TaLKing SHOP

SPACE & CYBERSPACE:

The Overlap and Intersection of Two Frontiers

BY JAC W. SHIPP

The pace of change and level of effort has increased dramatically with respect to operations in Space and Cyberspace, with both of these domains increasingly being influenced by multiple actors with access to the information environment. What is needed in supporting this trend is up-to-date thinking and dialogue about how the Space and Cyberspace domains and their operations overlap and intersect, and the synergies and opportunities created by each. Our journey involves the examination of Space and Cyberspace definitions and analyzes specific aspects to promote understanding of Space and Cyberspace. These areas are situational awareness, operations, training and leader development, capabilities development and acquisition. Our focus is on the discovery of ways to prepare our Nation's leaders — public and private sector — on ways to leverage these domains to advance our Nation's interests by improving integrated Space and Cyberspace support to full spectrum operations.

Key Areas of Intersection

- Space, like cyberspace, is a warfighting domain.
- Both domains are information-centric and information-enabled.
- Both Space and Cyber superiority support information superiority.
- Both Space and Cyber operations enhance situational awareness.
- Space capabilities enable, and may be enabled by the conduct of, cyberspace operations.
- Space capabilities are employed in the extension of the Army's portion of the GiG-LandWarNet, particularly in support of deployed forces.
- Space capabilities, particularly space control capabilities, are employed to deliver Cyber Attack and Exploitation payloads to our adversaries, systems and networks.

Key Definitions and Insights

Space and Cyberspace Domains. The Space domain is "a medium like the Land, Sea, and Air within which military activities shall be conducted to achieve US national security objectives."[1] The Cyberspace domain is a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] From these definitions we conclude each is a global warfighting domain where distinctive Space and Cyberspace military activities are conducted. Both generate effects in and through their own domains, and across the other domains (e.g. Air, Land, and Maritime). Both domains are information-centric and information-enabled and both advocate Space and Cyberspace superiority goals in support of domain and information superiority. These domains share networked systems and associated physical infrastructures. The primary objective for each is to ensure friendly freedom of action and as necessary deny adversary freedom of action, suggesting common elements for strategy development. Space and Cyberspace are the newcomers to the realm of warfighting domains, and as such have yet to be fully understood, exploited and integrated

The key area of intersection between Space and Cyberspace Situational Awareness is represented by the tools - technologies - techniques employed to support visualization of the situation

into military operations. Their respective operational architectures reflect considerable interdependencies, that is, an effect in one domain can have immediate and far reaching consequences in the other. The interconnected and highly technical nature of Space and Cyberspace has led to a specialized training and career force approaches which has resulted in limited leader awareness, slow progress in Space and Cyberspace planning, and a less than desired level of joint and Army integration. A summary insight is that the Space and Cyberspace domains demonstrate more similarities than any other domains, offering many opportunities for cooperative and synergistic efforts. Our journey will explore a few of those opportunities.

Space and Cyberspace Operations. Space operations are comprised of the following mission areas: Space force enhancement, Space support, Space control, and Space force application.[3] Cyberspace operations include the "employment of Cyberspace capabilities where the primary purpose is to achieve objectives in and through Cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[4] Both Space and Cyberspace operations require, and simultaneously enhance situational awareness; the speed of Space and Cyberspace activities demands timely and precise situational awareness. The operational framework and Concept of Operations for Space and Cyberspace are amazingly similar. Both rely on specialized intelligence and data fusion to enable a level of situational awareness that supports timely operational decisions and action. Each is heavily dependent on global connectivity, a support component (e.g., satellite operations for space, and forensics for cyber), and active and passive defensive measures. And both Space and Cyberspace operations depend on an offensive operations arm (space control and NetWar) to deny adversary freedom of action as required. Space capabilities enable, and may also be enabled by the conduct of, Cyberspace operations. Likewise, Cyberspace operations enable Space operations and are clearly enabled by Space capabilities. Many Space capabilities are employed in the extension of the Army's portion of the GiG-LandWarNet, particularly in support of deployed forces; an example is the dissemination of mission warning data initiated at space-based infrared sensors and disseminated via theater broadcast means and the Joint Tactical Ground Station platforms. Space capabilities can be employed to facilitate Cyberspace attack and exploitation data from systems, networks and device level activity. Space platforms and their attending links and ground systems are used to communicate friendly Cyberspace information both to defend and maintain situational awareness of those systems and networks. Cyberspace operations may also be employed to enhance the Army's ability to dominate Space through the delivery of Cyberspace capabilities to adversary Space platforms and their supporting networks. These similarities in the framework and conduct of Space and Cyberspace operations suggest synergies and efficiencies that can be achieved in developing, employing and integrating Space and Cyberspace capabilities and operations.

Intersect and overlap. It then becomes relevant to explore whether the Space and Cyberspace domains, and their associated operations intersect or overlap. To Intersect is defined by the 2010 Oxford English Dictionary as follows: inter-between secure to cut - to divide something in two by passing through or lying across (1412-Chronicles of Troy) Oxford p. 1137. An overlap is defined as a partial superposition, or coincidence (1813-Agricultural Survey of Galloway) Oxford p. 1096. As we examine the discreet components of each domain and operation we see that both occupy discreet and distinct points in time and place. A router in Space facilitating the flow of data across the Internet, GIG, or LandWarNet is overlapping the Space platform hosting its payload. The data passing through the router is intersecting the Space platform for a brief period of time. The employment of offensive Space capabilities to support the delivery of offensive Cyberspace tools creates an operational intersection. Both terms, then, seem equally applicable in different and distinct ways.

Insights into Areas of Space and Cyberspace Convergence

While there are many areas of convergence in planning, coordinating and executing Space and Cyberspace activities across both the operational and institutional Army, four specific areas are highlighted here: situational awareness, operations, training and leader development, and capability acquisition. Each has far reaching implications across Doctrine Organization Training Materiel Leadership Personnel Facilities[5] in terms of efficiencies by leveraging commonalities that exist between Space and cyber. Within situational awareness we see the potential for development of a single set of tools, technologies, and techniques that support visualization of the friendly and adversary Space and Cyberspace situation to empower situational understanding and decision-making. Within Space and Cyberspace operations there are opportunities for synergy in concept and Concept of the Operation development, inter-service crosstalk and coordination, and offensive and defensive integration. Within Space and Cyberspace training and leader development there are opportunities and potential cost savings to be found in identifying who, where, and how that training is conducted, and in how we manage Space and Cyberspace professionals. Finally, within capability acquisition synergy may be created between Space

- Space platforms and their attending Ground Systems are used to communicate friendly Cyber information both to defend and maintain situational awareness of those systems and networks.
- High Altitude Long Endurance platforms provide another means to accomplish many of the same tasks performed by Space capabilities, but provide capabilities in areas where more responsive and persistent coverage is needed.

and Cyberspace in how we incentivize the private sector to participate, and how we develop and sustain supply chain security.

Space and Cyberspace Situational Awareness

The U.S. Army Capstone Concept (December 2009) states that "a fundamental capability is establishing early and sustained situational awareness through all intelligence disciplines to enhance operations, planning and execution." Situational awareness is derived from detailed intelligence, understanding of the operational environment and friendly and adversary activities and capabilities. Both Space and Cyberspace situational awareness are essential for accomplishing Space and Cyberspace related tasks and operations as well as supporting operational situational awareness, understanding, and decision making. And both achieve SA through the collection, reporting, analysis and assessment of a set of common components (e.g., surveillance of Space and Cyberspace, intelligence, and environment) that contribute information to achieve SA. The key area of intersection between Space and Cyberspace SA is represented by the tools-technologies-techniques employed to support visualization of the situation to the commander. Currently, we would argue, no Space and Cyberspace visualization capabilities have been effectively integrated into the commanders' common operating picture. Nascent tools have certainly been developed that portray aspects of SA in both the Space and Cyberspace domains but nothing has appeared on the horizon that encompasses both domains—or points of intersection between the domains—or the key aspects of SA discussed above to be effectively integrated into existing COPs. The ideal setup would also allow for a degree of interoperability with our joint, interagency, intergovernmental and multinational partners. Given the high degree of similarity and numerous points of intersection between the Space and Cyberspace domains the development of a single visualization capability integrating data from each holds promise for more comprehensive understanding and potentially will save time and money in the process. Combining the efforts of the Space and Cyberspace communities of interest to identify technical solutions will help identify and account for the inherent interdependencies between these domains and operations. In addition these synergies are reinforced in an organizational sense as U.S. Strategic Command and a number of the Service Components are multi-hatting Space and Cyberspace commands.

Operations

Three key areas of synergy between Space and Cyberspace operations are concept and concept of the operation development, inter-service crosstalk and coordination and offensive-defensive integration. First, concept and CONOP development. Since the frameworks for Space and Cyberspace operations are similar it makes sense that collaborative development of future concepts and CONOPS would result in more complete and integrated concepts and CONOPS. This idea of Inter-Service Warfighter Talks suggests the benefits that would be derived from the formal coordination between the Services at the Major Command and at the Operational Command levels (e.g. Air Force Space Command and Army Space and Missile Defense Command, and 24th Air Force and Army Cyber Command). This concept of Army-Air Force and Army-Navy Warfighter activity would showcase and advance the ways that the services are approaching the planning and conduct of Space and Cyberspace operations to benefit utility and unify effort. Finally, the area of offensive and defensive integration is a promising area of collaboration. Both Space and Cyberspace operations require a level of integration between the defensive and offensive components, and both are characterized by classified and compartmented capabilities and are components of Army Special Technical Operations. It would be useful to collaboratively develop novel approaches to offensive and defensive integration and integrated STO in support of land campaigns.

Space and Cyberspace Training, Leader Development, and Career Field Management

Space and Cyberspace operations are hardware, software, and technical centric and require a significant level of commercial sector integration and coordination. Both involve considerable employment of communications and intelligence capabilities and related infrastructure considerations. Identifying the precise areas of intersection in the curricula, who provides this instruction, and what facilities and resources support this training and education for our military professionals is another potential cost saving and efficiency area of synergy. This education should be examined beyond the bounds of the Army, looking across the other services as well as training with academia and industry. We can admit that both Space and Cyberspace operations are poorly understood by the Warfighter. An examination of how we present these topics to our present and future leaders throughout the professional military education process may lead to a more holistic program of instruction that informs both areas work,

- Cyberspace Operations may also be employed to enhance the Army's ability to dominate Space through the delivery of cyber capabilities to adversary Space platforms and their supporting networks.
- Similarly, Cyberspace operations may be employed to enhance Air and Missile Defense Operations by simultaneously attacking adversary key Cyber nodes, while protecting our own from threat penetration and disruption.

and how they work together to effectively support full spectrum operations. A third potential area of synergy that should be explored is how we manage Space and Cyberspace professionals and subject matter experts. The Army Space professional cadre has been evolving over the last decade and there are surely lessons that could be applied to the development and management of an Army Cyberspace career field. Key questions need to be addressed. Does the Warfighter need a general knowledge of Space and Cyberspace operations, or does he simply need to know where and to whom to reach for advice and assistance in the integration of these areas? What about training with industry and how we can better understand and leverage commercial capabilities, ideas and processes?

Space and Cyberspace Capability Acquisition

It's no surprise that both Space and Cyberspace capabilities continue to push the research and development communities to the very edge of what is technologically possible, and both communities struggle with rapidly developing and effectively integrating capabilities for operational users. This continues to strain existing military acquisition processes which have principally been designed to produce hundreds or thousands of major end-items that come with a parts and logistic support cycle spanning years, or even decades. These processes are not well adapted to build a single Space platform, or a specialized Cyberspace capability. Both Space and Cyberspace operations require an acquisition process that favors speed and agility. The Army does not need to develop this process or capabilities alone. The tremendous strength inherent in effectively managing public-private partnerships is an area not yet fully exploited. Before this partnership can become *de rigueur* there are a few hurdles to surmount. Some of these include determining how we incentivize the private sector to participate; how we protect the intellectual property of private sector/academia while rapidly ingesting capabilities that are developed in support of validated requirements; how we address the many security and clearance issues to get the requirement to the widest possible audience; and how we ensure capabilities developed through this process are interoperable with existing capabilities. Another shared concern to address in Space and Cyberspace capability acquisition is supply chain security. We must conduct technologically informed risk management and identify those capabilities and platforms within which we cannot afford the inherent risk associated with foreign-designed and manufactured components, and those for which we have a greater degree of flexibility in their country of origin and build or acquire accordingly. Certainly there will be economies in the implementation of a single supply chain management process for both Space and Cyberspace capabilities rather than independent processes for each area.

Conclusions and Recommendations

Given the incidents of intersection and overlap between the Space and Cyberspace domains, and their associated platforms, capabilities, and operations we have outlined a few areas where leveraging cross-domain synergy can realize cost, effort, and resource savings. So what's next? The key players in this kind of synergy must include U.S. Army Cyber Command, U.S. Army Space and Missile Defense Command/Army Forces Strategic Command on the operational side, and their associated offices of Space and cyber proponency as well as the key elements within our institutional Army, notably the Mission Command Center of Excellence. Only through close and continuous coordination across these elements and organizations from the early concept and architecture work, through the various battle labs and centers of excellence, to the final fielding and employment of these capabilities can we hope to capitalize on these potential synergies and efficiencies for the good of our Soldiers and our Army.

Footnotes

[1] Joint Publication 3-14

[2] Deputy Secretary of Defense Memorandum, SUBJ: The Definition of Cyberspace dated May 2008.

[3] Joint Publication 3-14

[4] (August 2009 update to the Deputy Secretary of Defense approved definition of CyberOps)

[5] DOTMLPF refers to doctrine, organization, training, material, leadership, personnel, and facilities.

Bio

Mr. Shipp retired from U. S. Special Operations Command in 2009 and currently works for the Scitor Corporation supporting the USASMDC/ARSTRAT Battle Lab as a cyberspace operations subject matter expert. Mr. Shipp has been planning, leading and supporting the conduct of cyberspace operations for more than 10 years. He has been involved in the development of Army cyberspace concepts, training and leader development, advised senior military leadership on the integration of cyberspace operations in full spectrum operations, and briefed cyberspace operations and activities to the Vice President of the United States, White House and Congressional Staff, Director-Central Intelligence Agency, Director-National Security Agency, Director of National Intelligence, and Army, Air Force, and Navy flag officers.