Enabling Your TacCIS to Support Cyberspace Mission Objectives

The planning, deployment, and operation of a modern Tactical Communications and Information System (TacCIS) is a complex undertaking in and of itself. The challenges and threats of operating in today's cyberspace add further complexities which must be addressed for militaries to exercise effective command and control of operational forces.

GENERAL DYNAMICS
Mission Systems–Canada

Executive Summary

With the cyber threat landscape quickly growing beyond IT network level vulnerabilities and attack vectors, two concepts are emerging as key expansion drivers: a larger, multi-dimensional attack surface and the evolution of hybrid warfare where cyber activities are synchronized with more traditional land, sea, air and space activities.

An important distinction here is to recognize that although cyberspace is a separate domain from land, air, sea and space, it still has real-world kinetic requirements and won't change existing military doctrine. In fact, falling into the trap of viewing the introduction of "cyber" as a complete military paradigm shift will artificially raise the need to perform major overhauls to an existing Tactical Communications and Information System (TacCIS) while increasing the costs associated with supporting functions, such as training and system management.

The approach to enabling a TacCIS solution to support cyberspace mission objectives needs to follow an evolutionary path which builds on a cyber-primed and mission-focused architecture. Ultimately, the upgrade path must maintain existing cyber security capability and then further enhance cyber operational readiness and efficiency using a multi-layer incremental approach. This architecture must be intentionally designed to adapt to the threat landscape and technology innovations of tomorrow while meeting the cyber operations needs of today. This also means that in selecting, designing, and building an effective TacCIS solution, it is crucial to consider the ability to incrementally meet future requirements along the upgrade path.

In this paper, we detail one approach to upgrading a TacCIS using multi-layer cyber capability increments matched to operational requirements. The approach in this paper keeps the soldier at the forefront by delivering cyber operational capability supported by the TacCIS as required to achieve mission success.

Contents

What is Cyberspace?

In 2016, NATO established cyberspace as the fifth domain for military operations. Many nations around the world have since done the same. While many cyberspace definitions exist today, the U.K. Ministry of Defense's definition is comprehensive in that it clearly describes the inter-related and complex nature of this environment:

Cyberspace is a complex and dynamic environment, interdependent with the electromagnetic spectrum, and is key to all military operations on land, sea and in air and space. It is far more than just the Internet. Cyberspace is a pervasive and all-encompassing operating environment, incorporating for example, aircraft flight control systems, medical life-support systems, physical device controllers and national electricity distribution systems.[1]

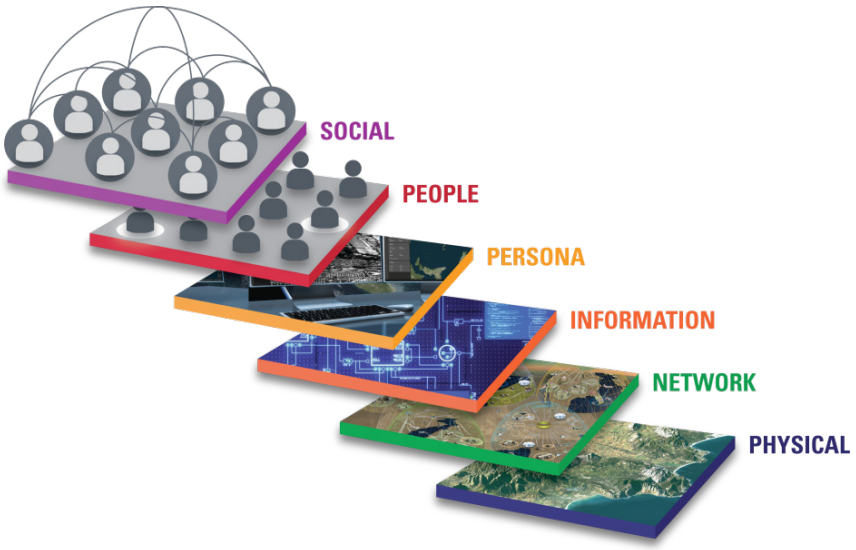

Figure 1: Layers of Cyberspace

Figure 1 illustrates the multi-dimensional and highly complex nature of cyberspace in comparison to the traditional domains of land, air, sea and space. Depicting cyberspace through multi-tiered planes allows us to better understand the possible attack vectors and the attack surface volume in relation to reactive, defensive, and active cyber operations.

TacCIS forms a component of the physical, network, and information layers of Cyberspace. While historically, the TacCIS could be viewed as operating independently of other control systems and networked devices within these three layers, the consideration of the persona, people and social layers are now causing this separation to weaken and, in some cases, to be non-existent. For example, historically, one could view a perimeter approach (physical layer) to protecting the TacCIS (cyber security) at a forward-operating base as the initial "defence in depth" layer: "If someone breaches my compound and accesses my TacCIS, I have bigger problems than unauthorized access". This historically trusted posture for the TacCIS is now being questioned as new attack vectors create a credible risk. Attack vectors at the social, persona and people layer (social engineering or insider attacks as examples) could easily bypass traditional perimeter controls or historically trusted network and information controls.

Further increasing the impact is the speed at which threats can enter and adapt or how long an adversary can remain undetected on a TacCIS using stealthy attack techniques such as Advanced Persistent Threats (APTs) or lateral movements across the network. An adversary may attack in cyberspace without causing physical harm, without breaching perimeter control, or without being detected by electronic warfare sensors. These challenges are compounded by considerations related to reactive, defensive, and active cyber operations. Through these examples, one can see that the increased complexity introduced by cyberspace is directly driving a shift into how the TacCIS addresses the fifth domain.

[1] UK Ministry of Defence, Cyber Primer Second Edition

Cyber Capability Layers of a TacCIS

One approach to evolving a TacCIS to support cyberspace missions is to trace mission objectives to cyber operational requirements to TacCIS cyber capabilities.

TacCIS cyber capabilities can be categorized into four layers (Figure 2) all based on a cyber-primed architecture. Cyber planning and capability development predicated on upgrading within specific layers allows a scalar and modular approach to filling specific mission requirements. For example, a NATO coalition mission objective could require TacCIS capabilities within select elements of the foundational, reactive, and active layers, while deliberately removing advanced sovereign active capabilities not appropriate for the multinational task force. This layered, modular approach also allows better definition and testing of new capabilities, allowing for rapid integration to battlefield networks at the time of an operator's choosing.

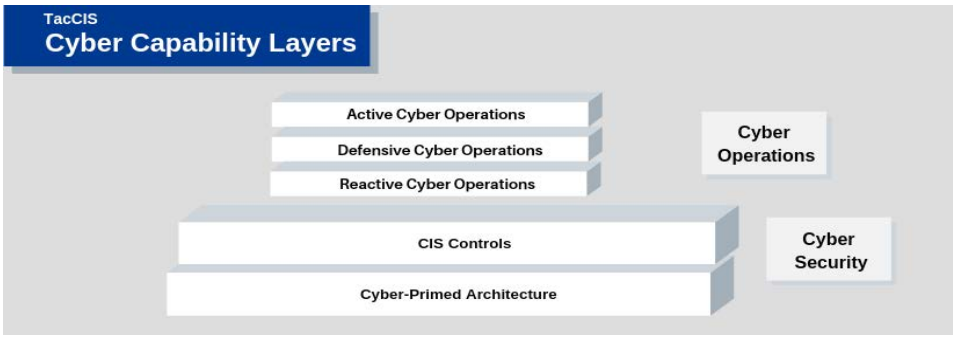

Figure 2: TacCIS Capability Layers

This approach allows for the TacCIS cyber capability to evolve and grow as mission objectives unfold, as new adversaries surface, or as existing adversaries change up their tactics.

CIS Controls

The objective of this layer is basic cyber security addressing the confidentiality, integrity and availability (CIA) information security triangle. While not directly used by the commander or the cyber operator during mission planning, this layer provides them a measure of information trust during an operation, and lays the foundation for advanced cyber capabilities. It includes:

- Network discovery and device inventory
- Identity management (authentication, authorization, auditing)
- System hardening (Hardening of hardware and software on networked devices)
- Network Hardening (Firewalls, Information Exchange Gateways, etc.)
- Data protection and integrity (encryption, hashing, steganography))
- Security Architecture (NW zones, segmentation, NW access control)
- Public Key Infrastructure (PKI)
- Malware protection
- Application Security (both hardening of commercial applications and ensuring secure software development practices)
- Penetration testing and red-teaming
- Physical Security controls and standards
- Training (Network Operator and User cyber awareness training)

The CIS Controls address current known threats, such as unpatched operating systems and software as well as misconfigured operating systems. At this stage, evolving threats, including polymorphic viruses and malware are also addressed. Several government and commercial standards, such as ITSG-33 and the Centre for Information Security Controls are available to inform the development of the CIS Controls.

Cyber Capability Layers of a TacCIS

Reactive Cyber Operations

Reactive cyber operations are used to respond to a breach or attempted breaches from an adversary. Disaster recovery and mission-continuity procedures and tools should be built into this layer.

Measures built into a TacCIS could include automated reconfiguration of a network based on dynamic asset prioritization so as to isolate the threat or create intelligence collection traps, shutdown of systems based on mission importance to limit damage, journaling and playback to detect damage, and cyber surveillance methods to observe adversary behavior for the purpose of enhancing threat intelligence. An essential element of TacCIS cyber development is ensuring that mission continuity is prioritized over traditional enterprise IT concerns.

After a breach - or an attempt - has been detected, new intelligence can be used to inform other deployments by disseminating this newly discovered threat intelligence through various means and common threat sharing languages and formats, such as TAXI, STIX, and CyBOX.

Defensive Cyber Operations

Defensive Cyber operations are used to plan and proactively defend against adversaries, and includeautomated processes such as continuous vulnerability scans, software baseline management and compliance, Artificial Intelligence, and behavioral analytics to identify abnormal system/network behavior are examples of TacCIS capabilities built within this layer.

The capabilities built into defensive cyber operations provide the ability to compute threat intelligence analytics, to merge threat intelligence data with existing situational awareness, and to simulate missions for the purpose of mission planning and training.

As part of this layer, an enhanced SIEM (Security Information and Event Management) capability is included as part of the TacCIS. A tactical Security Operations Centre (TSOC) is very different than a traditional enterprise SOC in that it needs to be portable (ex. at a forward operating base), distributed and adaptable to tactical networks. In addition, as the operational tempo increases, typically closer to the “edge”, even though more relevant or real-time data is available, there are fewer resources and less time to make decisions.

Additionally, defensive cyber operations provide the ability to assess the impact of malicious events and to automatically generate recommendations to remediate the threat. It will use threat intelligence gathered from multiple domains including cyber and electronic warfare and will fuse this additional information to increase overall situational awareness.

The defensive layer can analyze these threats and, through various analytics including deep learning and Artificial Intelligence, provide possible courses of action to remediate the threat. As part of a TacCIS, these courses of action are not exclusive to cyberattacks or defensive actions. Other approaches may be recommended that could include additional types of electronic warfare or kinetic effects. The defensive layer can also provide tools for analysts to perform “what-if” scenarios in order to predict the effectiveness of any recommended courses of action prior to engaging.

Active Cyber Operations

The ability to perform active cyber operations against adversaries, on friendly, neutral, and adversary-owned networks is activated at this layer. In addition to integrating with mission planning tools, the TacCIS provides the ability to complete cyber reconnaissance, select modes of attack based on threat intelligence data, and the ability to invoke attack vectors while minimizing/eliminating digital residue.

Furthermore, it addresses the workflows required to establish a “kill chain” and mission plans based on phases of reconnaissance, delivery, exploitation, command and control, internal reconnaissance and persistence.

TacCIS Cyber-Primed Architecture

Foundational to this innovative flexibility is an adaptable CIS architecture optimized for use in disconnected, intermittent and low-bandwidth (DIL) environments exhibiting the following cyber-primed characteristics:

- Hide cyber security complexity from users through rules-based automation and workflow-based activities.
- Enable rapid technology acquisition through a modular design, open technology standards, and a supporting architecture to support system evolution and technology insertion.
- Offer user-customizable interfaces and dashboards to provide cyber situational awareness fully integrated with existing situational awareness interfaces at the dismounted, mobile and headquarters domain.
- Provide fully supported software development kits to enable third parties to develop management plug-ins for new technologies and equipment.
- Deliver interfaces which effect and observe target networks and the ability to collect and distribute threat intelligence data beyond standard capabilities.
- Support SDN-compatible technologies: from a technology standpoint, SDN is a huge game changer as it allows operators finer control to detect lateral attacks, reconfigure the network as a defensive measure, and spoof attack success indicators.

This particular architecture allows for the flexibility to adapt the TacCIS cyber posture as the threat landscape changes and as mission objectives unfold. More importantly, it preserves the TacCIS solution space to address future mission requirements.

Cyber Challenges in a TacCIS

The challenges of operating a TacCIS in cyberspace range from understanding the threat and accepting that it could come from a traditional enemy, an unknown actor, a more traditional insider threat, or an intentional or unintentional piece of code introduced in one of the multiple computers or processors found in all military systems.

In planning and managing the deployment of a TacCIS, one must ensure that system vulnerabilities are minimized. Given the nature and interconnectivity of systems today, it is impossible to eliminate them. The rapid advancement of information technology results in a continual change to a TacCIS to leverage new capabilities for the warfighter, address vulnerabilities, and deal with obsolescence. Addressing these challenges requires reliable and predictable funding to achieve the required system evolution and train operators to plan, deploy and protect networks and the information they support.

Conclusion

The control of military operations throughout the spectrum of conflict is enabled through the deployment of an effective tactical communications and information system. As nations and militaries around the world establish and deploy their cyber operation forces, the TacCIS continues to be an essential enabler to support mission objectives. Cyber Situational Awareness must be included in SA tools used to manage other battlefield domains and available to commanders and warfighters at all levels. By incorporating cyber operations into the SA “picture” as a force multiplier, mission outcomes can be achieved through options not previously available.

As the method for fighting the battle has not changed, the TacCIS is well-positioned to quickly adapt and grow its existing capabilities as new missions come along, as adversaries adapt, and as new technology becomes available. A TacCIS that is built and deployed correctly can not only manage, but exploit opportunities to address current and future adversaries head-on.

GENERAL DYNAMICS
Mission Systems–Canada

www.gdmissionsystems.ca
info@gd-ms.ca