Nietzsche

Questions?


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