Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

Space Terrorism: A Historical Study

Cyprian Aleksander KOZERA
kozeracyprian@gmail.com (Corresponding author)
https://orcid.org/0000-0001-8620-9849
University of Warsaw, Warsaw, Poland

Paweł BERNAT
p.bernat@law.mil.pl (Corresponding author)
https://orcid.org/0000-0002-8150-9794
Polish Air Force University, Dęblin, Poland

Received: 14 December 2023 | Revised: 26 February 2024
Accepted: 06 March 2024 | Available online: 07 March 2024

Abstract

The rationale behind this article is to address a critical gap in research: the evolving threat of space terrorism. As space assets increasingly become integral components of both civilian and military security systems, their vulnerability to attacks escalates. The democratization of space weaponry, including advanced cyber technologies, signals an escalating risk to these space assets and their terrestrial infrastructure. This threat extends beyond traditional space powers to include non-state actors, such as terrorist individuals and groups or various proxy forces, who were previously considered marginal threats.
This paper aims to lay a foundational framework by providing a historical overview of terrorism and security incidents involving outer space assets, their cyber systems, and ground support structures. This compilation serves as a basis for a deeper, methodological, and systematic examination of the nature and implications of space terrorism.
In order to define the initial concept of space terrorism, this paper draws on an extensive literature review. The selection of security breach cases within the broad spectrum of the space sector was guided by their novelty, diversity, and relevance, of fering insights into the emerging phenomenon of space terrorism.

Keywords: space assets, space cybersecurity threats, space hybrid threats, space security incidents, space terrorism, space weapons

1. Introduction

It is often said that military strategists are always ready to wage the previous war. Consequently, it is rarely discussed in the Pentagon-like structures that a future armed conflict may not occur on the land, at sea, or in the air – primarily or at all. For many, outer space remains remote, inaccessible, and fictional. On the other hand, the progressive development of space technologies, their deployment and democratization, and their wide use for military and civilian purposes have made space assets important enough that outer space has been recognized by many states and transnational institutions as an environment of a potential armed conflict.

In 2019, the U.S. created a new branch of their armed forces – Space Force, which was established "to organize, train and equip the space forces needed to protect U.S. interests, secure freedom of action in the space domain (…)" (Department of the Air Force, 2023, p. 2). In the same year, NATO adopted the Space Policy, in which the Alliance declared space as an operational domain next to land, sea, air, and cyberspace (NATO, 2023). Neither China nor Russia have created a separate space branch of their armed forces but they restructured their militaries in 2015 in ways that addressed the growing need for space components. China established the Strategic Support Force (SSF) to integrate various strategic capabilities and functions previously carried out by several commands and units across the People's Liberation Army. Now, SSF consists of two divisions – the Space Systems Department, responsible for all space-related missions, including Bei-Dou constellation administration and intelligence, reconnaissance, and surveillance (ISR) services, and the Network Systems Department, for political, psychological, and information warfare (Nelson & Epstein, 2022).

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

In 2015, the Russian Federation formed Aerospace Forces by merging the Air Force and Aerospace Defense Forces (Harrison et al., 2018). Currently, the Russian Aerospace Forces are composed of three divisions: the Air Force, Space Force, and Air and Missile Defense Force (Ministry of Defense of the Russian Federation, n.d.).

Having recognized the importance of securing space assets, states with traditionally smaller space presence have also recently established, in various forms, space components, e.g. India – Defense Space Agency (2018), France – French Air and Space Force (2019), Iran – Space Command within the Islamic Revolutionary Guard Corps Aerospace Force (2020), U.K. – United Kingdom Space Command (2021), Spain – Spanish Air and Space Force (2022).

Among the main goals of the established space components is gaining space situational awareness (SSA) and creating defensive and of fensive means to secure their space assets and provide support (mainly satellite-related) for other forces in times of an increasingly tense geopolitical situation. However, irregular warfare threats, including space terrorism acts carried out by non-state, traditionally weak actors, have become gradually more dire. The argument here is quite simple: societies increasingly rely on satellite systems (and their ground infrastructure), and due to democratization, weapons (including cyber systems) become progressively more accessible, also for traditionally weak actors, including terrorist groups and individuals (lone wolves). Regardless of the reason behind the potential attack, the weapons used, and the organization behind the attack, the results could bear global consequences. This is especially the case with kinetic anti-satellite weapons (ASAT), which, after destroying the target, create large clouds of space debris (Schwartz et. al, 2021). This contributes to building up the Kessler syndrome in Low Earth Orbit (LEO) (Kessler & Cour-Palais, 1978), which, in turn, due to cascading collisions of space debris, may lead to partial or complete unusability of the orbit for generations (Bernat, 2020).

Still, the phenomenon of space terrorism, although already existent and perilous, is understudied and theoretically underdeveloped. Proper policy-making and development and deployment of countermeasures ought to hinge on an adequate understanding of space terrorism in all of its manifestations.

This article aims to bring together and report historical acts of terrorism, hybrid threats, and security incidents involving outer space assets, including supporting cyber systems and ground infrastructure. In order to qualify terrorist acts and security breaches as outer space terrorism, we broadly rely on previously coined space terrorism definitions. We will not, however, propose in this article a new conceptualization and definition of the phenomenon, for it requires a more in-depth and, hence, separate study. The rationale behind this research is to describe as many various attacks on space assets as possible and, on that basis to, later on, create an extensive conceptual framework of space terrorism useful for policy-makers and security practitioners.

2. Methodology and research methods

This article consists of five sections: (1) an introduction, (2) methodology and research methods, (3) a literature review of space terrorism definitions, (4) a discussion of historical space terrorism cases, and (5) conclusions. This structure reflects its ultimate goal, i.e., providing information on cases that might be qualified as acts of space terrorism, or, in other words, historical material for future, more systematic conceptual research on space terrorism.

In Section 3, which aims to delineate the concept of space terrorism theoretically, we carried out the literature review. There, we collected and synthesized previously proposed definitions of the phenomenon in order to gain a general notion of what can be accounted as space terrorism.

The main section of the article, Section 4, is dedicated to reporting on various cases of space terrorism in its various forms. The historical method was mainly employed for this task. We collected facts regarding generally conceived space terrorism from primary and secondary sources describing the attacks and incidents. The goal of this article, and thus our intention, is not to provide a complete list of such cases but to describe various ways in which non-state actors attacked the generally conceived space sector due to ideological reasons. Considering the relative novelty of the analyzed subject, we were particularly careful about verifying and falsifying our sources and eventually chose them in the process of a strict source quality evaluation, which included relying on at least two independent sources when possible.

3. The concept and definitions of space terrorism

Let us underscore that for the purpose of the leading argument of this article, we shall understand the phenomenon of terrorism as the use of violence, or a threat of it, aimed at political goals and executed by a non-state actor. It is, however, debatable if acts of violence directed against property (exclusively and without any hurt to human beings) should be considered terrorism and entail the same law enforcement response and legal consequences. In such cases, we may speak of political sabotage when no one is hurt, though property is deliberately destroyed for political reasons. Of tentimes, though, the group standing behind the act in question is a designated terrorist organization (guilty of terrorist acts), and the means they use, such as a bomb, constitute

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

an obvious and direct threat to human lives, thus, blurring the borders between an act of political sabotage and terrorism and making it very contextual. At this stage, we have also limited terrorism, and hence space terrorism, as carried out by non-state actors. The so-called state terrorism, which involves governments' "deliberate targeting of individuals that the state has a duty to protect" (Blake, 2009, p. 15) to invoke terror in the population, has been excluded from this study mainly due to the many objections to the actor-based understanding of terrorism. We lean towards Laqueur's approach, who argues (2003, p. 237) that "the very existence of a state is based on its monopoly of power," and therefore, it should not be understood as terrorism at all. We have also intentionally omitted cases of acts of terrorism, including sabotage, carried out by a state and targeting another state's space assets, which, as we believe, should be categorized as the grey zone conflict or a hybrid war that involves "the deliberate, multidimensional, and integrated use of various instruments of power" (Jordan, 2020, p. 3), including the military means.

It has to be stated, however, that the environment of outer space adds another variable to that equation. At this stage of space technologies development, and SSA limitations stemming from it, it is of ten difficult to determine whether a given malfunction or destruction of a satellite was caused by an attack or a technical defect, unintended collision with another active or defunct satellite, a meteorite or a piece of space debris.

As mentioned, the phenomenon of space terrorism, although posing a growing threat, has been understudied. It does not mean, however, that no reflection or conceptual analyses have been made on the subject. Based on the literature review, there are three definitions of space terrorism that attempt to address the phenomenon in its entirety but also its various manifestations. They will be presented below but will not be discussed or evaluated in this article (it will be carried out in a different study); they should be treated as a general starting point for the process of choosing the cases that might be initially qualified as space terrorism. The cases are described in Section 4 below.

According to Cain, space terrorism should be understood as "[a]n act of violence by one or more individuals or groups to prevent the development of a space settlement(s) and/or their aims including those of a spaceship or space station during Man's exploration of space" (Cain, 2016, p. 98).

Bernat and Posłuszna define it as "[a] purposeful act of destruction against human and/or material resources of space industry undertaken by individuals or groups out of ideological motivation, where space industry is understood as a sector of human activity dedicated to producing components that go into Earth's orbit or beyond, delivering them to those regions, and services related to these processes" (Bernat & Posłuszna, 2019, p. 32).

Mehmood and Ahmed propose understanding the phenomenon as "an act of violence or terror that targets space industry whether in space (such as space station, satellites, etc.) or on Earth (ground stations, rocket launcher sites, etc.) and particular individuals (astronauts) that will endanger human and material resources in space and Earth alike. These acts can be motivated by ideological factors that aim to target countries, and region as a whole since the world is increasingly becoming dependent on space technology" (Mehmood & Ahmed, 2021, p. 95).

4. Selected cases of space terrorism

The very first act of terrorism against space assets might have been the threat of the Palestinian terrorists in the turbulent times of the Munich Olympic Games massacre back in 1972. The group responsible for the brutal killings of eleven Israeli athletes at the Olympic Village and airbase in Munich, Germany, was an of fshoot of the Palestinian organization Fatah (itself a sub-group of the Palestinian Liberation Organization of Yaser Arafat) and called itself the Black September (*Aylūl al-Aswad*). The Black September Organization proved infamously capable of conducting a sophisticated infiltration into the Olympic Village during the Olympic Games, broadcast live all over the world. On September 5, 1972, the Palestinian terrorists took the Israeli team as hostages virtually in front of the cameras and killed them the next day during a tragically botched rescue mission led by unprepared and uncoordinated German authorities. The world was shocked by the boldness and brutality of the Black September terrorists. Not surprisingly, when the U.S. intelligence agencies issued a warning about the Black September supposedly planning an attack on the Apollo 17 space mission, it was taken seriously.

The Apollo 17 space mission, planned for December 1972, was to be the final crewed excursion to the Moon. Due to the space program's significance, the spaceport's premises at Cape Canaveral were already tightly secured even without any articulated terrorist threat. Eugene Cernan, the commander of the Apollo 17 mission, wrote in his memoirs that the Chief of Security and Fire Operations at the U.S. spaceport at Cape Canaveral, Charley Buckley, was informed about the threat by the authorities and quietly tightened the security procedures and measures, though initially keeping the information away from the Apollo 17 crew (Cernan, Davies, 1999). The facility was already accustomed to threats – as Buckley recalled later – yet this one was different: "We had many threats (…) Most were in the form of bomb threats and such, but the one for Apollo 17 was different" (Schlom, 2001, p. 21). At a later stage, though, the crew was informed about the threat as it was assessed that the Black September most likely would not plan to attack the facility yet rather – following their infamous Munich expertise – take astronauts' families, children in particular, as

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

hostages. As a result, the families were granted low-prof ile security details. Additionally, Cernan recalls that the doors to the crew quarters were replaced with bulletproof ones, supplementary guards with automatic rifles were deployed, and helicopter-borne patrols were swapping areas adjacent to the port (Cernan and Davies, 1999; Schlom, 2001). The Cape facility was an impregnated fortress, and the crew's families were discreetly watched. The Black September threat, however, did not materialize, and Apollo 17 securely landed on the Moon and safely returned home.

The first act of terrorism against space assets and installations materialized only in the following decade. On the evening of August 2, 1984, a bomb exploded outside the Paris headquarters of the European Space Agency (ESA). Six people were slightly injured due to flying glass in the nearby homes, and the ESA building was seriously damaged. The building attacked was found painted with the red inscription "*War against War, A.D.*". Thus, the attack was attributed to *Action Directe* (French for "Direct Action"), an extreme left-wing group that had taken responsibility for several dozen bomb attacks and assassinations of mostly military and law enforcement of ficers and businessmen (NYT, 1984; Dartnell, 1995). Régis Schleicher, a member of the group, called ESA a "practical base to apply the imperialist strategy of domination of NATO and its enfeof fed flunkey, the French state," which therefore constituted a legitimate target in the eyes of Action Directe due to ESA's Ariane space launch vehicle program (Dartnell, 1995, p. 114). The attack occurred two days before one of the launches of Ariane 1 from the French Guiana – it had no serious ramifications for the project that successfully continues today as Ariane 6.

The first ever recorded act of "satellite terrorism", or politically motivated space sabotage, occurred back in April 1986. Surprisingly, it was perpetrated by a disenchanted Home Box Of fice (HBO) subscriber, John R. MacDougall. MacDougall was frustrated with the rate of his monthly subscription (USD 12.95) for the satellite T.V. and wanted to protest that. Being a satellite dish dealer and knowledgeable electronics engineer, he decided to override the HBO satellite signal with a protest message. He ran a successful test on the night of April 20, and then a week later, at 12:32 AM on April 27, MacDougall superimposed the following message for four and half minutes over the HBO signal (original spelling):

GOODEVENING HBO
FROM CAPTAIN MIDNIGHT $12.95/MONTH ?
NO WAY !
[SHOWTIME/MOVIE CHANNEL BEWARE!]

Captain Midnight's protest message was visible to the eastern half of the USA, possibly reaching several million people. The hacker was an amateur individual acting on his own behalf, his motive was political (a protest against private companies exploiting customers), the damage was minimal; and, as a result, he was not tried for terrorism, even though the act was dubbed "space terrorism" or more mockingly "video terrorism" (Forester & Morrison, 2007; Ewalt, 2013). From our perspective, however, it was the first case of a known satellite jamming incident and could have served more malicious purposes.

Towards the end of the Cold War, with the Soviet Union bleeding economically, the third round of the Strategic Arms Limitation Talks (SALT III) and Strategic Arms Reduction Treaty (START) coming into force, the space race lost its impetus. Soviet space launches started to steadily decline in the mid-1980s and reached their lowest point in 2004-2005 (Harrison et al., 2017). The end of the Cold War in 1991 was also an end to what we may call the First Space Age (Harrison et al., 2017). It brought an end to the competition between great powers in every domain, including outer space, altogether with some types of terrorist threats. Accompanying the global transformation, the phenomenon of terrorism changed with many radical left-wing and pan-nationalist Arab groups losing – with the ultimate fall of communism in Europe – a patron, support, safe haven, and sometimes even *raison d'etre*. So evolved the threat towards space assets in the 1990s – it became more a matter of intelligence agencies and amateur individuals rather than terrorist organizations. It remained a threat, though. At the same time, it became less ideological and more espionage, technology transfer or income-oriented – as may be exemplified by the satellite hacking on NASA and British assets in the 1990s – the transition period towards the Second Space Age.

In September 1998, ROSAT, a research satellite shared by Germany and the U.S., became inoperative due to a malfunction of unknown origin. Seemingly, some kind of an error caused its X-Ray telescope to turn itself directly towards the sun, resulting in its overheating and thereby damaging the critical optical sensor. NASA's press announcement declared that the satellite "had been accidentally scanning too closely to the sun" (Epstein & Elgin, 2008). However, according to Keith Epstein and Ben Elgin, Bloomberg and Business Week investigative reporters, an internal investigation led by Thomas J. Talleur, the most experienced cyber-security investigator at the Inspector General's of fice at NASA, suggested something strikingly different. Still classified, Talleur's report (Cyber Defense Project, 2021) entitled *Russian Domain Attacks Against NASA Network Systems* concluded that the incident was directly related to a remote intrusion into NASA networks at the Goddard Space Flight Center in the Maryland suburbs of Washington, a year earlier (Epstein & Elgin, 2008).

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

In May 1997, unknown hackers penetrated computers connected to satellites in the X-ray Astrophysics Section of the Goddard Center. The infringement was not discovered for a year, during which the hackers exported massive amounts of data. According to the still classified Talleur's report: "[h]ostile activities compromised [NASA] computer systems that directly and indirectly deal with the design, testing, and transferring of satellite package command-and-control codes". Thus, intruders gained access to critical information allowing them to control the satellite. Furthermore, as the report continued: "[o]perational characteristics and commanding of the ROSAT were sufficiently similar to other space assets to provide intruders with valuable information about how such platforms are commanded" (Epstein & Elgin, 2008). In other words, the perpetrators could not only operate the ROSAT, but they also learned how to command every other U.S. satellite. Hence, plausibly, the malfunction of ROSAT a year later might have been the knowledge acquired successfully put to the test.

According to the following investigation by NASA, FBI, and the U.S. Air Force Of fice of Special Investigations, the data was transferred overseas and then to dozens of IP addresses associated with computers near Moscow. It was further suggested that the group responsible for the breaches was run by the Federal Agency of Government Communications and Information – a Russian signal intelligence agency. The Russian intelligence connection could not be independently verified. However, well into his retirement, Talleur re-affirmed his certainty about the origin of the attacks, saying in 2008 that "it's been state-sponsored for 15 years" (Epstein & Elgin, 2008). With such a knowledgeable, organized, and sophisticated case of hacking leading to a hub near Moscow, it would be indeed a striking coincidence had it not been the Russian intelligence community behind this operation.

In April 1998, a less prof essional but just as serious attack targeted the Pentagon. A group of hackers going by the name of "Masters of Downloading/2016216" admitted to breaching the Pentagon's computer defenses and accessing sof tware coordinating satellite-based Global Positioning System (GPS) and subsequently threatened to sell the sof tware to a terrorist organization or a foreign government. The group claimed that the incident occurred in October the previous year. The Pentagon admitted that an intrusion into "a telecommunications backbone for the Defense Department" had occurred, but downplayed the incident, claiming that the stolen sof tware did not contain any classified information. The group consisted of 15 young adults ranging in age between 19 and 28 and coming from the U.S., Great Britain, and Russia (Stout, 1998; Yale Daily News, 1998). In a later interview, they boasted of being capable of accessing computers that would allow them to control a satellite (CBS News, 1998).

A year later, a similar incident on the other side of the Atlantic threatened British military space assets. According to British news outlets, sometime in the middle of February 1999, the British aerospace authorities observed that one of its four military communications satellites, known conjointly as the Skynet, had altered its course. Shortly thereafter, an anonymous message was issued requiring a ransom payment for restoring control over the satellite and cessation of further interference. Police admitted that an investigation was being conducted, and the Ministry of Defense initially declined to comment (Chicago Tribune, 1999; Grossman, 1999). However, according to the Telegraph, the satellite was not moved at all, but rather the hacker "changed the characteristics of channels used to convey military communications, satellite television and telephone calls". The news outlet reported that the Scotland Yard spokesman admitted that a computer hacker was being investigated, who was "believed to be targeting several different international sites, some of which may include military installations," and was being tracked to the South of England. He supposedly had managed to intercept the link between Skynet's control center and the ground station (Telegraph, 1999). Furthermore, it is believed that a "recipe" for such an attack had been circulating among the hacker community for several years already and had been published by a British citizen who later escaped to Japan to avoid prosecution for his hacking activity (Telegraph, 1999).

The outcome of the incident is unknown, yet considering the early days of the internet and the lack of serious security systems in those days, it is highly likely that the British authorities were discredited by a group of amateur and audacious hackers who acted for the sake of financial gain. Another scenario is that a criminal ring like the one (or the very one) attacking NASA wanted to increase its operational budget with this attack, or it was an insider who also needed an extra quid. The lack of any further news about the incident nor criminal prosecution of the perpetrators suggests that it ended with a negotiable solution.

On the other hand, Duncan Campbell, a British investigative journalist, claimed in May 1999 on the pages of the Guardian (Campbell, 1999) that the incident did not happen at all, undermining revelations by Reuters, the Telegraph, and other news outlets. This would suggest that the British press agency and the media invented the news, were mistaken by their sources, and the police and Scotland Yard investigations never existed – such a scenario is, however, less plausible. Furthermore, the lack of serious security systems exposed in later hacking incidents only validates the likelihood of the Skynet satellite hijacking.

Since the 1999 incident was an income-oriented act, without any known political motive, and no damage was caused, it cannot be considered terrorism. Together with the HBO and ROSAT cases, it was, however, one of the very first acts of known remote interference in satellite systems. Considering that the Skynet cyber-attack could have led to the destruction of multiple satellites (through a collision, for instance) and technically could have been perpetrated from a home computer by a single or group of individuals – it underscored the fragility of the system and its vulnerability to what today we would call hybrid threats. Furthermore, the consequences of such a course of event would not only have been disastrous for the space project, with a hundred million pounds lost in damages, but also a terrible blow to the state's prestige and a serious hindrance to its intelligence and

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

military operations run through the Skynet system. It would, therefore, have been a very cost-effective attack on a budget with an immense return on investment.

The lack of proper security at the key IT components of space systems in those days was ultimately exposed by a 15-year-old, Jonathan J. James from Miami. Between June 29 and 30, 1999, he broke into 13 NASA computers at the Marshall Space Flight Center in Huntsville, Alabama. The U.S. Department of Justice claims that he "downloaded proprietary sof tware from NASA valued at approximately $1.7 million", including the sof tware that "supported the International Space Station's (ISS) physical environment, including control of the temperature and humidity within the living space". Furthermore, "[a]s a result of the intrusions and data theft, the NASA computer systems were shut down for 21 days in July 1999" (Department of Justice, 2000). The juvenile supposedly claimed in his interview for an American T.V. program, "The government didn't take too many measures for security on most of their computers. They lack some serious computer security (...)" (PBS Frontline, 2000). In the following years, computer network exploitation (CNE) attacks would become a major threat to space systems and installations.

The presented cases exemplify just a couple of series of attacks and breaches to which space agencies, and NASA in particular, were subjected in the following years. They were not terrorist in nature and, in many cases, led by a state actor and realized through a non-state proxy. They constitute rather a typical case of hybrid threats to space assets that have only been increasing in occurrence. Moreover, these cases underscore that such malicious attacks can be performed by a non-state actor, even a mere teenage individual, paving the way for possible terrorist attacks against satellites and space systems in the future.

The beginning of the twenty-first century saw a significant growth in space-related security incidents, mainly cases of satellite jamming and hijacking, CNE and APT cyber-attacks against air and space assets and facilities – with non-state actors becoming more and more active in this domain. Such incidents involved notably insurgents in Iraq and irredentist and terrorist organizations in Sri Lanka (Liberation Tigers of Tamil Eelam, LTTE, aka the Tamil Tigers) and in Israel/Palestine (Hamas).

Sometime in early 2005, Tamil Tigers of Sri Lanka took over a U.S. commercial satellite and through it broadcasted Tamil irredentist propaganda over the Indian subcontinent: the National Television of Tamil Eelam and Pulikalin Kural ("Voice of Tigers") radio transmissions. A transponder of the Europe Star 1 satellite (later known as Intelsat 12) exploited by the LTTE had not been in use, though it had been pre-configured to retransmit the signal that would reach it. This loophole was exploited by the LTTE "satellite pirates." At the time of the incident, the satellite belonged to PanAmSat, a company later acquired by Intelsat Ltd. in 2006. Having 52 satellites in geosynchronous orbit, the US-based Intelsat Ltd. was, at the time, the world's largest provider of fixed satellite services. Despite the fact that the hijacking was made public by a local newspaper and should have been known to Intelsat, the company was not able to neutralize Tamil Tigers' broadcast signal for a year. Finally, this act of 'satellite piracy' lasted for two years until Intelsat decided to shut the transponder down in April 2007 (Daly, 2007; Jayawardhana, 2007; McCoy, 2007). The incident was emulated by Hamas in 2012 and 2014 when the group hijacked the Israeli channel and broadcasted their own message accompanied by threats towards the Israelis (Leyden, 2014).

In 2009, it was revealed that the Iran-backed Shi'a insurgents in Iraq possessed recent feeds from the U.S. Predator drones. It turned out that the militias, founded and trained by Iran, used a Russian commercial sof tware called SkyGrabber. The program which cost barely USD 26 allowed militants to download live feeds from the U.S. drones operating overhead. The program was of ficially conceived to download free and legal content from the internet but, in fact, served to pirate legal content from the internet. Its capacity to intercept the military drone feed might have been an accidental discovery by the Iranian intelligence passed on to their Iraqi proxies. Such vulnerability on the part of the American UAVs was believed to have been known to the U.S. at least since the Bosnia War in the 1990s, yet it was decided that an irregular actor would not be in possession of the knowledge nor the tools allowing them to exploit their vulnerability (Gorman et al., 2009). It underscores the complacency of state actors towards threats from their asymmetric and non-state foes, the empowering potential of nexus between non-state and state actors, and at the same time exemplifies the growing capacity of irregular actors in the high-tech environment.

In the very same theatre, during Operation Iraqi Freedom (2003-2011), U.S. military communications beamed through commercial satellites were jammed on several occasions by local Iraqi insurgents (Rausch, 2006). Moreover, many other cases of satellite signal jammings were self-inflicted due to the multiplicity of signals and jammers. In 2015, there were at least 261 satellite jamming incidents, and virtually every case was due to a self-jamming incident involving interference of the U.S. own transmissions, radar or radio (Freedberg, 2015).

GPS jamming is even easier and widely available. It was exemplified in 2013 by a prof essional driver who wanted to hide his movements from his boss and installed a GPS jammer in his car to thwart the GPS tracker. The commercially available device for less than USD 100 was strong enough to interfere with GPS-based guidance systems tested at the nearby Newark airport (CBS News, 2013).

Satellite interference, piracy, accidents, and hostile attacks have only been increasing in numbers as the exponential growth of satellites orbiting the Earth is accompanied by proportional growth of satellite incidents (Manulis, 2020). Meanwhile, non-state actors and state proxies are becoming more and more skillful in targeting space assets.

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

In March 2022, NB65, a hacker group linked with the Anonymous movement claimed to have shut down the Control Center of the Russian Space Agency 'Roscosmos' causing interference with Russia's vehicle monitoring system. Their actions were deemed motivated by the Russian unlawful invasion of Ukraine the preceding week (Anonymous TV, 2022; Swinhoe, 2023). Moreover, it was not an isolated incident. In October 2022, a pro-Ukrainian hacker group, One-First claimed to have breached Gonets, a Russian satellite communications network operating in LEO, and deleted the database. Gonets was reportedly used by the FSB, the Federal Security Service of Russia (Petkauskas, 2023; Swinhoe, 2023). More recently, in June 2023, hackers were involved in another disruption of a Russian satellite communications provider, Dozor-Teleport. The company is believed to be a provider for Russia's Ministry of Defense, FSB, Gazprom, Rosatom, and other Kremlin-related institutions and companies. It happened during the tumultuous week in Russia when the Private Military Company (PMC) Wagner Group revolted against Moscow. The hackers claimed to have inflicted damage on several satellite terminals and compromised, as well as deleted, sensitive data housed on the corporation servers. To prove that, they uploaded 700 files, comprising documents and pictures, into a leaked website and their Telegram channel. The hackers claimed to be affiliated with the Wagner Group. Whether their affiliation is true or not remains debatable, though the damage to the company has been real and documented by several sites analyzing the web traffic – the Dozor-Teleport servers were down (Anonymous TV, 2022; Swinhoe, 2023; NetBlocks, 2023; Madory, 2023; IODA, 2023).

From the state's perspective, these incidents were not critical, and the damage was even more negligible. They exemplify, however, the increasing capability of non-state actors in tech-savvy operations involving space assets, especially in the context of Roscosmos head Dmitry Rogozin saying in the wake of the February 2022 attack that "of flining the satellites of any country is actually a casus belli, a cause for war" (Bender, 2022; Reuters, 2022). With ideologically motivated hackers acting independently, non-state actors acting as state proxies, and security services only trying to keep up with their civilian and more agile counterparts, the lines of responsibility are becoming blurred, and it is challenging to assign responsibility clearly. The plausible deniability of hybrid warfare extends to the cyber-space domain with its full force.

Last but not least, non-state actors have not only damaging potential but are also capable of using space assets constructively for their own gain. Notably, the PMC Wagner Group was capable of 'hiring' its own spy satellites. In November 2022, the group signed a contract worth USD 30 million with a Chinese satellite provider, Beijing Yunze Technology Co Ltd, acquiring satellite imagery to increase their intelligence capabilities. The Chinese were providing the Russian mercenaries with access to two high-resolution observation satellites (JL-1 GF03D 12 and JL-1 GF03D 13, operating at an altitude of 532 km above the ground) and their on-demand imagery. The imagery reportedly concerned not only Wagner's battlefields of Ukraine and Libya but areas of interest in the Central African Republic, Mali, Sudan, and even the Russian Army headquarters in Rostov-on-Don (seized during Wagner mutiny) or Grozny. Thus, a mercenary group acquired highly sophisticated intelligence capacity typically associated with state actors. Furthermore, the sensitivity of the deal means that it may have been known to the Chinese government in Beijing (France24, 2023). Thus, contrary to the intuitive belief that only states could be capable of acquiring or targeting space assets, state proxies, and individual non-state actors are more and more capable in this domain. Space warfare is democratizing, and so are space threats.

5. Conclusion

In the times of Space 2.0, it is a straightforward fact that outer space, especially the Earth's orbit, is becoming an area of future armed conflicts among the most geopolitically and technologically capable states. Space assets, including ground infrastructure and humans working in the space sector, have already been targeted and attacked. The source of the threat is not limited to hybrid attacks and armed conflict in space carried out by space powers. As history shows, the space sector was the target of non-state actors, including terrorists. With the virtually exponential development of space assets, accompanied by the democratization of space technologies, we are bound to witness yet more use of space assets, and targeting thereof , by non-state actors for political and military purposes. In fact, space terrorism and space insurgency have become threats of today's world.

The phenomenon of space terrorism is understudied and theoretically not developed enough, which, in consequence, translates into weak practical countermeasures and no adequate international law framework. This article is meant to galvanize the research by reporting various cases of attacks on space assets by non-state or proxy actors and, on that account, provide historical material for a comprehensive and unambiguous definition of space terrorism.

Declaration of interest
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

References

1. Anonymous TV [@YourAnonTV]. (2022, March 1). *JUST IN: Hacking group 'NB65', affiliated with #Anonymous has shut down the Control Center of the Russian Space Agency 'Roscosmos'*. [Post]. X. https://twitter.com/YourAnonTV/status/1498792639877074945
2. Bender, B. (2022, March 2). *Russia's space chief says hacking satellites "a cause for war."* Politico. https://www.politico.com/news/2022/03/02/russia-space-chief-hacking-satellites-war-00013211
3. Bernat, P. (2020). Orbital Satellite Constellations and the Growing Threat of Kessler Syndrome in the Lower Earth Orbit. *Safety Engineering of Anthropogenic Objects, 4.* 277–90. https://doi.org/10.37105/iboa.94
4. Bernat, P., & Posłuszna, E. (2019). The Threat of Space Terrorism in the Context of Irregular Warfare Strategies. In L. Aydemir (Ed.), Evaluation of Social Changes and Historical Events Based on Health, Economy and Communication in a Globalizing World (pp. 25–37). Dora.
5. Cain, J. R. (2016). Space Terrorism – A New Environment; New Causes. In C. S. Cockell (Ed.), *Dissent, Revolution and Liberty Beyond Earth* (pp. 93–110). Springer. https://doi.org/10.1007/978-3-319-29349-3_7
6. Campbell, D. (1999, May 20). Cyber Sillies. *The Guardian.* https://www.theguardian.com/uk/1999/may/20/military.defence
7. CBS News (1998, May 26). Beyond The Broadcast. *CBS News.* https://www.cbsnews.com/news/beyond-the-broadcast/
8. CBS News (2013, August 9). N.J. Man In A Jam, After Illegal GPS Device Interferes With Newark Liberty Operations. *CBS News.* https://www.cbsnews.com/newyork/news/n-j-man-in-a-jam-after-illegal-gps-device-interferes-with-newark-liberty-operations/
9. Cernan, E., & Davies, D. (1999). *The Last Man on the Moon.* St. Martin's Griffin.
10. Chicago Tribune (1999, March 1). *Hackers Reportedly Seize Control of Military Satellite. https://www.chicagotribune.com/news/ct-xpm-1999-03-01-9903010180-story.html*
11. Cyber Defense Project. (2021). *Terra Calling: Defending and Securing the Space Economy: From Science to Fiction and Back to Reality*. ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2021-01-Terra-Calling.pdf
12. Daly, J. C. K. (2007, June 5). LTTE: Technologically innovative rebels. *Energy Publisher.* http://www.energypublisher.com/article.asp?id=9803
13. Dartnell, M. Y. (1995). *Action Directe, Ultra-Left Terrorism in France, 1979–1987.* Frank Cass.
14. Department of Justice. (2000, September 21). Juvenile computer hacker sentenced to six months in detention facility. Case marks first time a juvenile hacker sentenced to serve time. Department of Justice [U.S.A.]. https://www.justice.gov/criminal/pr/2000/09/2000_3384_JUVENILE_COMPUTER_HA.htm
15. Department of the Air Force. (2003). *Comprehensive Strategy for the Space Force* (*Report to Congressional Committees*). U.S. Department of the Air Force. https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/CRR-FY23-Comprehensive-Strategy-Space%20Force-15-Aug-23.pdf
16. Epstein, K., & Elgin, B. (2008). Network Security Breaches Plague NASA. *Business Week.* www.businessweek.com/print/magazine/content/08_48/b4110072404167
17. Ewalt, D. (2013, March 18). The Tale of Captain Midnight, TV Hacker And Folk Hero. *Forbes.* https://www.forbes.com/sites/davidewalt/2013/03/18/the-tale-of -captain-midnight-tv-hacker-and-folk-hero/#286308a41053
18. Forester, T., & Morrison, P. (2007). Hacking and Viruses. In K. E. Himma (Ed.), *Internet Security: Hacking, Counterhacking and Society* (pp. 3–28). Jones and Bartlett Publishers.
19. France24 (2023, October 5). Chinese firm sold satellites for intelligence to Russia's Wagner: contract. *France24.* https://www.france24.com/en/live-news/20231005-chinese-firm-sold-satellites-for-intelligence-to-russia-s-wagner-contract
20. Freedberg, S. J., Jr. (2015, December 2). US Jammed Own Satellites 261 Times; What If Enemy Did? *Breaking Defense.* https://breakingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-an-enemy-tried/
21. Gorman, S., Dreazen, Y. J., & Cole, A. (2009, December 17). Insurgents Hack U.S. Drones. *The Wall Street Journal*. https://www.wsj.com/articles/SB126102247889095011
22. Grossman, L. (1999, March 1). Did Hackers Hijack a British Military Satellite? *Time.* https://content.time.com/time/magazine/article/0,9171,20673,00.html
23. Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017). *Escalation and Deterrence In the Second Space Age.* Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/171109_Harrison_EscalationDeterrenceSecondSpaceAge.pdf
24. Harrison, T., Johnson, K., & Roberts, T. G. (2018). *Space Threat Assessment: A Report of the CSIS Aerospace Security Project 2018*. Center for Strategic and International Studies. https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf#page=18
25. IODA [@IODA_live] (2023, June 29). *Follow the JSC Dozor-Teleport AS41942) outage in near realtime using IODA's dashboard*. [Post]. X. https://twitter.com/IODA_live/status/1674436879046029314

Safety & Defense 9(2) (2023)
DOI: https://doi.org/10.37105/sd.217

26. Jayawardhana, W. (2007, April 13). Intelsat to turn of f LTTE beam: Tigers' satellite piracy bared. *Daily News – Sri Lanka.* http://www.dailynews.lk/2007/04/13/news01.asp
27. Jordan, J. (2020). International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict. *Journal of Strategic Security, 14*(1), 1–24. https://www.jstor.org/stable/26999974
28. Kessler, D. J., & Cour-Palais, B. G. (1978). Collision Frequency of Artificial Satellites: The Creation of a Debris Belt. *Journal of Geophysical Research, 83*(A6), 2637–46.
29. Laqueur, W. (2003). *No End to War: Terrorism in the Twenty-first Century*. Continuum.
30. Leyden, J. (2014, July 15). Hamas hacks Israeli TV sat channel to broadcast pics of Gaza wounded. *The Register.* https://www.theregister.com/2014/07/15/hamas_hack_israeli_sat_tv/
31. Madory, D. [@DougMadory]. (2023, June 29). We can confirm that Russian satellite operator Dozor Teleport (AS41942) left the global routing table at about 02:00 UTC earlier today. [Post]. X. https://twitter.com/DougMadory/status/1674437865499947009
32. Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security, 20*, 287–311. https://doi.org/10.1007/s10207-020-00503-w
33. McCoy, J. J. (2007, April 27). Intelsat Shuts Down Transponder Hijacked By Terrorists. *Satellite Today (Via Satellite).* https://www.satellitetoday.com/uncategorized/2007/04/26/intelsat-shuts-down-transponder-hijacked-by-terrorists/
34. Mehmoodi, A., & Ahmed, S. (2021). Terrorism in Space: A Possibility. *CISS Insight, 9*(1), 90–109.
35. NATO. (2023). *NATO's Approach to Space*. The North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/topics_175419.htm
36. Nelson, A. J. & Epstein, G. L. (2022). *The PLA's Strategic Support Force and AI Innovation*. Brookings. https://www.brookings.edu/articles/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/
37. NetBlocks [@netblocks] (2023, June 29). *Confirmed: Metrics show a disruption to satellite internet provider Dozor-Teleport which supplies Russia's FSB, Gazprom, Rosatom and military installations.* [Post]. X. https://twitter.com/netblocks/status/1674447946689986561
38. PBS Frontline. (2000). Interview: anonymous. *PBS Frontline.* https://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html
39. Petkauskas, V. (2023, November 15). We breached Russian satellite network, say pro-Ukraine partisans. *Cybernews.* https://cybernews.com/cyber-war/we-breached-russian-satellite-network-say-pro-ukraine-partisans/
40. Rausch, H. (2006, April). Jamming Commercial Satellite Communications During Wartime: An Empirical Study. *Proceedings of the Fourth IEEE International Workshop on Information Assurance*. IEEE Satellite.
41. Reuters (2022, March 2). Russia space agency head says satellite hacking would justify war -report. *Reuters.* https://www.reuters.com/world/russia-space-agency-head-says-satellite-hacking-would-justify-war-report-2022-03-02/
42. Schlom, D. (2001). Target America 1972: When Terrorists Threatened Apollo – An Untold Story of Apollo 17. *Ad Astra, (November/December 2001)*, 20–24.
43. Schwartz, N. A., Williamsen, J. E., Heagy, J. F., & Moeller, R. A. (2021). Orbital Debris and Kinetic Anti-satellite Concerns: How a "Kessler Syndrome" Threatens U.S. Use of Space Assets. *Institute for Defense Analyses*. http://www.jstor.org/stable/resrep30922
44. Stout, D. (1998, April 22). Pentagon Acknowledges Hacker Intrusion Into a Computer System. *The New York Times.*
45. Swinhoe, D. (2023, June 30). Russian satellite comms firm Dozer taken of fline by Wagner-affiliated hacker group – report. *Data Center Dynamics.* https://www.datacenterdynamics.com/en/news/russian-satellite-comms-firm-dozer-taken-of fline-by-wagner-affiliated-hacker-group-report/
46. Telegraph. (1999, March 4). British hackers attack MoD satellite. *The Telegraph.* https://web.archive.org/web/20070510032306/http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/1999/03/04/ecnhack04.xml
47. Yale Daily News. (1998, April 23). Hackers break into Pentagon system. *The Yale Daily News*.