Volume XI, Issue 7

4 November 2026

Weekly Intelligence Brief

A Chanticleer Intelligence Brief Project



Ukraine Sanctions Russian and Belarusian Companies Building Satellite Internet System

Michael Bottego
Analyst | Russia Desk

On 28 OCT, The Ukrainian Ministry of Defense released information about imposing sanctions on 49 aerospace, engineering and technology companies from Belarus and Russia that are allegedly working together to develop a low Earth orbit (LEO) satellite broadband network, known as project RASSVET. This system is similar to the Starlink satellite communications and internet system that the United States has employed to help Ukraine with communications and data.

RASSVET has military and public safety applications and is advertised for commercial, industrial, and consumer utilization. Bureau 1440, the main Russian aerospace company leading the engineering and development of this satellite communications system, released the results of the tests on the satellite signal. The latter allegedly showed speeds of up to 10Gbits/s with a range of 1,000 km (approximately 621 miles). This system is an independent broadband communications system that could directly support Russian C4 (Command, Control, Communications, Computers) ISR (Intelligence, Surveillance and Reconnaissance). Since MAR 2026, Bureau 1440 has launched 32 satellites into LEO. The Ukrainian government has theorized that this network will use the data link in coordinated drone strikes using Shahed drones, though operational coverage of Ukraine remains limited at this time.

Russia, currently does not possess a modern internet satellite constellation capability. RASSVET would close that gap granting battlespace dominance. The required number for constant coverage of Ukraine is estimated to be 250 satellites. Ukraine is not known to have anti satellite weaponry in its arsenal.

We can assess with high confidence that it is very likely that Russia will continue to launch Rassvet LEO satellites to gain a strategic advantage in the Ukrainian battlespace.

Ebola Outbreak Leads to Civilian Violence in the DRC

Madison Bunting
Senior Analyst | Africa Desk

As of 26 OCT, the Ebola outbreak in the Democratic Republic of the Congo (DRC) had surpassed 10,000 cases, with the Centers for Disease Control and Prevention (CDC) reporting 10,172 confirmed cases and 4,932 confirmed deaths. On 24 OCT, a nurse responding to an Ebola patient was killed by a mob of people armed with machetes in Bafwasende, in the Tshopo province. Another health worker was injured in the attack. The attackers reportedly accused the nurses of spreading the disease by contaminating local water sources.

The attack is part of an ongoing series of violence against healthcare workers involved in the DRC's Ebola response. Misinformation and distrust of the government due to prior responses to Ebola have increased resistance by the population against public health measures. Previous incidents include attacks on health facilities and the murder of Congolese politician Marie-Célestin Karondwa, who publicly supported the government's response to the Ebola outbreak. These attacks, combined with the current conflict with the M23 rebels, have restricted access to humanitarian aid, including medical aid. The conflict has blocked transportation routes for delivering aid and increased the difficulty of the population receiving medical supplies, thus complicating efforts to treat those affected by the virus.

We can assess with high confidence that violence by civilians against healthcare workers is very likely to continue to complicate efforts to treat and contain Ebola. We can also assess with high confidence that without improved public trust in the healthcare system, public cooperation with the government's Ebola response is likely to decline, thus allowing the outbreak to worsen as the virus continues to spread throughout the region.



GMO Internet Cyberattack Results in Ransom Threat and Financial Losses

Atticus Brandenburg
Analyst | Cyber Desk

On 27 OCT, The Japanese company GMO Internet reported that attackers had begun leaking stolen customer information after breaching its Onamae.com Desktop Cloud service. The attack potentially affected 26,739 servers, although not all of them were confirmed compromised. Attackers demanded ¥8 billion, or approximately $50 million USD, in ransom. Unauthorized trades were also reported on customer accounts using credentials believed to have been exposed in the breach.

The incident has raised concerns about financial losses and unauthorized trading activity. Japan's Finance Minister Satsuki Katayama reported that five foreign-exchange trading companies operating in Japan, experienced unauthorized activity involving customer accounts. GMO has refused to pay the attackers, stating that payment would not guarantee the deletion of stolen information. The company is working with Japanese police and cybersecurity firms to investigate the breach, analyze customer devices for malware, and compensate affected customers. On 28 OCT, GMO announced a reward of up to ¥150 million, or $1 million USD, for information leading to the attackers' arrest or an international wanted notice. GMO is also investigating how the attackers gained access to its systems.

Although artificial intelligence-enabled penetration-testing tools developed in China have been linked to other cyber-attacks in Japan and South Korea, no confirmed evidence connects these tools or a Chinese state-sponsored group to this incident.

We assess with moderate confidence that the attackers will likely continue to release stolen information to pressure GMO into paying the ransom. The continued exposure of customer credentials could increase the risk of unauthorized transactions, financial losses, and further damage to customer trust in the coming weeks.

Weekly Intelligence Brief

Editor-in-Chief
Connor Ellinghaus

Associate Editors
Malena Santa Ana
Olivia Connell
Anna Howard

For access to past issues and other Chanticleer Intelligence Brief projects, visit our website, cibrief.org/publications/wib