



Home Office

Proxies partner pack



OFFICIAL

Contents

Purpose of this pack	1
Letter from Director State Threats, Home Office	3
How to use this pack	4
Key messages	6
Understanding state threats and the National Security Act 2023	9
National Security Act 2023	10
What are state threats?	11
Case studies	12
Case studies – UK and beyond	13
What might increase an individual's risk of being approached?	16
Thank you	17
Useful resources and links	19

Purpose of this pack

This pack is designed as a guide for frontline service providers who have regular contact with individuals who could be susceptible to recruitment by foreign states.

If you are one of these providers, this pack is for you. It will equip you with the messages, knowledge, and examples you may need to brief the people you support on the risks of working for a foreign state, even unwittingly.

- This pack explains how foreign states may use individuals in the UK to carry out malicious activity, how the people that you support may be susceptible to recruitment, and the potential legal consequences they may face under the National Security Act 2023.
- Raising awareness of the risks helps make the UK a harder place for states to target and recruit in, strengthening our national security.



Purpose of this pack (continued)

Objectives

1. Help you understand:

- How and why foreign states target and recruit people, often hiding their involvement.
- How this threat can apply to your cohort and what state threats can look like.
- The National Security Act 2023 (www.gov.uk/government/collections/the-national-security-bill).

2. Deliver key messages:

- Individuals may be at risk of committing an offence if the activity they are undertaking could help a foreign state carry out activities harmful to the UK, even if the request appears minor.
- Working on behalf of a foreign state is taken seriously and carries severe sentences if caught.
- Tasks can be small or informal, like taking a picture of a building or person, or damaging things.
- Individuals will be considered disposable to foreign intelligence services and will face the consequences on their own.

3. Spot potential risks or vulnerabilities so you can:

- Be aware that some individuals that you engage with may be more vulnerable to this type of activity.
- Understand the warning signs of concerning behaviour.
- Provide appropriate support to vulnerable individuals.
- Report concerning activity to the authorities.

Letter from Director State Threats, Home Office

Dear partner,

Thank you for taking part in this campaign to increase awareness of the risks of working for foreign states. Foreign states are increasingly seeking to recruit people in the UK, often through social media and anonymous online approaches, to carry out activity on their behalf. Tasks can appear small or low-risk at first but can quickly escalate and represent a threat to the UK's national security. This activity is now explicitly addressed in UK law: the National Security Act 2023 makes it a criminal offence to assist a foreign intelligence service or act on behalf of a foreign state in ways that threaten the UK.

We are asking partners to actively share the messages in this pack with the audiences you interact with. Every team with reach into communities, public-facing services, or frontline practitioners can play a crucial role.

Your networks give you access to individuals and groups who may see, hear, or experience things that central government cannot.

When you help build this messaging into your own communications, safeguarding work, and outreach, you extend our collective ability to disrupt hostile activity, protect vulnerable individuals, and prevent harm.

This partner pack provides material that you can tailor for your audiences while maintaining a consistent national message. By using this shared approach, you help ensure that the public receives clear, aligned guidance on what the threat looks like, why it matters, and how to respond safely.

Thank you again for your continued support. Your involvement is essential to strengthening the UK's resilience to state threats and protecting people from being exploited by hostile foreign actors.

Cathryn Ellsmore,
Director State Threats

How to use this pack

We would like partners to:

1.

Tailor messaging

- Partners are requested to tailor the language of these key messages to resonate best with the target audiences which you engage with.

2.

Embed messaging into existing work

- These messages can be embedded into your existing work, such as safeguarding conversations, briefings to frontline staff, community outreach, or existing communications campaigns.



How to use this pack (continued)

We would like partners to:

3.

Use your networks to disseminate messaging

- As partners, you have a greater reach and level of trust within your communities that allow these messages to be shared more broadly than central government can manage alone. Given the breadth of people that could be susceptible to recruitment, we need help in sharing these messages as widely as possible.

4.

Share routes to report suspicious behaviour or approaches

- Anyone can report by calling the **Anti-Terrorism Hotline on 0800 789 321**, going online at gov.uk/ACT or visiting a local police station. Counter Terrorism Policing is responsible for responding to threats from states as well as terrorism.
- Even if you're not sure or it seems trivial, please contact the police so specially trained officers can look into it. No call or online report will be ignored. Call handlers will ask you for information like your name and contact details, but providing this is your decision. The hotline is staffed 24 hours a day.



Key messages

Key messages

General messages to partners

- **Foreign states sometimes try to get people in the UK to carry out tasks for them.**

They do this because it allows them to stay hidden, avoid detection, and distance themselves from activities they don't want traced back to them.

- **They may reach out online or in person and offer incentives for quick, simple, or one-off jobs.**

These requests may seem harmless at first, such as taking photos, sharing details about a place, or passing on information about a person. Foreign states often target people who may be more vulnerable.

- **You should report suspicious activity, including recruitment attempts.**

Information can be shared via the **Anti-Terrorism Hotline (0800 789 321)** or online at **gov.uk/ACT**. If a crime is ongoing or may be committed, call **999 or 101**.

Key messages (continued)

Specific messages for partners to relay to their cohort

- **When a foreign state or intelligence service is behind it, even small tasks can become serious crimes.**

Under the National Security Act 2023, these activities can be classed as espionage, sabotage, or foreign interference. Acting for a foreign state is treated seriously and can lead to severe criminal charges under the National Security Act 2023.

- **Foreign states use individuals to give themselves distance. They do not protect or support the people they recruit.**

Once a task is done, or once someone is caught, those who recruited them often disappear, leaving the individual to face the full consequences alone.

- As the Director General of MI5 has warned:

“If you are a proxy, you are disposable. When you’re caught, you’ll be abandoned. You’re on your own.”

In this context, ‘proxy’ means an individual being used by foreign states to carry out tasks for them.

As a reminder, partners have discretion over how these key messages are landed with the audiences you engage with.



Understanding state threats and the National Security Act 2023

National Security Act 2023

The National Security Act 2023 means that if individuals commit a crime for, on behalf of, or with the intention to benefit a foreign power, they could be charged and face a severe prison sentence. The Sentencing Act 2026 means that those convicted under the National Security Act now face longer sentences.

An individual does not need to be tasked or paid directly by a foreign state to commit an offence under the National Security Act 2023, and several offences within the Act capture individuals who are tasked to carry out small or indirect actions.

Assisting a foreign intelligence service – if you are assisting a foreign intelligence service, you may face prosecution. This includes providing information, access to information, goods, services, or financial benefits. Even small tasks can count as assisting a foreign power.

Obtaining a material benefit from a foreign intelligence service – if you accept or agree to accept a material benefit that is provided by or on behalf of a foreign intelligence service, you may face prosecution. The benefit could be received indirectly through one or two intermediaries. You may face prosecution if you know or ought reasonably to have known that it is provided by or on behalf of a foreign intelligence service.

Carrying out malign foreign interference activity for, on behalf of, or with the intention to benefit a foreign power – foreign interference is intended to sow discord, manipulate public discourse, discredit the political system, bias the development of policy, and undermine the safety or interests of the UK.

Designation Power

The Home Secretary now has the power to designate bodies engaged in state threat activity, equivalent to proscription under the Terrorism Act 2000.

On 13 July, the Home Secretary laid regulations in Parliament to designate the Islamic Revolutionary Guard Corps (IRGC), the Islamic Movement of Companions of the Right (IMCR), and the volunteer corps of Russia's military intelligence service, the GRU (GRU VC). **New offences will apply to those supporting, assisting, or obtaining material benefits from a designated body.** Those conducting acts of sabotage, including arson, on behalf of these groups could face life imprisonment.

This law makes it easier to disrupt these designated groups, with **offences that deal with them in the same way as foreign intelligence services.** Prosecutors will no longer need to prove that there is a connection to a foreign power, making it more **straightforward to bring charges against individuals acting for designated groups** and ensuring they face the full force of the UK's national security laws.

More groups may be designated going forward, making it a criminal offence to support or aid them.



What are state threats?

Foreign governments target the UK using both discreet and visible methods known as state threats.

- These are below the threshold of direct armed conflict with the UK but go beyond peaceful diplomacy and acceptable statecraft to harm or threaten the safety or interests of the UK. This can include attempts to interfere with politics, steal sensitive information, disrupt vital services, threaten individuals, or undermine our economy, values, and security.
- **MI5 and Counter Terrorism Policing have identified state threats as one of the UK's most significant and fast-growing national security challenges.**

To avoid detection, foreign states often use people to carry out state threats on their behalf.

- These people, sometimes unknowingly, carry out activities usually in exchange for money or in response to pressure. You might have heard these people referred to as 'proxies'. They may be approached in-person or recruited through social media or online platforms. States often try to disguise their involvement so it can be hard to identify who is pulling the strings.

Using people gives foreign states deniability, and these individuals are treated as disposable.

- Recruited individuals are not intelligence officers, and they carry all the risk. Once they are no longer useful, or are caught, they are abandoned by the state that recruited them and left to face the criminal consequences alone.

The growing use of individuals to carry out malign activity on behalf of a state is not just specific to the UK but is increasing across Europe.



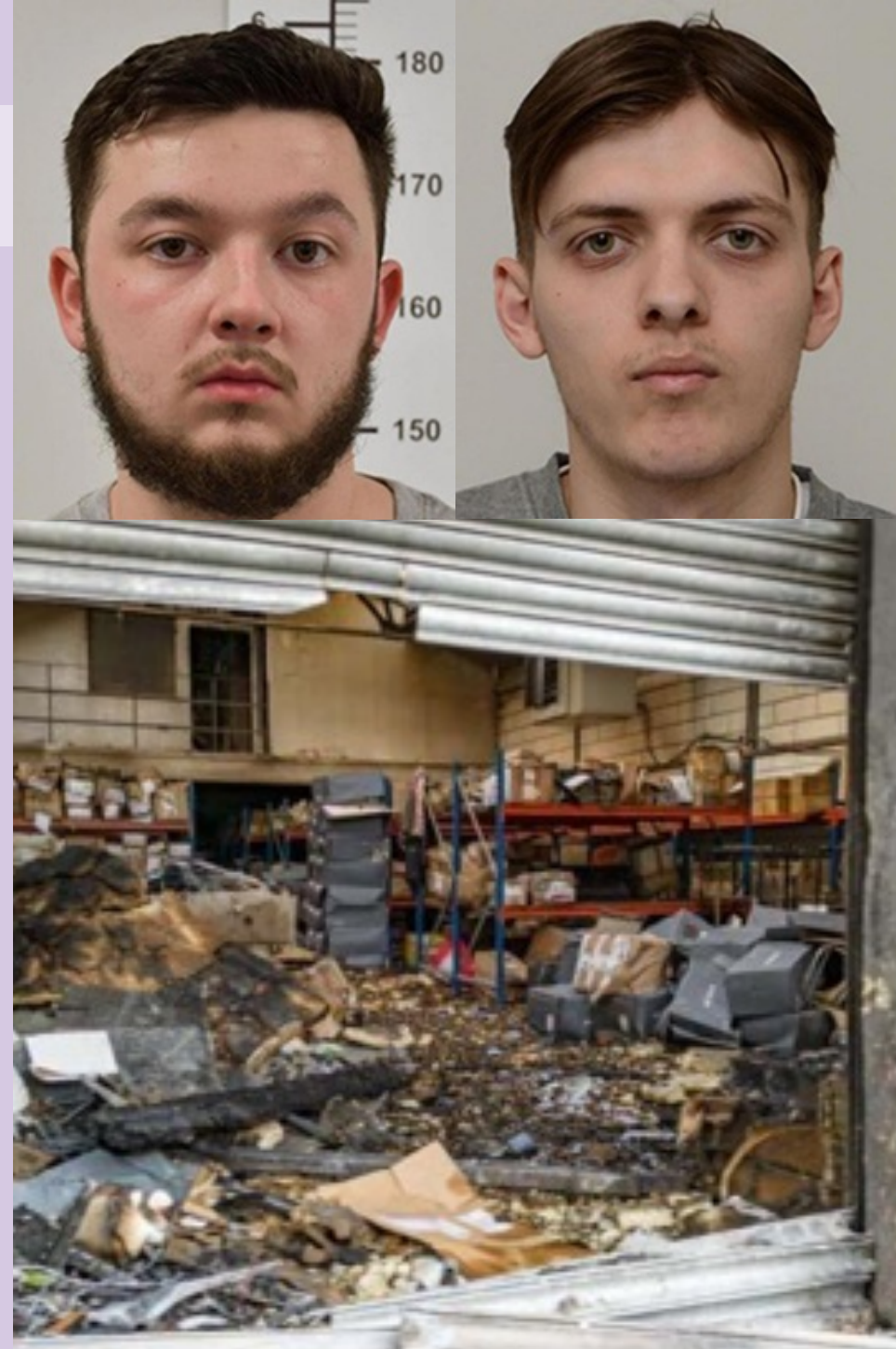
Case studies

Case studies – UK and beyond

UK

In 2024, a **Ukrainian-linked warehouse in east London was firebombed** causing around £1 million in damage and endangering lives. **A group of British recruits, contacted and directed via encrypted channels by Wagner operatives** (a Russian linked private military contractor), set fire to the site.

Investigators found that the ringleader had established contact with the Wagner Group in 2023 and recruited several others, who livestreamed parts of the attack and went on to plot additional crimes at the instruction of their online recruiters. They were arrested and in 2025, the Old Bailey handed down **a 23-year sentence for the ringleader, and between 7 and 13 years for his co-conspirators.**



Case studies – UK and beyond (continued)

Europe

In 2024, Swedish police arrested a **13-year-old boy** after shots were fired outside the offices of an Israeli defence company in Gothenburg. In related incidents the same year, **teenagers aged 16 and 19** were detained following attacks near Israeli embassies in Stockholm and Copenhagen. Sweden's security service has stated that **Iran is suspected of using Swedish criminal networks** to recruit and direct young people to carry out attacks, allowing the foreign state to operate through criminal proxies while exploiting minors' vulnerability.

On the night of 13 to 14 May 2024, **red handprints** were sprayed on the Wall of the Righteous at the Shoah Memorial in Paris, as part of a co-ordinated vandalism campaign. The act was carried out by **three Bulgarian men, recruited through informal criminal networks and directed by organisers linked to Russian intelligence services**. CCTV, travel and hotel records showed the group had arrived in Paris days earlier and acted under instruction, with one filming the graffiti for online dissemination. French investigators concluded the perpetrators were low-level recruits, selected due to financial insecurity and used as proxies in a wider Russian strategy to destabilise European societies while insulating the state from direct attribution.

Case studies – UK and beyond (continued)

UK case study two

In March 2024, **a journalist who worked for a TV and radio broadcaster that was critical of the Iranian government was attacked with a knife in Wimbledon, London.** The defendants, who acted as part of a three-man team, were working for financial reward and had spent weeks monitoring the journalist's movements before carrying out the attack outside his home.

Following the attack, the defendants abandoned their vehicle, disposed of clothing, and travelled by taxi to Heathrow Airport, where they boarded a flight to Geneva later the same day. They were arrested in Romania in December 2024 and **extradited back to the United Kingdom** to face trial.

At sentencing, the judge stated that **“the evidence overwhelmingly supports the conclusion that this attack was ultimately carried out in the interests of, and on behalf of, the Iranian state.”**

In 2026, George Stana (25) was sentenced to **12 years' imprisonment**, and Nandito Badea (21) was sentenced to **8 years' imprisonment** for their role in the attack.



What might increase an individual's risk of being approached?

Anybody could be a target for state actors seeking to undertake state threat activity in the UK, but they often look to exploit an individual's vulnerabilities.

Financially motivated or in debt

Foreign states can offer quick money in return for tasks. Individuals who are either in financial difficulty or motivated by money can be more susceptible to these taskings as way of earning 'easy money'.

Involved in, or on the periphery of, criminal networks

Foreign states often target those with criminal histories, or with connections to networks, to outsource criminal activity.

Individuals with access

Those with access to sensitive information, technical expertise, or potential influence within communities can be attractive targets for recruitment.

The direct involvement of a state may not be immediately obvious. Many state actors operate covertly or anonymously online, making it harder to discover their intentions or involvement.



Thank you

Thank you

Thank you for partnering with us on this vital initiative.

Your local knowledge and trusted community position make you essential to the success of this campaign.

We'd love to hear from you.

Please share your feedback on what's working effectively, challenges encountered, and suggestions for improvement.

Please email your feedback to STProxyComms@homeoffice.gov.uk

Useful resources and links

MI5 and the National Protective Security Agency have published guides and advice on state threats

www.npsa.gov.uk/national-security-act/defending-democracy/countering-espionage-and-foreign-interference

www.mi5.gov.uk/what-we-do/countering-state-threats

www.counterterrorism.police.uk/what-we-do/countering-state-threats

The National Security Act 2023 and the Sentencing Act 2026 guidance

www.gov.uk/government/news/longer-behind-bars-for-espionage-in-national-security-boost

www.gov.uk/government/publications/national-security-bill-factsheets



Home Office