SATELLITE NAVIGATION SYSTEMS – AN AVOIDED TARGET? –

Colonel Dorian LUPARU

Defence Geospatial Information Agency “Division General Constantin Barozzi”, Bucharest

DOI: 10.55535/RMT.2022.3.04

In the current geopolitical context, the Black Sea region has become the scene of the conflict in which a wide range of weapons and ammunition are used. It is their directing/guiding by using signals transmitted by satellite navigation networks – GNSS that categorically makes the difference. Their contribution can be instantly noticed, even though it is not a novelty. The weapons that benefited from the augmentation of the satellite signal proved the accuracy of their shots. This is the reason why the actions of jamming or falsification of the satellite signal appeared in the battlefield and even threats of GNSS attack were launched. In the present article, I intend a disambiguation of the subject, in an attempt to delimit military declarations from political ones, in the space environment, which has become essential in the conduct of modern military actions.

Keywords: GNSS; jamming; satellite signal; spoofing; GLONASS;

INTRODUCTION

The Black Sea region has been a central place of the competition between Russia and the West for the future of Europe. The region experienced two decades of heated conflict even before Moscow's annexation of Crimea in 2014, and Russia has used military forces against countries in the region four times since 2008. It should be noted how Russia uses a variety of military and non-military tools to promote its objectives by analysing how the three North Atlantic Treaty Organisation allies – Bulgaria, Romania and Turkey – and five NATO partners – Armenia, Azerbaijan, Georgia, Moldova and Ukraine – in the Black Sea region perceive and respond to Russia's activities and where those countries' interests align or diverge. As it is a world economic and military power, there is a continuous fear that in the strategic plan it always has in a latent state various possibilities to assert its power, and an unconventional option, but with an overwhelming impact, is to attack satellite navigation systems (GNSS – Global Navigation Satellite System), in particular GPS. Does this possibility exist?

The Black Sea region has been a central place of the competition between Russia and the West for the future of Europe. The region experienced two decades of heated conflict even before Moscow's annexation of Crimea in 2014, and Russia has used military forces against countries in the region four times since 2008.

The massing of Russian military convoys at the beginning of this year, in the area of the Russian city of Belgorod up to the border with Ukraine, was noticed and followed closely by the whole world with obvious political concerns and with great anxiousness and attention from both the military and civilian environment. The civilian interest may seem surprising, but the movements (marches), stations or manoeuvres were analysed on the basis of satellite images obtained from various sources, most of them from the high-tech space environment in which various commercial companies operate. At some point, in late February, Google stated it would temporarily halt live traffic updates in Ukraine *"after consultation with multiple sources on the ground, including local authorities"* (Culliford, 2022), without giving explanations regarding the concerns that determined this decision. The statements were veiled and suggested that Google would not want to be part of providing targeting data in an international conflict, but analysts believed that traffic data provided by the company could reveal the locations of troops or refugees and could be used for military strikes.

Far from being called the *“first satellite conflict”*, this label being carried by the Gulf War three decades ago, it should be noted that during this time the belligerent environment also included the space segment, as a natural, evolutionary component of the modern conflict and created the opportunity for the fruition of space information generated by commercial satellites and for military purposes. The general public appreciates the show, the fireworks, and therefore modern weapons and especially the ammunition (missiles, bombs) that have satellite support give impressive strikes, of great accuracy, called as such *“surgical strikes”*, in a *“precision warfare”*, having a major impact on media exposure. A well-known example is the elimination of the *“terrorist butcher”* (Inside GNSS, 2007), Abu Musab al-Zarqawi; a *“smart bomb”* was launched at his home in the suburb of Hibhib, Iraq, killing him and several close associates in June 2006. The idea is that a bomb with a small explosive charge, precisely guided by GPS, was used in order to achieve the desired result with a minimum of collateral damage or even avoiding it. It was considered a success and a clear demonstration of GNSS technology support in the military field.

The satellite signal supports a multitude of military activities/ operations that include the field of information, intelligence, navigation, transport management, terrain study, action dynamics and many others that give a privileged position to the one who possesses it.

But the satellite signal supports a multitude of military activities/ operations that include the field of information, intelligence, navigation, transport management, terrain study, action dynamics and many others that give a privileged position to the one who possesses it. It is obvious that this state corresponds inversely to the opponent, who will seek to eliminate this advantage or neutralise it.

Obviously, a number of questions arise, among which:

1. *Is it possible for satellite navigation networks to be attacked?*
2. *Could the entire world be affected by the damage, alteration or cessation of space support?*

I must specify that in this article I will address navigation systems with satellites operating in high orbits, at approximately 20,000 kilometres altitude and not satellites located in low orbit (LEO or Low Earth Orbit), a region that extends up to 2,000 kilometres from the Earth, whose main functions are to ensure communications, the Internet and meteorological observations.

THE SCENE OF SATELLITE NAVIGATION SYSTEMS

In the modern world economy, a series of major activities are no longer conceivable without the signals of satellite navigation systems, which influence us and have been part of our daily life for a long time. Thus, the infrastructure and management of air, sea and land transport, communications, land mapping and measurements, search and rescue operations and many others have developed dependence on satellite data, without omitting the military interest embodied in the applications of location, tracking, directing, guidance of troops, materials, ships, aircraft, equipment, armaments and ammunition.

There are several satellite navigation systems in the world. It is a separate community differentiated mainly by space tasks (orbital or geostationary satellites) or global or zonal coverage. The best-known is the American GPS, but there is also the Chinese version – BeiDou (COMPASS), and the Russian one, called GLONASS. Europeans have Galileo GNSS, but it does not play an important role in satellite navigation as it is only for civil use, it is limited and has a number of restrictions. Indian IRNSS and Japanese Quasi-Zenith can also be mentioned, but they are zonal and augmentation systems. Satellite navigation systems are expensive investments for any country – USA, China, Russia or even Europe, therefore countries try to combine their efforts when satellites of one system can complement another. For example, Russia actively cooperates in this direction with China and it was assumed that similar steps would be taken with Europe and the USA, but it can no longer be a topical approach, for obvious geopolitical reasons.

There are several satellite navigation systems in the world. It is a separate community differentiated mainly by space tasks (orbital or geostationary satellites) or global or zonal coverage. The best-known is the American GPS, but there is also the Chinese version – BeiDou (COMPASS), and the Russian one, called GLONASS.

The evolution of GLONASS was winding, it started in the USSR and, after years of decay, in the ’90s, the system was restored, enabling full global coverage. There is now a full constellation of satellites in orbit, for both civilian and military use. There are no differences from the same GPS.

The advantage of GLONASS in the northern area is undeniable, in Scandinavia the system allows obtaining coordinates faster and more precisely, complementing GPS. In fact, all chipset manufacturers add support for all existing navigation systems to their solutions – it is cheaper and easier, and the consumer gets the highest possible accuracy. Moreover, even military applications have dual systems and can use signals from another satellite constellation for navigation or other needs, being a benefit to use all available data.

ALTERATION OF SATELLITE SIGNALS – JAMMING VERSUS SPOOFING

For states that do not have their own satellite navigation system, in the event of a conflict, it is possible that the satellite signal will be stopped or contain errors, meaning it will be altered, damaged or falsified. A clear example was during the Kosovo war in 1999 – while NATO was bombing Yugoslavia the satellite signal was turned off, then an error was deliberately introduced into the work of the civilian public GPS segment.

There are essentially two ways to interfere with GPS signals: jamming and spoofing. Jamming completely blocks the signal, and this type of interference is known from military bases. Spoofing is a more advanced interference where a radio transmitter sends fake GNSS signals that make the receiver think they are real satellite signals.

More recently, between 22-24 June 2017, incidents were reported with the assumption of falsification of the GPS signal, specifically a series of ships in the Black Sea reported anomalies with their position derived from GPS and found themselves apparently located in the continental area, at an airport (Rogoway, 2017). In addition to the events in the Black Sea, GPS outages were also reported in eastern Finland, in the eastern Mediterranean near Cyprus, Turkey, Lebanon, Syria, Israel and northern Iraq.

There are essentially two ways to interfere with GPS signals: *jamming* and *spoofing*. As the word *jamming* suggests, this method completely blocks the signal, and this type of interference is known from military bases, where one would not want to allow the enemy to track movements, having GPS support. *Jamming* is at hand because the GNSS signals transmitted by the satellites are relatively weak; a portable one-kilowatt jammer is said to block a GPS receiver from up to 50 miles away!

Spoofing is a more advanced interference where a radio transmitter sends fake GNSS signals that make the receiver think they are real satellite signals. This is a significantly more complex method of jamming, as it must be able to reproduce several GNSS signals in parallel so that the receiver does not detect that they are false signals.

Spoofing is not a new threat – it has been around for decades, but it is only in recent years that it has received more attention. As with jamming and anti-jamming technology and most other GNSS topics, spoofing has its roots in the Cold War radar era. In those days it was often known as *"false image jamming"*, where garbled radar returns were transmitted to create a false image on the adversary's radar screen.

When GPS came along, it was understood that the C/A (Coarse or Clear/Acquisition) code would be vulnerable to forgery, being an open code, so anyone can reproduce it. After all, what is a GPS simulator? A GPS spoofer. GPS receivers are usually checked using test signals from a GPS simulator. Of course, this is precisely why GPS satellites also transmit the military code P(Y) and continue to do so. The P code provides improved accuracy and other benefits, but more importantly, it is modulated with the W scrambling sequence to provide the encrypted P(Y) code. Since the anti-spoofing module has been activated, unless there is security access, it is not possible to spoof the P(Y) code.

When GPS came along, it was understood that the C/A code would be vulnerable to forgery, being an open code, so anyone can reproduce it. After all, what is a GPS simulator? A GPS spoofer. GPS receivers are usually checked using test signals from a GPS simulator.

Therefore, at the initial moment it can be argued that the threat of spoofing was solved, but it was only when GPS became ubiquitous in the commercial and civilian realms that spoofing became problematic. The fact that the vast majority of GPS receivers in the world relied solely on unencrypted C/A code became a cause for concern – especially where those GPS receivers were essential to critical infrastructure. Even so, the threat of falsifying the satellite signal has been debated for a long time, but experts have concluded that it is a theoretical threat, or that it is far too difficult to spoof, so there would be no cause for concern. However, some relevant demonstrations were performed by the University of Texas Radio Navigation Laboratory in 2012, when laboratory personnel conducted an exercise at the White Sands Missile Range where a GPS-guided drone was subjected to a signal spoofing test remote satellite. The drone was tricked into thinking its altitude was increasing, causing it to compensate by falling. Then, in 2013, the same team demonstrated how a yacht could be thrown off course by a spoofing attack. Therefore, what was thought improbable became real, the threat of spoofing existing from the beginning and proving its attack potential.

Later, evidence of an even more bizarre threat emerged, a mobile phone game, Pokemon GO, where players travelled with their phones, searching fixed locations and scoring points by collecting creatures in an augmented reality world. It did not take long for people to look for new ways to earn points in the game without having to make the effort to travel around the world from the comfort of their own home. Thus, they made the phone *"think it's somewhere else"* by distorting and falsifying the location, raising the alarm level of the threat again. Specifically, it is not known *"who set the tone"*, because in 2017 GPS signal spoofing caused chaos for phone app receivers in central Moscow, making them to show erroneous results. The extent of the problem became apparent when people played the same Pokemon GO: the fake signal, which appeared to focus on the Kremlin, moved anyone nearby to Vnukovo Airport, 32 km away!

DEMONSTRATION TIME

Navigation failures could also lead to airspace violations. Airspace over Ukraine, Moldova, Belarus and southern parts of Russia is currently off limits to operators because of the safety risk of operating in or near an active war zone.

In March this year, the European Union's Aviation Safety Agency (EASA) warned in a statement that satellite navigation systems – the American GPS service and Europe's similar Galileo signal – were affected in areas around Russia and warned of disruptions of vital air navigation safety equipment by what appears to be a malicious party (Katz, 2022).

EASA suggests that the problems of the system are caused either by blocking it or by providing misleading data. The number of such cases that have emerged has intensified in regions close to Russia's borders, along the Kaliningrad province. The effects of spoofing were observed in various phases of flight, forcing pilots to divert planes or change the final destination of an aircraft mid-flight, EASA said in the safety bulletin to operators (Ib.). The impact of interference ranges from loss of basic waypoint navigation to preventing runway approach or false triggering of terrain warnings.

Navigation failures could also lead to airspace violations. Airspace over Ukraine, Moldova, Belarus and southern parts of Russia is currently off limits to operators because of the safety risk of operating in or near an active war zone. Russia has also banned almost all European operators from flying in its skies after Britain, the European Union and others sanctioned Russian airlines.

The effects of GNSS jamming and/or possible spoofing have been observed by aircraft in various phases of their flights, leading in some cases to rerouting or even changing their destination due to the inability to perform a safe landing procedure. *"Under the present conditions, it is not possible to predict GNSS outages and their effects. The magnitude of the issues generated by such outage would depend on the extent of the area concerned, on the duration and on the phase of flight of the affected aircraft"* (Johnson, 2022).

Therefore, some of the problems that have been encountered or potential malfunctions that can occur due to jamming include:

- Loss of ability to use GNSS for waypoint navigation;
- Loss of Area Navigation Approach (RNAV) capability;
- Inability to conduct or maintain Required Navigation Performance (RNP) operations, including RNP and RNP approaches (clearance required);
- Triggering terrain warnings;
- Inconsistent aircraft position on navigation display;
- Loss of automatic-broadcast dependent surveillance functionality;
- Failure or degradation of air traffic management (ATM), air navigation services (ANS) and communications, navigation and surveillance (CNS) systems and aircraft using GNSS as a time reference;
- Potential airspace violations and/or route deviations due to GNSS degradation (Matei, 2002).

"Under the present conditions, it is not possible to predict GNSS outages and their effects. The magnitude of the issues generated by such outage would depend on the extent of the area concerned, on the duration and on the phase of flight of the affected aircraft".

Seen as potential threats, but not considered to be conduct, a number of mitigation measures have been issued, including requiring aviation authorities to be prepared to provide alternative terrestrial and non-satellite navigation systems in affected areas and issuing instructions to pilots to be prepared to revert to classical landing procedures excluding satellite services.

Following the outbreak of the conflict in Ukraine, jamming was detected by US reconnaissance aircraft in the Black Sea area, but did not interfere with US support operations, according to a spokesman for the US Space Command: *"There is no impact on US forces and allies in Europe at this time"* (Hitchens, 2022). It is also unclear whether the jamming had an effect on Ukrainian operations in the country.

The Russian military has routinely jammed GPS receivers in eastern Ukraine since the 2014 Crimea conflict and often spoofs GPS simply to disguise President Vladimir Putin's movements around Moscow, according to a 2019 report by the non-profit Centre for Advanced Study of Defence. Localised jamming of ground-based GPS receivers – rather than jamming or cyberattacks on the 30 GPS satellites currently operated by the Space Force – has become almost routine since the 1998 Kosovo War in many of today's conflict zones, like Syria, experts say.

COUNTERMEASURES – VIABLE OR USELESS?

Let us imagine a situation where the GLONASS satellite navigation system is sanctioned and asked to shut down the system. Given that this is a Russian system, there is only one way to physically stop it – to take the satellites out of orbit. Currently, no one owns such weapons, so it is an inactive option. It is also impossible to force a state to abandon its own system, Russia can anyway build and launch satellites on its own, as the Russian military-industrial complex is immune to various sanctions from most states. It seems that disabling GLONASS is practically impossible, and this leads to the impossibility of sanctions against Russia's satellite constellation.

Russia can anyway build and launch satellites on its own, as the Russian military-industrial complex is immune to various sanctions from most states. It seems that disabling GLONASS is practically impossible, and this leads to the impossibility of sanctions against Russia's satellite constellation.

Continuing the scenario, GLONASS will no longer exist, but it is possible that the new satellite configuration will not change anything: a handy example is represented by smartphones that will have support for other satellite systems, will work and display coordinates regardless of the owner nationality and the country/region/space they are active. Private chipset companies may be forced to remove GLONASS support, but even if this happens, it is unlikely to happen instantly, the development of new chips is not a fast process, so it could take several years before the physical disappearance of GLONASS in chipsets. Disabling GPS on Russian territory is difficult and certainly not necessary for anyone, the USA is unlikely to do it. In addition, there is the Chinese system that cannot be influenced.

The most important indication that disabling the Russian satellite constellation is not the goal to be pursued is that Russian Military Doctrine assumes that GLONASS and other GNSS will not be available once a battle begins, therefore Loran-C[1] will be relied upon instead for navigation! (Cozzens, 2022). In other words, Russian forces, as they are experts in jamming and falsifying GNSS signals, believe that signals from space, including their own GLONASS and other GNSS, will not be available once a battle begins, or will be tampered with. According to the Radionavigation Plan for Russia and the Commonwealth of Independent States (CIS), the ground-based Chayka system, a version of Loran-C, is maintained to protect its territory with navigation and timing services when signals from space are not available. There is also the portable Skorpion System which is designed for military use during expeditions to areas where Chayka or Loran are not available.

"Russia has three Chayka stations that surround Ukraine", explained UrsaNav CEO Charles Schue, referring to a graphic provided by GPS World. *"They should provide coverage throughout Ukraine with a navigation accuracy of between 20 and 50 meters. If Russians have a so-called eLoran system, which is an upgraded version of Loran, they may possibly get up to 5-to-10-meter accuracy"* (Hovgaard, 2002).

One of Loran's three transmission sites is in Crimea, a territory annexed by Russia in 2014. *"The main reason Crimea was annexed may have been to provide access to the ocean"*, Schue said, *"but it allowed them to regain control of the Loran transmission site there. This provided them with sovereign terrestrial PNT (positioning, navigation and timing) for the entire region, including the Black Sea"* (Cozzens, ib.).

There is the possibility, at least in theory, that Russia might be able to render the GPS satellites useless using a cyberattack. As I said before, physical suppression is unlikely, even if there are belligerent statements in this regard, the orbits on which the satellite navigation systems operate being at an altitude of about 20,000 kilometres from Earth. Even if there were such a strike, the entire satellite constellation cannot be suppressed, there are spare satellites, others can be launched and the other existing navigation systems must also be considered.

ROMANIAN MILITARY THINKING

According to the Radionavigation Plan for Russia and the Commonwealth of Independent States (CIS), the ground-based Chayka system, a version of Loran-C, is maintained to protect its territory with navigation and timing services when signals from space are not available. There is also the portable Skorpion System which is designed for military use during expeditions to areas where Chayka or Loran are not available.

[1] Long RAnge Navigation/LORAN is a hyperbolic radio navigation system developed during the Second World War in the USA. It allowed a receiver to determine its position by listening to low frequency radio signals that were transmitted by fixed land-based radio beacons. Loran-C combined two different techniques to provide a signal that was both long-range and highly accurate, features that had been incompatible. Its disadvantage was the expense of the equipment needed to interpret the signals (https://lwvworc.org/ro/which-is-the-counterpart-system-of-loran, retrieved on 22 August 2022).

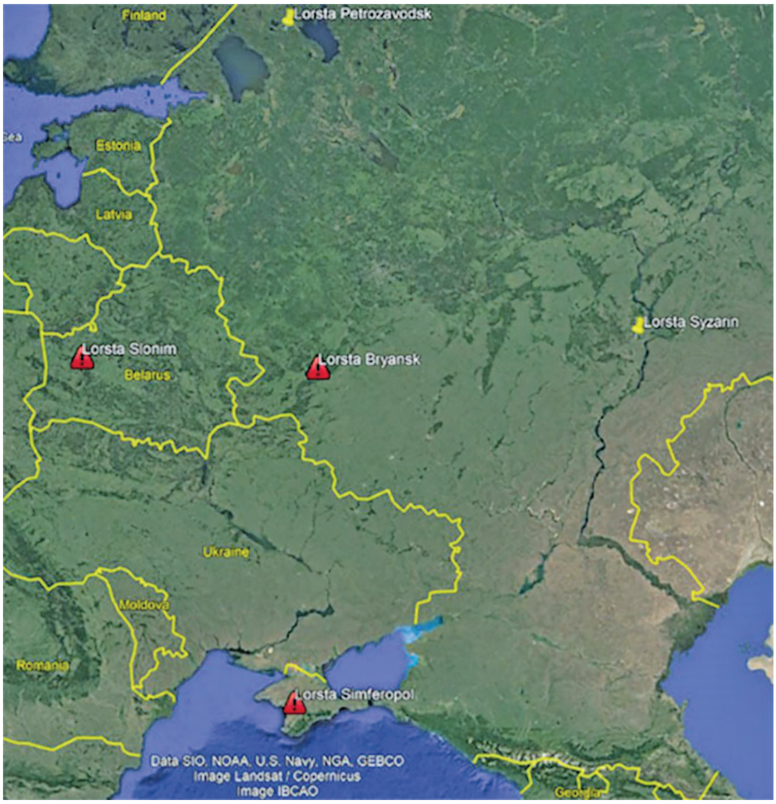

Figure no. 1: According to GPS World, Russia has three Loran stations that, at least in theory, can cover Ukraine.
Image: Charles Schue, UrsaNav (https://www.gpsworld.com/russia-expected-to-ditch-glonass-for-loran-in-ukraine-invasion/, Hovgaard, ib.).

Otherwise, an attack on GPS would be an attack on the USA and the obvious risk is to draw NATO into the conflict. But it is very unlikely to resort to such a dramatic step just to prevent the Ukrainian attacks, the action practiced remaining at the level of altering the satellite signals at the receivers.

An attack on GPS would be an attack on the USA and the obvious risk is to draw NATO into the conflict. But it is very unlikely to resort to such a dramatic step just to prevent the Ukrainian attacks.

But Russia made a show of force by destroying its own satellite in orbit! This is what a true piece of news from 2016 sounded like: *"Russian anti-satellite missile test draws condemnation"*, said Ned Price, a representative of the US diplomatic department (Amos, 2021). I do not want to develop the subject as in the political environment, where the serious consequences on the orbital environment through the waste produced have been revealed, but to express what everyone understands – the development of anti-satellite weapons also generates

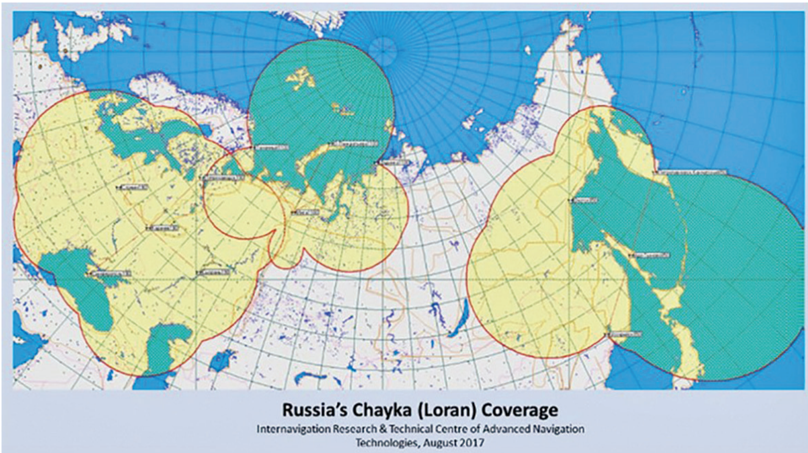

Figure no. 2: 2017 coverage map from Internavigation Research Centre and Advanced Navigation Technical Centre of Russia showing that Chayka serves Eastern Europe, Western Russia and almost all of the Black Sea (Cozzens, ib.).

tests as an exhibition of power. That is why it should be remembered that on this chessboard, China made the first move in 2007, followed by the USA in 2008 and India in 2019, each shooting down their own decommissioned satellites. In 2020 London and Washington accused Moscow of testing a *"Matryoshka doll"* satellite that opened up and released a smaller craft to track a US satellite; so how long was until Russia's test? However, all the demonstrations presented were in orbit about 500 kilometres from Earth, and the GNSS are at 40 times higher attitudes!

To counter such a threat, the USA also developed alternatives to satellite navigation, even though they abandoned LORAN. Thus, in June of this year, the US Air Force conducted its final test of a radar-assisted targeting system for the B-2A bomber, which enables precision guidance of weapons in a GPS-degraded environment. The Radar Aided Targeting System (RATS) bomber dropped a B61-12 nuclear bomb during the final test at Tonopah Test Range, Nevada. The test was the first production unit version of the Joint Test Assembly (JTA) B61-12, whose full-scale production began in May this year: *"We have flown several sorties testing the new RATS capability over the past nine months and collected test points on its performance"*, said 72d Test and Evaluation Squadron (TES) B-2 Weapons Flight Commander Capt. David Durham. TES also tested an in-house designed software

In June of this year, the US Air Force conducted its final test of a radar-assisted targeting system for the B-2A bomber, which enables precision guidance of weapons in a GPS-degraded environment. The test was the first production unit version of the Joint Test Assembly (JTA) B61-12, whose full-scale production began in May this year.

tool that provides early indications of RATS functionality, verifying that the system is working properly before the weapon is launched (Bisht, 2022).

CONCLUSIONS

The state of conflict generates real challenges that dismantle or confirm scenarios prepared in peacetime, but history shows us that, most of the time, neither the aggressor nor the aggressed had the necessary data to obtain the expected results. Success was almost always achieved by those who knew how to adapt, use and discern the available information, exploit intensively and secure what they possess.

"I would tell everybody that the important thing is to go off and ensure that your systems are secure and that you're watching them very closely because we know that the Russians are effective cyber actors".

In the days before the Russian invasion, US space officials warned satellite companies that the conflict could extend into space. *"I would tell everybody that the important thing is to go off and ensure that your systems are secure and that you're watching them very closely because we know that the Russians are effective cyber actors"*, National Reconnaissance Office Director Chris Scolese said at a National Space Security Association conference held on 23 February. *"And, again, it's hard to say how far their reach is going to go in order to achieve their objectives. But it's better to be prepared than surprised"*. (Erwin, 2022).

"And, again, it's hard to say how far their reach is going to go in order to achieve their objectives. But it's better to be prepared than surprised".

Navigation systems with satellites will continue their missions unhindered, because there are no such sophisticated weapons capable of attacking them, but there is also no intention of any state to stop them. The synergistic desire is GNSS cooperation for the benefit of humanity by increasing the quality of life on Earth, considering that satellite solutions become much more accurate and fast when signals are received from several satellites; if a constellation of at least 24 satellites is required for global coverage, we have to imagine what the information update rate would be like if we received signals from *"united satellite constellations"*, which would mean, at this point, around 75 satellites.

BIBLIOGRAPHY:

1. Amos, J. (2021). *Russian anti-satellite missile test draws condemnation*, https://www.bbc.com/news/science-environment-59299101, retrieved on 21 August 2022.
2. Bisht, I.S. (13 July 2022). *USAF Tests B-2 Bomber System for GPS-Denied Environments*. The Defence Post.

3. Cozzens, T. (2022). *Russia expected to ditch GLONASS for Loran in Ukraine invasion*, https://www.gpsworld.com/russia-expected-to-ditch-glonass-for-loran-in-ukraine-invasion/, retrieved on 17 August 2022.
4. Culliford, E. (2002). *Google temporarily disables Google Maps live traffic data in Ukraine*, https://www.reuters.com/technology/google-temporarily-disables-google-maps-live-traffic-data-ukraine-2022-02-28, retrieved on 12 June 2022.
5. Erwin, S. (2022). *NRO warns satellite operators of possible Russian attacks*, https://spacenews.com/nro-chief-warns-satellite-operators-to-secure-their-systems-as-ukraine-crisis-unfolds, retrieved on 12 June 2022.
6. Hitchens, T. (2022). *Local Russian GPS jamming in Ukraine hasn't affected US support ops, so far*. Breaking Defense.
7. Hovgaard, L. (2002). *Russia does not trust satellite navigation: Revives old land-based radios*, https://ing.dk/artikel/russia-does-not-trust-satellite-navigation-revives-old-land-based-radios-254607, retrieved on 22 July 2022.
8. Johnson, K. (2022). *Airlines Report Russian GPS Jamming in Four Regions*, https://www.flyingmag.com/airlines-report-russian-gps-jamming-in-four-regions, retrieved on 22 July 2022.
9. Katz, B. (2022). *Someone Appears to Be Messing with GPS Near Russia, Europe's Air Safety Agency Warns*. In *The Wall Street Journal*, https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-17/card/someone-appears-to-be-messing-with-gps-near-russia-europe-s-air-safety-agency-warns-KVcaNmYR7uzWOiuiyPLu, retrieved on 22 July 2022.
10. Matei, A. (2022). *Posibile interferențe* în *transportul* aerian, https://traficmedia.ro/posibile-interferente-in-transportul-aerian/, retrieved on 12 June 2022.
11. Rogoway, T. (2017). *Russia may be testing its GPS spoofing capabilities around the Black Sea*, https://www.thedrive.com/the-war-zone/13549/russia-may-be-testing-its-gps-spoofing-capabilities-around-the-black-sea, retrieved on 21 July 2022.
12. Inside GNSS (2007), *Why War, Precisely?,* https://insidegnss.com/why-war-precisely/, retrieved on 22 July 2022.
13. https://lwvworc.org/ro/which-is-the-counterpart-system-of-loran, retrieved on 22 August 2022.