András Edl[1]

Deterrence in Space

DOI 10.17047/Hadtud.2022.32.E.256

The recent increase in space activity brought space security considerations more to the forefront. As the chances of conflict in space are growing, scientific research aims at finding the possibly most effective tools to avoid or to win conflicts in this new domain.
However, equipment deployed in space, in case it is destroyed, is hard to replace and due to the generated debris field, it can also endanger the capabilities of the attacker. Therefore, many experts consider deterrence as one of the most effective methods and try to adjust it for the space domain. However, there is a fundamental difference between the Western and the Russian or Chinese concepts of this strategy. For the latter, coercion is an acceptable and logical part of deterrence.
Keywords: space, deterrence, coercion, United States, China, Russia

Elrettentés a világűrben

Az űrtevékenység közelmúltbeli növekedése az űrbiztonsági megfontolásokat még inkább előtérbe helyezte. Mivel az űrbeli konfliktusok esélye egyre nő, a tudományos kutatás célja, hogy megtalálják a lehető leghatékonyabb eszközöket a konfliktusok elkerülésére vagy megnyerésére ezen az új területen. Az űrben telepített berendezések azonban - amennyiben megsemmisülnek - nehezen pótolhatók, és a keletkező törmelékmező miatt a támadó képességeit is veszélyeztethetik. Ezért sok szakértő az elrettentést tekinti az egyik leghatékonyabb módszernek, és megpróbálja azt világűrhöz igazítani. E stratégia nyugati, illetve orosz vagy kínai koncepciója között azonban alapvető különbség van. Az utóbbiak számára a kényszerítés az elrettentés elfogadható és logikus része.
Kulcsszavak: világűr, elrettentés, kényszerítés, Egyesült Államok, Kína, Oroszország

Introduction

The growing interest in deterrence has its origins in a seemingly obvious fact. The chance for an actual attack has to be possible so people will think about how to make sure this attack does not happen. Italy does not need to worry about deterring an attack from Thailand because there is no chance or reason for it to unfold in the current geopolitical situation. The reason for strategists revisiting the idea of deterrence (mainly rooted in the nuclear opposition during the Cold War) is that there is a real chance for an attack against space assets. Technological developments of recent years and the increasingly assertive behavior of potential rivals made it clear that space is not a 'sanctuary' anymore, as it was assumed by the U.S. for many years. Deployed equipment is no longer safe from harm and must be protected from potential adversaries.

The United States is still the leading space power in 2021, both in quantity and quality. Based on the database of the Union of Concerned Scientists, the number of active satellites on the 1st of September 2021 was 4 450. Most of them (3 390) were in LEO orbits, and the U.S. owned 2 788 of them. Out of these, the commercial sector owned 2 359, the rest was divided between government, military and civilian users. The increase was dramatic thanks to the construction of satellite constellations like Starlink.[2] But other spacefaring nations make great efforts to improve their space activities and this can make orbits more congested and contested. These nations all noticed the need to protect their space assets and they see a benefit in developing offensive capabilities, especially when they might get into a conflict with the United States. The U.S. is not only the most advanced but also the most reliant on

[1] *University of Public Service, EJRC Institute of Space Law and Policy; Doctoral School of Military Sciences*; e-mail: edlandras@gmail.com; ORCID: 0000-0002-4250-7112
[2] Union of Concerned Scientists 2021.

space, which makes those assets a logical target. Several countries present a real threat to U.S. space capabilities, although not at the same levels.

The main contender is China. In 2007, a kinetic anti-satellite weapon test was carried out by the Asian country, which caused an international uproar due to the generated debris field. Ever since that China made sure not to create additional debris, yet it kept developing kinetic ASAT weapons, jammers, cyber capabilities, lasers and other offensive methods. Russia tested a kinetic ASAT weapon in late 2021, but it also experiments with ground-based lasers, GPS jammers and satellites able to manoeuver in orbit. Way behind these two major space powers comes Iran and North Korea.[3] Nevertheless, they are not the only countries with an increased interest in space security. India is a good example of an emerging space power, with kinetic ASAT capabilities as proven by a 2019 weapons test. Even if a country does not aim to develop kinetic ASAT weapons, they wish to protect their space assets with other means, and one of them could be deterrence.

Different approaches to deterrence

Deterrence in Western strategic thinking, mainly dominated by the U.S. and NATO, is a form of prevention. The main idea is to stop an opponent from taking some kind of unwelcomed action. To achieve this goal, deterrence can be divided into two subcategories: deterrence by punishment and deterrence by denial. The former means making a threat that the defender – even after a successful attack – will be able to retaliate and cause damage, and this damage is more serious than the attacker would like to pay as a cost for their actions. Deterrence by denial on the other hand tries to convince the potential attacker that their aims are out of reach. Even if they commence an attack, it would be insufficient. Both types of deterrence can be achieved with an adequate show of force. The whole concept rests on the rationality and the cost-benefit calculus of the two actors. However, as Michael Rühle also pointed out, there are known examples (such as the 1973 Arab-Israeli war or the 1982 Falklands War) of a superior military being attacked by weaker opponents due to various other factors in their decision-making. Potential adversaries might take risks way above the seemingly rational limits because of internal political reasons, emotions, fear of losing power, etc.[4]

Denial is the most effective when a defender knows what kind of attack to expect, and for punishment to work, the side carrying out the counter-attack must know who was the attacker and which one of their assets could be attacked. In both cases, having the correct information is vital. Western deterrence theory usually uses three critical pillars. These must be met otherwise deterrence will fail.

1. Capability: An actor must have the power to do what it says in its threats.
2. Credibility: The opponent must believe that the threat is credible, so that state has the capability and the will to carry out the threat.
3. Communication: this is how the image of capability and credibility will arise in the mind of the opponent. This might be the most difficult part of deterrence. As it was known already at the creation of deterrence strategy, countries might bluff, or make their serious intentions public but they might not be believed, etc. It can get even more complicated if one country tries to expand their deterrence umbrella, and protect allies. The adversary might believe that they will not risk an escalation because of a third country.[5]

[3] Defense Intelligence Agency 2019.
[4] Rühle 2015.
[5] Schelling 2008, 35.

The problem with deterrence is that it is very difficult to determine to what degree the deterrence strategy is effective when nothing happens.[6] Al Mauoruni notes that deterrence should not be regarded as a tool, which might give some extra time to the own forces to prepare, but truly as an ongoing multi-domain preparation. Of course, an adversary might be determined to carry out an attack anyway, because their political goals can be achieved even in case of a stalemate or a defeat.[7]

Achieving political goals can be done in multiple ways. How Chinese strategic thinking approached the problem of deterrence shows that the focus is more on the goals instead of the way to get there. The main difference between the Chinese and the Western interpretation of deterrence is that the Chinese term (*wēishè*) also encompasses compelling an enemy.[8] Deterrence is a threat of force to keep the status quo. Compellence is the actual use of force to make an adversary change its behavior. Based on this concept there is no surprise that Chinese sources make a distinction between offensive and defensive deterrence strategies, and at the same time, they regard them as strongly interconnected. In conclusion, *wēishè* is closer to coercion than the Western idea of stopping an enemy from trying something. For China to reach the desired goal using economic, diplomatic, or cultural assets is just as valid as using military force. Deterrence is a multi-domain activity.[9] In military terms, Chinese strategic thinking knows the concept of "deterrence campaigns" and "warfighting campaigns" and these can be both nuclear and conventional.[10] The three core concepts of Chinese deterrence are Capability, Resolve and Communication. It is important to add that capability does not only mean military force but also the overall capability of a nation. Territory, population, economic power, science and technology levelsalso adds to deterrence power. In addition, deterrence is applied in various ways in three possible escalation stages. The Chinese strategists distinguish peacetime, crisis and wartime. Deterrence would also play an important role when a war starts, and China needs to make sure that other actors do not try to use the war to their advantage in other regions.[11]

The Russian concept of deterrence is expressed in the 'strategic deterrence' expression (*strategicheskoe sderzhivanie*). It is also connected to 'hybrid warfare doctrine'.[12] Sometimes it is translated as cross-domain coercion by Western analysts to highlight the differences. Just like the Chinese variant of deterrence, it also lays a great emphasis on cross- or multi-domain operations. Economic, diplomatic, and intelligence maneuvers are also part of the tools they could use to reach their goals. Furthermore, Russian strategists regard coercion and intimidation also as a part of deterrence and limited scope conventional military strikes are still a viable option to change the course of action of the enemy. The lines between defense and offence are blurred, and so is the Western distinction of peace and war not fully applicable in Russian strategic thinking. One key concept is struggle (*bor'ba/protivoborstvo*), which refers to strategic interaction in its totality and has a long-term perspective at its core. An ongoing, never-ending struggle, which only varies in intensity, but not in meaning itself.[13]

[6] Stocker 2017.
[7] Maoruni 2019.
[8] 威慑 *wēishè*
[9] Cheng 2020, 178.
[10] Scouras et al. 2017, 16–17.
[11] Beauchamp-Mustafaga et al. 2021, 20–23.
[12] Ven Bruusgaard 2016, 7–26.
[13] Adamsky 2020, 172.

Space deterrence

As can be expected the general ideas and guidelines of deterrence are also present in a narrower, specific field of space deterrence. Space based capabilities take part in general deterrence. For example, reconnaissance satellites could detect enemy troop movements and make large-scale surprise attacks nearly impossible; hence, the chance for success decreases. Nevertheless, deterrence is also important when it comes to protecting the very same space assets. However, space also has unique features mostly due to the physical attributes of space. These laws of physics will define how to access, move in it, and what is possible on the current technological level. At this point, there are numerous unknown factors. Rapid development and expansion in previously inaccessible regions further increase uncertainty.

Various researchers and organizations approach space deterrence from a different angle. Sometimes even the basic guidelines and rules are unclear, partly because there was never a conflict in space until this day. However, exactly for this reason, the current debate is very thought provoking and offers interesting concepts. As a contribution to this exchange of ideas, Bleddyn E. Bowen suggests that there are five key points to observe:

1. Space deterrence is closely attached to deterrence in general and thus it is also an extension of politics and strategy on Earth. Therefore, the methods to achieve a certain goal might be connected to space, or applied in space, but not necessarily confined to the space domain.
2. Space is still strongly connected to nuclear deterrence, due to the early warning systems. Some of these systems like the American Space-Based Infrared System (SBIRS) can also provide tactical information. As a consequence, any effort from a rival to disrupt the system – because they wish to conceal a tactical move – might be misinterpreted by the American side and taken as an attempt to damage the nuclear early warning infrastructure.
3. The loss of space equipment does not mean a direct loss of life, so emotional reactions are low in comparison to losing an aircraft or a ship when people on board will be injured or die.
4. The fragility and the necessity of space infrastructure might bring leaders to escalate the situation, therefore a large-scale attack on a space asset of any nation is to be avoided by the opposing side, even more so when they are dependent on space.
5. The most likely type of attack is solitary action against specific key equipment, which could enable the attacker to neutralize a few space assets for a short period. In the meantime, they could create a new situation on the surface of Earth.[14]

Although space deterrence is still connected to nuclear deterrence, there is mostly a consensus that the usage of nuclear weapons in space warfare should be avoided. The attack carried out by an adversary would rather fall into the conventional category. There might be significant collateral damage when using kinetic weapons, but still not such immense damage as by a nuclear strike. At the same time, developing and deploying a strong space infrastructure that is able to destroy objects in space will also enhance the ability of a nation to defend against nuclear attacks. This is because nuclear power and therefore nuclear deterrence mainly is based on intercontinental ballistic missiles.[15]

Furthermore, among most scholars, there is an idea, that a space conflict could be very quick. This brings its own set of problems with it because as Mearsheimer writes in one of his books if an enemy has the impression that a Blitzkrieg of some form is possible, deterrence is

[14] Bowen 2018.
[15] Lefebvre 2017, 136–139.

likely to fail.[16] In the current information era, speed and controlling information is even more important, so a 'space blitzkrieg' might be quick but even more devastating. How to counter such a threat and breakdown of space systems is a major concern for strategic planners. One of the most frequently offered solution is resilience.

The common interpretation of resilience is that space systems should be so flexible that even a large-scale attack could not decrease space capabilities below an acceptable level. One method could be to make a large number of satellite constellations (numbers rising into thousands), that even losing hundreds of satellites would not be a real setback. Another method would be to use commercial tools or the equipment of allies who are not affected by the conflict. The third solution would be (and this could even be very useful at times of major solar outbursts, etc.) to have systems in place which could function even when all space assets are lost. From this perspective, the less advanced societies would be the most resilient. Such seemingly redundant and obsolete communication methods as messenger pigeons could be very useful under extraordinary circumstances. This is the reason why the French and the Chinese military forces still have some pigeons at their disposal.[17]

The example of the United States

Naturally, as approaches to deterrence in general differ, so do space deterrence concepts. These also reflect themselves in the organizational structures and doctrines of space powers. In the case of the U.S., the four major organizations are the Space Force, the Space Command, the Space Development Agency, and the National Reconnaissance Office (NRO). The main task of the Space Development Agency is to oversee the creation of a multi-layered network-based satellite constellation, called the National Defense Space Architecture.[18] The NRO still has control over the most intelligence satellites.

The Space Force got considerable attention in recent years. The establishment of the Strategic Support Force in China, and the Russian Aerospace Forces in Russia (both in 2015) helped to tip the balance in the debate about the Space Force, and the U.S. recognized space as a warfighting domain. In 2021, Space Force was responsible for about half of the U.S. military launches and satellites. The budget is likely to increase in the coming years. The Biden administration asks for a budget of 17.4 billion USD for the year 2022, which is a 2 billion USD increase compared to 2021. The extra amount should be dedicated to counter advances in Chinese and Russian ASAT capabilities. The Space Force acquisition system is still in flux, no certain structures have been established yet. Smaller companies hope for a chance to supply the new organization. The same goes for the SDA which is a small organization therefore reliant on private industry. The desired quick and lean acquisition structure is not in place yet, so replacing lost equipment in a reasonably short time is still not a viable option.

Research and development are nevertheless on their way. Examples of major projects include the GPS III system, which offers greater protection against jamming, or the Next-Generation Overhead Persistent Infrared system that will replace the Space Based Infrared System (SBIRS). The Space Force also awarded Lockheed Martin with 4.9 billion USD for three Next-Generation Overhead Persistent Infrared satellites and ground mission software in January 2021. There is also some news about the classified USA-299 unmanned vertical takeoff spaceplane.[19] While developing new technologies and equipment, there were attempts

[16] Mearsheimer 1983, 203–204.
[17] Lefebvre 2017, 207–210.
[18] According to official statements, in late 2022 the SDA will become part of the Space Force
[19] Course 2021.

to offer solutions to the space vulnerability on both the doctrinal and tactical level. In 2015, the U.S. founded the Joint Interagency Combined Space Operations Center (JICSpOC). Its task was to analyze data, conduct wargames and enhance information sharing between space operation stakeholders.[20] This organization was later renamed to National Space Defense Center and is now operating under the U.S. Space Command.

Evaluating U.S. developments in 2019, Lambakis came to the conclusion that the U.S. space deterrence strategy is based on denial. He also claimed that due to the fast development in China, this w be enough, the punishment element must be strengthened and for that, the U.S. must be able to carry out offensive operations. The new capabilities of China might be enough to deter the U.S. or severely decrease its operative efficiency.[21] As it seems decision makers in the U.S. still mainly focus on denial in space deterrence.

The U.S. dependence on its space assets might give ample motivation for China and Russia to attack the space capabilities, even if they must endure similar losses in consequence. In some situations, they would not even need space capabilities. For example, during a conflict close to Taiwan, due to geographical factors, the People's Republic of China could rely on their ground-based radars, while the U.S. would need to heavily rely on space to conduct an effective military operation.[22]

Cyberattacks and attribution - unique challenges in space

Deterrence is mainly about perception and the image built about the rivals in the minds of the decision makers. As Robert Jervis discussed in his works, these images can fail on multiple levels and make deterrence ineffective. This can lead to surprise attacks when one side incorrectly believes that they have deterred the adversaries and yet they commence an attack. It is also possible to fall into a trap of self-deterrence, when actors may see something that is not there, so they will be deterred by their own imagination.[23] There are clear signs that rationality is much less in charge of decision-making than people like to assume. All kinds of cognitive errors, the lack of information, self-deception, etc. influence the image of the adversary and the possible best course of action.[24] Getting the right information can mitigate some of these problems, but not eliminate them.

Attribution means that an actor can identify the source of the attack. Without this, deterrence by punishment can hardly work, for there would be nobody to punish after an attack and they could avoid the consequences. This can be challenging in the new space environment. A kinetic attack aimed at a satellite is comparably easy to identify, especially if the launch itself is detected. However, directed energy weapons, jamming, spoofing or cyberattacks can become increasingly difficult to attribute, or might take a considerable time. In fact, it can take so long that the whole conflict could be over before the results are seen. Due to their covert nature and low collateral damage cyberattacks usually do not stir up public reactions as much as a very visible kinetic attack. The reaction of cyberattack victims is usually also rather reserved. By some key cyber infrastructure elements, the resolve to defend them, as well as the available capacities can function as a deterrent, but in contrast low and medium value targets might be subject to more attacks, because the defender knows they are under a retaliation threshold, and they operate in a grey zone.[25] Therefore, it would be a

[20] Dawson 2018, 160.
[21] Lambakis 2019, 497–553.
[22] Dawson 2018, 157–159.
[23] Jervis 2017, 201–204.
[24] Jervis 2017, 205–214.
[25] Lindsay 2015, 53–67.

mistake to assume that the detected cyberattacks are the full extent of the capabilities of the adversary. In a full-scale conflict, key space systems might also be attacked because the stakes would be so high (i.e. winning or losing the conflict) that the attacker will not be too concerned about a possible attribution. Derek Tournear, the director of the Space Development Agency recently stated that attacks in the cyber domain are the most dangerous to satellites because a well-executed cyberattack could take out multiple satellites or even whole constellations. The other great danger he highlighted was the vulnerability of the supply chains, which similarly to IT infrastructures, could break down even if only attacked at a few key points.[26] In addition, applying pressure on the supply chains can be a tool of coercion or deterrence via economic means. It could slow down or stop the replacement and production of any space equipment. Hackers could shut down satellites, permanently damage them (like the 1998 case of the ROSAT X-Ray satellite), hold them hostage or take control of them.[27] The required resources to have a capable cyber unit to carry out operations affecting space is not that high. As chemical weapons were once called the poor man's atomic bomb, cyber units operating in the space domain could be called the poor man's ASAT weapon.

Attribution might be easier in case of other types of attacks, but they also need a sophisticated capability deployed. The tracking and identification of objects in space are part of space situational awareness (SSA). All major space actors lay great emphasis on the improvement of their SSA systems. The United States in March 2020 finished building a new, more advanced space radar, called Space Fence on the Marshall Islands. It can track marble-sized objects, mainly in low Earth orbit and is maintained by the 20th Space Control Squadron of the U.S. Space Force. The new base will work in conjunction with the earlier Space Surveillance Network, increasing the number of tracked objects while decreasing the size of detectable objects. This will also prove valuable in space debris detection.[28]

According to the Missile Defense Agency, the newly constructed Long-Range Discrimination Radar (LRDR) in Alaska is operated by the Space Force and it is part of the Ground-Based Midcourse Defense (GMD), a crucial part of the missile defense system. The main purpose was to aid the ballistic missile defense components of the armed forces, but it can also bolster the space situational awareness (SSA) of the United States. The new base is operated by 150 personnel and cost around 1,5 billion USD. After some testing and required software updates scheduled to end in 2023, it will be able to detect hypersonic missiles and track small, baseball-sized objects in space.[29] Lt. Gen. A.C. Roper, deputy commander of the U.S. Northern Command emphasized in an interview that this base will help the U.S. to shift from a "deterrence by punishment" stance to the "deterrence by denial" stance and convince the rivals that there is a high chance that their attack might not succeed.[30]

Although ground-based capabilities are still the most important in SSA, in-orbit satellites providing video surveillance are becoming more and more popular. Their biggest advantage is cost and proximity to other space objects. The weather or other aerial phenomena will not disturb the sensors, and they are comparatively cheap. Satellites using video surveillance are not that new, in 2014 the Chinese deployed the Tiantuo-2 satellite. Other examples are the Skysat-1 and 2.[31]

Naturally, the U.S. is not the only country that makes considerable effort to build up its space situation awareness infrastructure. There are bases all around the world completing this

[26] Erwin 2021.
[27] Akoto 2020.
[28] Erwin 2020.
[29] Rhode 2021.
[30] Lopez 2021.
[31] Zhang et al. 2017, 1–9.

mission. One example is the Chinese SSA base in Argentina, which stirred debates in the country and also raised concerns in Washington. The base is in a perfect position to observe American satellites covering the eastern regions of the U.S.[32] Ships in international waters can also provide SSA data for China.

At the same time, there is an emerging trend that could make SSA and attribution more difficult, and by its nature decrease trust and transparency between space actors. The build-up of a more sophisticated and capable space situational awareness infrastructure belongs to detection, but different actors also invest in countering these capabilities. One example is the research carried out at Nanjing University of Aeronautics and Astronautics (NUAA). The aim is to develop a composite coating that would make satellites – especially already hard to detect small satellites – much harder to track for adversaries.[33] The idea is nothing new, declassified documents show that the United States already tried to deploy stealth satellites as part of the CIA's Misty program. These satellites had an inflatable coating that would help to mask the laser, radar, visible or infrared signatures of satellites. One of them, the USA-53, was carried to orbit during the 36th space shuttle mission (STS-36) in 1990. By their orbital deployment, staged malfunctions or accidents might have been used to cover the real importance of a mission. The program had several critiques due to its inflated budget, yet it still continued for many years.[34]

The problem of escalation and the echo of the Cold War

Because we are highly dependent on space, any attack in this domain would greatly heighten the chance for escalation. This is well known to possible adversaries as well, therefore attacks would be evaluated as an initial phase of a war.[35]

The driving power behind the Cold War rocket development was the need for reliable methods to deliver nuclear warheads to their targets. Parallel to this the number of nuclear weapons increased, the United States lost its nuclear monopoly and there was a possibility that in a conflict such weapons would be used with a devastating effect, or even destroy the entire human race. This threat had to be dealt with and strategists in the West came up with the strategy of Mutually Assured Destruction. The whole idea rested on the notion that the two sides cannot trust each other, so they have to rely on the opponent's will to survive. Even if the Soviets would opt for a nuclear attack, they must know that the U.S. will be able to retaliate and still destroy the Soviet Union.

Early military satellites were partly early-warning satellites with the task to detect enemy launches and give enough time to implement defensive measures or to initiate a counterstrike. Therefore, any attack against space systems could have been considered as an initial phase of a nuclear war. This led to not harming these systems, because both sides wanted to avoid any kind of misunderstanding. However, as space systems and nuclear weapons were developing, more refined strategies were required to manage the complexity. One of the leading theoreticians was Hermann Kahn, who created an Escalation Ladder, as a guide to decision makers, so they could evaluate a conflicts intensity and current stage.

This escalation ladder has 44 stages. One of the advantages of this system is that it encompasses all kinds of diplomatic and economic actions, not just actual military measures. The model was influential during the Cold War and because it was strongly connected to

[32] Vogrincic 2020.
[33] Chen 2021.
[34] David 2005.
[35] Smith 2018.

nuclear deterrence. It comes as no surprise that his theories were an inspiration to current Western strategists and some of them try to use a modified ladder for space deterrence. One such "space ladder" is the 18-level model by Szymanski, presenting a gradual system of escalation and deterrence including pre-conflict and post-conflict phases.[36]

Of course, for U.S. strategists China is the center of attention. After evaluating Chinese sources and past behavior, RAND suggests using a six-point scale as a starting tool to interpret the Chinese actions and figure out how dedicated they are. The six points are:

1. Official protest and/or warning above the level of the Foreign and/or Defense Minister?
2. Messages through trusted intermediaries?
3. Multiple occasions of nonmilitary signaling, like economic coercion?
4. Military redeployments or mobilization close to the problematic area?
5. Are military exercises close to the problematic area?
6. Any previous military tests relevant to the scenario?[37]

In space, the Chinese sources outline four different steps for deterrence, they can be taken at any order in any time, and they do not represent a strict step-by-step approach. The actions are the following:

1. Display space forces:[38] these could be carried out in peacetime as well. Displaying equipment, inviting foreign specialists, etc. could all fall under this category.
2. Space military exercises:[39] these do not only show resolve but also prepare the troops for actual combat. Even regular exercises could be interpreted by the opponents as signaling deterrence.
3. Deployment of space forces:[40] this could mean launching new spacecraft or adjusting existing systems.
4. Space shock and awe strike:[41] these are strikes to warn the enemy, and they could be "soft" like a cyberattack on the enemy C4ISR systems or "hard strikes" like a limited kinetic attack.

Needless to say, the importance of perception and psychological factors are also prevalent in space deterrence.[42] In addition to the four types mentioned above, Chinese documents introduce the concept of space blockades.[43] These types of actions aim to stop an enemy from reaching space or use it to their advantage. To reach these goals, Chinese forces might attempt to blockade ground installations, blockade specific orbits with debris clouds or space mines, blockade launch windows, or disrupt data connections.[44]

Due to the different approaches, institutions and equipment, there has been a will to do a comparative analysis of the main space-faring nations. Based on capabilities, plans, economic and technological backgrounds, the two countries having the most influence in the 21st century space domain will be the United States and China. Their relationship will have the biggest impact on how the space environment will evolve. In addition to the ones already

[36] Szymanski 2019.
[37] Beauchamp-Mustafaga et al. 2021, 62–63.
[38] 空间力量显示 *kōngjiān lìliang xiǎnshì*
[39] 空间军事演习 *kōngjiān jūnshì yǎnxí*
[40] 空间力量部署 *kōngjiān lìliang bùshǔ*
[41] 空间震慑打击 *kōngjiān zhènshè dǎjī*
[42] Beauchamp-Mustafaga et al 2021, 34–36.
[43] 空间封锁作战 *kōngjiān fēngsuǒ zuòzhàn*
[44] Cheng 2018.

mentioned, there are other major differences in how these two actors view the space domain. One recently conducted analysis found nine significant points:

1. China is a revisionist power in space, while the U.S. tries to keep the status quo;
2. China views space as a geographical area, not as a functional area;
3. Armed forces of China have an insurgent mindset comfortable with grey zone warfare, while the U.S. is more conventional;
4. China is more about position and reinforcing that position, while the U.S. is more about maneuver and attrition;
5. China focuses rather on the future, not the present, they prefer gradual long-term build-up;
6. The U.S. sees space from a separated military, commercial, aspect. China looks at it as a comprehensive all-in-one aspect;
7. The U.S. is more geocentric, while China is more cis-lunar centric;
8. For China, the economy and industry in space are more important;
9. The Chinese economic and industrial space goals are out of the scope of any U.S. department.[45]

The points above are not set in stone and do not mean that any side would neglect other aspects, or will be able to comprehend them. It rather gives a description of trends and current characteristics, greatly influenced by the strategic culture of these two countries.

Space wargames, communication and secrecy

Communication is not simply a verbal or written communication, but it also includes signaling. Signaling could be compared to body language in human communication. The sight of different gestures can already tell a lot about the intentions and inner state of a person. Displaying or using a different kind of equipment, initiating research programs, using satellite capabilities apart from their practical use, are all signals towards adversaries. For deterrence, the ideal outcome is that the opponents view the enemy forces strong; decision makers are able and ready to make difficult decisions as well as carry out previously communicated goals and threats.

However, as it is well known, communication can falter because of different reasons. Actors clearly know that disclosing information about their space assets can strengthen deterrence and at the same time, it can also help the enemy to better prepare for an attack. Thus, secrecy and keeping information confidential must be balanced with information sharing and openness, which can also build trust between actors. Enough information should be disclosed to convince the enemy that not worth attacking, but not too much so, it helps the adversaries get the upper hand during a conflict.

However, there is one part of deterrence that is impacted by the lack of communication. To make reasonable assumptions about the strength of deterrence, the value system and decision making process of the adversaries should be known to each other.

Actors conduct different types of space wargames, to prepare key personnel for possible confrontations and develop new procedures and strategies. Most of the results and conclusions of these wargames remain classified in order to maintain the advantage over the rivals. This secrecy, as noted by the Center for Strategic & International Studies (CSIS), could lead to serious misunderstandings and flawed planning. Therefore, the CSIS conducted their own space wargame experiment and decided to make the results public. There were three scenarios

[45] Wright (ed.) 2018.

during the experiment, with space experts involved from various space-related fields, and the results proved to be very valuable. These were the following:

1. How teams regarded the importance of attribution was in correlation with their space capabilities. Teams with a smaller space infrastructure did not worry about larger space-faring nations identifying them as the attacker. Blaming other teams was sometimes successful.
2. Reversible attacks were perceived differently by attackers and defenders. Attackers thought that their actions were less escalatory compared to the defenders', who sometimes viewed reversible attacks just as serious as irreversible attacks.
3. Resilience was very important in case of a more severe attack. Using commercial assets or allies, teams could replace lost capabilities.
4. Teams tried to avoid using kinetic weapons, but they were ready to take escalatory steps in other areas, like attacking ground infrastructure with conventional forces.
5. All participants used cyber attacks early and frequently.
6. The perception and evaluation of attacks were highly dependent on the circumstances.
7. It was difficult for the players to draw the line between tactical and strategic space systems.[46]

The results could help better understand the decision making process, but it is very unlikely that the potential rivals would reveal all of their results and research data. Simply put it: what helps my rival understand me better aids transparency but could also be used against me. This is the reason why such interesting wargames as the ASTERX space wargame organized by the French armed forces did not publish all the details and conclusions.[47]

Conclusions

Deterrence and as a subcategory space deterrence is a quickly developing field of military science. Space deterrence although rooted in general deterrence theory has its specifications and limitations. The lack of previous experience, the high amount of classified research and the rapid expansion of space activity make it more difficult to plan and design a reliable evaluation or escalation system. Meanwhile, space actors keep improving and expanding their SSA infrastructure and asymmetric and/or offensive capabilities. Some kinds of strategic restraint might be beneficial in an environment like this to avoid an arms race and possible accidents, which could lead to a severe conflict in space. The main guidelines of deterrence are still valid regarding the space domain. Capability, credibility, and communications are all necessary for deterrence in order to work. However, there is a significant difference between the approaches of Western concept of deterrence and Chinese and Russian strategic thinking. They both consider coercion – especially combined with hybrid methods – as an acceptable part of deterrence. In the case of space deterrence decision makers must consider specific factors: its connection to nuclear deterrence, the critical nature of space infrastructure, emotional factors, the possible limited and quick nature of an attack directed at space assets, increased chances for a cyberattack, and the problem of escalation and debris clouds. The development of new methods, strategies and technologies will pay a key role in keeping deterrence capabilities, while at the same time transparency and trust building measures can help mitigate the chance of a conflict.

[46] Harrison et al. 2017.
[47] Delaporte 2021.

BIBLIOGRAPHY

Adamsky, Dmitry 2020. „Deterrence á la Ruse: Its Uniqueness Sources and Implications.” In *NL ARMS Netherlands Annual Review of Military Studies 2020. Deterrence in the 21st Century*, edited by Frans Osinga and Tim Sweijs, 161–175. Breda: Springer Publishing.

Akoto, William 2020. „Hackers could shut down satellites – or turn them into weapons.” accessed December 10, 2021. https://gcn.com/cybersecurity/2020/02/hackers-could-shut-down-satellites-or-turn-them-into-weapons/291164/.

Beauchamp-Mustafaga, Nathan, Grossman, Derek, Gunness, Kristen, Chae, Michael S., Black, Marigold, Simmons-Thomas, Natalia 2021. *Deciphering Chinese Deterrence Signalling in the New Era: An Analytic Framework and Seven Case Studies*. Santa Monica, CA: RAND Corporation.

Bowen, Bleddyn E. 2018. „The Art of Space Deterrence.” accessed December 5, 2021. https://battle-updates.com/the-art-of-space-deterrence-by-bleddyn-bowen-lecturer-in-international-relations-at-the-university-of-leicester/.

Chen, Stephen 2021. „Chinese researchers look at how to keep satellites under the radar.” accessed December 8, 2021. https://www.scmp.com/news/china/science/article/3142902/chinese-researchers-look-how-keep-satellites-under-radar.

Cheng, Dean 2018. „Evolving Chinese Thinking About Deterrence. What the United States Must Understand About China and Space.” accessed December 2, 2021. https://www.heritage.org/global-politics/report/evolving-chinese-thinking-about-deterrence-what-the-united-states-must.

Cheng, Dean 2020. „An Overview of Chinese Thinking About Deterrence.” In *NL ARMS Netherlands Annual Review of Military Studies 2020. Deterrence in the 21st Century*, edited by Frans Osinga and Tim Sweijs, 177-200. Breda: Springer Publishing.

Course, Megan 2021. „Space Force zeroing-in on satellites, launch vehicles, radar, electro-optical sensors, communications, and cyber security.” accessed December 7, 2021. https://www.militaryaerospace.com/home/article/14210254/space-force-zeroingin-on-satellites-launch-vehicles-radar-electrooptical-sensors-communications-and-cyber-security.

David, Leonard 2005. „Anatomy of a Spy Satellite.” accessed December 7, 2021. https://www.space.com/637-anatomy-spy-satellite.html.

Dawson, Linda 2018. *War in Space.* Chichester UK: Springer Publishing.

Defense Intelligence Agency 2019. „Challenges to Security in Space.” accessed December 2, 2021. https://apps.dtic.mil/sti/citations/AD1082341.

Delaporte, Murielle 2021. „ASTERX 2021: French Space Forces Reach for Higher Orbit.” accessed December 10, 2021. https://breakingdefense.com/2021/04/asterx-2021-french-space-forces-reach-for-higher-orbit/.

Erwin, Sandra 2021. „DoD Space Agency: Cyber attacks, not missiles, are the most worrisome threat to satellites.” accessed December 6, 2021. https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/.

Erwin, Sandra 2020. „Space Fence surveillance radar site declared operational.” accessed December 6, 2021. https://spacenews.com/space-fence-surveillance-radar-site-declared-operational/.

Harrison, Todd, Cooper, Zack, Johnson, Kaitlyn, Robert, Thomas G. 2017. „Escalation & Deterrence in the Second Space Age.” accessed December 3, 2021. https://www.csis.org/analysis/escalation-and-deterrence-second-space-age.

Jervis, Robert 2017. *How Stateman Think.* Princeton: Princeton University Press.

Lambakis, Steve 2019. „A guide to thinking about space deterrence and China.” *Comparative Strategy* 38, no. 6: 497–553.

Lefebvre, Jean-Luc 2017. *Space Strategy.* London: ISTE Ltd.

Lindsay, Jon R. 2015. „Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack.” *Journal of Cybersecurity* 1, no. 1 (September): 53–67.

Lopez, Todd 2021. „Long-Range Discrimination Radar Reshapes Adversaries’ Calculus for Attack Against U.S. Homeland.” accessed December 10, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2865134/long-range-signalling

Maoruni, Al 2019. „Deterrence: I don’t think it means what you think it means.” accessed December 8, 2021. https://mwi.usma.edu/deterrence-dont-think-means-think-means/.

Mearsheimer, John J. 1983. *Conventional Deterrence.* Ithaca US: Cornell University Press.

Rhode, Scott 2021. „New Radar Complete at Clear Space Force Station.” accessed December 7, 2021. https://www.akbizmag.com/featured/new-radar-complete-at-clear-space-force-station/.

Rühle, Michael 2015. „Deterrence: what it can (and cannot) do.” accessed December 8, 2021. https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/index.html.

Schelling, Thomas C. 2008. *Arms and Influence.* New Haven: Yale University Press.

Scouras, James, Smyth, Edward, Mahnken, Thomas 2017. *Cross Domain Deterrence in US-China Strategy,* Maryland: John Hopkins University.

Smith, Simon J. 2018. „Space Warfare and the Implications for Extended Deterrence, Capabilities and the Character of War in the 21st Century.” accessed December 11, 2021. https://www.eustudies.org/conference/papers/download/705.

Stocker, Jeremy 2017. „The Nature of Deterrence.” Joint Air & Space Power Conference 2017, Memorandum, accessed December 8, 2021. https://www.japcc.org/deterrence-in-the-21st-century/.

Szymanski, Paul 2019. „Space Escalation Ladder – How to Control and Limit Space Outer Space Conflicts.” accessed December 12, 2021. https://apps.dtic.mil/sti/pdfs/AD1091673.pdf.

Union of Concerned Scientists 2021. „UCS Satellite Database.” accessed December 5, 2021. https://www.ucsusa.org/resources/satellite-database.

Ven Bruusgaard, Kristen 2016. „Russian Strategic Deterrence,” *Global Politics and Strategy* 58, no. 4 (July): 7–26.

Vogrincic, Victoria 2020. „China’s Heightened Space Presence in the Heart of Argentina’s Patagonian Desert.” accessed December 11, 2021. https://chinafocus.ucsd.edu/2020/11/19/chinas-heightened-space-presence-in-the-heart-of-argentinas-patagonian-desert/.

Wright, Nicolas (ed.) 2018. „Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation.” accessed December 9, 2021. https://nsiteam.com/social/wp-content/uploads/2018/08/SMA-White-Paper_Chinese-Persepectives-on-Space_-Aug-2018.pdf.

Zhang, Xueyang, Xiang, Junhua, Zhang, Yulin 2017. ”Space Object Detection in Video Satellite Images Using Motion Information.” *International Journal of Aerospace Engineering* Vol. 2017: 1–9.