HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 91–100.
DOI: 10.32567/hm.2019.3.8

Attila Horváth[1]

Countering the Counterspace – Doctrinal and Operational Aspects of Preserving Space Capabilities

Ellenállás a világűrben – az űrképességek megőrzésének doktrinális és műveleti aspektusai

This paper presents the outer space as a military operational domain, describes the various means an adversary could affect our space capabilities, and also our ways to protect them.

Keywords: space operations, counterspace

Ez a cikk bemutatja a világűrt, mint a katonai műveletek egyik színterét, leírja, milyen módszerekkel tudja a szembenálló fél befolyásolni az űrképességeinket, és egyúttal azt is, hogyan tudjuk megvédeni azokat.

Kulcsszavak: űrműveletek, űrtámadás

Introduction

Space is a military operational domain. That is not new, it has been since the 1960s, whether it was declared in doctrines or not. Since time immemorial, there were military and national security services which operated by wartime regimes even in peacetime. Counterespionage, strategic missile forces, national air defence and cyber are like that. And space also. Our space operators are safeguarding our own space assets, are searching for weaknesses in those of the enemy, and are, of course, developing solutions to exploit those weaknesses. The enemy does the very same.

[1] National University of Public Service Doctoral School of Military Sciences, PhD student, e-mail: horvatt@gmail.com, ORCID: https://orcid.org/0000-0001-9768-5357

Of course, with the advance of technology, the weapons and tactics change. The main focus of this article therefore is not those, but the analysis of the relevant US [1] and NATO [2] doctrines to clarify the strategic viewpoint regarding counterspace, anti-counterspace and counter-counterspace military activities.

In the context of this article, counterspace means actions taken to hinder one actor's space activities by another; anti-counterspace means actions taken to increase the resiliency of the one actor's space assets against counterspace operations, and counter-counterspace means active actions taken to prevent the use of enemy counterspace weapons or to minimise their effects when they strike.

It is important to remember that, just as space systems do not necessarily reside on orbit in outer space, the counterspace and counter-counterspace activities can be executed in all operational domains, be it space, land, air, sea or cyber. Likewise, offensive and defensive actions are defined by their outcome, not by their execution. It is entirely possible to mount an operation with an offensive execution to prevent the deployment of a counterspace asset, and this way the operation can be classified as defensive.

Components of Space Systems

Traditionally, space systems are subdivided into ground segment, link segment and space segment [1: I-2, I-3].

The ground segment resides on the surface of the Earth (including the lower atmosphere where aircraft operate), and typically contains the user terminals and the system operation facilities (tracking, telemetry and control stations, communication teleports and mass data downlink receivers). The terrestrial communication network connecting the space system to the end users can also be included in the ground segment, but just as well it can be considered a separated system which provides service for the users by enabling the data flow between the space system and the end user systems.

The space segment resides in outer space, and consists of the orbiting spacecraft (unmanned artificial satellites in the majority of cases today). The characteristics of these spacecraft define the services and capabilities offered by the space system.

The link segment connects the two other segments, and it is typically a radio (microwave) connection, or nowadays laser links are also used, especially in the uplink (ground to space) path. In space systems where more than one spacecraft is operated for the purpose of providing a service, intersatellite links can be used to connect the individual satellites to each other, without the use of ground stations. One of the most representative examples of intersatellite link usage is the architecture of the Iridium satellite telephone constellation, which uses microwave links to interconnect the spacecraft, but laser links can also be used this way. These intersatellite links, while residing in outer space, should be considered parts of the link segment, because of their vulnerability profile.

In a complex architecture of "system of systems" space capabilities, I recommend adding a fourth element to the mix, namely the service segment. The service segment (in contrast to the first three) is intangible, as it consists of the actual services provided by the end users, regardless of their physical or system-specific base. Emphasising the service segment is important because that is what the end users ultimately care for, and services also have a different and very specific vulnerability profile. Moreover, in many practical space systems, services of one space system are used as enablers of the operation of another one. Two easy to understand examples are the use of communication satellites as data relays between remote sensing satellites and ground control/downlink stations, and the use of positioning, navigation and timing services (such as the NAVSTAR GPS) in the tracking and time synchronisation of various space, link and ground segment elements. Therefore, the protection of such embedded services ultimately results in the protection of end-user services.

The service segment is different from the first three segments because it cannot be attacked directly, as all service degradation originates from attacks on any one of the first three. However, it can be protected directly, when the diversity of the space system portfolio allows for a successful attack on one space system or asset, because the service can be provided from a different source.

Attack Options and Vulnerability Profiles

The unique physical characteristics of outer space, the complex architecture of space systems and the various level of ambition of the adversary create a very diverse portfolio of attack options on space assets.

The military space operation which concerns itself with inflicting damage to the enemy's space assets is the Offensive Space Control, as defined by the relevant US doctrine [1: II-2]. The actions of the Offensive Space Control are:

- Deceive: deception injects information into the decision-making cycle of the enemy which is not true, out of context or gives rise to false interpretation. In itself it has no permanent damaging effects (however, the decisions made based on the deception, for example, orbital manoeuvres using valuable fuel, can have lasting negative effects).
- Disrupt: disruption lowers the level of operational quality of a system or a service, for a period of time, again without causing permanent damage.
- Deny: denial is disruption elevated to the next level, that is, the denied system becomes completely unavailable, its usefulness for the operator becomes zero. This action is also non-physical.
- Degrade: degradation lowers the level of operational quality of a system or a service, but this time the effects are long-lasting, even permanent. To cause such effects, physical damage might be required.
- Destroy: destruction removes permanently and completely the space system or service from the usable portfolio of the enemy. It is usually a physical action.

The means of attacks can be subdivided into kinetic, electronic warfare and cyber categories. Sometimes electronic warfare is considered a part of cyber operations, but for the context of this article, I treat them separately. The reason behind this is the inherent differences of the execution and outcome of the two approaches.

Kinetic attack against the ground segment is not different from any traditional military strike. The identified and selected ground segment components are subjected to land, aerial and seaborne fires, or overrun and captured by conventional or special operations forces. Because the ground segment components of space systems can be located very far from the area of actual military operations, the employment of special operations forces using infantry weapons (long-range, large calibre anti-material rifles, shoulder-launched antitank or bunker-buster missiles, small-calibre mortars) against the outdoor equipment, or providing target designation for aerial or long-range missile artillery bombardment can be surprising, very effective and limits collateral damage.

Kinetic attacks against the space segment can be achieved by co-orbital or direct-ascent anti-satellite effectors [3: xv].

Co-orbital assets are launched into orbit like any space vehicle, where they perform rendezvous and proximity operations to establish themselves near their target. From this position, effectively formation-flying with the target, they can observe it (providing valuable reconnaissance information and/or positive target identification), and then execute their attack by colliding onto the target, firing projectiles toward it or physically grabbing and reorienting it. This makes co-orbital weapons very dangerous: the operators of the target, even if they detect the forming-up of the attacker with their satellite (we should keep in mind that the attacker can reduce the optical, infrared and radar signature), cannot know the intentions of the weapon. Close inspection of a satellite, while it can be considered an unfriendly act, does not necessitate counteractions in itself, as long as the co-orbital weapon is not interfering directly with the operation of the satellite. The formation flying can be continued for hours, days, even weeks, and the weapon can visit several satellites, if it carries enough fuel to supply the necessary delta-v (the description of such an operation can be found in [3: 1–5, 1–6]). Therefore, while the operators of the target satellites can be aware of the threat in general, they cannot know when the actual strike will come, if ever. So co-orbital operations can be used to coerce the operator of the satellite to change orbit, therefore using up its own delta-v budget prematurely, which in itself can be counted as a mission kill in the long term.

Direct-ascent weapons are launched into a suborbital collision course towards their targets. They can carry conventional or nuclear explosive warheads, but the relative velocities of the interceptor and the target makes this unnecessary, as long as the interceptor, most often called kill vehicle, can actually strike the satellite. The kinetic energy released during the collision will do the job. The main difference between co-orbital and direct-ascent is the timeline of the attacks. As we have seen, co-orbital weapons take longer to reach their targets, but the actual destructive strike can be executed very fast; direct-ascent weapons finish the whole attack sequence faster, but the intention is known from the very beginning of the attack. Therefore, the satellite operator knows immediately what to expect, and can execute defensive manoeuvring, and the kill vehicle can only attack once. In addition to this, direct-ascent assets are destructive weapons with no other purpose. There is no time to collect intelligence, and positive target identification must occur before the actual interception.

Kinetic attacks executed with surgical precision against the antennas, amplifiers (or laser upbeam equipment) of the ground stations can be considered link segment kinetic attacks, but this is only playing with words. Such attacks have already been considered above.

On the other hand, the link segment is the very area for electronic warfare (and directed energy weapon) attacks. In this article I will not elaborate on interception, traffic analysis and exploitation of the electromagnetic radiation originating from the space systems, just the offensive jamming of them.

Both ends of the link segment can be subjected to jamming [1: II-15]. When operating against the receivers onboard the satellite, the action is called uplink jamming. This attack can be very effective against the traffic carried by communication satellites, but every satellite is vulnerable to control channel jamming. Uplink jamming is received by the satellite from anywhere within the receiver antenna beamwidth (the projection of which onto the surface of the Earth is called footprint). This way, if the antenna has a wide beamwidth, the satellite is very vulnerable, and the adversary is in a very advantageous position.

Such jammers can be installed onboard ships or (theoretically) aircraft, which can operate from international waters or airspace, therefore attribution of the attack is even more difficult. Moreover, jamming does not have a lasting effect, it does not cause any permanent harm, can be applied and turned off instantly, so it can be applied when it is necessary within the operational timeline, and leaves no recoverable evidence.

Uplink jammers can theoretically be installed onboard co-orbital anti-satellite space vehicles. Such application would be very surprising to the victim, and as the jamming signal would arrive from much closer that the user signals, even a very limited power jammer would be effective.

A special case of uplink jamming is executed against the sensors of remote sensing satellites. This will be detailed below, together with directed energy weapons.

Downlink jamming is executed against the terrestrial end of the link. It is especially effective against satellite navigation receivers, and communication ground terminals with omnidirectional antennas. In these scenarios, small power (therefore, small size) jammers can be effective, because of the limited power of the user signal and the receiver antenna cannot discriminate between the user signal and the jamming signal. Such jammers can even be deployed from aircraft or artillery rockets.

The drawback of downlink jamming is the necessity of line-of-sight between the jammer and the jammed equipment, therefore, the limited operational range. However, this also makes it possible to tailor the jamming to the operational area. Such limited range can be overcome via numbers, with the deployment of a large number of jammers. An example of this is the prepared area defence against satellite navigation based precision-guided munitions or drones [4].

Electromagnetic energy can be used against the sensors of remote sensing satellites. Such energy, depending on the power level, can be used to temporarily disable the sensor or distort the recorded data, in which case it is usually called dazzling (this expression is usually used in relation to optical sensors, but the mechanics of a microwave beam directed against a radar or ELINT/MASINT satellite are no different)

[3: 1–18]; or can cause permanent damage, in which case we are talking about directed energy attack. It is important to repeat that the only difference between dazzling and directed energy attack is the power level. Therefore, a dazzling can readily be a strategic warning or a means of coercing, by the implication of a much more serious, damaging attack. Moreover, directed energy weapons with a level of power in the destructive range can also be utilised against other types (like communications) satellites, not just against recon ones.

Theoretically, nuclear electromagnetic pulse effects (also known as high-altitude electromagnetic pulse, or HEMP) can be used against space systems. Such attacks are, however, by their very nature, indiscriminate and it is practically impossible to target a specific adversary. Moreover, most military space vehicles are hardened against electromagnetic pulse effects. On the other hand, such attacks would be very destructive to the civilian space (and terrestrial) infrastructure, therefore they can be considered as counter value operations initiated to damage the enemy society as a whole.

Just as with kinetic attacks, cyberattacks against space systems are not fundamentally different from similar attacks against any other type of computer systems [3: 7–1]. As the onboard networks and computers of satellites are pretty much isolated from any other computer system, the only link being the tracking, telemetry and control system, they can be very well protected against cyber operations. But if this separation can be overcome by some means, the attacker can access the onboard systems and, lacking protection in depth, can freely wreak havoc. Therefore, the separation must not be the only protection, the other best practices of the cyber industry must be applied to satellite onboard systems, as well. Cyberattacks can have any level of effect listed above, and just in the case of dazzling, a carefully limited strike can be a precursor or warning of another one with much sever consequences.

Cyberattacks are well suited to disable services without inflicting any harm to the actual components of the space system. For example, disabling the terrestrial network used to disseminate the raw sensor data to the analyst has the same tactical consequence as blowing the satellite up. Therefore, it is better to have a holistic approach regarding cyber security which covers all levels and subsystems of one's information infrastructure, instead of focusing on single assets and treating them as islands. Just as with real-life island groups, even if the single land masses are left unharmed, blockading the sea and air lines of communications between them will hurt the group as a whole.

Protection of Space Assets and Service Assurance

Naturally, the doctrines which define counterspace actions also define the means to preserve and protect space systems and services [2: 5–7]. We can classify these means as [1: II-3]:

- active defensive actions taken to reduce the effectivity of enemy offensive systems by taking actions against them,

- reactive actions taken upon the realisation of an imminent or ongoing enemy attack,
- and passive protective actions which are included in the design and operation of space systems, and are aiming to reduce the effectiveness of any future attacks,
- finally, deterrent actions [1: I-9] which discourage the potential enemy from even considering any attack.

The active defensive actions are similar to their offensive counterparts, but as their targets are the attack capabilities of the adversary, their outcome is defensive from our point of view.

The last category can build upon the first three, because the adversary can be persuaded that a successful attack is simply not possible within their technological means and/or political will. Therefore, they are better to leave the space systems alone, as their attack simply cannot be successful. However, deterrence can be achieved via proof-positive attack attribution and the demonstration of military means and political will to act against any adversary following an attack on our space systems. This assured post-attack strike makes the enemy realise that the advantage of an attack on our space capabilities will be nullified by the consequences of our counterstrike.

More attention needs to be focused, however, on the second and third categories. The reactive actions are initiated when Space Situational Awareness, Satellite Operations or service system operations activities signal that an attack is under way (or, preferably, is being initiated). After the characterisation of the strike, Satellite Operations or the service system operation must react without delay, and execute some kind of manoeuvre to counter the attack. Depending on the attack, the manoeuvre can be, for example:

- orbital, to counter a direct-ascent or co-orbital kill vehicle,
- frequency or transmit power adjustment, to counter a downlink jamming,
- antenna radiation pattern modification, to counter an uplink jamming (or downlink jamming, if the technology permits it).

All the possibilities of manoeuvre should be identified based on the architecture of the actual systems, and operational procedures should be developed for them.

Regardless of the potential of the aforementioned three categories, the most important, in my opinion, are the passive protective measures, built into the systems during their design and maintained during operations. They enable the manoeuvres and support the deterrence, therefore they are essential for the preservation of the space capabilities. Moreover, these measures readily offer protection against natural and unintentional man-made threats.

The US doctrine, on which this part is largely based, classifies reconstitution as an active, follow-up action to the actual attack [1: I-8]. In my opinion, however, reconstitution must be planned in advance, preferably during system design, and the means of reconstitution must be readied well before the attack. Reconstitution means the activities taken after the loss or degradation of a space system or service, to restore the services themselves, not necessarily the actual systems. For example, the loss of a SATCOM asset can be followed up by the activation of a service contract with a different service provider, utilising a different satellite. This way, from the user perspective, the loss is mitigated or even eliminated, if the newly activated service can replace the lost one entirely.

The US doctrine considers resilience [1: I-8] the designed and built-in approach to ensure the continuation of space systems and services in the face of an attack. According to the doctrine, resilience can be achieved via:

- Disaggregation, that is, the careful assignment of different services to different assets. As the name implies, it is the opposite of aggregation, and this way the systemic approach can easily be understood. Focus the assets to a limited set of services, and deploy a combination of them to enable the required level and spectrum of space support to the forces. For example, the combined weather-and-SATCOM satellites of the early stages of the INSAT program of India were designed with aggregation in mind (to save on satellite buses and launches), and when later they decided to deploy specialised, separated communication and weather satellites, they executed disaggregation.
- Distribution, that is, the elimination of single points of failure (from the service point of view), by deploying independent, but interrelated groups of assets to realise any given task. So, the disaggregated space systems become even more fragmented, as more than one satellite is used to support a mission. Distribution is not the same as proliferation (see later), because in a distributed system the components work together, not simply next to each other. A distributed system is capable of "graceful degradation", when the loss of one or more system elements, while undoubtedly has some negative effects on the service quality, does not make the system completely unusable. There exists, however, a critical point, when enough of the elements is taken out of service, and consequently the system as a whole ceases to operate. It takes a lot more effort to achieve this (from the adversary's point of view), than it would take against a system which is concentrated.
- Diversification, that is, the use of different systems to provide a similar service to the users. This way, the user is (ideally) not concerned with, or (realistically) is prepared to switch between, the systems that operate to support their mission. When one system is completely taken out of operation, another one takes over with minimal outage, and the mission can go on.
- Protection, that is, to build and deploy components and systems which are capable of continuing their operation even in a hostile or adverse environment. The threats protection required against are identified during the design phase and appropriate countermeasures are added to the system. This means that a protected, hardened satellite is generally heavier than a non-protected satellite with similar capabilities. Electromagnetic shielding, ballistic armour and extra delta-v budget are expensive in weight.
- Proliferation, as mentioned earlier, means the deployment of a large(er) number of system elements than required for normal operation. A commercial SATCOM satellite operator can successfully operate with a single satellite anchored to a single teleport. For a military operator, this approach is risky.

By proliferating the teleports, the job of the attacker becomes harder, as any one of the teleports can support the missions, therefore, all of them must be taken out. This is the main difference between proliferation and distribution. In a distributed system, the workload is shared among the system elements, but there is no individual element which can carry all the load. In a proliferated system, any element can carry the minimum required workload, and by adding extra elements, we achieve resiliency and at the same time, extra capacity within the system. During an attack, this extra capacity will be lost, but as long as a single element is operational, the minimum requirement is met.

- Deception, that is, the hiding of the full capability spectrum of a space system from the adversary, is the final element of resilience. During peacetime operations, the full capabilities are not utilised. A part of them are kept in reserve, and no indication is given about their existence. In an ISR system, this can be the resolution, when the peacetime data is not as well-detailed as the full physical resolution of the sensor. In SATCOM, this can be output power or bandwidth, or even waveforms.

Conclusions

In this article I summarised the doctrinal basis of counterspace operations, and at the same time, the basis for the protection, preservation, and if all else fails, the restoration of space capabilities. This topic is getting all the more important. If we look at the dynamics, India tests an anti-satellite weapon system, while at the same time NATO is working on their space policy, and the US is planning to create a new branch of their armed forces, the space force. This also shows that outer space is not losing its traditional importance in military operations.

Added to this are the proliferation of space technology, space systems and services, and also the proliferation of counterspace (including counter service) and dual-use solutions. The outcome is that we need to concentrate on the hardening and protection of our own space assets. This is only possible if at the same time we ourselves also study those counterspace activities, not necessarily to use them, but at least to get to know our enemies.

The basics of a successful and credible space capability are space situational awareness and satellite operations. Connected to those are the credible deterrence (to warn off any adversaries) and restoration capabilities, to assure the adversary that their efforts would be in vain. Nations with smaller economies and space programs can acquire these via alliances, and this way even they could be meaningful contributors to collective defence efforts.

References

[1] *Space Operations.* US Department of Defense Joint Publication, pp. 3–14, 2018.

[2] *Allied Joint Doctrine for Air and Space Operations Edition B Version 1.* NATO Allied Joint Publication 3.3, 2016.

[3] B. Weeden, V. Samson, Eds., *Global Counterspace Capabilities: An Open Source Assessment.* Washington, D.C.: Secure World Foundation, 2019. [online] Available: https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf [Accessed May 5, 2019].

[4] R. Beckhusen, *Russia Plans to Turn Cell Phone Towers Into Cruise Missile Jammers,* 2016. [online] Available: https://nationalinterest.org/blog/the-buzz/russia-plans-turn-cell-phone-towers-cruise-missile-jammers-18067 [Accessed May 5, 2019].