Protecting the Marine Corps' Technological Advantage

A continuously critical process

by Mark Billow, James Proctor, Aaron Speer, GySgt Stuart Stone, SSgt Casey Talley & SSgt Jane Thibado

>Mr. Billow serves as the Intelligence Liaison Officer at Marine Corps Systems Command (MARCORSYSCOM).

>>Mr. Proctor is a member of the Program Management competency assigned to MARCORSYSCOM and serves as the USMC Service Lead to the Secretary of Defense's Protecting Critical Technology Task Force (PCTTF). He has an extensive acquisition background that includes board select positions of Product Manager (PdM).

>>>Mr. Speer is a Senior Intelligence Analyst Contractor with MANTECH and serves as the Lead Support Contractor to the Intelligence Liaison Officer at MARCORSYSCOM. He has experience in support to the counterintelligence and research, development and acquisitions (RDA) communities. His start in support to RDA is rooted in his work from supporting the Joint Acquisitions Protection and Exploitation Cell (JAPEC)

>>>>GySgt Stone is currently assigned to Marine Corps Base Quantico supporting technology protection efforts.

>>>>> SSgt Talley is currently assigned to Marine Corps Base Quantico supporting technology protection efforts.

>>>>>>SSgt Thibado is currently assigned to Marine Corps Base Quantico supporting technology protection efforts.

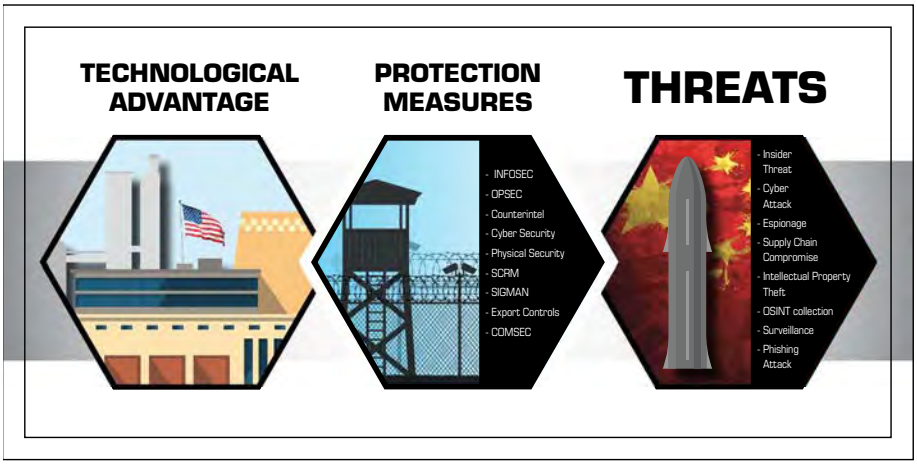
The contemporary capabilities and limitations of our military systems and critical technologies have never been at a greater risk because of the accessibility of open-source information. Our adversaries are using open-source information to gain critical insight into our systems and capabilities.

Open-source information provides an easier path to target vendors, academia, and government organizations to gain knowledge about key equipment and system capabilities, as well as their limitations. Enemy forces are using this information to counter U.S. technology and improve their own capabilities while saving costs associated with research and development.

The culture of information sharing in today's public sphere needs to be addressed. We must stress the importance of protecting and policing open-source information to guard our program information and critical technologies with the same level of importance in which we reference cost, schedule, and performance.

ALNAV 010/19, Our Responsibility to Protect Information, published in January 2019, includes a memo by the Secretary of Navy titled, "Our Responsibility to Protect Information." The message is the latest example of a top-level leader acknowledging the need to protect DOD technologies from adversarial exploitation. Failing to address this exploitation creates a risk of forfeiting the advantages that our technology provides, along with the significant costs incurred during the research, development, and acquisition process.

In a Secretary of Defense memo published on 24 October 2018, then-Secretary of Defense, James N. Mattis, estimated that American industry loses "more than $600 billion to theft and expropriation" every year, which is nearly the entire DOD annual budget. The rapid increase in adversarial capabilities to analyze "big data" and open-source information allows them to capitalize on our mistakes more efficiently than



Protecting the Corps' technological advantage. *(Image by authors.)*

ever, making this an increasingly urgent problem to solve.

A cultural change is necessary to successfully protect our technological capabilities. Fortunately, many organizations have already begun making changes. Other DOD organizations bring significant bandwidth and resources to technology protection through the development of the Critical Technology Protection Center at the Defense Counterintelligence and Security Agency: the organization in charge of the National Industrial Security Program.

The National Industrial Security Program governs security programs for companies within cleared industry working on behalf of the DOD. Exemplified in news reporting from the last several years, cleared industry partners are at significant risk of exploitation by adversarial personalities.

A strong partnership between acquisitions, intelligence, and requirements personnel with vendors and our industry partners is necessary to decrease the occurrences of open-source exploitation. Former and retired military and government personnel in addition to members of the defense industry often seek employment or advancement on public Internet sites. This results in the increased use of social media websites, such as LinkedIn and Facebook, where key personal information can be accessed by both potential employers and adversarial actors.

Physical security is just one aspect of protecting our technological capability. *(Photo by Sgt George Melendez.)*

At the corporate level, it is culturally important for publicly traded industry partners to announce multi-million-dollar contracts through press releases and other public messaging. Government messages, such as DOD press releases, also provide similar information.

The funds allocated, organizations involved, and purpose of the contracts are examples of information that can be cross-referenced for exploitation by our adversaries to determine and refine who and what to target through various methods of cyber activity such as phishing. These efforts can lead to adversaries gaining unfettered remote access to internal corporate or government data where sensitive program information can be extracted.

Those involved with research, development, and acquisition are familiar with cost, schedule, and performance as community accepted measures of success. Delivering a new capability on time and within budget can be a difficult task, but the value added to the warfighter is the yardstick by which we should measure success. A compromised technology is a major vulnerability on the battlefield.

We must shift our culture to one that balances the importance of cost, schedule, and performance with the need for uncompromised capabilities. In addition to evolving organizational culture, procedural and policy changes are required. Efforts that can spur change include: developing a formalized mechanism to share failures and compromises throughout the research, development, and acquisition community—including a research-, development- and acquisition-specific counterintelligence threat brief and case study to support the programs of instruction for acquisition officers and specialists; and developing a process to quantify the impact of compromise and potential compromise.

Other practical measures involve using contract language with vendors and industry partners, which requires

the mandatory reporting of security incidents to Marine Corps counterintelligence elements, Naval Criminal Investigative Services, or other relevant organizations such as a local Federal Bureau of Investigation office.

Technology protection, as a process, involves operations security, information security, cyber security, physical security, counterintelligence, supply chain risk management, signature management, and more. Each aspect is complex and can be applied to more than just technology protection.

The overall process of protecting information is continuous and independent of any single program or portfolio. Additionally, the responsibility to protect the Corps' capabilities does not rest solely with acquisition professionals. Every person involved in research, development, and acquisition has a contribution to make. These individuals might include researchers, contract specialists, and program managers.

MARADMIN 037/19, Organization for the Protection for Marine Corps Technology, published in January 2019, specifically lists the organizations tasked with participating in the Marine Corps Capability Protection Cell, as well as their relationship to the Navy Capabilities Protection Cell underneath the Chief of Naval Operations. The report shows why all members involved need to be invested in the technology protection process.

The Marine Corps Capability Protection Cell involves representatives from the offices of the Deputy Commandants for Combat Development and Integration, Programs and Resources; Plans, Policies, and Operations; Installations and Logistics, and Information as well as Communication Directorate, Marine Corps Systems Command, Marine Forces Cyber Command, and the Counsel for the Commandant of the Marine Corps. Protecting technologies involves everyone in the Corps and even those who support it.

Changing the culture associated with protecting program information and critical technologies will not happen overnight. The importance of safeguarding our program information and critical technologies could be the difference between winning and losing the next war.

Before you click on that link, publish that message, send that email, or update your online profile, think twice about the information you are sharing. Our adversaries are actively gathering and exploiting information. We *must* make every effort to protect the Corps' technological advantages.

USMC