CENTRE FOR AIR POWER STUDIES

In Focus

New Delhi

CAPS InFocus: 19/2022

15 March 2022

Counterspace Efforts in Russia's Military Action in Ukraine

Group Captain TH Anand Rao
Senior Fellow, CAPS

Keywords: Radio frequency, Interference, Military, GPS, Starlink, Ukraine

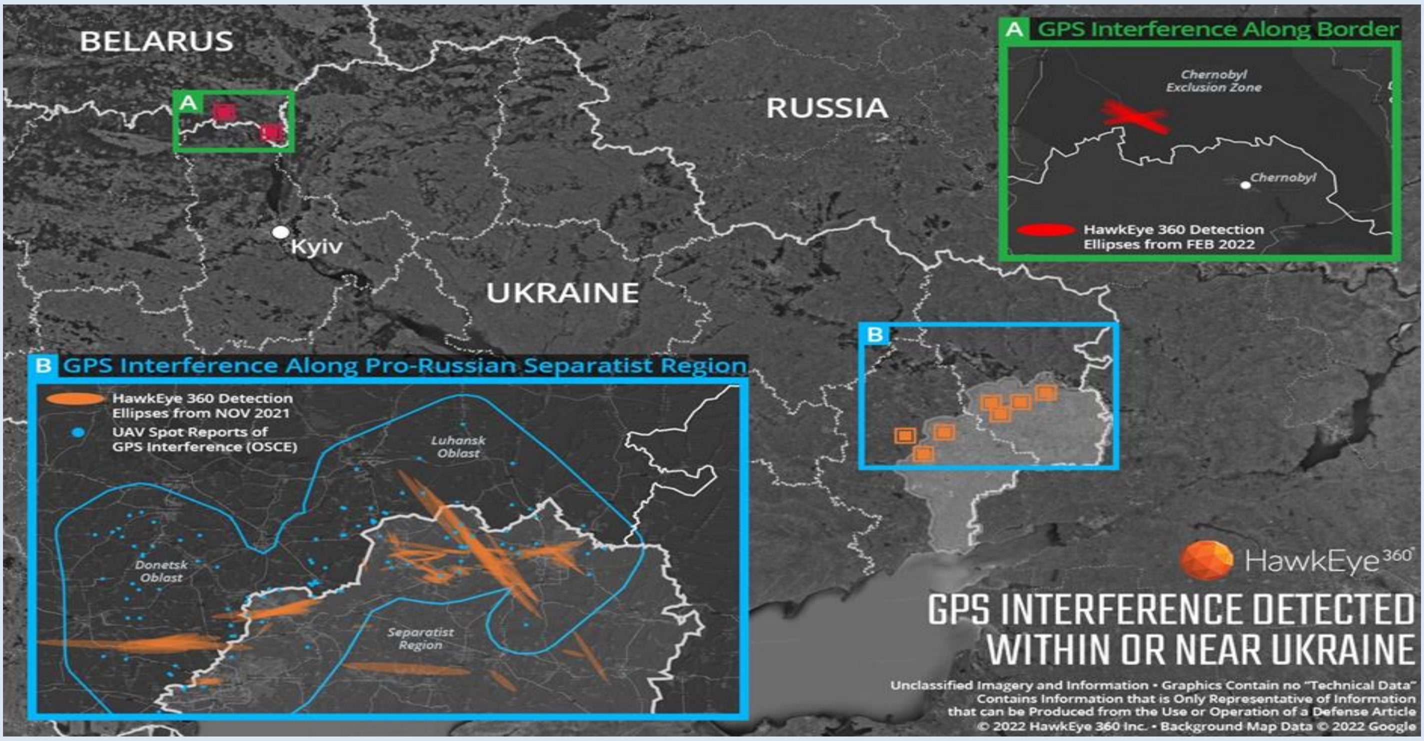
BELARUS
A
RUSSIA
Kyiv
UKRAINE
A GPS Interference Along Border
Chernobyl Exclusion Zone
Chernobyl
HawkEye 360 Detection Ellipses from FEB 2022
B
B GPS Interference Along Pro-Russian Separatist Region
HawkEye 360 Detection Ellipses from NOV 2021
UAV Spot Reports of GPS Interference (OSCE)
Luhansk Oblast
Donetsk Oblast
Separatist Region
HawkEye360
GPS INTERFERENCE DETECTED WITHIN OR NEAR UKRAINE
Unclassified Imagery and Information • Graphics Contain no "Technical Data" Contains Information that is Only Representative of Information that can be Produced from the Use or Operation of a Defense Article
© 2022 HawkEye 360 Inc. • Background Map Data © 2022 Google

Image Source: www.he360.com

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS]

Space has long been an enabler of military functions, and it goes without saying that modern wars cannot be fought without utilising space assets by the land, sea, and air forces. The Gulf War (Op Desert Storm) demonstrated how the US forces could make use of the Global Positioning System (GPS) to have an advantage in unfamiliar overseas terrain. The air war over Kosovo is perhaps a fine example of how satellites played a vital role in intelligence gathering and targeting, which improved the precision factor in aerial strikes and reduced collateral damage. Successive military conflicts since the Cuban missile crisis of 1962 have seen a rising component of satellite usage. Military satellites can be employed for multiple tasks that have a direct bearing on operational capabilities, such as early warning, intelligence, surveillance, reconnaissance (ISR), communication, data relay, navigation, and weather prediction.

As for the Russian special military operations in Ukraine, it was expected that military operations would be preceded by cyber-attacks, electronic warfare, and space support prior to any movement of military troops and equipment across the borders. How much of that has happened is still to be discovered, though there is evidence of some electronic interference and cyber activity from both sides and disruptions in the use of space resources.

Disruption of Communications

The initial evidence of loss of data services and communication in some parts of Ukraine surfaced when Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, appealed to Elon Musk on Twitter, saying, "while you try to colonize Mars -- Russia try to occupy Ukraine! While your rockets successfully land from space -- Russian rockets attack Ukrainian civil people! We ask you to provide Ukraine with Starlink stations and to address sane Russians to stand."[1] There was a sense of desperation in the tweet, which called for an urgent action. The response from SpaceX CEO Elon Musk was swift, and the Starlink satellite internet service was extended to the Ukraine region within a day. The satellite terminals required to make the data service operational were also shipped to Ukraine to restore essential communication and data services. However, end-users in far-flung areas will still remain blacked out unless they import Starlink satellite dishes or improvise with locally available dish antennae to receive signals from the service. Even though additional consignments of satellite receiver equipment have been sent by SpaceX, it is unclear how those supplies will reach the Ukrainian people when the battle has reached the streets. The Ukrainian government has made innovative use of the messaging application Telegram, to keep its citizens informed of various information required during the war. The availability of the internet is the backbone of their messaging services.[2]

With the Starlink network being the only non-Russian communications system operating in Ukraine, there are high chances of it being targeted. Despite the robust Starlink satellite network and the use of the latest software update to bypass the jamming, some Starlink terminals near conflict areas have experienced jamming for several hours at a time. Viasat's KA-SAT satellite in geostationary orbit, which provides broadband service to Ukraine and other parts of Europe, has suffered service disruptions since the military operations started on February 24, 2022, which has been attributed to cyber-attacks.[3]

Prior to the war, connectivity in Ukraine was provided by the Inmarsat and Iridium satellite constellations. Many of these services are still intact but may be unreliable due to outages. Terrestrial mobile connectivity has still eluded the Russian forces in some areas. Starlink remains the only non-Russian communications system still working in some parts of Ukraine affected by military operations.[4]

GPS Interference

Given the dependence on it for navigation and targeting, interference of GPS signals is perhaps the simplest of all means of disrupting adversaries' tactics. It has become a ubiquitous military action towards shaping the battlefield since the conflict in Kosovo. It was anticipated that Russia would undertake GPS interference, given its wide-ranging capability to jam and/or spoof GPS receivers. The Russian military is known to have routinely jammed GPS in Eastern Ukraine since the Crimean conflict in 2014 and often spoofs GPS. As enumerated by Brian Weeden of Secure World Foundation, Russian soft kill counter-space capabilities are fully integrated into their warfighting tactics at the doctrinal and operational levels.[5]

A US-based radio frequency spectrum geo-analytics company, HawkEye 360 Inc, which has the capability to detect and geolocate GPS interference, claims to have examined Ukraine through space-based geo-analytics over the months preceding the Russian special military operations. They discovered a high level of GPS interference across the region. The data analysis indicated extensive GPS interference in November 2021 in the regions of Luhansk and Donetsk. It was later confirmed through open-source intelligence that Ukrainian Unmanned Aerial Vehicles (UAVs) operating in the area faced disruptions due to erroneous GPS signals. Later, in February 2022, the company detected GPS interference along the border between Ukraine and Belarus (near Chernobyl), shortly before the Russian military operations started. These inputs further confirmed the integration of electronic warfare and counter-space tactics into Russian military operations, which degraded Ukraine's defences.[6]

What Next!

Besides the SpaceX Starlink network support for internet and data services, Ukraine is dependent on western sources for imagery intelligence on Russian troop movements. This real-time tactical intelligence has been a vital link in bolstering Ukraine's military counter-offensive operations, which has resulted in heavy losses for the Russian forces. There are speculations that these satellites could be targeted by Russian anti-satellite weapons, but that would be an act of escalation. Russia may not resort to the targeting of NATO's space infrastructure unless provoked. In contrast, the head of Russia's space agency made a statement to caution that Russia will treat any hacking of its satellites as a justification for war.[7]

Russia has significant counter-space capabilities like kinetic ASAT weapons, laser directed energy weapons, electronic interference, and cyber warfare tactics. These could be used in full measure to blunt the space support to Ukrainian armed forces. However, Ukraine enjoys space support of American and European origin. Any attempt to disrupt this space support would invoke a collective response from NATO in terms of Article 5 of the North Atlantic Treaty. In 2019, NATO allies adopted a space policy recognising space as a new operational domain, alongside air, land, sea, and cyberspace. Therefore, any escalation of the war over Ukraine is certain to extend into space.

NOTES

[1] Emma Tucker, Melissa Alonso and Jackie Wattles, "SpaceX Starlink user terminals arrive in Ukraine, officials says" *CNN report*, March 1, 2022, https://edition.cnn.com/2022/02/27/business/starlink-activated-ukraine/index.html, accessed on March 13, 2022.

[2] Eamon Barrett, "Elon Musk says Starlink has expanded its internet service to Ukraine, but it's unclear if anyone can actually use it", *Fortune*, February 28, https://fortune.com/2022/02/28/elon-musk-starlink-station-ukraine-internet-russia-spacex/, accessed on March 13, 2022.

[3] Jeff Foust, Brian Berger, "SpaceX shifts resources to cybersecurity to address Starlink jamming", *Space News*, March 05, 2022, at https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/, accessed on March 05, 2022.

[4] Ibid.

[5] Theresa Hitchens, "Russia could target American space firms to blind Ukraine", *Breaking Defense*, February 15, 2022, https://breakingdefense.com/2022/02/in-ukraine-conflict-russia-could-go-after-american-commercial-isr-providers/, accessed on March 06, 2022.

[6] Press Release, "Hawkeye 360 Signal Detection Reveals GPS Interference In Ukraine" *HawkEye 360*, March 04, 2022, https://www.he360.com/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine/, accessed on March 05, 2022.

[7] Alexander Smith, "Russia space agency head says satellite hacking would justify war -report", *Reuters*, March 03, 2022, https://www.reuters.com/world/russia-space-agency-head-says-satellite-hacking-would-justify-war-report-2022-03-02/, accessed on March 09, 2022.