THE THREAT OF SPACE TERRORISM IN THE CONTEXT OF IRREGULAR WARFARE STRATEGIES

Paweł Bernat[*]
Elżbieta Posłuszna[**]

INTRODUCTION

For ages, the belief that conflicts are won by strong actors has seemed to be an incontestable tenet. Moreover, reality tended to confirm that dogma. However, in the second half of the 20th century, the situation changed, and the weak started to gain the advantage. It was caused by several, among which the most important are: globalization and the identity crisis that it has generated, and the fact that weak actors have moved away from hierarchical and centrally governed organizational structures and adopted new irregular warfare strategies. In this respect, the following questions arise: Will this trend continue? What will it lead to? How will it influence the threat level? Will it contribute to the emergence of new threats?

The above questions constitute the context of the discussion about the growing threat of space terrorism.

In the time of accelerating space technologies development (e.g., reusability of rocket boosters, new rockets under testing and

[*] Polish Air Forces University, National Security and Logistics Faculty, p.bernat@law.mil.pl

[**] Polish Air Forces University, National Security and Logistics Faculty, e.posluszna@law.mil.pl

development, including SpaceX's Falcon Heavy and BFR, NASA's SLS, Blue Origin's New Shepard), progressive number of launches (52 orbital launches in 2005, 70 – in 2010, 114 – in 2018, and planned 173 for 2019), growing space industry market (currently estimated around $350 billion, expected to almost triple in 2040, and reach $2.7 trillion in 30 years) space terrorism becomes to be recognized by many researchers and policymakers as a serious threat. In other words, space systems become more affordable, more available, more disseminated, easier to manage, but also more vulnerable to be targeted by traditionally weaker actors like terrorist groups.

The motivation for such potential terrorist acts mirrors the one for aviation terrorism but would have a more significant impact due to its exceptional symbolic weight, probably greater media exposure, and enormous economic consequences for the targeted agency/company, and nation.

The main purpose of the paper is to briefly introduce the phenomenon of space terrorism in the context of irregular warfare as carried out by traditionally weak actors that are terrorist groups and individuals. It is divided into three main sections, where the first one is dedicated to discussing how historically speaking weak actors started to gain advantage over the strong ones thanks to implementing new organizational and management solutions like leaderless resistance, the second – to introduce the concept of space terrorism and to list and describe plausible reasons for carrying out a terrorist attack on space industry; the third and final part discusses the potential and actual threats of space terrorism.

WEAK ACTORS AND LEADERLESS RESISTANCE

For ages, it was believed that the basis for the military success is a material advantage that would usually manifest itself in the number of troops, the quantity and quality of weapons, efficiency of the logistic support and economic capability of the state. It was, of course, strong actors, mainly states, who enjoyed such material advantage, so they usually won the conflicts[1]. Ivan Arrequin-Toft in his paper *How the Weak Win Wars: A Theory of Asymmetric Conflict* (2001) demonstrates that in the majority of asymmetric conflicts[2], i.e., such where the difference of potentials is 1:10, the strong adversary[3] usually wins (70.8% of conflicts). That means that it did not win 29.2% of them, i.e., it was not able to realize the goals it adopted.

However, in the second half of the 20th century something changed. The weak actors, doomed to failure from the start as it seemed, began to gain an advantage. In 1950-1998 the weak actors won 55% of wars, which denied the dogma of the simple correlation between material power and strategic advantage.

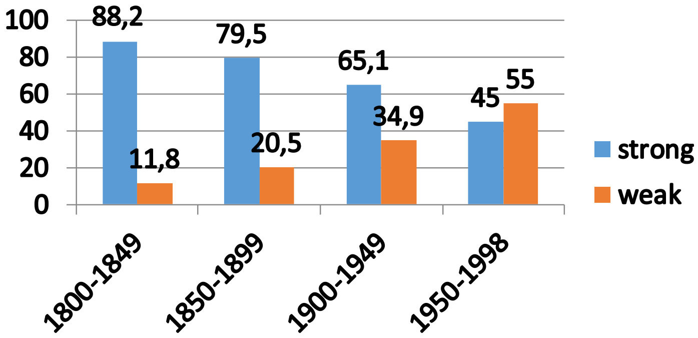

Figure 1: The percentage of victories in asymmetric wars depending on the type of actors in particular periods. (Source: Arrequin-Toft, 2001: 93-128).

[1] Winning the conflict means, in this instance, to realise the adopted goals.

[2] The basis for I. Arrequin-Toft's consideration was an analysis of 197 armed conflicts that took place in 1800-1998 (2001: 93-128).

[3] A strong adversary is, according to I. Arrequin-Toft, such an actor, whose material potential tops the potential of its adversary or adversaries at least ten times; and conflict is defined as war, during which the number of casualties amounts to at least one thousand.

Why did it happen this way? Why did weak actors start to win more and more frequently despite their military potential that condemns them to lose? Since the real power (i.e., such that translates into a real victory in conflicts) is more and more often on the side of the potentially weaker, what fosters such a state of affairs?

Making an attempt to answer these questions, we would like to turn attention to two factors that, as it seems, have played a key role here, namely, abandoning by the weak actors hierarchical and centrally governed organizational structures and employing new communication technologies. These two factors are strongly mutually interconnected, although the first one, it has to be admitted, has a much longer history.

The postulate to reject centralized organizational structures occurred already in the 1950s thanks to Colonel Ulius Louis Amoss, a CIA officer, who believed that fight against communism should be founded on uncentralized, that is such, where the unifying element is not the leader but the shared goal (both, of ideological and tactical nature) (Bayo, 1963). Louis Beam, an American right-wing radical activist, expressed similar views and claimed that it was high time to give up the pyramidal organizational forms and consider other ways of organization that could be best defined as an organization without organization (Beam, 1992). An organization without organization, usually called "leaderless resistance" is a strategy (and at the same time a new form of organization) that presupposes giving up all hierarchical structures that are exchanged with a loose configuration of small and autonomous cells, which are not governed by any decision center. The factor that cements the movement is the ideology, from which its members obtain information on effective and morally proper forms of combat.

The advantages of that form of fighting (and at the same time organization) are significant, especially when it comes to security.

It is well known that in a hierarchical structure if a police agent or an intelligence gathering individual succeeds in infiltrating a particular level of organizational hierarchy, they will, with no problems, destroy all levels below and will endanger the levels above their own. It is only a matter of time and the effectiveness of the individual who is dismantling the given organization when it will be taken control of (usually also destroyed) by adverse powers. In the case of "organizations" where single individuals or small groups have no organizational center, but also act without any structural connection between them, the threat of invigilation drops off practically to zero. For, in such circumstances, there is nothing to invigilate (there is no structure that could be subject to invigilation). There are more benefits to this form of organization. The leaderless resistance model also allows to dissociate from unwanted actions with an excuse that they do not fulfill ideological criteria and adopt as one's own acts that suit the adopted pattern of direct actions but were carried out by someone else and fueled by entirely different motivation. In such a case, it is the type of action that prejudice, whether a particular act will be included in the activity of a particular agent. Such an "organization" may hence seem much more powerful than it is in reality.

Although the strategy of leaderless resistance already appeared in the 1980s, it started to be widely used at the end of the 1990s. The reason for that was the Internet that enabled unlimited communication. It not only facilitated instant information exchange but also efficient management of ideology that in the leaderless resistance model plays the role of the only organizational cement. Moreover, the Internet not only allows to successfully maintain the anonymity of the network members but it also unifies them ideologically (the strength of the interpersonal contacts does not seem to be weaker, than in real life interactions) and enables unlimited "organizational" activity; the activity that is beyond any type of formal structure. Internet webpages play a key role here; they are nodes that facilitate in information exchange and at the same time centers of ideological influence. The activists that act under the name of a particular organization (what of course does not mean a formal membership) disseminate the information about their activities with the use of anonymous, often encrypted messages, which are then published on the webpages (one can find there detailed clues regarding security rules and information encryption). Thanks to the Internet, it is also possible to disseminate extremist messages all over the world. In the past, there was a limited number of potential recipients within reach of any radical idea. Looking for them and convincing them was in itself a risky endeavor. Today, finding them (which is relatively safe) with the use of the Internet is not a problem.[4] Finally, the Internet may be used for offensive purposes, e.g., in attacks the information systems or the adversary's data. Such practices are usually called "cyberterrorism." In the situation when offensive actions are combined with the functioning in accordance with the leaderless resistance model, the effectiveness of a given "organization" seems to be formidable.

SPACE TERRORISM AND WEAK ACTORS

Terrorism is a very complex phenomenon that undergoes constant changes in time – it is rather of dynamic and ephemeral nature than fixed once for all state of affairs. Due to that reason, as well as to the fact that it is also politically relevant what actions we actually name "terrorism," there is no one definition of terrorism. Of course, it does not mean that there are no attempts to do it – there are, but they are inevitably very general and oversim-

[4] Roger Eatwell, a researcher of fascism and populism, cites the following reasons for the Internet's popularity among extremists: (a) the low-cost and potentially high-quality presentation and distribution of information, (b) the ability to tailor messages to specific audiences who self-select the type of information they seek, (c) the ability to create an effective image of ideological community, and (d) the ease of global distribution across jurisdictional boundaries (Jewin, 2002: 965).

plifying. Moreover, there are more than one hundred definitions of terrorism that quite often contradict one another. A. Schmid and A. Jongman carried out a meta-analysis on account of which they stated that among the most common factors constituting terrorism there were violence and force – 83.5% of definitions, political character of the phenomenon – 65% of definitions, and fear and terror – 51% of definitions (Schmid and Jongman, 2017: 5).

We can conclude that brief terrorism presentation with the claim that there cannot be one definition of terrorism. Still, it does not mean that we are helpless, on the contrary, a good strategy seems to be to forget about trying to confine such a convoluted issue in one definition and construct narrower and more detailed elucidations that describe and are dedicated to particular types of terrorist activities.

There are, of course, many criteria one may use to distinguish among different types of terrorism. (Below, we discuss three most common set of criteria that in no way exhaust the variety of different sorts of terrorism.)

Politically motivated terrorism can be divided on account of various doctrinal assumptions and ideological goals, and hence, there are, e.g., national liberation terrorisms, left-wing terrorisms, right-wing terrorisms, religious terrorisms.

Due to the area of operation, terrorism can be divided into state terrorism (e.g., authorities use it as a way of fighting against guerrilla groups), international terrorism (e.g., aviation terrorism), and separatist terrorism (that aims to gain political, ethnic, or religious independence).

And finally, the most significant for the purpose of this paper, the typology of terrorism that is built upon the differences where terrorist attacks occur. Here we distinguish aviation (air) terrorism, maritime terrorism, land terrorism, cyber-terrorism, and space terrorism.

Space terrorism is a relatively new phenomenon, and there are not many scholars who have put their interest into it. As far as we are aware, there is just one definition available in the specialist literature that addresses that issue. It was coined by J.R. Cain and defines space terrorism as "an 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: 98).

The definition is too narrow in its material scope and does not take into account the acts of violence/destruction that can take place on earth and have nothing to do with developing a space settlement but still target a generally conceived space sector, e.g. rocket launch sites or any part of ground infrastructure, including a cyber-attack. On the other hand, it is too broad because it counts as terrorism all acts violence or terror regardless of the motivation. If we adopted such a stand, then every crime against "the development of a space settlement(s) and/or their aims" including petty theft or vandalism would be treated as terrorism, and that would be, for a number of reasons, including legal ones, an absurd.

Therefore, we propose our own definition, which, we believe, is more adequate and defines space terrorism as a purposeful and well thought-out 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 an economic sector dedicated to producing components that go into Earth's orbit or beyond, delivering them to those regions, and related services.

Now, the question arises why the space sector would be an attractive target for weak actors like terrorist groups or individuals.

A good way to answer it is to draw an analogy between the space sector and civil aviation because the latter for decades has been subject to various terrorist attacks. J. Laskowski names four main reasons why it has been so, i.e., (1) extensive media coverage, (2) symbolic meaning – by attacking the industry, the terrorist attacks the state the agency or company is registered in, (3) relative easiness to carry out such an attack, and (4) severe economic consequences (Laskowski, 2013:159-162). We can extend this list by the ones recognized by J. Harrison, namely that (5) such attacks are international events, (6) they can generate a sense of shame among the politicians of the attacked state, (7) they are effective (Harrison, 2012: 49-52).

It seems that the abovementioned reason could also apply to the space industry and because of the unique and special character of it, like the amount of money involved, its symbolic significance, and worldwide media coverage, any act of space terrorism would release the goals the terrorists had in mind and hoped for. This is also why traditionally weak actors and adversaries of the states like the USA, Russia, or China would be potentially interested in targeting the space industry of those countries. For, a successful attack, i.e., such that would result in death and/or bring a lot of destruction to the infrastructure, would be a real blow to the country's internal and external perception, its finances, and would definitely slow down the development of space exploration. As we can see in figure 1, all the odds are against strong actors and in favor of the weak ones, like more or less organized terrorist groups.

THE ACTUAL AND POTENTIAL THREAT OF SPACE TERRORISM

The actual threat of space terrorism is minor. It is so because the global space industry is still in its infancy phase – there are no many programs and facilities that could be attacked, and the existing one, due to their small number, are well guarded. However, the sector is growing exponentially.

As already mentioned, there are new important players in the industry, both private companies (e.g., SpaceX, Blue Origin, Virgin Galactic and Virgin Orbit, Bigelow Aerospace, Rocket Lab), and national agencies (e.g., ISRO, China National Space Administration) that joined the key actors like NASA, Roscosmos, ESA, JAXA, and CSA.

The current record of rocket orbital launches was established in 1967 when 139 missions took place (Kyle, 2018). It may be surprising for many readers that for over 50 years we, as a global community, have not beaten it. However, since the mid-200s we have observed a constant growth in numbers (52 orbital launches in 2005, 70 – in 2010, 114 – in 2018), and this year, i.e., should finally be the one brining a new record of 173 launches (Kyle, 2019).

From the economy point of view, the space market is growing as well. It is currently estimated to be about $350 billion, and according to various consultancy companies, it is expected to be worth between $1-2.7 trillion in 2040 (Foust, 2018).

What is more significant from the safety and security perspective is the fact that the space industry has been gaining more and more strategic importance. Nowadays, we witness an unprecedented process of democratization of space technologies, including weapons, that could become a serious threat for orbital objects in the future. Obviously, weak actors are not in possession of ASAT weapon systems able to destroy satellites in the orbit (as for today, there are just five nation-states that have that capability, i.e., USA, Russia, China, Israel, and India); they do have though significant potential to disrupt / jam signals from and to satellites that may turn out to be lethal.

The cases of the latter have already happened. For example, Sri Lankan terrorist group the Liberation Tigers of Tamil Eelam, otherwise known as the Tamil Tigers, hacked an Intelsat satellite and used a vacant Ku-band transponder to broadcast its message in Sri Lanka and the surrounding region without Intelsat's knowledge for over a year (de Selding, 2007) until Intelsat decided to shut down the satellite transponder in late April 2007 (McCoy, 2007).

There might have also been cases of sabotage. In early 2015, a twenty-year-old U.S. Air Force Defence Meteorological Satellite Program Flight 13(DMSP-F13) craft blew up. The U.S., according to S.M. Pekkanen, attributed the event to a power failure and minimized its importance. However, the delay in admitting the event to the public caused speculations, whether it was an actual act of sabotage (Pekkanen, 2015). Of course, for obvious reasons, it is difficult to determine what truly happened.

Another case worth mentioning is the launch of four rogue satellites on Indian PSLV launch vehicle on 12 January 2018. The satellites belonged to the Swarm Technologies – a space start-up based in California that had been denied placing them onto the orbit due to the small size of the devices (the concern was that they were too small to be tracked in space) (Christensen, 2018). While, as it seems, this case did not pose any danger for global security, it raises many questions regarding our current control system what is sent to the outer space. If it was possible for an American company to place in the orbit unlicensed satellites, it seems, that any other agent, including weak actors adversaries discussed in this paper, could do the same.

CONCLUSIONS

The aim of the paper was to introduce the concept of space terrorism as a new possible way of attacking traditionally strong actors – large national states by the weak ones, like terrorist groups and individuals.

Space terrorism is definitely a new phenomenon, and as such, it is rather a concern of the future, than a current threat. However, as it was demonstrated, there have already been attempts to disrupt the operation of the broadly conceived space industry. What is more, it seems very likely that we are at the beginning of such activities, and the threat will be growing. Space sector occurs as a very attractive target for terrorists due to its immense symbolic significance, potential excessive international media coverage, and tremendous economic damage. Therefore, all the involved agents (e.g., policymakers, security forces, space industry staff) should become aware of that fact and act accordingly.

REFERENCES

Arrequin-Toft, I. (2001). How the Weak Win Wars: A Theory of Asymmetric Conflict. International Security, 26(1), 93-128.

Bayo, A. (1963). 150 Questions for a Guerrilla. Panther Publications. Colorado.

Beam, L. R. (1992). Leaderless Resistance. The Seditionist, 12. It was accessed on June 8, 2019 at http://www.louisbeam.com/leaderless.htm.

Cain, J. R. (2016). Space Terrorism – A New Environment; New Causes. Dissent, Revolution and Liberty Beyond Earth. ed. by Charles S. Cockell. Springer. Switzerland. 93-110.

Christensen, I. (2018). Unlicensed Swarms in Space. The Space Review, 02.04.2018. It was accessed on June 7, 2019 at http://www.thespacereview.com/article/3465/1.

de Selding, P. B. (2007). Intelsat Vows to Stop Piracy by Sri Lanka Separatist Group. Space News, 18.04.2007. It was accessed on June 8, 2019 at https://spacenews.com/intelsat-vows-stop-piracy-sri-lanka-separatist-group/.

Foust, J. (2018). A Trillion-dollar Space Industry Will Require New Markets. Space News, 05.06.2018. It was accessed on June 7, 2019 at https://spacenews.com/a-trillion-dollar-space-industry-will-require-new-markets/.

Harrison, J. (2012). International Aviation and Terrorism: Evolving Threats, Evolving Security. Routledge. New York.

Jewin, B. (2002). Legal and Historical Analysis of Extremists' Use of Computer Networks in America. American Behavioral Scientist, 45(6), 958-988.

Kyle, E. (2018). Worldwide Orbital Launch Summary by Year. Space Launch Report, 31.12.2018. It was accessed on June 9, 2019 at https://www.spacelaunchreport.com/logyear.html.

Kyle, E. (2019). 2019 Space Launch Report. Space Launch Report, 12.16.2019. It was accessed on June 9, 2019 at https://www.spacelaunchreport.com/log2019.html#onpad.

Laskowski, J. (2013). Terroryzm lotniczy – charakterystyka zjawiska. Studia Humanistyczno-Społeczne, 7, 133-163.

McCoy, J. J. (2007). Intelsat Shuts Down Transponder Hijacked By Terrorists. Via Satellite, 26.04.2007. It was accessed on June 8, 2019 at https://www.satellitetoday.com/telecom/2007/04/30/intelsat-shuts-down-transponder-hijacked-by-terrorists-2/.

Pekkanen, S. M. (2015). How Space Trash Can Be Used Against The U.S. Forbes, 30.06.2015. It was accessed on June 9, 2019 at https://www.forbes.com/sites/saadiampekkanen/2015/06/30/how-space-trash-can-be-used-against-the-u-s/#f1caf6857826.

Schmid, A. P. and Jongman, A. J. (2017). Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature. Routledge. New York.