Social Transformations in Contemporary Society, 2020 (8)
ISSN 2345-0126 (online)

LEGALITY OF TARGETING SATELLITES UNDER *JUS IN BELLO*: SPECIFIC FOCUS ON NON-KINETIC ASAT WEAPONS

Tomas Marozas

Mykolas Romeris University, Lithuania
tomasmarozas@gmail.com

Abstract

Purpose – Satellites are attractive military objectives due to their trajectorial predictability and essential functions they provide to military operations. In the last 13 years, at least three States (namely, USA, China and India) have successfully conducted kinetic anti-satellite (ASAT) missile tests which significantly increased amount of low-Earth orbit space debris, some of which are still orbiting and pose threat to space assets (Miglani, 2019, Wolf, 2007). All of these ASAT weapon tests were conducted against the self-owned space assets of the state conducting the test, therefore, these events did not trigger application of the law of armed conflict (*jus in bello*). However, that does not mean that legal evaluation of these tests, especially in terms of *jus in bello,* is practically insignificant, bearing in mind that technical destructive capabilities are already present and legitimacy of the use of these weapons is not evident. Indeed, some authors have already stressed out difficulties of legitimizing kinetic ASAT weapons, or, to be more precise, armed attacks against space assets. It has been argued that kinetic ASAT attacks in some cases could hardly fit principle of proportionality due to unpredictability of the amount of space debris and secondary collateral damage a blast-generated space debris could potentially cause (Stephens and Steer, 2016) or even attacks themselves in some cases might be indiscriminate in nature (Koplow, 2009). It could be observed that legitimacy of ASAT weapons is questionable mainly due to effects of kinetic attacks, but there are weapons, which aim to jam communication systems or cause malfunction with directed energy without generating space debris, except probably one inactive orbiting satellite. Therefore, most of the arguments applicable to kinetic ASAT attacks may not be applied to non-kinetic ones. In this article, the author argues that the use of non-kinetic ASAT weapons in certain conditions is hardly compatible with general principles of *jus in bello*, especially rules of targeting. The purpose of this article is to analyze whether the use of non-kinetic anti-satellite weapons during armed conflict is in accordance with *jus in bello* and, if not, what are conditions of their legitimate use.

Design/methodology/approach – this piece of research is based on information analysis, linguistic, systemic analysis and analogy methods. Research covering aspects of the law of outer space warfare will be analyzed and systemized while linguistic method is a helpful tool to interpret statutory rules governing weaponization. Analogy method is used to disclose definition of non-kinetic ASAT attacks using arguments applied to cyberattacks.

Finding – the use of non-kinetic ASAT weapons has limits under *jus in bello*.

Research limitations/implications – research is limited to non-kinetic weapons. This article does not disclose detailed technical aspects of non-kinetic ASAT weapons. It only highlights capabilities and function of these weapons and legal implications that the use those weapons against objects in outer space. Protection of persons under *jus in bello,* including targeting rules related with humans as targets, is not the object of this article.

Practical implications – since kinetic and non-kinetic space weapons are already present and still being developed, this research could contribute to determine legal boundaries of satellite attacks in practice.

Originality/Value – the focus on non-kinetic ASAT weapons is novel, since most of the research involves legal issues related to the effects of the use of kinetic ASAT weapons.
Keywords: *jus in bello,* non-kinetic ASAT weapons, law of war, distinction, precaution in attacks.
Research type: research paper.

Introduction

The dominance and victory in war is always sought by lessening the military advantage of the opponent. It is evident that the equipment which offers greatest military advantage becomes the primary target. Satellite imaging, accurate weather forecast and positioning services led to ultimate success of operation 'Desert Storm', known to be 'The First Space War' (Watkins Lang, 2016). Since then, the military spectrum of outer space technologies has been boosted to lift their owners into more dominant positions bearing greater military advantage. Alongside this development, States have also invested in anti-satellite technologies to reduce the military advantage of the opponent. These technologies are commonly called anti-satellite (hereinafter ASAT) weapons and are discussed in this article.

The topic of targeting satellites gains more and more popularity among international lawyers not only because military superpowers establish separate space force branches (Stone, 2019) or military alliances recognize space as fifth military domain (Brzozowski, 2019), but that ASAT technologies are present, already actively tested and pose threat to space services used by civilians and military personnel to be damaged or disrupted (Weede, 2013, Mackey, 2009, Ross, 2011, Macias and Sheetz, 2019, Popovkin, 2018, Langbroek, 2019). It needs to be emphasized that satellite services provide essential commodities in daily life without which, bank services, rescue missions, plane flights, logistics, energy production and supply, broadcasting, weather forecasting as well as some phone services would not work properly or would not work at all. The loss of satellite services would mean a giant leap backwards for humanity cutting links of globalized world. Unfortunately, it is only a matter of time when ASAT weapons will be used against the space assets of other States' and invoke application of *jus in bello*. Rules of targeting military objects form part of *jus in bello*, however, needless to say that none of these rules were specifically designed to govern outer space operations. Therefore, in this article, these relatively general targeting rules will be embodied in the specific context of outer space technologies to reveal issues related to targeting satellites.

There were four major kinetic ASAT tests when missiles actually hit satellites conducted by the USA (twice), China and India. All of them generated enormous amounts of space debris and were already inscribed by lawyers to hardly fit the rules of war, if kinetic-kill ASAT weapons were actually used during any armed conflict. Most of the arguments against legality of the use of these weapons float around consequential obscurity, that is, unpredictable results of each kinetic attack (such as the amount of newly generated space debris) which could be so disproportionate to perceived military goal, that the attack itself would be rendered unlawful. Launching an attack which causes damage to civilians, civilian objects or natural environment which would be clearly excessive in relation to the concrete and direct military advantage anticipated is a war crime.[1] What if the attack did not involve any kinetic energy and would not result in uncontrollable movement of space debris towards any assets in space? Clearly, arguments on proportionality would not play a big role, if any, in the context

[1] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002), UNTS 2187, 3. art. 8(2) b) (iv).

of non-kinetic ASAT weapons, since these weapons only render a satellite unfunctional or disrupt their signals, but not shatter them. However, there are other rules of targeting including the obligation to distinguish between military and civilian objects and take necessary precautions before launching an attack. Since the function of non-kinetic ASAT weapons and the consequences they may cause are essential for legal analysis, it will first be briefly explained what these weapons are capable of. The second chapter deals with only selective general rules of targeting that could be applicable to the targeting of satellites, since some rules (such as prohibition to cause unnecessary suffering) are aimed at human beings, not objects. Notion of attack under *jus in bello* will also be explained in the third chapter, in order to clarify activities which would fall under targeting rules and which would not. Finally, last chapter determines whether the targeting of satellites using non-kinetic means is compatible to the requirements of *jus in bello.*

The functioning and capabilities of non-kinetic ASAT weapons

All ASAT weapons are deemed to cause damage or malfunction of satellites. These weapons may be classified in various grounds: whether they are placed in orbit or they are direct-ascent, whether their launch mechanisms are portable or fixed, whether they use kinetic, or non-kinetic energy, whether they are destructive or disruptive, etc. In this article, non-kinetic ASAT weapons mean all ASAT interceptors that do not use ground, sea, air or orbit-launch kinetic-kill vehicles that are capable of destroying satellites due to their direct impact with the satellite or indirect energy impact due to a close-up blast. In general, for the purposes of this article, non-kinetic ASAT weapons mean all weapons that do not cause any space debris but one – permanently or temporarily dysfunctional satellite. The various types of non-kinetic ASAT weapons are discussed below.

Satellite signal jamming. Satellites communicate with each other and send signals to Earth through electromagnetic waves (Campbell, 2012). Any disruption of these waves, like radiation, reradiation, or reflection of electromagnetic energy could lead to loss or disruption of signal either from Earth towards satellite (called uplink) or from satellite to Earth (called downlink) (DOD Dictionary, 2020). The intentional interference with an adversary's radio frequency transmissions to or from a satellite is often called 'jamming'. Uplink jamming occurs when an unauthorized user transmits a different signal than authorized users (such as tv broadcasters) onto the same satellite on the same frequency and both signals combine and make a signal that a receiver cannot decode, or in other words, the desired signal is lost. The interfered, or decreased signal is being re-transmitted to users who receive an indecipherable noise. The other type of jamming – downlink jamming – is terrestrial, because jamming targets are ground satellite services, the satellite suffers no interference, nor would users outside the range of jammer (Weeden and Samson, 2019).

Jamming satellite signals could be very beneficial for one party to the conflict, since jamming satellites could lead to navigation errors of the opponent using global navigation satellite systems, disrupt the opponent's military communication network or prevent from sending accurate intelligence information or other images. China and Russia have a range of technologies specifically designed to jam Global Positioning System (hereinafter GPS) signals (Gordon and Page, 2018). In 2016 Russian Ministry of Defence announced to install GPS jammers in 250 000 phone towers to reduce enemy missile and drone accuracy in the event of large-scale conventional war (Рамм and Зыков). Before and during 2018 NATO exercise GPS jamming affected not only the military, but also civilian air traffic navigation over Finland and Norway territories. Norway claimed to have proof that the jamming was caused by Russian military (Norway says it proved, 2019). In February, 2020, Russian jamming system

ISSN 2345-0126 (online)

Krashuka-4 deactivated control systems of hostile drones in Syria's Hmeymim air base (Russian Electronic Warfare, 2020). Krashuka-4 is also capable of countering early warning and control systems and could even cause damage to enemy radar electronic warfare and communications systems (Electronic warfare complex, 2015). Similar case happened in Iran with a U.S. drone, when Iran supposedly spoofed GPS coordinates to make the drone land in Iran's territory, not the base in Afghanistan as was programmed (Rawnsley, 2011). Although GPS is owned by the U.S. government, the United States themselves are capable of jamming GPS networks so as the opponents did not use their services (Counter communications, 2020). That actually happens more than 20 times per month (Kehler, 2018).

Jamming is usually a temporal activity and it does not have a permanent effect on the satellite. However, as seen from the capabilities of these weapons, the effects of jamming might be unpredictable since the same jammed GPS satellite might be used by the military and civilians at the same time. Jamming and spoofing could cause devastating effects – GPS guided missiles could miss military and hit civilian targets, jamming could affect both, military and civilian air traffic and cause plane crashes, spoofing GPS could affect law enforcement agencies failing to receive information about incidents and their location, etc.

Directed energy weapons. Conventional weapons rely on either the kinetic or chemical energy of a sizable projectile while directed energy weapons use deposing energy on the target (Directed-Energy Weapons). Directed energy weapons (hereinafter DEWs) are devices that produce a beam of concentrated electromagnetic energy or atomic or subatomic particles which incapacitate, damage or destroy enemy equipment, facilities and (or) personnel (DoD Dictionary, 2020). There are three major types of these weapons: lasers, microwave radiation emitters and particle beams. Lasers can cause damage to electronic devices with intense heat on the device's sensor screens or by the sudden surge of electricity produced by the laser's energy (Directed-Energy Weapons). Lasers can cause melting, vaporization or mechanical effects due to vaporization. Microwaves are another type of electromagnetic radiation, but have much longer wavelength and much lower frequency than light. Microwaves can severely damage or destroy electronic components of the mechanism, especially receivers which are designed to detect, amplify and process microwaves at the same frequency. They do it by overloading the components with electrical current. Particle beam weapons use directed flow of atomic or subatomic particles to cause target damage, including melting or fracture of target material (Nielsen, 2012).

DEWs differ from signal jamming equipment since they are capable of causing physical damage to a target due to direct contact with it while satellite signal jamming only interferes with electromagnetic waves. It is also worth mentioning that DEWs might also cause only temporal effects, such as dazzling satellite's imaging sensors.

It is claimed that Russia has created a plane-mounted laser that is capable of hitting satellites (Tucker, 2018). The U.S. military is investing significantly in various DEW weapons applications, some prototypes of such weapons are being developed for tactical use, to defend against missiles, artillery and drones (Weeden and Samson, 2019). It was announced in 2019, that France will develop powerful anti-satellite laser weapons which would be placed on ground and in space (France to develop, 2019). These are only a few examples illustrating the variety of weapons that States possess and plans of their further development. It should also be borne in mind that offensive and defensive counter space capabilities are usually classified and all openly available state practice might be, and most probably is, only a tip of an iceberg.

ISSN 2345-0126 (online)

Selective general rules of targeting under *jus in bello*

The fundamental rule around which other targeting rules and *jus in bello* is built is inscribed in Art. 22 of the 1899 Hague Convention (II) (and repeated in many subsequent treaties) and reads as follows: "the right of belligerents to adopt means of injuring the enemy is not unlimited."[2] *Jus in bello* does not prohibit collateral damage to civilians and civilian objects, it only sets limits under what conditions this damage is unacceptable, therefore, rules of *jus in bello*, including targeting rules, balance between military necessity and humanity. Broadly speaking, there are four key questions that need to be answered by the commander before passing a decision to engage: 1) is the target military or civilian? 2) will the means and methods used in attack be legal? 3) would the attack cause excessive collateral damage in relation to the anticipated military advantage? 4) Have all necessary precautions been taken before the attack? These four questions include legal notions of principle of distinction, principle of proportionality, prohibition of indiscriminate attacks and principle of precautions in attacks, all of which will further be explained in detail.[3]

Principle of distinction. Art. 48 of the 1977 Additional Protocol I to 1949 Geneva Conventions (hereinafter API)[4] elaborates principle of distinction: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." This rule highlights a very important characteristic of targeting: there are only two types of objects – civilian and military. There is no and may not be an intermediate status of object, even if it serves both, civilian and military purposes. Art. 52(1) defines civilian objects by negation – "Civilian objects are all objects which are not military objectives". Art. 52(2) defines military objectives as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." This definition has two essential elements: 1) military objects contribute military action because of their nature, location, purpose or use; 2) their damage, destruction or capture offers a definite military advantage. Only a combination of both of these elements could qualify for the military object. The defining characters of the first element – nature, location, purpose or use – are listed with a good reason, since military objects are not only those constantly and directly used by the military (equipment, weapons, transportation, military bases, etc.), but also those which are used or even might be used only temporarily. Some objects might serve a military value due to their location, e.g. bridges that are essential for military transportation. Even though they are not used at the present time, their location might render them as legitimate objects of armed attack. It is explained in the Commentary of API that the criterion of 'purpose' is concerned with the intended future use of an object, while that of 'use' is concerned with its present function (Pilloud et. al., 1987). Although schools, hospitals and mosques are protected civilian objects, they might as well become military if they are used for military purposes. It needs to be emphasized that almost

[2] Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. (Adopted 29 July 1899, entered into force September 4, 1900).

[3] Important thing to note is that rules that are specifically designed to protect human beings (such as unnecessary suffering or determination and loss of civilian status) as opposed to objects will only be briefly discussed, since the goal of analysis is to provide considerations related to objects, not people.

[4] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978). 1125 UNTS 609.

ISSN 2345-0126 (online)

any object could potentially be used for military purposes in the future, but it does not render them military objects under the umbrella of 'purpose'. For example, schools cannot be attacked, even though they could potentially become military bases. There should be sufficient evidence (e.g. intelligence data) to show that the object is planned to be used for military purposes for the attack to be justified. Y. Dinstein argues that intelligence data may be faulty, therefore particular caution should be given to factual circumstances (e.g. if munitions are already placed in civilian object or not yet) (Dinstein, 2010). In case of doubt whether an object is normally dedicated to civilian purposes, it shall be presumed that it is a civilian object (Art. 52(3) of API). The second element requires destruction, capture or neutralization to offer a 'definite military advantage' in circumstances ruling at the time. It is not legitimate to launch an attack which only offers potential or uncalculatable military advantage, there needs to be some proof to show the military value (Pilloud et. al., 1987). Advantages that are hardly perceptible and those which only appear in the long term should be disregarded (Pilloud et. al., 1987). However, military advantage does not have to be tactical and limited only to one military operation, it may as well be calculated as a general result of all military campaign (Dinstein, 2010).

Prohibition of indiscriminate attacks. Prohibition of indiscriminate attacks is a derivative of principle of distinction. Indiscriminate attacks are those which 1) are not directed at specific military objective (such as bombardment of the inhabited area instead of targeting specific military building in that area); 2) use means and method which cannot be directed specifically at military objective (such as inaccurate long range missiles); 3) use means or methods effects of which cannot be limited at specific military objective (such as viruses).

Principle of proportionality. The military status of the object does not automatically un-fuse the gun – there are more considerations to be made before pulling the trigger. It is prohibited to launch an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated (API, art. 51(5)). This prohibition is customary and equally applies to all parties to the conflict, even if they did not ratify API (Rule 14). There are few elements of principle of proportionality that need to be stressed out. Firstly, the attack which caused disproportionate collateral damage is not necessarily disproportionate in legal terms. Principle of proportionality applies before launching an attack. The words 'may be expected' and 'advantage anticipated' support that logic. Firstly, even if military advantage surprisingly increased (e.g. the attacker bombed civilian building full of civilians knowing there was one low-rank enemy officer, however, later it was found that many enemy top-commanders were also at place), the attack would still be considered disproportionate, because proportionality should always be measured before the attack, not after. Secondly, collateral damage represents civilian injuries or casualties, damage to civilian objects or both. Principle of proportionality does not apply to combatants and other military objectives. Thirdly, principle of proportionality applies only to attacks, but not all military operations (see *ASAT operations as attacks: applying arguments for cyber attacks*). Fourthly, principle of proportionality measures all effects of attacks, including indirect ones (Broad, Corsi and Kamhi, 2008; Jensen, 2013). For example, if a dam was attacked, not only the damage to the dam should be evaluated (direct effect), but also the damage that the water flow caused to surrounding areas (indirect effect). Fifthly, principle of proportionality is rarely mathematically calculable. The life of the general might be worth hundreds of lives of civilians. Collateral damage needs to be 'excessive', which means that disproportion is not in doubt, it is obvious (Dinstein, 2010). It is important to assess 'overall' military advantage, not a specific attack, since the advantage could be mistaken through the eyes of a soldier (Dinstein, 2010). International Criminal Tribunal for the former Yugoslavia

(hereinafter ICTY) has established a standard of evaluation of the principle of proportionality. In Galic judgement, ICTY stated, that "In determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack."[5] That 'reasonable-commander' standard equally applies to indirect effects estimation mentioned before, since a commander may not always know all possible outcomes of attacks.

Precautions in attacks. Civilian population should be cared for constantly during armed conflict. All decisions should involve adequate considerations whether they would negatively impact civilian population. As it is stated in the Commentary of the API, "it is clear that precautions should not go beyond the point where the life of the population would become difficult or even impossible" (Pilloud et. al., 1987). Decisions to attack should be made carefully following instructions of precautions in attacks. Art. 57 of API lists the following precautions in attacks: decision makers of attacks should 1) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects; 2) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects; 3) refrain from disproportionate attacks; 4) cancel attacks if it becomes apparent that the objective is not a military one or the attack would cause disproportionate collateral damage; 5) if possible, effectively warn civilian population, if the attack could negatively affect them; 6) if there are alternative means to choose similar military advantage, choose the one, which would cause least danger to civilian lives and civilian objects. These six general duties have further implications rising directly from them. Obligation to verify military objectives requires constant care from the commanders to gather and assess information about the target. This obligation does not impose the requirement to possess most advanced reconnaissance equipment, but to use most effective and reasonably reliable information which would convince the commander that the object is military. If that information does not convince, the commander should seek for more. Information must relate to more than just the nature of the objective. Other circumstances, such as surrounding area of the target, should also be taken into account.

None of the targeting rules actually require a hundred percent accuracy or feasibility from commanders when making decisions. In general, it is required by commanders to constantly care for civilian population, never directly attack civilians or civilian objects and reduce collateral damage if possible or if that damage evidently appears for a reasonable commander to be excessive in circumstances at the time, refrain from targeting.

ASAT operations as attacks: applying arguments for cyber attacks

As it was discussed earlier, targeting rules are created to regulate only one specific form of military operations, that is, attacks. Not all military operations involve active engagement with the opponent, some have no direct offensive character, such as reconnaissance missions, mine clearing, securing buildings, etc. Military operations might even involve aggressive acts without actually causing physical harm, such as cyber-attacks during 2008 Russia-Georgia armed conflict (Haddick, 2011). It is therefore important to enclose the legal meaning of the word 'attack' to distinguish which activities are regulated by targeting rules and which not.

According to Art. 49(1) of API, 'attacks' are "acts of violence against the adversary, whether in offence or in defence". 'Violence' is a key word in the definition meaning that non-

[5] *Prosecutor v. Stanislav Galic,* no. IT-98-29-T, § 58, ICTY.

violent operations (such as espionage) are not limited with targeting rules. However, it does not mean that 'attacks' may only constitute a kinetic force on the target, since it is widely accepted that the use of radiological, biological and chemical weapons constitute attacks in terms of *jus in bello*.[6] Consequences of the attack that are destructive would render the military operation to legally qualify as an 'attack'. The discussion on what constitutes destructive consequences was raised during the procedure of drafting the Tallinn Manual. During that process, experts agreed that the notion of consequential harm encompasses any reasonably foreseeable consequential damage, destruction, injury or death (Norris, 2013). Experts also agreed that little or minimal interference to physical infrastructure by cyber-attacks is unlikely to meet requirements of a 'cyber-attack'. However, it is more difficult to determine, whether cyber-attack qualifies as attack, if it targets computer systems and data upon which the functionality of physical objects relies. Most of the experts agreed that only if after attack certain components of the target need to be replaced, the cyber attack might qualify as an attack (Norris, 2013). Same could not be said about temporal effects which could be restored by mere restarting of the operational system. International Committee of the Red Cross (hereinafter ICRC) in one of its papers argued that it is immaterial whether an object is disabled through destruction or in any other way, what matters is if the attack offers a military advantage which could be achieved not only through destruction or capture of the object, but also through neutralization (ICRC report challenges, 2015). Neutralization means an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it (Droege, 2012). The word 'neutralization' seems to be appropriate, since some operations against civilian networks (especially strategic objects as electricity grids, banking systems) could cause only temporary dysfunction of objects, but unbearable consequences on civilians and still would not have to meet targeting requirements. On the other hand, the word 'damage' is also conditional, since military objects might be damaged in the way which would not affect their functioning. Under strict interpretation of the notion of attack under *jus in bello*, throwing a stone towards the tank and scratching its surface could qualify as an attack while launching a cyber attack against bank systems which would preclude civilian population from using their savings to buy foodstuffs would not. Strict interpretation of Art. 49 would be contradictory to *jus in bello* goals.

Certain non-kinetic operations such as espionage or jamming of radio communications traditionally are not considered attacks under *jus in bello* (Boothby, 2017). Some suggest using criterion of 'inconvenience' to determine whether the activity is an attack. Activities which only cause 'inconvenience' should not qualify as attacks. However, ICRC admits that 'inconvenience' is not a legal term and does not have unanimous understanding (ICRC report challenges, 2015). Jamming, spoofing, damaging and destroying a satellite would all cause inconvenience. There is another argument that if these activities form part of military operation, e.g. shutting down anti-missile systems, they would be qualified as attacks (Droege, 2013). However, that suggestion also has drawbacks, since some military operations are not related to the use of force, such as reconnaissance. Couple of examples could help to clarify the issue. In the first example, a drone is on the mission to take photos of a military object. However, it is known that the enemy has capabilities to shoot down the drone or take over its control. Therefore, seconds before the drone took off, radars were jammed so the drone could safely complete the mission. In the second example, a GPS downlink signal was jammed and the opponent operating in the area of the jammed signal had to switch control of the military plane to manual mode and return to base. As an analogy, a self-driving car stopped at the

[6] *Prosecutor v. Dusko Tadic.* Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, no. IT-94-1 § 58, ICTY.

highway due to loss of the signal and was hit by a fast-moving truck. The crash was fatal. The author is of opinion that qualification of activities should be dealt on a case-by-case basis. Any disruption of functionality of the object should qualify as attack. Specific focus should be given to the likely consequences of the activity which would most likely cause death, damage, destruction or injury of persons or objects protected under *jus in bello*. In other words, if it is evident that due to the activity of the party to the conflict protected persons or objects might face negative consequences to their health or functioning, that activity should be limited under targeting rules of *jus in bello*. As it is noted in the Art. 49(3), the provisions of protection of civilian populations against the effects of hostilities apply in all cases when civilian population, individual civilians or civilian objects might be affected by the military activity. Following this logic, jamming the radar would not necessarily constitute an attack, while jamming GPS satellites would, since it would also negatively affect civilian infrastructure and civilians. In any case, it should be refrained from any attacks which would cause life of the population difficult or even impossible and in the given circumstances at the time that would be evident for a reasonable commander.

To sum up, anti-satellite activities should be determined not only by the type of attack, the damage to be caused or functions lost, but also by the estimation of possibility to cause negative effects to protected persons or objects. Not all possible outcomes from attacks should be estimated (that requirement would be hardly implementable), but generally the evident likelihood that the attack will most probably affect civilian population or objects. Non-kinetic ASAT attacks having kinetic destructive consequences, such as melted components of the satellite constitute attacks under *jus in bello*. The author suggests that non-kinetic ASAT attacks which do not damage or leave satellite dysfunctional (neutralize) at least temporary, should qualify as attacks only if it is evident from circumstances prevailing at the time that civilians or civilian objects will most probably be negatively affected by the activity.

Legality of targeting satellites using non-kinetic means

Legality of targeting satellites under IHL will further be analyzed in the sequence of the four key questions listed earlier.

Are satellites military objectives? Some satellites are specifically made to serve only military functions. Usually, these functions relate to reconnaissance, early warning systems and military communications. Under the definition of 'military object' provided earlier, satellites which serve these functions fall under criteria of 'nature' and 'use' (they are of military nature and they are used by the military) and are legally qualified as military objects. However, most of the satellites are used for both, military and civilian purposes. The notion of dual-use technologies is not new. Civilian dual-use infrastructure is full of examples – railroads, civilian airports, energy plants, telecommunication centers, oil platforms – all would have a significant military value during armed conflict. If these objects are used for military purposes, they would instantly become military objects. However, even if they are not used for military purposes, they have potential to be used in the future. While civilians lose protective status only for the time, they take direct part in hostilities (API Art. 45), civilian objects lose protection and become military objects once they are used or even have potential to be used (under future-orientated category of 'purpose') (Pilloud et. al., 1987). Therefore, dual use satellites as any other dual-use technologies are military objects. Satellites which are specifically used for civilian purposes are civilian objects and may not be targeted. Satellites which are used for military purposes, however, there is no evidence to show that should be presumed to be civilian objects (API Art. 52(3)). It is also important that the principle of distinction, as mentioned before, requires to have sufficient information which would show

that the object is used for military purposes. There might be satellites orbiting the Earth whose military function could be hidden. For example, Chinese satellite SY-7 has a robotic arm to support China's space station program (Weeden and Samson, 2019). That arm may be used not only for civilian purposes (e.g. repairing other satellites) but also military (e.g. destructing other satellites). Should this satellite be considered as a military object? At first it would seem that it could, since that object could fall under 'purpose' category, however, its use as a military objective is only hypothetical and if sufficient information was given to show that this satellite is planned for military use, or it would make maneuvers and approach opponent's satellite, only then it would become a military object.

Will only legal means and methods be used in attack? Most of the requirements and prohibitions for means (weapons) and methods (the way war waged) under *jus in bello* are directed at protection of persons, not objects (e.g. prohibition to cause unnecessary suffering, perfidy, prohibition to use poison, chemical weapons, etc.). However, prohibition of indiscriminate attacks is applicable to all attacks. Non-kinetic ASAT weapons, especially DEWs are very precise, they might even target a specific part of the satellite, not a satellite as a whole, therefore, they are discriminate in nature. The effects of kinetic ASAT weapons are hardly controllable, since space debris might hit other assets in space and cause even more damage. However, non-kinetic ASAT weapons do not produce space debris, does that mean that these means of warfare may not be used indiscriminately? As it was mentioned before, the disproportionate attack constitutes an indiscriminate attack under API art. 51(5) b). Moreover, even if non-kinetic ASAT weapons do not generate space debris, their use might cause indirect uncontrollable effects, some of which would even be almost impossible to predict. The dependence of ground infrastructure from GPS network is a good example. It is practically impossible to calculate the number of technologies that at the given moment of the orbital spin of satellite could be affected by the loss of that precise GPS satellite's services. It is even harder to predict the effects these technologies would face from the loss of GPS signal. That leads to considerations whether a prudent-commander could turn a blind eye on his or her duty to care for civilian population not knowing what the effects from attack would be? The situation of attacking GPS or other navigational network satellites would be somewhat similar to blind shooting at the area, which is prohibited and considered as an indiscriminate attack (Fleck, 2008). It is impossible to predict the chain of events that the attack on the satellite would invoke, therefore, a commander is not required to what is impossible to do. However, if a commander should at least appraise himself or herself with information about the function of the satellite and theoretical implications what consequences might occur due to its damage.

Would the attack cause excessive collateral damage in relation to the anticipated military advantage? In most cases, principle of proportionality is hardly calculable before launching a non-kinetic ASAT attack, since only the direct effect of the attack is known (destruction or malfunction of the satellite). However, as already indicated, indirect effects, dependent on the functions of the attacked satellite, might be countless. As was already illustrated many times in this article, attack on GPS or any other navigational network could cause devastating effects and many civilian casualties. Attacking other satellites, such as co-orbiting ASAT weapons or even imaging satellites at geostationary orbit, would probably pass the test of proportionality.

Have all necessary precautions been taken before the attack? This last question is probably most important when launching attacks against satellites. As mentioned, precautions in attacks require to take all feasible precautions in the choice of means and methods of attack to have least possible collateral damage. Technically, when jamming a satellite collateral damage would depend on whether it is orbital or terrestrial jamming. Orbital jamming (or uplink jamming) occurs when an attacker sends a beam of contradictory

signal directly toward a satellite via a rogue uplink station. The whole transmission to the recipient would be blocked (Hudaib, 2016). In terrestrial jamming (or downlink jamming), the attacker transmits rogue frequencies in the direction of terrestrial targets (ground satellite dishes). Terrestrial jamming involves transmitting rogue frequencies in the direction of local consumer-level satellite dishes. The jamming frequencies are limited to a specific area and are able to interfere only with the frequency emanating from the satellite in a specific location. Jamming area could be up to 20 kilometers while in orbital jamming – the whole geographical field that satellite operates on (Hudaib, 2016). Therefore, jamming downlink could have less collateral damage than uplink and could probably be an alternative to achieve the same military goal. The attacker should also take precautionary measures choosing timing of attack. Since satellite services are mostly used by civilians during day-time hours, less collateral damage could be achieved if attacks were waged during night or at least during non-rush hours. However, it would also depend on the function of the satellite. It is also required to warn the civilian population (if possible) if the attack could have negative effects on them. If the attack could affect power grids, banking and other essential functions of civilian life, warning could be very effective to lesser collateral damage and achieve the same military advantage. Commanders should seek as much information about the targeting satellite as possible, preferably, their function and which specific infrastructure on the ground could be affected due to attack. Attacking a satellite merely because it belongs to the opponent without prior analysis of its function and capabilities would contradict targeting requirements under *jus in bello*.

As seen from these four questions, the main problem legitimizing non-kinetic ASAT attacks is unpredictability of indirect effects which could result in breach of principle of proportionality. Some difficulties could raise identifying the target and establishing its impact on ground technologies and that could impede principle of precautions in attacks. Non-kinetic means of attacking satellites are more preferable than kinetic ones, since they would not generate space debris, however, certain legal issues similar to ones identified by scholars in kinetic attacks are similar.

Conclusions

Not all anti-satellite activities fall under the notion of 'attacks' which is underpinned by targeting rules. The use of DEWs against satellites would in most cases constitute attacks under *jus in bello,* however, signal jamming might not. Rules of targeting under *jus in bello* would apply if a satellite component was damaged, a satellite was left at least temporary dysfunctional (neutralized) or otherwise, there would be a great chance that the attack could negatively affect protected persons or objects under *jus in bello*.

Commanders who pass decisions to engage in non-kinetic ASAT attacks should appraise themselves with information on what the attacking satellite is capable of and how ground technologies could at least in theory be affected by the attack. Moreover, if the primary function of the satellite is civilian, but it has a wider range capabilities that could negatively affect other space assets (such as robotic arm or ability to maneuver between different orbits), the attack without having prior information about intentions to use that object for military purposes would be contrary to principle of distinction. Such satellites should be presumed to be civilian objects. Special means of precautions should be taken when targeting GPS or other similar networks, since in most cases collateral damage can only be relatively estimated in advance, but the results may be devastating. If possible, alternative means of non-kinetic attacks, such as downlink jamming instead of uplink, should be chosen.

References

Boothby, B. (2017). Space Weapons and the Law. *International Law Studies,* 93(179), 180-214, p. 210.

Broad, E., Corsi, J., Kamhi, A., 2008. *Cluster Munitions and the Proportionality Test: Memorandum to Delegates of the Convention on Conventional Weapons.* 10.

Brzozowski, A. (2019, November 21). NATO braces for the new space age. Retrieved March 30, 2020, from https://www.euractiv.com/section/global-europe/news/nato-braces-for-the-new-space-age/.

Campbell, A. (Ed.). (2012, October 14). How do satellites communicate? Retrieved March 29, 2020, from https://www.nasa.gov/directorates/heo/scan/communications/outreach/funfacts/txt_satellite_comm.html.

Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. (Adopted 29 July 1899, entered into force September 4, 1900).

Counter Communications System Block 10.2 achieves IOC, ready for the warfighter. (2020, March 13). Retrieved March 29, 2020, from https://www.losangeles.af.mil/News/Article-Display/Article/2111775/counter-communications-system-block-102-achieves-ioc-ready-for-the-warfighter/

Dinștein Yoram. (2010). *The conduct of hostilities under the law of international armed conflict* (2nd ed.). Cambridge: Cambridge University Press. 90, 94, 131, 134

Directed-Energy Weapons. (n.d.). Retrieved from https://www.globalsecurity.org/military/library/policy/army/fm/71-1/711apxlf.htm

Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, *94*(886), 533–578, p. 558.

Droege, C. (2013, June 26). IHL Challenges Series - IHL & New Technologies, Part IV: Cyber warfare. Retrieved March 29, 2020, from https://intercrossblog.icrc.org/blog/ihl-challenges-series-ihl-new-technologies-part-iv-cyber-warfare.

Electronic warfare complex "Krasuha-4". (2015, July 14). Retrieved March 29, 2020, from https://web.archive.org/web/20150714165635/http://kret.com/en/product/12/

Fleck, D., & Bothe, M. (2008). *The handbook of humanitarian law in armed conflicts* (2nd ed.). Oxford: Oxford University Press, p. 199-200.

France to develop anti-satellite laser weapons. (2019, July 25). *RFI.* Retrieved March 29, 2020, from http://www.rfi.fr/en/france/20190725-france-develop-anti-satellite-laser-weapons

Gordon, M. R., & Page, J. (2018, April 9). China Installed Military Jamming Equipment on Spratly Islands, U.S. Says. Retrieved March 29, 2020, from https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320

Haddick, R. (2011, January 28). This Week at War: Lessons from Cyberwar I. Retrieved March 29, 2020, from https://foreignpolicy.com/2011/01/28/this-week-at-war-lessons-from-cyberwar-i/.

Hudaib, A. A. Z. (2013, September 19). Hacking Satellites ... Look Up to the Sky. Retrieved March 30, 2020, from https://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/

International Committee of the Red Cross. 2015. *International humanitarian law and the challenges of contemporary armed conflicts. 32nd International Conference of the Red Cross and Red Cressent.* Geneva, p. 41-42

Jensen, E. T. (2013). Cyber Attacks: Proportionality and Precautions in Attack. *US Naval War College*, 89(218), 198–217. 207-209.

Kehler, R. C. (2018, April 11). Space Threat Assessment 2018. Retrieved March 29, 2020, from https://aerospace.csis.org/spacethreat2018/

Koplow, D. A. (2009). ASAT-isfacton: Customary International Law and the Regulation of Anti-Satellite Weapons. *Michigan Journal of International Law,* 30, 1187-1272, p. 1235.

Langbroek, M. (2019, May 1). Why India's ASAT Test Was Reckless. Retrieved March 30, 2020, from https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/.

Macias, A., & Sheetz, M. (2019, January 18). Russia conducted another successful test of an anti-satellite missile, according to a classified US intelligence report. *CNBC.* Retrieved March 30, 2020, from https://www.cnbc.com/2019/01/18/russia-succeeds-in-mobile-anti-satellite-missile-test-us-intelligence-report.html

Mackey, J. (2009). Recent US and Chinese Antisatellite Activities. Retrieved March 30, 2020, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a594484.pdf

Miglani, S. (2019, March 28). India says space debris from anti-satellite test to 'vanish' in 45 days. *Reuters.* Retrieved March 30, 2020, from https://www.reuters.com/article/us-india-satellite/india-says-space-debris-from-anti-satellite-test-to-vanish-in-45-days-idUSKCN1R91DM

Nielsen, P. E. (2012). *Effects of directed energy weapons: lasers, high power microwaves, particle beams*. Albuquerque, NM: CreateSpace Independent Publishing Platform. 173-174, 244.

Norris, M. J. (2013). "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace." *Inquiries Journal/Student Pulse*, *5*(10). Retrieved from http://www.inquiriesjournal.com/a?id=775

Norway says it proved Russian GPS interference during NATO exercises. (2019, March 18). *Reuters.* Retrieved March 29, 2020, from https://www.reuters.com/article/us-norway-defence-russia-idUSKCN1QZ1WN

Office of the Chairman of the Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms, Retrieved March 29, 2020, from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Pilloud, C., Sandoz, Y., Swinarski, C., & Zimmermann, B. (1987). *Commentary on the additional protocols: of 8 June 1977 to the Geneva conventions of 12 August 1949*. Geneva: International committee of the Red Cross. 636-637, 677, 684, 692

Popovkin, V. (2019, February 28). Space Threat 2018: Russia Assessment. Retrieved March 30, 2020, from https://aerospace.csis.org/space-threat-2018-russia/

Prosecutor v. Dusko Tadic. Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, no. IT-94-1 § 124, ICTY.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978). 1125 UNTS 609.

Quéguiner, J.-F. (2006). Precautions under the law governing the conduct of hostilities. *International Review of the Red Cross*, *88*(864), 793–821. 798

Rawnsley, A. (2011, December 12). Iran's Alleged Drone Hack: Tough, but Possible. *Wired.* Retrieved March 29, 2020, from https://www.wired.com/2011/12/iran-drone-hack-gps/

Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002), UNTS 2187, 3.

Ross, T. (2011, February 2). WikiLeaks: US and China in military standoff over space missiles. *The Telegraph.* Retrieved March 30, 2020, from https://www.telegraph.co.uk/news/worldnews/wikileaks/8299495/WikiLeaks-US-and-China-in-military-standoff-over-space-missiles.html

Rule 14. Proportionality in Attack. (n.d.). Retrieved from https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14

Russian Electronic Warfare System Brings Down Hostile Drones In Syria. (2020, January 3). *Defenseworld.* Retrieved March 29, 2020, from https://www.defenseworld.net/news/26265/Russian_Electronic_Warfare_System_Brings_Down_Hostile_Drones_in_Syria#.XoDfvIj7SUl

Stephens, D. and Steer, C. (2015). Conflicts in Space: International Humanitarian Law and its Application to Space Warfare, *McGill Annals of Air and Space Law* XL(1), 1-32, p. 26.

Stone, M. (2019, February 19). Trump signs directive in step to create U.S. Space Force. *Reuters.* Retrieved March 30, 2020, from https://www.reuters.com/article/us-usa-military-space/trump-signs-directive-in-step-to-create-us-space-force-idUSKCN1Q82H2.

Tucker, P. (2018, February 26). Russia Claims It Now Has Lasers To Shoot Satellites. Retrieved March 29, 2020, from https://www.defenseone.com/technology/2018/02/russia-claims-it-now-has-lasers-shoot-satellites/146243/

Watkins Lang, S. (2016, January 20). SMDC History: 25 years since first 'Space War'. Retrieved March 30, 2020, from https://www.army.mil/article/161173/smdc_history_25_years_since_first_space_war

Weeden, B and Samson, V. *Global Counterspace Capabilities: An Open Source Assessment.* [interactive]. April, 2019. [accessed 2020-03-29]. https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf, 1-2, 1-15, 3-14

Weeden, B. (2013, August 16). Anti-satellite Tests in Space – the Case of China. Retrieved March 30, 2020 from https://swfound.org/media/115643/china_asat_testing_fact_sheet_aug_2013.pdf

Wolf, J. (2009, February 27). U.S. satellite shootdown debris said gone from space. *Reuters.* Retrieved March 30, 2020, from https://www.reuters.com/article/us-space-usa-china/u-s-satellite-shootdown-debris-said-gone-from-space-idUSTRE51Q2Q220090227

Рамм, А., & Зыков , В. (2017, April 7). Минобороны заглушит GPS с вышек сотовой связи. Retrieved March 29, 2020, from https://www.nextbigfuture.com/2016/10/russia-will-place-gps-jammers-on-250000.html