The teens drawn to acts of mayhem

Minors are being recruited by Russian and Iranian agents to carry out hostile activities from Ukraine to western Europe. Preventing this hybrid warfare has become a top priority for the authorities.

Financial Times Europe
05 giu 2026
By Helen Warrell and Christopher Miller

One late afternoon last September, a 17-year-old Dutch boy was doing his homework in his family's house in Rotterdam when there was a knock at the front door.

When his father opened it, eight police officers wearing balaclavas rushed past him and stormed upstairs to the boy's bedroom. They were there to arrest the teenager on charges of rendering services to a foreign country.

The details that have emerged since have shocked both his family and Europe's security community: the boy is accused of having been recruited by Russian agents on Telegram to spy on law enforcement organisations in The Hague using a "sniffer" device, which intercepts WiFi networks.

Through interviews with police and intelligence officials in six countries across Europe and the Middle East, the Financial Times has established that this 17-year-old is one of a growing number of teenagers who are being recruited online by hostile states for spying and sabotage.

The boy — "an avid gamer who is good with computers", according to an interview with his father in De Telegraaf — is now awaiting trial. His father, who described his son as "naive", remains bewildered. "We raise our children to prepare them for all kinds of dangers in life: smoking, vaping, alcohol and drugs," he told the Dutch newspaper. "But not for something like this."

Russia and Iran have long enlisted proxies to perform hostile acts on European soil, but targeting minors represents a new twist on their subversive gig economy.

The tactic first emerged in Ukraine, where teenagers have been recruited online for sabotage, espionage and to spread propaganda. Moscow has since sought underage foot soldiers west towards Poland, the Netherlands and the UK. Tehran, spotting an opportunity to accelerate operations against Iranian dissidents in Europe, was quick to follow suit.

“Hostile states are absolutely trying to target teenagers,” says Dominic Murphy, who stepped down six weeks ago as head of the London Metropolitan Police’s counterterrorism command, which oversees investigations into national security threats across England and Wales. “I was surprised by the scale of the challenge because it really seemed to come very suddenly, 18 months ago. I was then equally surprised by the volume of youngsters that were ready and willing to engage online . . . and how quickly this was moving to real-world activity.”

Ukrainian intelligence officials tell the FT that 21 per cent of those arrested for collaborating with Russia in 2025 were teenagers. A significant proportion of the arrests made in connection with antisemitic attacks across Europe claimed by the Iranian-backed militia group Ashab al-Yamin — also known by the longer name Harakat Ashab al-Yamin al-Islamia, or Hayi — involve local perpetrators in countries such as Britain, France and the Netherlands who are under 18.

The recruitments follow a similar pattern: young people are usually approached on online channels which are well-hidden and hard to track: from Telegram to TikTok, Snapchat, Facebook and Discord. They are offered money, commonly cryptocurrencies, in exchange for completing tasks. Their recruiters depend on anonymity; many work for criminal groups which, like cyber hackers, may be independent from the state but co-opted by intelligence agencies for covert operations.

Gaming sites — the most widely consumed entertainment media among 13to 24-year-olds — have become an obvious hunting ground for potential saboteurs with a proven interest in problemsolving.

In Ukraine, the chat function in the popular online game World of Tanks is commonly used as a recruitment portal, from which agents then move the conversation to Telegram. Some statebacked agents, especially those working for Russia, also invoke the mission format and “quest” mentality of online games to entice young people to move beyond the virtual battlefield to realworld action. It is, says one western military official, “like a game of Pokémon Go, but with air defence systems”.

Preventing minors from being drawn into this net has rapidly become a top priority for Europol, the EU’s intelligence and crime-fighting agency. “We have a young generation which is slightly detached from their parents, that are educated online, often by social media or gaming platforms,” the agency’s director, Catherine De Bolle, tells the FT, in an interview conducted just before she stepped down from her post last month.

The states view the teens they employ as disposable. There is little risk for them if the operations fail, and only upside if they succeed. Any connection to Russia or Iran is hard for European intelligence agencies to prove, and for the aggressor states, entirely deniable. The jeopardy lies with the recruits, like the Dutch teenager, whose lives will be irrevocably changed if they convert online tasking into an actual mission.

The result, according to police and intelligence officials, is that Russia and Iran are exploiting a generation of digital natives to further their aims in socalled hybrid warfare — the no man's land between peace and armed conflict.

"The anonymity of the online environment gives [minors] the ability to engage in what they might see as edgy behaviour," says one British security official. "They might not see the impact or real-world consequences."

Just over a year ago, Ukrainian police arrested two groups of suspected Russian agents who were covertly photographing air defence systems on the outskirts of Kharkiv.

At first, this looked like standard espionage, directed by Moscow's FSB spy agency to advance its conflict in eastern Ukraine. But the perpetrators were not Russian infiltrators or trained agents but local teenagers.

The children, all aged 15 or 16, had been unwittingly recruited by the FSB to collect intelligence under the guise of a "quest" game — a citywide scavenger hunt in which participants compete to finish a list of challenges.

They received geographical co-ordinates of the defence systems from their Russian handlers via a chatroom, according to details of the operation uncovered by Ukraine's SBU intelligence agency. They were asked to travel to the area, take photos and videos and provide a description; Moscow later used this information to carry out air strikes on Kharkiv. Other tasks given to the groups included setting fire to Ukrainian military vehicles.

SBU intelligence officials tell the FT that far from being the exception, Russia's recruitment of minors, and even children — which began a year into the conflict — is now the norm. The Kremlin widened its net after Ukrainians who might previously have had some Russian sympathies became alienated by the war. Enlisting young Ukrainians had the benefit of destabilising the country internally, by co-opting the younger generation to subvert the war effort.

For Moscow, Ukrainian minors represent "the line of least resistance", says Laura Brady, a Ukraine-Russia analyst at the Earendel Associates consultancy. "A younger person will be less curious, perhaps, about why they're being asked to do something," she says. "They'll be cheaper to employ. There'll be less caution about going through with an activity which might seem a bit odd. Children are fundamentally more impulsive."

The SBU now believes that Russia is scaling up its targeting efforts. Brady adds that young people who are successfully drawn into Russia's sphere of influence are often challenged to recruit their peers through TikTok or Telegram or their gaming platforms, "so the recruits themselves are force multipliers".

The first signs that Moscow's hunt for young saboteurs was expanding in Europe were seen in the countries along Ukraine's border. In Poland, teenage Ukrainians were caught

spraying anti-Polish slogans on national monuments. In Latvia, Moscow has co-opted young people to distribute pro-Russian propaganda leaflets and to attack cars and buildings belonging to the Ukrainian diaspora. In Lithuania, a 17-year-old Ukrainian national, Daniil Bardadim, set fire to an Ikea store in Vilnius in 2024 on behalf of Russian security services. He pleaded guilty to arson and is currently serving a threeyear prison sentence.

At the headquarters of Latvia's VDD domestic security service in Riga, the agency's director-general, Normunds Mežviets, describes how Moscow's agents guide novice recruits through a thicket of ever riskier activities.

The first task might be just to set fire to a car. "You need guts to do it at night time, when you are alone. You have to buy a liquid, to make this Molotov cocktail, then you have to look for the target, do some reconnaissance," Mežviets says. "The risk is not very high, but there is lots of pressure. You are nervous about how to approach this target, you have to then run away, to hide yourself.

It takes something from the person, especially if this person is not experienced."

Latvian saboteurs might graduate to targeting cars with Ukrainian number plates, then Ukrainian trucks, then set fire to a property belonging to a Ukrainian émigré. The next step would be attacking critical infrastructure — an army base, where there is a fence, surveillance, and security staff. "By this time, you are emotionally and psychologically prepared to do it," Mežviets explains. Often these more sophisticated attacks are reserved for older recruits in their twenties or thirties.

Russian agents invent a range of cover stories to explain why a task needs doing. "There is some kind of legend. They'll say, 'this is a bad person who owes money to someone . . . so to punish him, here is €500. Why not burn down his car?'" says Mežviets.

The VDD chief has little sympathy for those who are taken in. "If you are not a total blockhead, sooner or later, you will understand very well what you are doing," he says.

Moscow's agents are now recruiting teenagers in western Europe, including the UK.

These cases are particularly hard to track because they only reach public attention if they come to court and there are multiple reporting restrictions around any offences involving minors.

However, the Met has acknowledged that it is arresting teenagers for sabotage and reconnaissance activities. "Children and young people are vulnerable to . . . hostile activity," Vicki Evans, the UK's senior national co-ordinator for counterterrorism policing, admitted last year. "It is a huge concern for us."

Murphy, the former Met commander, recalls that about 18 months ago the force started to notice youngsters "conducting hostile reconnaissance for a variety of different reasons on behalf of a foreign state", citing both Russia and Iran. "We were increasingly seeing younger people engaging in what looked almost like a parallel universe."

The Met has previously released data showing that 20 per cent of the people it arrests in counterterrorism cases are aged 17 or under. Murphy estimates that a similar proportion of minors are now being arrested by the force in connection with national security activity.

Just this week, a court at London's Old Bailey heard that a Norwegian teenager had been hired by a Swedish organised crime group used by the Iranian regime, to murder an unknown target in the UK.

The three people charged in connection with an arson attack on Jewish community-run Hatzola ambulances in north London, which was claimed by Hayi, are aged 17, 19 and 20.

Investigators at Europol have observed teenagers across the continent being lured to action in similar ways.

Nefarious actors congregate in online forums such as extremist right-wing Discord groups and Telegram channels. "It could be a Swedish organised crime group trafficking cocaine, or a terrorist recruiter, or a state looking for people to carry out hybrid attacks," says De Bolle, the former Europol director. "All these different actors have the same interests in trying to find young people and give them tasks."

The Dutch 17-year-old arrested in Rotterdam last year, along with an accomplice of the same age, is accused of using a WiFi-intercepting technology to eavesdrop on government and law enforcement buildings in The Hague, including Europol's own headquarters.

For De Bolle, the exploitation of minors by criminals of all types is Europol's top priority and a rapidly growing risk. Children massing on social media and gaming platforms are, she says, "super simple" to identify and recruit.

"For the groups who are using them — if they are successful, fine, if they are partly successful, fine, if this person is killed, so what? And if this person is arrested, so what? It's a fire-and-forget weapon," De Bolle adds. This is, she says, "the criminal adaptation of our throwaway society".

The first step to countering this threat is greater awareness — especially among parents, who are typically ignorant of the risks their children might encounter online.

"The public might understand the danger of young people getting drawn into terrorism in some way," says the former Met commander Murphy. "But that same concern needs to exist for young people conducting activity on behalf of foreign states."

The proliferation of new platforms and online ecosystems, which are central to teenagers' social interactions but often alien to their parents, is another significant hurdle to effective oversight.

Just as the SBU has seen Russian agents contacting young people through the World of Tanks online game, British and Swedish intelligence officials tell the FT that gaming platforms are being used for recruitment — both by terrorists and hostile states.

“Criminal gangs, terrorists and state actors will inevitably be drawn to the same online spaces, including gaming platforms, because this is where young people are gathering and communicating in large numbers,” says one official from MI5, the UK’s domestic intelligence agency. “Whether you are looking for followers, proxies or disposable agents, you might initially make contact on gaming sites or gaming-adjacent platforms before continuing to a secure communications app.”

Chat platforms such as Discord — commonly used by gamers to communicate while they are playing — have multiple functions, including text, audio and video calls across large communities. “If you think your kids are on Discord and just chatting to their mates from school, then you’re likely to be wrong,” the MI5 official warns.

A spokesperson for Discord described radicalisation and recruitment into violence as “complex societal challenges” and said it works to “identify and disrupt this behaviour where it appears, including removing content, banning users, and working with law enforcement”.

Jonathan Hall, the UK’s independent reviewer of state threats legislation, argues that a wider public conversation is needed about how young people use these platforms.

“The internet is a portal into young people. It’s incredibly powerful. It provokes strong emotions and engagement and commitment, and you’ve got manipulative people in Silicon Valley and manipulative people sitting in Tehran and Moscow. As a society, we’re beginning to understand the first category,” he says. “But I don’t think we’ve started to think about the second category at all.”