The Cyber and Information Domain and the Space Domain: Links and Interdependencies

111

By Maj Gen Juergen Setzer, GE Army
Vice Chief Cyber- and Information Domain Service Bundeswehr

Introduction

For a long time in NATO's history, the three traditional operational domains – Land, Sea and Air – were the basis for deriving the necessary capabilities and providing the framework for both the strategic and operational approaches to warfare. More importantly, those three operational domains which are representing the physical environment were naturally the most appropriate order to deal with military operations. Technical as well as social developments led to accelerated interconnectivity between the three operational domains. Today, civil society and the military rely on Space as well as Cyberspace. Adversaries want to deny the use of Space-based capabilities and create operational and strategic effects in and through Cyberspace in order to deter and influence whilst remaining below the threshold of an armed conflict. Peer and near-peer opponents, who may not be capable of directly challenging NATO on a large scale and enduring conventional manoeuvre warfare, could achieve considerable effects through Cyberspace by denying the use of Space through kinetic and non-kinetic means. However, should a crisis escalate to armed conflict, where the will of an adversary to achieve its goals at any cost, then the availability of Space-based capabilities is vital for civil societies as well as for operations and combat in theatre.

New Operational Domains

Based primarily on technological developments and their social implications, – which all together make up 'the information age', NATO declared Cyberspace (2016) and Space (2019) as operational Domains, thus answering the developmental and technical challenges of warfighting in the 21st century. Closely linked to NATO's establishment of Cyberspace as a new operational Domain, Germany chose a complementary approach: the definition of the Cyber and Information Domain (CID). This was followed by the establishment of the German Cyber and Information Domain Service (CIDS) in 2017. The CID conceptually integrated the overlapping elements of Cyberspace, the Electromagnetic Environment and the cognitive layer of the information environment. The CIDS is a holistic approach to contributing to CID Operations in a Joint Operation and to provide CID capabilities as an enabler. CIDS ensures information security, provides IT-Services and ISR, as well as geospatial and environmental information. In accordance with a domain-centric perspective, the Bundeswehr located the space-based CID capabilities within the CIDS. Further, the distinction between the two domains does not depend on the physical location of the assets, but their primary military purposes from an operational point of view.

In broad outlines, this article investigates the developments that led to the revolutionary declaration of the two new operational domains, their common aspects and their relationship.

An Approach to Operational Domains

Nobody would deny the relevance of technical and social development in warfare or for use within military operations. For example, it was not just the invention of the aircraft and their military employment which turned Air into

an operational domain and to bring reason to the foundation of specific Air Forces. Just the aspect of operational relevance made the difference. It is the insight that a specific approach towards a 'sphere of activity' is promising to bring about a decision of operational relevance and raise it to an operational domain. The operational effects, which can be created in such a domain, are the ends that require specific ways and means. Ways and means have to match the specific circumstances of an operational Domain and require specific leadership. These are the essential elements that all operational domains have in common.

Although the face of warfare is constantly changing, the principles and the conduct of operations are quite constant. However, how are the new operational Domains distinct? The main aspect of the shared understanding of operational art and tactics is the need to apply capabilities in time and space to compel an adversary to the point of culmination. The three traditional domains are well understood by their physical nature. The ways and means to create the physical presence of troops and capabilities at a particular place have always been dependent upon the physical nature of Land, Sea and Air. Additionally, war, conflict and constant competition create complex and dynamic environments, which make information a relevant factor for decision making, command and control, as well as a means to affect the dynamics of the operational environment, e.g. by deception. Technological developments have had a significant influence on the classical domains, primarily through constant adaption in the relevant scale of time and space. Firepower, mobility and information have always been the main influential elements which create speed, precision and effectiveness in physical domains. This enables commanders to determine the where and when of decisive actions; however, to a certain degree, the confidentiality, integrity and availability of information have always been preconditions for military efficiency and effectiveness.

Space and the Cyber and Information Domains are Information Centric

The employment of Space technology and the developments in the Cyber and Information Domains are cross-correlated from an early stage. For CID, this applies not only to Cyberspace (and computing), but also to the Electromagnetic Environment and the Cognitive Layer of the Information Environment. The human need to communicate and to gather information have always been drivers for the development of Space technology and conversely the employment of Space technology fuelled the development of technologies which constituted the CID. Both domains were catalysts for military operations in the second half of the 20th century. Space and CID changed the significance of time and space without neutralising their relevance. However, Space support to operations by satellite communications, imagery intelligence and geospatial information allow early warning, the collection and processing of vast amounts of information (big data), Command and Control, navigation and finally, quick actions, in many cases regardless of distances and in far less time than without these technologies. These aspects are of increasing relevance and often represent core elements of the centres of gravity of warfare in the information age at the strategic and operational levels, namely the confidentiality, integrity and availability of information. Space and CID are information-centric and with the introduction of the Multi-Domain Operations approach, aiming to overcome Anti Access/Area Denial, underpin the mission-critical and decisive relevance of Space support to operations also at a tactical level. These insights, connected with a growing number of capable adversarial actors, make Space and the CID a congested and contested environment. The military use of Space is well known through the Russian anti-satellite missile test on 15 November 2021. It highlighted the vulnerability of satellites to interference. Space-based capabilities can be affected by exploiting elements of the Cyber- and Information Domain. This is commonly linked to the buzzwords hacking, jamming and spoofing. In other words, attacks to, from and within Space and CID are possible. It is clear that, the impending denial of Space sup-

port to operations would, at the very least, hinder every important element of operations and mark a total loss of crucial capabilities. Therefore, the availability and resilience of Space support to operations is a persistent need for military functions and capabilities. Furthermore, they are of utmost importance for deterrence at the political level. Adversaries operating in the grey zone could create a situation in which a loss of space-based capabilities sets the conditions for decisive military action on the ground. Interference with satellites can lead to debris, creating problems on a large scale for a longer period of time,which would affect civil societies in the aftermath. That said, NATO must be vigilant as actors may take that approach and hope for a strategic window of opportunity.

Information Technology-Dependent Operational Domains

The space race of the 21st century has just begun. Today information-centric equals technology dependent. Until the turn of the millennium, nation-states and militaries have been pioneers in technological development. This has changed. Increasingly, civil companies have been shaping the progress of modern information and Space technologies. For example, Apple's invention of the iPhone was revolutionary and brought CID and Space-dependent technology into one's hand[1]. Companies like SpaceX pushed Space technology forward and changed the whole technological environment. The development cycle in Space and Cyber domains is much faster than in classical domains. Still, at the same time, it affects the need for ongoing development and of established systems. The B-52 Stratofortress has been in service for about 70 years and will most likely experience a lifespan of a full century. Just its hull will be of that age and will have seen numerous reconditioning developments due to advances in technology.

However, the life cycles of IT are much shorter and faster, and the developments labelled New Space will also shorten the life cycle of Space technology. This leads to Space and CID as constantly evolving operational environ-

ments, both characterised by growing numbers of nodes and constant development of the functionality of those nodes and their connections. It is important to note that these connections are very often cross-domain connections between Space and CID. Nodes and connections also sprawl physically and significantly into the classical domains, thus changing their nature as operational environments. In conjunction with the dynamics and complexity of both Space and CID, shorter life cycles constitute an enormous challenge for military procurement. This also sets the condition for opportunities to create synergies and enhance flexibility and resilience. The term 'constant competition' in international relations and security politics is perhaps the most concrete and tangible description of this development. Realistically the modern space race will not be about winning, but will be about a leading group of a few nations, and the number of competitors is growing.

Unexpected Actors Entering the Stage

Although potent Space and CID capabilities need cutting-edge technology, a growing number of actors are playing a relevant role. This is primarily due to the necessary technology being generally available. Considering the potential strategic and operational benefits, CID and even Space technology is relatively cheap, compared to keeping capable ground, maritime and air forces ready. Not only global powers, but also emerging powers can afford Space technology, specifically for military purposes. Additionally, terrorist groups could target space-capabilities. Attacks on ground-based infrastructure, jamming, cyberattacks and other means are readily available. This has the potential to affect positioning, navigation and timing and other critical systems. Moreover, the risk of proliferation of anti-satellite weapons is much more likely, compared to weapons of mass destruction like nuclear weapons. The number of potential hacking, disinformation and propaganda actors is literally unlimited as nation-states, companies, terrorists and criminals seek to employ Cyberspace in favour of their own goals.

Conclusion

From a CID perspective, the reliance on space-based capabilities is as multifaceted as the means to deal with the diverse challenges. Political and military decision-makers are well aware of the relevance of Space and the criticality and the vulnerabilities of space-based capabilities must be understood. Space aspects must be considered from a holistic perspective by policymakers as well as from a military point of view requiring a whole government approach. NATO and its partners need a coordinated approach towards any actions regarding Space to ensure the continuous availability of space-based capabilities for civil societies and military use in peacetime and war. States need to identify an appropriate architectural approach to finding synergies between different Space systems in order to reduce costs, maximise benefits and enhance resilience. Additionally, there is an obvious need to develop responsive space capabilities.[2] Ultimately, the world community should aim toward creating an agreed space order, aiming at the peaceful use of Space and reducing security risks.

Major General Juergen Setzer is currently assigned as Vice Chief Cyber- and Information Domain Service and Chief Information Security Officer Bundeswehr. He is in charge of Space related aspects for the Cyber and Information Domain Service Headquarters. Major General Setzer started his career as an Infantry Officer and absolved the German as well as the US Command and General Staff Course. He held several posts as a Commander, also during operational deployments in Afghanistan.

Endnotes

1. For example: GPS, Satellite Imagery, Weather Forecasts.
2. Responsive Space is understood to be the ability to launch small satellites (up to 500 kg) on demand and on call into Low Earth Orbit (LEO = ant doe start operating within day, in order to reconstitute lost capabilities, augment existing – capabilities, fill unanticipated gaps in capabilities, and enhance survivability and deterrence (www.japcc.org/responsive-space-for-nato-operations).