Analiza KBN

Nr 1 (116) / 2023 23 stycznia 2023 r.

Space Security and the War in Ukraine – A Preliminary Assessment

Marek Czajkowski

Introduction

The course of the current war in Ukraine highlights profound changes in space security, which have been undergoing for some time. Improving access to multiple space-derived services due to the spread of related technologies among the increasing number of commercial entities leads to a qualitatively new strategic situation. Military-grade observation and other security-related satellite services are available on the market, so even non-spacefaring nations and non-state actors can wield capabilities that, until recently, were available only to the several most advanced countries. This article offers a preliminary assessment of changes in the space security environment caused by the abovementioned process against the background of the conflict in Ukraine.

The war in Ukraine is sometimes dubbed the first commercial space war to highlight the importance of services the Armed Forces of Ukraine (AFU) have obtained from private space companies. Indeed, developments during this conflict underline profound changes in space security, which have been undergoing for some time. The process we refer to is often termed the democratisation of space which, in short, means increased access to multiple space-derived services due to the spread of related technologies among an increasing number of commercial entities. This process has led, among others, to a qualitatively new reality in which military-grade observation

and other security-related satellite services are available on the market. This way, even non-space-faring nations and non-state actors can wield capabilities that were available only to the several most advanced countries until recently. This article offers a preliminary assessment of changes in the space security environment caused by the abovementioned process against the background of the conflict in Ukraine.

We understand space security as the use of space systems for security-related purposes, along with the security and safety of space systems; this perspective defines the scope of the analysis.

Background

It is not necessary to describe in detail how commercially available earth observation and communications services, including secure broadband Internet, have exerted an impact on the course of action in Ukraine. It has been and is being depicted and highlighted very clearly in the information space. Suffice to say that space applications serve as one of the crucial *force multipliers* which have helped the Ukrainian side to offset the initial advantages of the Russian Armed Forces (RuAF) and create advantages for itself. These applications belong to all three categories of supportive missions provided by existing space systems:

- military-grade GPS service and modern weapons using difficult-to-jam/spoof positioning receivers;
- secure communication, including difficult-to-hack broadband Internet service; and
- military-grade earth observation services delivered on a frequent basis.

Ukraine uses these services on a commercial basis because military-grade GPS receivers, secure communication terminals and military-grade observation services are offered on the market by multiple private enterprises. This way, a customer can obtain crucial security-related capabilities without possessing expensive satellite constellations and without submitting requests to foreign governments to be given access to their space-borne capabilities. This state of affairs represents one of the important facets of the democratisation of space.

On the other hand, it must be emphasised that the military-grade high-end satellite service market is not a free market. Companies which possess capacities of that sort are, for the most part, located or registered in the United States and Western Europe. These countries restrict access to the most sensitive information, which can be obtained using commercial satellite services and the most advanced hardware for end-users. For example, no one can simply buy a high-resolution photograph of a US Army military base taken by one of the western commercial firms an hour ago without the permission of the US government. At the same time, no one can buy a western-made military-grade GPS receiver without the consent of the same authority. This way democratisation of space is not fully democratic, but the process is ongoing and spurs important changes in space security.

There is no direct and detailed information about the cooperation between Ukraine and commercial space companies, but it is apparent that the US government has greenlighted the delivery of up-to-date military-grade commercial observation services to the Ukrainian side. AFU probably have been allowed to use secure GPS receivers as well. Furthermore, Kyiv has also been presented with a large quantity of Internet broadband Starlink terminals financed by the US government.

Ukraine has also received large stocks of GPS-guided precision strike weapons. Note that we do not exactly know what techniques are used in modern military jamming-resistant GPS devices. However, related technologies are well-known, and many devices using them are commercially available, although their distribution is limited.

Another very important process highlighted by the conflict in Ukraine is the decreasing capability of the Russian Federation to sustain its space architecture. The overall crisis of the Russian economy, which has persisted for more than a decade, plus the debilitating effect of sanctions implemented after Russia had annexed Crimea in 2014, resulted in the decreased spending on new military space systems and diminished access to crucial western technologies. In effect, the Russian military space architecture remains relatively robust only regarding strategic communications and early warning. Other satellite services are much less available, and, most importantly, Russia, in fact, lacks up-to-date tactical information regarding the battlefield situation, which critically hampers the war effort.

The main problem of the Russian military space is that many satellites that form the backbone of the Russian military space architecture were launched a decade ago. For example, according to the available information, the Russian military operates only two optical imaging satellites launched in 2013 and 2015 and two SAR (Synthetic Aperture Radar) imaging satellites launched in 2015 and 2022. Given their expected service life of some five years, it is uncertain if the satellites in question are operational at all. For comparison (as of May 1, 2022): California-based Planet Labs Plc operates 88 optical and multispectral imaging satellites (although not all of them provide military-grade services) and Finland-based company ICEYE operates 12 SAR satellites.

Therefore, it is very likely that the Russian military space architecture will degrade even further in the future. Even the flagship of the Russian space architecture, the GLONASS positioning system, is in jeopardy, despite plans to refit it with new generation craft. Moreover, it may have already been degraded, as Russian aviation reportedly use civilian GPS receivers in combat planes. Thus, we may safely assume that an expanded sanctions regime, degraded economic situation, and tight war-time budget, which certainly prioritises funding of the production of military hardware necessary on the frontline, will preclude the growth of the Russian military space architecture.

Strategic Assessment

Space commercialisation and the resulting process of disseminating military-grade services and hardware brings significant changes to the state of the international security environment. Looking from the point of view of space security, as defined above, we can see three distinct but intertwined developments:

1. Space-borne military-grade services have a high potential to alter regional security dynamics.
2. Counterspace measures (CSMs) are evolving very fast, and satellite systems are increasingly frequently targeted by jamming, spoofing, blinding, and dazzling attacks and cyber intrusions.
3. Strengthening the resilience of existing and future space systems has become critically important, particularly for the leading space-faring nations.

Dissemination of military-grade services, listed as point 1 above, may change the strategic equation regionally and worldwide in several ways:

- allowing weaker states to offset some of the advantages of more powerful adversaries,
- giving local adversaries more capacity to assess one another's potential, what may bring many consequences starting from fostering hostilities through enabling mutual deterrence to support disarmament processes,
- giving space-faring nations additional instruments to interact with allies or dependants by offering or withdrawing assistance from commercial entities,
- and finally, a growing number of commercial companies possessing access to high-end military-grade space technologies increase the likeliness that these technologies would leak to unauthorised actors like unfriendly nations or rogue non-state actors (terrorist or criminal organisations, for example), giving them immense new capabilities.

The Russo-Ukrainian war exemplifies a good part of the abovementioned observations. The pre-war Russian advantage over Ukraine has been nullified or even reversed, largely thanks to the extensive use of satellite systems. This way, a theoretically more powerful nation-state finds itself bogged down on the periphery of the smaller and weaker adversary due to, among others, a lack of up-to-date satellite services. Conversely, the weaker side gains a huge advantage on the battlefield by using commercial satellite systems. In essence, Ukraine is much more powerful in space than Russia, even though it is not a space-faring nation.

Furthermore, the extensive use of commercial satellite systems and information released to the media in the run-up to the war allowed AFU to assess its strengths and shortcoming versus the Russian forces and prepare its actions accordingly. In fact, the Russians went to war virtually without an element of surprise and having their forces entirely exposed to the enemy's intelligence. Conversely, sparse information from the Russian military space architecture precluded the RuAF from gaining information sufficient for effectively planning and executing the invasion.

And finally, the United States used commercial satellite services to conduct an information operation against Russia by exposing the Kremlin's intentions in the last months and weeks of peace. At the same time, Washington allowed commercial space companies to render aid to Ukraine, which was critically important for the preparation of the nation's defence. There are two strategic advantages of this situation. Firstly, the U.S. has not exposed its secret assets and capabilities to the public or the Ukrainian ally. Secondly, the United States could argue that it was not directly a side of the conflict, what would be difficult if Washington decided to supply Ukraine with own intelligence resources, subsequently used for the execution of military operations.

The dynamics listed above represent a radical transformation in strategic relations worldwide, which has been emerging for a decade or so – the war in Ukraine just highlighted this process. Let us underline the essence of the new situation. Technological powers leading in the developing commercial space applications are now able to allow allied non-spacefaring nations to use certain space capabilities as *force multipliers* without providing them with the direct support of their own assets. The latter may be politically difficult and operationally inconvenient, so the use of commercial capabilities gives immense new opportunities to influence local or regional security environments and translates into global changes as well.

Referring to point 2 above, we can notice a growth in the capacity and sophistication of counter-space measures in recent years. However, the war in Ukraine did not demonstrate a radical increase in counterspace activities, which makes us to share several interesting observations. Firstly, it appears that some modern communication space systems, particularly Starlink broadband Internet satellites, are more difficult to jam or spoof than it was previously believed. Secondly, Russia did not decide to aggressively counteract commercial optical and SAR satellites, either because it lacks the capabilities to compromise these systems significantly or because some unclear political limitations to using CSMs are at play. And thirdly, Russian jamming and spoofing of the GPS service in Ukraine are not frequent because RuAF need western civilian services for their own operations, and, on the other hand, Russians understand that Ukraine employs modern jamming-resistant receivers and weapons which are to a great extent immune to countermeasures.

In essence, counterspace measures are increasingly developed and increasingly frequently used, but it does not necessarily mean that they are able to paralyse military-grade systems. Moreover, technical, operational and political limitations may also restrain the use of CSMs, as exemplified during the Ukrainian war to date. Thus, the space Pearl Harbour, envisioned by some analysts and politicians two decades ago, probably is much farther away than usually believed.

The third point listed above refers mostly to future developments, but it represents, first of all, the acknowledgement that the resilience of the current systems is in jeopardy. Consequently, a concerted effort is required now for the security and safety of space architecture in the future. This understanding is particularly profound in the United States and has resulted in generous funding of multi-pronged efforts to augment the resilience of space systems. Some of the projects are already entering the demonstration phase.

Future Developments

Bearing in mind strategic developments related to the democratisation of space, we may safely assume that space security will undergo significant changes in the coming years. It is certainly very difficult to predict exactly what is going to happen, as these changes are of mainly qualitative character, so they are naturally difficult to fathom. However, we can observe several trends that will shape the near future of space security.

1. The role of satellite services as a *force* multiplier is well known, there is nothing new in that respect. Space-borne earth observation and communication services have played a crucial role in military planning, particularly on the strategic level, since the very beginning of the Space Age. The Gulf War in 1990-91 highlighted space systems' profound tactical and operational importance, including positioning services provided by GPS. The current process of the democratisation of space gives opportunities to non-spacefaring nations to augment their capabilities by buying services and/or hardware on the market. The war in Ukraine has advertised these capabilities among wide publicity and politicians, spurring efforts to secure military-grade satellite services in many countries. In the future, we will most certainly witness the quick pace of development of military-grade commercial space architecture and non-spacefaring nations' efforts to obtain military-grade satellite services from commercial entities.

2. On the other hand, we will surely observe an increased pace of development of counterspace measures. Many countries, and possibly non-state actors, will seek to negate adversaries' capabilities, particularly with the use of cheaper and more difficult-to-attribute measures like tools of cyber intrusion or electronic warfare equipment. It is also highly possible that some progress will be made with regard to directed energy weapons, particularly non-destructive ones. It is also likely that works will continue on destructive ASAT weapons, however, we reiterate our assessment that deployment of anti-satellite weapons in militarily significant quantities is highly unlikely but not impossible in the foreseeable future. Furthermore, it is very likely that particularly Russia will increase the pace of the development of CSMs to offset its weakness in space systems and the strength of adversaries. It is also very likely that counterspace measures will form yet another part of the commercial space industry.

3. As a consequence of the development of counterspace measures, we will surely witness increased efforts to create more resilient and less prone to disruption space architecture. These efforts will be visible everywhere, particularly among first-rate space powers and commercial entities. The new military space architecture will be more distributed and easier to reconstitute and upgrade and the push to achieve this goal is already underway. Particularly the United States invest heavily in new concepts and technologies, so it will lead the technological and organisational revolution in military space in the future. Firstly, because it will be a rather expensive revolution, thus only the richest will be able to execute it in due time. Secondly, because the United States relies most heavily on its space assets, and that is why it is particularly interested in securing operations of military space architecture. And thirdly, because the U.S. technological prowess in space applications and the extensive industrial base will allow a quick and sustained progress. We also believe that the American effort will be difficult to emulate by less technologically advanced and economically weaker adversaries. In turn, the technological and operational gap between the U.S. and its competitors will probably widen.

4. Additionally, we may witness an increased pace of the creation of commercial military-grade space capabilities outside the Western nations. Particularly China may be interested in wielding commercial space capabilities and using them the way the United States does.

Citation: Marek Czajkowski, 'Space Security and the War in Ukraine – A Preliminary Assessment', *KBN Analysis* 2023, no. 1 (116), 23 January.