Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: The Editorial Board

Leakage of satellite images - the end of control over the observation of digital space?

In the last two weeks, a security challenge that is difficult to predict has emerged in underground digital networks: the mass distribution of high-resolution satellite images from commercial platforms available via dark web forums and closed Telegram channels, as Tomorrow's Affairs has learnt from well-informed intelligence and security sources.

These are not generic images from open sources, but data that is usually only available with a commercial licence and often through contracts with state institutions.

Between 14 and 22 June, experts from Western intelligence agencies and security companies monitoring illegal digital data flows discovered dozens of packages containing photos of facilities of high strategic value: ammunition depots, military ports, industrial areas, and energy facilities in Eastern Europe, the Middle East, and South Asia.

The photos apparently originated from the networks of American and European companies, such as Planet Labs, Capella Space, ICEYE, and BlackSky.

In some cases, the metadata of the film footage indicated that it was created immediately after the overflight with a delay of only a few hours.

This suggests that access was not limited to public archives, but that it was an active exploitation of the distribution systems.

Technically, the incident is not a cyber-attack on the satellites themselves. There is no indication that objects in orbit were a target. The problem lies on the ground, in the infrastructure for managing, storing and transmitting data.

Companies that provide satellite imagery use standardised access interfaces (APIs), through which authorised users — including military authorities, crisis teams, universities, and research organisations — download images directly from servers. It was precisely these access channels that proved to be vulnerable.

According to the analyses available to Tomorrow's Affairs, the most likely exfiltration vector was a compromised client subscription with access to a large number of recordings.

This means that the data was most likely "leaked" via internal accounts and not through a traditional external security breach.

However, for understandable reputational reasons, not a single company has publicly acknowledged the breach, while investigative networks of experts and journalists (Wired, Defence One, and The Intercept) are intensively investigating and checking these significant security incidents.

When openness becomes vulnerability

The biggest danger of these leaks lies not in the images themselves but in the fact that there is no longer any control over who accesses them, when and with what intention.

In practice, high-resolution, low-latency data is becoming a tool that goes beyond research or commercial use.

Security institutions, including NATO and EU members, have for years used commercial satellites' services as an additional source for mapping hotspots, migration routes, military activities, and the aftermath of disasters.

> Openness can turn into a vulnerability when it becomes unclear who has access to the same data concurrently

Their main advantage is flexibility and availability. However, this openness can turn into a vulnerability when it becomes unclear who has access to the same data concurrently.

In practice, this means the following: if someone outside the system comes into possession of unfiltered material used by a European army, for example, they can

reconstruct the patterns of interest of this army.

By analysing the frequency of requests, the coordinates, and the time of download, it is possible to deduce which objects are the focus of attention, when surveillance is intensified, and whether there is operational preparation. Such an analysis can reveal more than the image itself — it reveals the logic of the action.

A tool in disinformation campaigns

One of the most serious examples of such a risk concerns the surveillance of military convoys and logistics routes.

When images documenting the movement of armoured vehicles or ammunition depots appear on the black markets at intervals of less than six hours, this enables precise reconstruction and possible targeting.

In an active conflict, such as the one in Ukraine, this approach eliminates the advantage of surprise and exposes critical points to attack.

An even more serious case concerns highly sensitive infrastructures, such as nuclear facilities and important energy systems.

> Footage showing the layout of cooling systems, fencing positions, access roads, and surrounding facilities can be used to plan acts of sabotage

Footage showing the layout of cooling systems, fencing positions, access roads, and surrounding facilities can be used to plan acts of sabotage.

If such data is made available unattended, even the best protected systems in operation are not operationally invisible.

The third level of threat comes from the area of narrative control. The individual who first possesses the image can decide when and how it is made available to the public.

In modern conflicts, perception is just as important as the outcome. Satellite images can be used as a tool in disinformation campaigns if they are selective, taken out of context or accompanied by suggestive commentary.

An image of a military base hours after an explosion can become an accusation — even if the explosion has nothing to do with the location.

Who controls the orbit?

This crisis also shows how different the security standards of commercial operators are.

Some use multiple layers of protection, actively log all requests and perform complex authorisations. Others allow images to be downloaded through simple commands without detailed verification of the customer's identity.

This creates an uneven playing field in which the systemic weakness of one player can threaten the entire user chain.

When a commercial network becomes vulnerable, the security of its users is jeopardised

The reactions are underway, but still without political effect. We have learnt that EUROPOL has launched a preliminary investigation.

The German Federal Office for Information Security has contacted several operators. The

European Union Agency for Cybersecurity is considering introducing minimum technical requirements for all providers doing business with public organisations.

The Pentagon is unofficially considering a "closed-loop" model for the distribution of footage used by the military — whereby each delivery would be subject to double authorisation and encryption.

More generally, this incident shows how far remote observation has moved out of the hands of states and into private systems.

And this is not just a technical change. It is also a change in the distribution of control. States no longer control all the data they use, let alone the conditions under which they obtain it.

When a commercial network becomes vulnerable, the security of its users is also jeopardised.

At a time when the digital space is expanding faster than the legal framework, the question of control over information from the orbit is no longer academic.

When such incidents happen without clear attribution, without responsibility, and without consequences, they are no longer an isolated weakness.

It is a new rule — that critical data for operational security no longer belongs to those who use it but to those who can take it without authorisation.