Various Threats of Space Systems

45

Xavier Pasco

Contents

Abstract

For roughly two decades, orbital systems, beyond their traditional strategic value, have gained a pivotal role in modern conventional security and defense activities. As a consequence, they have been considered as possible new targets in military confrontations, and the recent years have indeed demonstrated a renewed activity in the field of antisatellite researches and tests. This piece attempts to put these efforts in perspective and detail their different forms. It appears that besides the traditional kinetic destruction of satellites, leading to uncontrolled long-lived debris, other threats may have equally destructive consequences with more limited side effects. Directed energy weapons in orbit or even cyberattacks may

X. Pasco (✉)
Fondation pour la Recherche Stratégique (FRS), Paris, France
e-mail: x.pasco@frstrategie.org

K.-U. Schrogl (ed.), *Handbook of Space Security*,
https://doi.org/10.1007/978-3-030-23210-8_9

become weapons of choice in the new space landscape. These likely perspectives must lead the international community to rethink the reality of threats related to space systems.

Introduction

Space systems have gained an increasing importance in the everyday life of the modern societies: telecommunications by satellite, broadcasting of television programs, observation of the Earth's surface and oceans, observation of the atmosphere for weather forecasts, navigation, and worldwide broadcasting of universal time have so many applications that they contribute intimately to the day-to-day making of our contemporaneous world.

Besides, the needs for the defense of States and for the security and safety of their citizen feed widely on data resulting from the use of observation, electronic intelligence, or early warning satellites. These have contributed in an essential way to producing a strategic piece of information during these last 50 years, helping in the prevention of the bipolar crises. Chastely qualified as "national technical means," observation, electronic intelligence, or early warning satellites became one of the touchstones of the strategic dialogue of the 1970s and 1980s. In this context, keeping space safe and preventing any evolution leading to putting space systems in jeopardy became a key word. In particular, American presidencies of the Cold War had effectively resigned themselves to this established fact. For decades, according to recently published official US documents, it was clearly recognized that any preparation of an antisatellite interception would have been contrary to the spirit if not the letter of the SALT (Strategic Armements Limitation Talks treaty signed in 1972 by Richard Nixon and Leonid Brezhnev) protection of "national technical means" with the risky perspective "to stimulate satellite interception since we are more dependent on intelligence from space sources and would have more to lose." (Memorandum from the President's Assistant for National Security Affairs (Scowcroft) to President Ford, Washington, July 24, 1976. For a more complete vision of the position of the US authorities at that time, refer more largely to the archives recently published under the direction of McAllister (2009).) In spite of two Soviet campaigns of antisatellite attempts during the 1970s which led to the US executive authorities to reexamine this position and realize a first antisatellite test in 1985, this particular form of militarization of the space was hardly pushed, the possible earnings remaining considered very thin with regard to the incurred strategic risks. The "stabilizing" function of these national technical means during the Cold War had been already well established and has been well informed since.

Considering this central aspect, the club of the space countries quickly agreed on the interest of keeping space free of weapons, in an explicit way or more implicitly. The text of the main legal body, the "treaty on principles governing the activities of States in the exploration and use of the outer space, including the Moon and the other celestial bodies," came into effect in 1967, has established the idea according to which the exploration and the use of the space are the privilege of the whole humanity. It has dedicated the freedom of research and circulation in space and

has clearly indicated that the notion of State sovereignty cannot be extended in outer space or in the celestial bodies. Establishing the founding principle of the "peaceful uses" of outer space, the text does outlaw the deployment of weapons of mass destruction in outer space as well as any military activity on the Moon and on the other celestial bodies. (By the end of 2011, 100 countries had already ratified the Treaty, among which any major space nation.)

Nevertheless since approximately two decades, the international debate on the theme of the security of the spatial activities and more exactly on the militarization of the space returned to the front scene by becoming more radical. In the course of the transformations occurred during the 1990s, the initial preventions against a too extensive militarization of the Low Earth Orbit (LEO) have unmistakably weakened. Two main explanations can be called:

- The relative "downgrading" of the nuclear order as an international regulating principle and the consecutive "unbolting" of the debate on an increasing supposed vulnerability of the national spatial means: The United States in particular has mentioned the perception of an increased vulnerability considering the more and more central role played by satellites in the political, military, and economic life of most of the developed countries, with the United States in the first place.
- The emergence of new space actors, who may "threaten" to radically change the way space has been regulated under the auspices of a "club" of a few spacefaring countries, driving precisely these countries to anticipate this situation and bend over the elaboration of new international rules for the use of the space.

Change of Strategic Landscape: A Succession of Disturbing Events

More than in the 50 last years, this decade has known several events that have underlined the fundamental fragility of satellites. A series of destructions in orbit, deliberate or not, put space in full light, worrying the largest part of the diplomatic and military community. It came in a way to punctuate harder and harder debates in Geneva on the prevention of the arms race in space.

1. First of all, the shooting by China of a ballistic missile towards an old weather satellite on January 11, 2007, leading to its destruction and to the generation of a 3000 long-lived fragments on a very busy orbit, surprised the whole world. This test was the first of its kind since the one undertaken in 1985 by the United States which proceeded to the interception of one of their satellite by using a missile embarked under an F-15 fighter plane.
   At the very moment of the 2007 interception, the Chinese representatives were supporting without reserve the international efforts in the United Nations intended to limit the creation of space debris and opposed against the United States within the conference on disarmament in Geneva on the theme of the militarization of the space with a very proactive posture about prohibiting anti-satellite weapons.

2. Although they denied having had such intentions, the United States did not delay "answering" their Chinese counterparts by proceeding themselves on February 21, 2008, to the destruction of one of their military satellites in perdition. According to the American authorities, the point was to destroy a satellite which reentry was considered dangerous. Nevertheless, the successful attempt demonstrated, at least incidentally, the efficiency of one of the components focusing for the antimissile defense, whereas that it also meant the American intention "to mark" clearly its strategic territory. To complete the "state communication" picture, the American authorities did not miss to let know that this interception occurred at a much lower orbit than the Chinese interception, showing that this had been managed on the side of the United States in a more "appropriate way" by generating very short-term fragments of life. (Official US information has stated the figure of 175 detected debris (at the difference of 3037 for the Chinese event) with the last one reentered in the atmosphere by the end of October 2009.)
3. Less than a year later, on February 10, 2009, two satellites, one Russian (Cosmos 2251) and another one registered in the United States (a satellite of the Iridium constellation), collided and destroyed each other, generating some 1800 fragments on equally very frequented orbits. This collision, the first one in the history of space activity, was going to finish putting the question of space safety and security in the broad sense as one of the priority themes of the future space cooperation.
4. Finally, India performed an antisatellite test on March 27, 2019, using a two-stage ground based missile equipped with a terminal kill-stage that impacted a 750 kg Microsat-R satellite launched only about 2 months earlier in January 2019. This event was hailed by Prime Minister Modi as bringing "utmost pride" and having "a historic impact on generations to come." Communication was visibly prepared to avoid the level of criticism brought about in its time by the Chinese test. In particular, a FAQ document published by the Indian MoD immediately after the test underscored that "the test was done in the lower atmosphere to ensure that there is no space debris. Whatever debris that is generated will decay and fall back onto the earth within weeks." (See https://www.mea.gov.in/press-releases.htm?dtl/31179/Frequently+Asked+Questions+on+Mission+Shakti+Indias+Anti Satellite+Missile+test+conducted+on+27+March+2019 – accessed 29 March 2019.) Indeed, Miscrosat-R, supposedly an imaging satellite, was orbiting at about 280 km making it a "cleaner" target than the Chinese satellite, with debris supposed to burn in the atmosphere after only several months. It remains that this event has triggered the criticism of several operators of small low altitude satellites, such as Planet or Astroscale. However, it must be noted that the general reaction of governments, including China, has been limited to date.

Besides these well-known events, other recent disruptions in space have dramatized the space scene further, whether due to presumed cyberattacks (suspected in 1998 in the case of the US-UK-German satellite ROSAT recently reentered in the atmosphere), to laser blinding or tagging (as suspected from Chinese origin towards

an US NRO satellite in October 2006), to interferences, whether purposeful as in the recent case of an Eutelsat satellite jammed from a source in the Middle East or accidental with the so-called zombiesat belonging to Intelsat and uncontrolled between April 2010 and January 2011 while emitting at full power and interfering during this period of time with a number of telecommunication satellites. As it will be explained below, these latest cases must also be considered as potential major sources of disturbances.

Early Armed Threats in Space

For a few years, the news has been dominated by controversies nourished by the supposed plans in a few countries of a possible deployment of weapons in the outer space. Such a subject is not new and has in fact been considered since the launch of the space activities. While no genuine "space arm race" has indeed been triggered during the Cold War, it is useful to remind nascent achievements in the 1960s, mainly carried out by the then USSR.

It must be noted that the "*weaponization*" of space has been considered very early in the history of space bipolar relationships. As early as February 1957, eminent US military officers did not hesitate to present space as a new "theater of operations": "*In the long haul, our safety as a nation may depend upon our achieving 'space superiority.' Several decades from now, the important battles may not be sea battles or air battles, but space battles, and we should be spending a certain fraction of our national resources to ensure that we do not lag in obtaining space supremacy.*" (See excerpts of the famous 1957 speech by B. Schriever at http://www.af.mil/news/story.asp?id=123040817 (accessed August 2012).) A few weeks after Sputnik, that same year, the Air Force Chief of Staff, General Thomas D. White, reiterated this general assessment, ensuring that "*whoever has the capability to control space will likewise possess the capability to exert control of the surface of earth*." (Quoted in Stares (1985, p. 48). Military strategies would be also made public, for example, in a 338-page book, *The United States Air Force Report on the Ballistic Missiles* written by Colonel Kenneth Gantz (and forwarded by the well-known Generals White and Schriever). It was published by Doubleday and Comp in 1958. Besides the most common proposals aiming at developing antisatellite weapons, the US Air Force was proposing as soon as 1956 two different strategies for the military investment of space. One of those consisted in using a manned ballistic rocket (*Manned Ballistic Rocket Research System project*), while the other one (*Manned Glide Rocket Research System*) proposed the use of a reusable glide body launched from a main carrying rocket. If this latest project may recall the early NASA studies made about the shuttle at the end of the 1960s, this last project was purely military by essence as it envisioned the possibility to bomb the Earth surface since the altitude of 64 km! On its side, the Army, via the Army Ballistic Missile Agency (where Wernher Von Braun would ultimately help the United States to launch their first working satellite in January 1958), had the project of a super powerful rocket that would allow

"colonizing" the Moon as well as other planets for military purposes. For a detailed expose of the military position at that time, see also Baker (1985, pp. 12–30)).

If many projects aiming at militarizing space *stricto sensu* have emerged in the United States, none of them were given real credits by the successive presidencies in this country. The political authorities were more inclined to capitalize on the nascent nuclear ballistic force to ensure the strategic balance with the USSR. However, first initial developments made in relation with the ballistic threat can be cited that paved the way for ground-based space weapons. A first "missile defense" capability was proposed in 1958 with the two-stage Nike-Ajax nuclear armed antiballistic missile, later on followed by the more powerful Nike-Hercules and Nike-Zeus. First ABM interceptions occurred in 1962, opening the way to newer ABM missiles, namely, the Sprint and Spartan version leading to the "Sentinel" and "Safeguard" program in 1969 with the objective to defend a limited number of strategic missile silos. It must be noted that as early as May 1962, the then Secretary of Defense McNamara allowed the conversion of the Nike-Zeus model into an ASAT program (Program 505) which led to simulated interceptions and then to a successful hit in May 1963 against a cooperative target. Another existing ASAT capability based on the THOR missile was also operational and led to the shutdown of the Nike-Zeus capability. The THOR capability would also be terminated a few years later in the mid-1970s.

The USSR gave itself the first role in developing threats actually *coming* from space orbital systems. A first series of "co-orbital" tests were indeed carried out starting from 1968 with a first alleged success in November that year and ended in 1971, obviously at a time when the new "*Detente*" was to be consolidated after the US-Soviet signature of Salt-1. (Signed in 1972 in Moscow, this test was incidentally pleading for the use of National Technical Means for treaty verification.) Realizing an alleged total of five successful interceptions during the first series of seven tests, the technique used by the USSR was the "co-orbital" explosion carried out by a specifically designed orbital system within a kilometer-wide radius of the target. A second series of similar tests was undertaken between 1976 and 1982, based on the advocated need for the USSR to respond to future presumed ASAT capabilities expected from the US space shuttle then in construction.

The Soviet activity in the field was then perceived as highly intensive, and President Ford directed the start of an equivalent ASAT program that would ultimately take the form of an airborne missile launched from an F-15 *Eagle* airplane. After a few test launches performed in 1982 and 1985, a third launch ended up with the interception of a US satellite target directly hit by the so-called Miniature Homing Vehicle (MHV), the third stage of the ASM-135 Vought missile. Again, the program was officially phased out in 1988, in a context when the strategic and budgetary soundness of such projects was questioned.

In any case, this early history amply demonstrates that initial ASAT programs had been envisioned as being possibly part of the global arsenals from a military perspective if not from a political one. Only the key role played by spy satellites in the mutual nuclear deterrence prevented weapons in space from becoming operational during the Cold War. This did not prevent national R&D projects to develop, paving the way for possible future threats in space.

A Generic List of Possible (Intentional) Threats in Orbit: Assessing Offensive Realities of Today

In today's completely renewed strategic context, these early antisatellite efforts have regained some momentum. Early programs have clearly served as a basis for more sophisticated projects allowed by technical advances, while new research domains seem to have emerged. The analysis of over more than two decades of R&D efforts lead to the following list of existing R&D orientations, possibly leading to actual space weapons:

- *Kinetic energy weapons* (KEW) implying a physical effect on the target, either by direct impact (so-called "hit-to-kill" techniques) or nearby explosion creating killing debris (such as in the case of the co-orbital Soviet systems)
- *High-altitude nuclear weapons* (EMP) creating ionization and/or electromagnetic effects on objects in the affected zone
- *Directed energy weapons* (DEW) mainly using laser or microwave techniques depositing energy on the target

Obviously other kinds of threats on space systems exist such as electronic warfare weapons (EW) using jamming techniques rendering communications impossible, or cyberattacks. Exactly like in the case of ground-based interceptors, such threats do not necessitate the use of space platforms to be effective. For this reason, such threats have not been treated as a key issue in the context of this chapter, as they do not define per se a threatening "space system." However, they shall not be discarded as their reality is largely tangible today as it will be explained further below.

- *Kinetic energy weapons*, while simple in their principle (physical collision), do not use simple techniques. They imply the use of maneuvering satellites as well as the mastering of precise "*rendezvous*" techniques, the least to achieve in case of "*hit-to-kill*" weapons! This can be related to techniques implemented by a number of existing systems, going from experimental surveillance satellites (or so-called "inspector" satellites) used, for example, to picture other orbital systems (such as in the case of the US XSS 11 and 12 or the Chinese SJ-12 or SJ-06F systems), to the European *automated transfer vehicle* (ATV) used for service and precise docking with the International Space Station (ISS). All these systems have in common highly maneuvering capabilities as well as precise terminal guidance systems allowing effective orbital "*rendezvous*." Mastering such technologies would theoretically allow developing kinetic energy ASAT. Protecting any satellite against the kinetic effect at orbital speeds becomes virtually impossible with pellets more than a few centimeters in size. As a matter of fact, protecting any satellite against a kinetic threat is almost paradoxical in itself. Satellite architectures are indeed based on the use of as light materials as possible involving some level of fragility. This is the case for satellite buses or for on-board solar arrays. "Armored" space systems are then hardly feasible and in any case would increase

cost at all levels, from development to launch. Only some level of physical protection against small-sized debris (in the millimeters scale) can reasonably be applied nowadays.

However, if they can represent deadly threats, KE techniques remain highly costly in terms of energy (most notably when changes of orbits would be needed for performing an intercept) and, in a more sensitive manner, would create more debris that would add to the already rather congested orbital traffic. For sure, creating more debris would not account among the most preferred offensive strategies for most of the spacefaring countries whose space systems rely on an undisturbed and clean orbital space. Nations that do not intensively use space might possibly be less deterred from such actions.

- *High-altitude nuclear explosions* would make use of a nuclear bomb sent at an altitude of a few hundreds of kilometers with the objective to create highly intensive electromagnetic disturbances for Low Earth Orbiting (LEO) and even geostationary (GEO) objects. Cold War years were soon followed by the fear of an increasing nuclear proliferation that would make such a possibility more probable. Such an attack could indeed have an enormous effect on the whole activity in space, with, in the first place, the possibility for the attacker of annihilating a number of military systems precisely destined to warn against nuclear attacks, such as early warning systems, Earth observing, signal interception, or strategic communication satellites. In such a situation, most of the non-protected space systems would also be destroyed.

  Major studies (such as the HALEOS study published in 2001 under the auspices of the U.S. DoD Defense Threat Reduction Agancy - DTRA) have shown that, compared with a terrestrial explosion, electromagnetic effects of a nuclear charge in space might be increased leading to potentially devastating impact beyond the only targeted orbits with short-term effects on the propagation of radio and radar waves, and longer-term effects involving the permanent excitation of Van Allen belts, with even the possibility of creating new magnetic belts resulting from the sudden expulsion of charged particles.

  While ionizing effects would be specific to such explosions, other effects, such as electromagnetic effects, would be no different from those created by *directed energy weapons* (DEW) using high-power microwaves (see below). As a consequence, protecting any system against such threats would mean protecting it partially from a major consequence of a high-altitude nuclear detonation. In other terms, the main characteristic of such a nuclear threat would remain its “nondiscriminatory” effects on the whole orbital population. In any instance, such an attack would mean that a situation of war would preexist. This makes the use of nuclear attack clearly different from other intentional actions that might take place in more ambiguous scenarios or even in a covert manner.
- *Directed energy weapons* (DEW) are sometimes perceived as presenting a coming threat for space systems. Indeed, this threat is theoretically characterized by some level of intensity leading to likely modulated effects on the target. It can be

considered that DEW may have basically three classes of effects ranging as follows:

- Level 1: *A jamming effect*, i.e., time-limited disturbance of the satellite functioning that ceases when exposure to the weapon is over
- Level 2: *A disruption effect*, i.e., permanent disturbance (without definitive destruction) requiring an external intervention or reset
- Level 3: *An annihilation/destruction effect*, i.e., definitive disruption requiring an external replacement or repair at best. (This subjective scale can be paralleled to what has been almost theorized, or at least symbolized, in some US Air Force doctrinal documents using the infamous "5 Ds" to materialize the scale of gravity of any space attack: "***D*** *eception*, ***D*** *isruption,* ***D*** *enial*, ***D*** *egradation*, ***D*** *estruction*." See USAF (2004), Counterspace Operations, Air Force Doctrine Document, 2-2.1.)

DEWs may have different effects according to their domain of functioning: For example, an intense laser ray has a thermomechanical effect on any material and as such can neutralize or destroy sensors or even some structures. By contrast, a microwave weapon would not have any thermal effect but would produce instead a high-power electrical effect on electrical components, whether directly or indirectly. Low-level components such as receivers or some class of sensors would prove particularly vulnerable to such threats. As envisioned by largely publicized projects very early on (such as the US Space-Based Laser project), equipping space platforms with powerful lasers for ASAT kind of activities might be theoretically possible with the objective to overflow or even destroy targeted sensors. However, aiming at sensors might not be an easy task, with the additional possibility of the development of self-protection devices for the most sensitive satellites.

The literature has frequently referred to powerful lasers in orbit, mainly inherited from the early R&D experiments engaged during the Ronald Reagan years under the auspices of the United States, so-called Strategic Defense Initiative (SDI) often dubbed "*Starwars*." (In this respect, it must be reminded that, at its apex, one of the several versions of this project was envisioning the deployment of many space and ground-based laser systems, possibly relayed by orbiting mirrors in order to destroy reentry nuclear heads. This complex network of sensors and effectors was considered as an addition to some more conventional 4000 intercepting "hit-to-kill" missiles or even satellites.) Laser-based ASAT developed under such concepts would be much more powerful with the objective to bring about mechanical destructions on the structure itself of space systems, most notably on deployed solar panels. Obviously, the development of such an armament would require much more energy generation that would make their development very problematic given the usual constraints applied to any space systems (size, weight, reliability). It is highly probable that these many technical constraints have largely put into question the development of such systems, even if it is probable that more or less secretive R&D has not ceased in this area. Following this logic, powerful microwave systems may represent a more threatening technology from an operational point of view than space-based lasers.

What Vulnerability, in Which Context? Very Different "Defensive" Situations

Of course, any offensive weapon will focus at the main vulnerabilities of spacecrafts. These vulnerabilities are usually related to support functions such as:

- Attitude control
- Tracking and telemetry
- Thermal management
- Power management

The dysfunctioning of any of these technical functions would generally mean a shutdown of the entire system in short or longer term. As a result, the attack modes may be very diverse, whether they involve the destruction of the solar arrays, the thermal increase of the satellite structure, or a cyber intrusion in automated management processes.

In addition, the vulnerability of any spacecraft can vary quite largely considering their very nature, the applied management processes, and even the very mission it has to fulfill. As an example, telecommunication satellites are controlled by multiple operators, private or public, which sell their services to many customers. In this particular case, many motivations can exist for attacking the space system, from a hostile action against a specific customer to a more "wide-range" terrorist-like attack. This means that the ways and means used for attacking the "satcom" function can be very different from an action to another, implying the need to protect many dimensions of a complex system. (Obviously, the uplink remains the targets of choice for any action against the satellite itself.)

As for the navigation satellite, their systemic redundancy makes them less an easy target. In this case, jamming may be used but this time with local effects, as it has been sometimes the case during the recent conflicts using GPS-guided munitions. In the case of Earth observation satellites, in addition to their highly critical pointing and control systems, their sensing payload and their downlink communication systems appear as high-value potential breaches. This vulnerability is indeed increased by their relatively few numbers and by the accessibility of the Low Earth Orbit (LEO) they usually make use of. Last but not least of this non-exhaustive list, the weather satellites, while mainly on the geostationary orbit, may also be vulnerable due to the reliance on the good functioning of their sensors as well as on their communication downlink capacity. It is obviously reinforced for those satellites that orbit on LEOs.

The Notion of "Space Threats" and Its Relevance for the Security of Space Activities

As just shown above, the notion of "space threats" as strictly defined by space systems posing a threat in orbit might not reveal itself as the most urging issue to tackle. Indeed, most of the space systems that might be considered as potential offensive candidates seem to remain fairly confined to the prospective horizon. From

a technical standpoint first, using space systems as offensive weapons is not a simple operation. It involves relying on very demanding systems (in terms of sensing, maneuverability, energy management, cost, etc.) that may not make them so easy to produce and use. From an operational point of view also, this complexity may not be what a military user is looking for, notwithstanding the fact that, in the case of using offensive KEWs, the consequences of any attack will make no discrimination in the end between the victim and the attacker. For this reason, and from the policy perspective, it seems reasonable to put into question the very relevance of "threats in space" as a central notion for building the core of the future of space security. For sure, such a view does not imply that the international community should not pay attention to these developments. On the contrary, the fact that such techniques might be used one day should trigger a widespread awareness that in this field, earliest actions against the development of such weapons will be the most efficient. But in parallel, the rather prospective nature of these kinds of threats must not lead space-leading countries to underestimate the importance of other sorts of threats that may be much more meaningful on the shorter term. A brief (non-exhaustive) list of such threats may be recalled.

Ground-Based ASAT Tests

The most recent ASAT tests performed in 2007, 2008, and 2019, respectively, by China, by the United States, and most recently by India provide a good example of the practicability of and efficiency of ground-based ASAT missiles. As mentioned at the beginning of this chapter, the first one performed by China in January 2007 destroyed a decommissioned Chinese weather satellite on an 800 km circular orbit. A little bit more than 1 year later, the United States did hit a lower orbiting military satellite (246 km) with the stated goal to prevent an uncontrolled and dangerous reentry. In the first case, the interceptor used was a modified SC-19 missile, while the US military used the SM-3 sea-based intercepting missile developed for ABM purposes. Obviously, the proximity of anti-ballistic missile research and ASAT interceptors has been clearly apparent in all cases. While not completely known to date, the interceptor used by India has been officially acknowledged as a "DRDO's Ballistic Missile Defence interceptor (. . .) which is part of the ongoing ballistic missile defence programme" (Idem). It must also be recalled that China did several allegedly ABM high-altitude related tests in the aftermath of the 2007 ASAT experiment.

Even if it must be recalled that the targets were mainly cooperative and their trajectory well is known from their "attackers," these three cases have however amply demonstrated how much mastering space interception from the ground has become accessible to the most prominent ballistic and space powers.

Alleged Risks of "Cyberattacks"

Another type of risks, the "cyberattacks," has been alleged as becoming a major cause of concern for space systems. Cyberattacks can indeed take many forms and

affect many elements of the entire space and control system. Tracking, telemetry, and control networks can be subject to such cyber-threat with the impossibility to transmit reliable data for the control of the satellite platform. As a consequence, any satellite can virtually be taken over by a non-authorized user who can force a system shutdown or a wrong maneuver leading the system to put itself in a safe mode or in any other uncontrolled mode. In theory, such a takeover can be implemented via cyber intrusions in the command center or through key ground stations. Awareness about the possibility of such attacks has increased over the recent years. In 2001, a NASA audit report pointed out that "six computers servers associated with IT assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable." (The report goes on blaming that "moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA's operations." Source: NASA (2011).) These conclusions have been largely commented and have motivated the adoption of unprecedented protection measures for the Agency space systems.

A few recent cases have sometimes been cited that seem to sustain this assessment:

- Some reports have claimed that the German X-ray satellite ROSAT (made famous recently due to its uncontrolled reentry during the night of October 22–23, 2011) had been targeted in September 1998 by a cyberattack leading it to wrongly orient towards the Sun, ultimately causing its shutdown. This "wrong maneuver" (the cause of a loss of the satellite sensors) is reportedly related to a cyberattack carried out against computers of the Goddard NASA Center as unveiled in 1999 by one of the specialists in charge of the center computer services. At this time, the attack perpetrated against the X-ray department of the center was attributed to a Russian origin. However, those facts have never been confirmed, just a "troubling" coincidence between the move of the satellite and an intrusion in the computer system having been officially mentioned by the inquiry.
  Another satellite, INSAT-4B-S, this time a telecommunication satellite belonging to India has been mentioned as having been affected by a cyberattack (*Stuxnet Worm*) that would have caused a severe loss of power, ultimately leading to reduction of the telecommunication capacity of the satellite by more than 50%. (Again, this case has not been fully acknowledged, yet some other hypothesis (supported by ISRO) points out the loss of one of the solar arrays of the spacecraft. No official position about the incident has been confirmed up to this day.)
- Other examples have been cited in draft U.S. Congress reports citing interferences having affected the Earth imaging Landsat-7 satellite at least twice in 2007 and 2008, while another NASA EO satellite, TerraAM-1, experienced the same disruptions in 2008, for more than a single day in one occurrence. More recently, the U.S. National Oceanographic and Atmospheric Administration (NOAA) is reported having suffered a disruption of its Satellite Data Information System due to a severe hacking incident in September 2014. This implied for the Agency being denied sending weather forecast data for 48 h. (These episodes are

mentioned in Lewis (Patricia), Livingstone (David), "Space, the Final Frontier for Security," Research Paper, Chatham House, September 2016, p. 10. See also 2011 Report to Congress of the U.S.-China Economic and Security Review Commission, pp. 215–217 (https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf).) Some other attacks occurred on NOAA satellite in October the same year, with press reports about Chinese hacking attempts. (See "Chinese Hack U.S. weather system- satellite network," Washington Post, 12 November 2014.)

Of course, another more generic risk is represented by a cyber intrusion in the information chain itself (data collection, processing, and dissemination) without affecting the satellite itself. This type of attack, even if indirect, may have consequences as serious as if the space segment itself was the target, for example, ending up with wrong data, unreliable imagery, and false alarms. While targeting only information, this type of intrusion can barely be deterred by strictly "space segment-oriented" defensive strategies and doctrines.

Cyberattacks will probably account for the most preferred offensive strategies when the objective will be to disrupt an entire "space system," especially when they are old generation, i.e., not protected against the latest software offensive devices. Here again, the capability to detect the origin of the attack and to attribute its responsibility will be the key for an effective deterrence strategy. At this level, there is no magic for space systems, and this type of vulnerability is essentially linked to a domain that remains partly external to the space sector itself.

The General Vulnerability of the Ground Segment

More generally, the ground segment represents a key node for ensuring the functioning of any space system. Losing the ground segment necessarily means losing the space segment. In theory, the consequences on the long term might be less definitive than when a spacecraft is destroyed, as regaining control on the operation of the space system might be possible once the functions of the ground segment have been recovered. Hence, losing the control of the ground segment might be considered as a reversible situation and might not imply the same kind of strictly deterring positions as in the case of the space segment.

However, the border between both situations may sometimes be very thin, as taught by a case occurred to Russian satellites more than 10 years ago, in May 2001. As reported at that time, a fire destroyed almost completely a main control station leading to a total loss of communication with four military early warning satellites placed on a highly elliptical orbit Podvig (2002). Only one satellite has been recovered after a while, the three others having derived well beyond their nominal position. Those remained well out of reach by their dedicated ground segment. This "ground" damage has then become irreversible for the space segment itself. It may even include risks for other spacecraft, proving at this occasion that the safety management of satellites may be key in collective space security.

Here again, protecting the ground segment against attacks or hostile actions does not directly imply the protection of the space segment only. It may involve some level of "systemic" thinking, some redundancies (ground and space), as well as some parallel hardening techniques (e.g., against high-power microwave devices or even to prevent possible EMP effects). In addition, the adoption of degraded modes must also be considered for any key node on the ground. It is important to note that such measures must apply to both military and civilian satellite owners to be fully efficient.

The Case of Orbital Hazardous Events: The Example of "Zombiesats"

A contrario, from April 2010 to January 2011, Intelsat, the largest telecommunication satellite operator, has lost control over Galaxy 15, one of about sixty satellites composing its geostationary fleet. This spacecraft has derived over a large portion of the geostationary orbit without offering any possibility for being recovered during that 8 month long time. This event has had a double consequence:

- An increased collision risk affecting the whole community of the satcom users, civilian, and military.
- A powerful jamming of satellite telecommunications as Galaxy 15 has kept on emitting at full power during the whole period of time. One of the most documented consequences was the loss of WAAS (the US regional GPS *Wide Area Augmented System* for improved satellite navigation) in Alaska.

The control of this satellite (quickly nicknamed "zombiesat" in the large amount of literature devoted to this case) has finally been recovered in January 2011 by Intelsat. However, this case has amply shown what kind of disturbances such an event can create with the necessity for operators to avoid possible collisions and interferences. (For example, it has been reported that, at this occasion, SES, the second largest geostationary satellite operator, had to proceed with many very precise maneuvers around some of its strategic orbital positions.) It shows how much non-intentional actions can also present serious threats to space security that do not clearly relate to deliberate actions. There may be a specific vulnerability in face of such "zombiesats" on the geostationary orbit due to the vicinity of the satellites around some key orbital positions. This must be taken into account as a complexity factor of the collective space security, as this makes disturbances rather quick to produce, intentionally or not, both for civilian and for military systems. It must be noticed that operators have seized the importance of such potential developments and have chose to share their knowledge by setting up a common database allowing them fostering early and precise coordination when needed. (Via the creation in 2009 of the Space Data Association, based on the Isle of Man. Obviously, considering the wealth of information contained in those databases, such a private initiative cannot be without consequences on the general management of international relations in space.)

The Jamming of Space Telecommunication from the Ground

Of course, last but not least, the simple jamming of space telecommunications by using ground-based devices must also be evoked in this list of "indirect" space threats. One of the most recent Iranian episodes (spring 2009) can be quoted as the Iranian government has decided to jam two satellites (*Hotbird 6/8 W6*, *Eurobird 9A/2*) managed by Eutelsat, one of the two major European telecommunication operators. The goal was then to prevent the broadcast of information perceived as contrary to the Iranian regime interest. The cost to access such technologies is relatively low at the level of a government, and these interferences remains sometimes hard to detect when they occur and in any case highly difficult to prevent. A contrario, the example quoted here, has shown that, for a time, operators themselves had been dissuaded to broadcast the controversial information (BBC and VoA notably).

All these examples show clearly that direct threats on space systems, as evoked in the first part of this chapter, do not represent the sole source of possible security breaches. They may not even appear as the most probable cause of space insecurity, at least for the short to middle term. The difficulty remains both the attribution of responsibilities and, more difficult even, the establishing of the intentional nature of any catastrophic event. Any questioning about the setting up of international regulation, whatever their form, or of some sort of "space deterrence" must take this complexity into account.

Some Effects on Space Deterrence: Protecting Against What Threat and/or Vulnerability?

In light of these possible developments, thinking about future threats on space systems means thinking about the probable nature of those treats as well as the kind of possible enemy using them. At first glance, the most developed spacefaring nations have used their space assets in a strongly asymmetrical context in which only a few countries were able to use similar orbital systems, possibly in a hostile way. However, it is probably necessary to take into account other kind of threats that countries on the verge of becoming space powers might likely use in case of political or military showdown.

Generally, deterring any threat to develop against space assets will imply a large appreciation of this diverse nature of possible threats, whether intentional or non-intentional. This approach will probably go through a few preliminary protective postures and actions:

- **Establishing the capability to attribute an effect to a certain cause:** This capability, addressing either intentional or non-intentional threats, relies on very specific technical capacities whether they aim at monitoring LEO or GEO orbits. But, in parallel, according to the nature of the threat in orbit (KEW, DEW, Jamming, etc.) or from the ground (using the same kind of techniques in a different way), very different means will have to be implemented to protect the

satellites. Some strategies may envision having on-board devices allowing detection (and characterization) of laser attacks, for example. This may bring about a certain deterrent effect against an adversary who would rather have acted stealthily. Some other will possibly envision satellites more directly dedicated to detection and inspection. Of course, ultimately, these "defensive" systems may appear in reverse as potentially challenging this quest for permanent capacity to attribute any event to a certain cause. Indeed, by definition, such protective devices would make use of technologies that may allow discreet and more offensive actions. This is not the least of the paradoxes that such efforts would imply.

- **Creating a "red line" against any attack:** Provided the cause of any event solidly established, the difficulty remains to establish a sort of "red line" beyond which military protective action would be legitimate. First, characterizing between the intentional or the non-intentional move will be key in determining the reaction of the "victim." There probably lays the most difficult issue to tackle when it comes to ensuring a comprehensive protective posture (including military) against any threat on space systems. It must be noted that even in the case of a recognized intentional action, the possible "graduate" nature of the hostile action (from deception to *destruction* to recall the "5 Ds" approach) may render difficult any decision about the nature of the counteraction itself. This aspect may be at the center of the current effort to establish "rules of the road." No doubt that it will also raise expectations about the resistance capacity of the next-generation space assets. This is the approach followed for the hardening of the electrical components, for example, with two (possibly contradictory) principles. Making well known that the considered system has been hardened while, at the same time, keeping any possible adversary in the impossibility to determine the methods and the techniques used, as well as the very level of this hardening.

Conclusions

In any event, the road towards limiting by principle threats on space systems in a significant manner will probably remain quite bumpy for a while.

At this stage, satellites have remained vested with a highly symbolic value that continues to put them at the center of the current strategic relationships. The latest events (comprising the March 2019 Indian ASAT test as well as the Chinese ASAT in 2007 and in a way the US-made satellite destruction in 2008) have shown that affirming this kind of capability was also a part of "deterrence" postures or "state communication policies." It is well documented that satellites will become smaller and smaller, more and more able while less and less costly. The generalization of smaller high-performance spacecraft (whether military or civilian), possibly "launched on demand," announces the beginning of a new era for which a new equilibrium will have to be found. These progresses, sometimes promoted through concerted national efforts, are also a part and parcel of the "equation" aiming at balancing the protective approach with bolder technology-led solutions that are

supposed to give an edge to the more advanced space countries. (Such as in the case of the US *Operationally Responsive Space* program, for example, even if this effort seems to remain in question nowadays.) Answering this question and finding a workable balance will determine the fate of our collective security against the threats on space systems as well as it will orient the future nature of a possible "space deterrence."

References

Baker D (1985) The history of manned spaceflight. New Cavendish Books, London

Caldicott H, Eisendrath C (2007) War in heaven: the arms race in outer space. The New Press, New York/London

Department of State (2009) Foreign relations of the United States, 1969–1976, vol E-3, documents on global issues, 1973–1976. United States Government Printing Office, Washington, DC

Gantz K (1958) The United States air force report on the ballistic missiles. Doubleday & Comp, New York

HALEOS, High-Altitude Nuclear Detonation against Low Earth Orbit Satellites (2001) Defense threat reduction agency briefing. http://www.fas.org/spp/military/program/asat/haleos.pdf. Accessed Aug 2012

McAllister WB (2009) Foreign relations of the United States, 1969–1976, volume E-3, documents on global issues, 1973–1976. United States Government Printing Office, Washington, DC

NASA (2011) Inadequate security practices expose key NASA network to cyber attack, office of audits, Washington, DC. For the complete audit document, see http://oig.nasa.gov/audits/reports/FY11/IG-11-17.pdf. Accessed 20 July 2012

Podvig P (2002) History and current status of the Russian early warning system. Sci Glob Secur 10:10–60

Schriever B (1957). http://www.af.mil/news/story.asp?id=123040817. Accessed Aug 2012

Stares P (1985) The militarization of space, U.S. policy, 1945–1984. Cornell University Press, New York

Stares P (1987) Space and national security. The Brookings Institution, Washington, DC

USAF (2004) Counterspace Operations. Air Force Doctrine Document 2–2.1. http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_2_1.pdf. Accessed Jan 2010