#CRIME AND CORRUPTION

ORBÁN'S SPYING KIT REVEALED: ISRAELI SURVEILLANCE TOOL COMBINED WITH HUNGARIAN TECHNOLOGY

Szabolcs Panyi

hundreds of millions of people via smartphone advertising data —

(VSquare)
Photo: Shutterstock

2026-04-09

Investigations
Our Investigations

making Hungary the first confirmed EU country to deploy it, in likely violation of GDPR. Moreover, our investigation confirms the existence of "homegrown" OSINT and spyware tools.

The text has been corrected to reflect that Tamás Berki's tenure at SCI-Network Ltd. ended in 2022.

Hungarian intelligence and law enforcement agencies have been operating AI-powered, open-source intelligence tools developed by Israel's Cobwebs Technologies for at least five years, an investigation by VSquare, in collaboration with Citizen Lab, reveals.

Foreign technologies are used alongside tools allegedly developed in Hungary. Such tools include an OSINT software and a mysterious spyware tied to SCI-Network Ltd., the same Hungarian firm that purchased Cobwebs' licenses for the Orbán government.

The most powerful previously unknown Cobwebs product used by Hungarian authorities is called Weblock, also known as WebLoc or Webloc.

According to Citizen Lab's fresh full research paper, "Webloc is a global geolocation surveillance system that monitors hundreds of millions of people based on data purchased from consumer apps and digital

advertising." In short, Webloc uses smartphone apps' advertising data for mass surveillance without the knowledge or consent of users.

Hungary is the first confirmed country to deploy Webloc within the European Union, where data protection and privacy rules under the General Data Protection Regulation (GDPR) effectively prohibit such use of personal and advertising data.

Documents on Cobwebs licenses reviewed by VSquare as well as multiple sources with ties to Hungary's intelligence community confirm that Hungarian authorities have been using tools from Cobwebs Technologies, including Webloc, since at least early 2022. A new round of Cobwebs license renewals — including Webloc — was completed in March 2026, weeks before the country's April 12 parliamentary elections.

The recent license renewals were first reported by Hungarian weekly HVG and later confirmed by VSquare's sources. As intelligence procurements in Hungary are classified, no public records of these contracts exist.

However, our investigation has also uncovered the use of native, Hungary-developed OSINT surveillance tools and a spyware, linked to the same broker company – SCL Network Ltd. – involved in the

SCI-Network Ltd. – involved in the Cobwebs deal.

The revelation adds a new chapter to Hungary's long and controversial relationship with advanced Israeli surveillance technology, already marked by the Pegasus and Candiru scandals documented by international researchers and journalists, including in the Pegasus Project, in prior years.

Hungary's Special Service for National Security (NBSZ), which is responsible for license purchases for Hungarian intelligence, as well as the broker company SCI-Network Ltd., did not respond to our request for comment.

Penlink, the US company which has since acquired Cobwebs Technologies, contested Citizen Lab's findings but did not provide details. The company also did not deny selling its products to Hungary. (Its full reply can be found in Citizen Lab's paper.)

The New Israeli Toolkit

Cobwebs products were first purchased in late 2021 and likely deployed from early 2022 by at least three of Hungary's main civilian intelligence agencies: the National Information Centre (NIK/NIC), the Constitution Protection Office (AH), and the Special Service for National Security (NBSZ). The last of these is Hungary's signals intelligence agency,

responsible for surveillance and interception on behalf of other national security bodies. This was corroborated by sources with direct knowledge of the matter and documents with details of the licenses reviewed for this article.

The latest round of licenses was purchased exclusively in March 2026 by the NBSZ, which then distributed the tools to partner agencies across the Hungarian intelligence and law enforcement community.

This March 2026 procurement covered five distinct Cobwebs products. According to documents reviewed by VSquare, the NBSZ purchased dozens of licenses for Tangles, almost two dozen for CoAnalyst, a few for a blockchain analysis module, and fewer than 10 for what is listed internally as “Full AI.” As for Webloc, the main focus of our investigation, NBSZ has renewed six licenses, which pertains to the number of workstations, or computers, the software can be run on.

Tangles is Cobwebs’ flagship platform — an AI-powered web investigation tool that allows users to search and monitor activity across social media, the open web, the deep web, and the dark web simultaneously. The software can be configured with an AI layer that adds capabilities including image recognition, facial recognition, optical character recognition, and natural language

recognition, and natural language processing. It allows law enforcement and intelligence agencies to search and monitor specific individuals online using AI, and can connect targets to contacts, locations, and events.

CoAnalyst is Cobwebs' generative AI layer, designed to handle complex investigations by transforming large data sets into actionable intelligence through natural language queries.

The blockchain analysis tool enables investigators to trace cryptocurrency transactions. Cobwebs' platform allows financial investigators to type in a digital identifier or blockchain address and find the identity of the person it is linked to. It can also help them find unknown addresses and accounts found by searching across the open, deep, and dark webs.

The "Full AI" package is understood to refer to the full suite of AI-enhanced add-ons — facial recognition, natural language processing, and automated insight generation — bundled as a single upgrade to the base Tangles platform.

Finally, the crown jewel of the intelligence toolkit, Webloc, is a location intelligence module and an extremely intrusive mass surveillance system. The platform gathers and analyzes web data fused with geospatial data points, using interactive layered maps to connect the digital world with physical data. It allows for the tracking of mobile

It allows for the tracking of mobile devices within a user-designated area, in a process known as geofencing, relying on location data gathered by smartphone applications for advertising purposes, including unique identifiers for each Google or Apple device.

Citizen Lab obtained, via a research partner, a leaked document from 2021, tied to a Webloc contract with El Salvador's National Civil Police. The file offers a detailed overview of the system, including several user interface screenshots. One example shows Webloc tracking a person traveling from Germany through Austria to Hungary, based on 39 past location points out of 500 collected by the system.

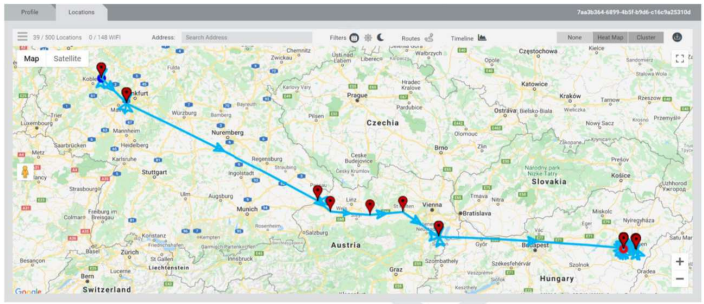

Figure 3: Webloc example screen taken from the El Salvador document

Another Webloc table, from the leaked El Salvador document, shows the profile attributes of a person in Budapest. However, it is unclear which country used the tool to surveil this individual.

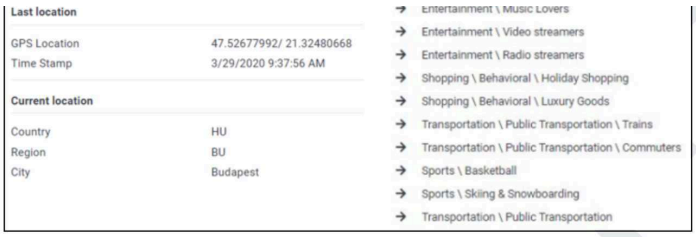

Figure 6: Webloc table on profile attributes taken from the El Salvador document

In Europe, sharing data collected for advertising purposes with governments that use it for surveillance has been widely considered illegal under the General Data Protection Regulation (GDPR).

In Hungary, it is the responsibility of the Hungarian Data Protection Authority (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH) to enforce the GDPR and investigate the use of Webloc by Hungarian intelligence and law enforcement.

In previous revelations about political use of spyware, such as NSO Group's Pegasus, NAIH has exclusively issued "nothing to see here" conclusions — providing legal cover for the Orbán government's abusive cyberespionage operations rather than showing any concern for citizens' personal data.

NAIH did not respond to our request for comment.

Cobwebs and PenLink: Israeli Roots, American Ownership

Cobwebs Technologies was founded in 2015 by Udi Levy, Shay Attias, and Omri

Timianker, all veterans of Israeli Defense Forces special units. They developed a search engine capable of scouring the dark web and the deep web for potentially illegal or terrorist activity. The company, headquartered in Herzliya, built its client base primarily among national security agencies and law enforcement in the United States and Western Europe.

In July 2023, American private equity firm Spire Capital acquired Cobwebs Technologies for approximately $200-250 million. Spire Capital's existing portfolio included PenLink, an American company specializing in intelligence analysis based on digital evidence, and the two companies were subsequently merged into a single platform. PenLink is headquartered in Lincoln, Nebraska, and formally describes itself as American-owned and operated.

Despite the corporate restructuring, Cobwebs' Israeli character has remained largely intact. The company's founders remained in executive roles after the merger, and its product development teams continue to operate out of Israel. The firm's intelligence and engineering staff are drawn from the same pipeline of IDF and Mossad veterans who built the Israeli

cyber industry.

The company has not been without controversy. In 2021, Meta banned Cobwebs and six other companies that it had identified as participating in an online surveillance-for-hire ecosystem, removing 200 accounts operated by Cobwebs and its customers.

Meta's report noted that Cobwebs customers were not solely focused on public safety activities, and that its researchers also observed frequent targeting of activists, opposition politicians, and government officials in Hong Kong and Mexico.

Developing a Failed Homegrown System — then Returning to Cobwebs

Hungary's 2026 Cobwebs license renewals did not come in a vacuum. Multiple sources with ties to Hungary's intelligence community say they followed the collapse of a costly domestic alternative.

SCI-Network Ltd. is a company headed until May 2022 by former Hungarian counterintelligence colonel Tamás Berki, who reportedly has close ties to Antal Rogán, the influential head of the Prime Minister's Cabinet Office. Rogán

oversees Hungary's civilian intelligence agencies as well as Prime Minister Viktor Orbán's vast propaganda machine.

According to sources with ties to Hungary's intelligence community, SCI-Network Ltd. — the broker company later used to purchase the Cobwebs licenses — had previously been contracted to build a homegrown OSINT platform at Hungarian taxpayers' expense. One source recalled the system by the name Quvasz or Q-VASZ, an apparent reference to the kuvasz, one of Hungary's most ancient and storied dog breeds.

How much public money was spent on Quvasz/Q-VASZ is unknown, but multiple sources described the sum as running into tens of billions of forints — equivalent to tens of millions of euros. The verdict, according to everyone who discussed it, was that it was a failure: the system proved technically inferior to commercial alternatives like the Cobwebs suite, and Hungarian intelligence officers were reluctant or unable to use it.

Rather than writing off the investment and procuring Cobwebs directly, the state opted to keep routing purchases through SCI-Network Ltd. — the very company behind the failed system.

That arrangement has come at a price. Multiple sources alleged that

the inclusion of SCI-Network as a broker has inflated the cost of the Cobwebs licenses by at least 100 percent compared to a direct procurement. Hungarian weekly HVG reported that the broker company applied a 3x markup on the manufacturer's price when selling the licenses to NBSZ.

We could not independently verify that figure, and the company did not respond to our questions about the price or what value it adds as a broker compared to purchasing licenses directly from Cobwebs. What is clear is that routing the procurement through a middleman adds a substantial layer of opacity to an already classified process.

According to multiple sources with direct knowledge, an officer of the Special Service for National Security (NBSZ) conveyed the message at a security industry exhibition in Dubai that Hungary wished to purchase the tools through SCI-Network rather than directly.

SCI-Network Ltd's Tamás Berki established himself in the private cybersecurity and AI market after leaving the counterintelligence. Multiple intelligence sources interviewed for this story described Berki as a "fixer" for Antal Rogán, head of the Hungarian Prime Minister's Cabinet Office.

A 2019 conference agenda confirms

that BerKI specialized in AI and cybersecurity tools during his counterintelligence career. Multiple sources alleged that he has spoken openly about his close ties to Rogán.

Hungary's Homegrown Spyware or Cover for Foreign Technology?

SCI-Network's ambitions appear to extend well beyond OSINT platforms. Multiple sources with ties to Hungary's intelligence community told VSquare that the company has also developed a spyware tool capable of targeting mobile phones — placing it in a category of technology more closely associated with spyware vendors such as NSO Group or Candiru than with an open-source intelligence vendor.

One source claimed the SCI-Network spyware is, at least in some cases, capable of zero-click attacks — the most sophisticated category of mobile intrusion, in which a target's device is compromised without any interaction from the user, such as opening a link or an attachment. Zero-click exploits are expensive, technically demanding, and have historically been the hallmark of elite state-sponsored or government-contracted surveillance firms.

A separate source alleged that the "successor to Pegasus" is significantly easier to deploy, but could not provide details.

Others who discussed the tool

described significant operational shortcomings. This anonymous Hungarian spyware is reportedly “too visible” — meaning it leaves detectable traces on compromised devices. Sources also said it drains mobile phone batteries at an abnormal rate. Both are classic signatures of poorly optimised intrusion software, and the kind of tell-tale characteristics that can alert technically sophisticated targets or security researchers to a covert infection.

Whether the tool is exclusively licensed to Hungarian state agencies or private companies with ties to the intelligence world can also obtain access to it also remains unclear. No source was able to confirm the full scope of its distribution.

It is also unknown how much Israeli technology was used in developing this secret, homegrown Hungarian spyware, and which Israeli companies SCI-Network Ltd. was cooperating with, if any.

The Israeli Pegasus spyware offers a useful precedent: very few people within Hungary’s intelligence community knew the tool’s origins or real name. Multiple sources confirmed that inside Hungarian national security agencies, the spyware was referred to as “Rája” — the Hungarian word for ray, the fish — with most officers unaware of its actual name or provenance.

It is therefore possible that tools currently described as “Hungarian-developed” are in fact of foreign origin, operating under a different product name.

Hungary’s Abusive Surveillance Track Record Raises Concerns

The same sources alleged that the Cobwebs OSINT suite and Webloc could also serve purposes beyond legitimate national security work — including the monitoring of opposition figures and journalists. Neither provided direct evidence that this has occurred. They framed the concern in terms of capability rather than proven fact: the tools make such targeting technically straightforward and operationally invisible, they said, particularly given the absence of independent judicial oversight of intelligence collection in Hungary.

Hungary has already been at the center of multiple surveillance scandals involving high-end Israeli spyware.

The most well-documented is the Pegasus affair. The Pegasus Project — a cross-border investigation published in July 2021 — identified Hungary as one of the few EU member states whose governments were believed to have used NSO Group’s military-grade spyware against its own citizens, targeting journalists, lawyers, businesspeople, and opposition politicians

and opposition politicians.

The Ministry of Interior purchased Pegasus for approximately €6 million through an intermediary company, Communication Technologies Ltd., from an NSO Group subsidiary registered in Luxembourg in 2017. In November 2021, Lajos Kósa, chair of the Hungarian parliamentary committee on defense and law enforcement, publicly admitted the purchase.

Direkt36, one of the Pegasus Project's media partners, identified multiple confirmed targets in Hungary, including journalists; the owner of one of the country's largest independent media groups; a former minister who had become a government critic; and an opposition politician. The author of this article was himself among those whose phone was found to carry traces of Pegasus infection.

The second Israeli spyware detected in Hungary is Candiru. In July 2021, Citizen Lab and Microsoft reported widespread usage of Candiru spyware by various government clients, with spyware control infrastructure identified in several countries — including Hungary. Candiru's spyware, which exploits Windows vulnerabilities to deploy a persistent implant known as DevilsTongue, was used in precision attacks against targets' computers, phones, network infrastructure, and internet-connected devices. The

spyware can exfiltrate private data from numerous applications including Gmail, Skype, Telegram, and Facebook, capture browsing history and passwords, and activate the target's webcam and microphone.

German Member of the European Parliament Daniel Freund, an outspoken critic of Viktor Orbán, filed a criminal complaint after an alleged Candiru attack. "In 2024, in the middle of the European election campaign, attackers unsuccessfully attempted to install spyware on our devices," Freund claimed.

More recently, in the run-up to Hungary's April 2026 elections, new spyware allegations surfaced. Péter Magyar, leader of the opposition Tisza Party, alleged that Hungarian intelligence services deployed military-grade spyware, later naming Candiru as the tool in question, against his movement and suggested the operation may have involved cooperation with foreign powers.

Those allegations follow a Recorded Future report from 2025 that identified active Candiru DevilsTongue infrastructure linked to Hungary, with researchers assessing with high confidence that clusters of command-and-control servers in Hungary were operational.

Read Citizen Lab's report:

Uncovering Webloc. An Analysis of Penlink's Ad-based Geolocation Surveillance Tech.

Choose the amount

10.00 $	**25.00 $**
50.00 $	100.00 $
250.00 $	Custom Amount

Make this donation monthly

Who's giving today?

We'll never share this information with anyone.

First Name

Last Name

Email Address

How would you like to pay today?

This donation is a secure and encrypted payment.

Stripe - Credit Card

Credit Card Info

This is a secure SSL encrypted payment.

Card Number *

Card Number

CVC *

CVC

Cardholder Name *

Expiration *

MM / YY

Stripe - Checkout

Stripe - SEPA Direct Debit

Stripe - BECS Direct Debit

Here's what you're about to donate:

Subscribe to “Goulash”, our newsletter with original scoops and the best investigative journalism from Central Europe, written by Szabolcs Panyi. Get it in your inbox every second Thursday!

Email address:

Your email address

By filling in the data and subscribing to the Newsletter, you consent to the sending of the “Goulash Newsletter” to the e-mail address provided. The data provided in the form will not be used for any other purpose.

☐ I agree

Sign up

#CRIME AND CORRUPTION
#HUNGARY #VIKTOR ORBAN

Szabolcs Panyi

VSquare's Budapest-based lead investigative editor in charge of Central European investigations, Szabolcs Panyi is also a Hungarian investigative journalist at Direkt36. He covers national security, foreign policy, and Russian and Chinese influence. He was a European Press Prize finalist in 2018 and 2021.