EUROPEAN POLICY CENTRE

POLICY BRIEF

EUROPE'S POLITICAL ECONOMY PROGRAMME

17 MARCH 2026

Cyber sanctions: Strengthening EU–UK responses to escalating threats

Philipp Lausberg

INTRODUCTION

The EU and the UK face an increasingly complex security environment characterised by escalating geopolitical confrontation, the weaponisation of economic and technological links, and an erosion of global norms. In this context, hybrid attacks including sabotage, disinformation and migration manipulation have proliferated. Notably, transnational cyberattacks have posed a massive and fast evolving threat for the security, prosperity and political stability of the EU and the UK. Both sides have developed increasingly elaborate resilience and response architectures, which they have more recently complemented with sanctions regimes to deter malicious actors.

A comparative analysis evaluating the strengths and weaknesses of the two frameworks could offer important lessons learnt. Moreover, the potential benefits of deeper EU-UK cooperation are evident at a time of intensifying threats and an increasing fragmentation of the transatlantic alliance. Greater alignment in cyber sanctions could provide greater weight to both sides' foreign and security policies and strengthen collective responses to the increasing number of malicious cyber operations.

The potential benefits of deeper EU-UK cooperation are evident at a time of intensifying threats and an increasing fragmentation of the transatlantic alliance.

Moreover, the strengths of the EU and the UK in sanctioning are often complementary. The EU brings considerable leverage through its geographical spread, market size and its role in global trade, while the UK offers greater agility in decision-making and implementation, considerable financial sector expertise and global reach through the City of London, as well as significant intelligence capabilities within the 'Five Eyes' alliance.[1] Closer cooperation could therefore unlock important synergies, amplifying the deterrent, disruptive, signalling and norm setting impact of sanctions and help more effectively counter threats emanating from cyberattacks.

BACKGROUND

A rapidly evolving cyber threat landscape

Cyberattacks by State and non-state actors have become more frequent, intensive, sophisticated and strategically integrated into geopolitical competition. They are a direct threat to the EU's and the UK's security, prosperity and social cohesion, as hostile actors disrupt critical services and infrastructure, public administrations, value chains and finance, steal sensitive information and undermine political processes with disinformation campaigns. To do so, they employ tools such as Distributed Denial of Service (DDoS) attacks, ransomware, spyware, malware attacks and troll farms, all increasingly empowered by AI.[2]

Malicious actors linked to Russia and other State actors often launch huge amounts of 'below-the-threshold' attacks using 'salami-slicing' tactics designed to avoid triggering a clear collective defence response. Repeated intrusions are often used for pre-positioning – gaining long-term covert access to networks to enable rapid escalation later.[3] Russian-linked cyberattacks

are increasingly integrated with kinetic attacks on infrastructure and with AI-enabled information operations (including deepfakes), blurring the line between cyber, information and conventional security.

Tracking and responding adequately to such attacks is complex. Malicious cyber actors often sit abroad, beyond the reach of European law enforcement and are frequently supported and protected by states like Russia, China or North Korea and often affiliated with their intelligence services. They also rely on elaborate eco-systems that enable and obfuscate their activities. These include technology infrastructure providers such as hosting services, domain registrars and cybercrime-as-a-service platforms, as well as financial intermediaries including cryptocurrency exchanges, mixers and payment processors that facilitate the laundering and monetisation of cybercrime proceeds.

From prevention to deterrence: The growing role of sanctions in countering cyber threats

Until later in the 2010s, policy approaches to tackle these threats in most states including the EU and the UK focused mainly on reinforcing resilience, prevention and crisis response. This included instruments such as cyber security standards, cyber defence and recovery planning. States relied primarily on law enforcement to punish malicious actors. The intensifying threat environment has prompted a move towards more deterrence and imposing political and economic costs on malicious actors.

Sanctions such as travel bans and asset freezes can be useful in this respect because they transcend some of the limitations of traditional law enforcement, such as high evidentiary thresholds and limited jurisdictional reach.[4] They are unlikely, on their own, to change the

WHERE CYBER SANCTIONS SIT IN THE EU'S CYBERSECURITY ARCHITECTURE

The EU's cybersecurity architecture combines resilience, crisis response and deterrence tools to manage and counter malicious cyber activity.

Resilience – preventing and mitigating cyber risks

EU legislation and standards aim to reduce vulnerabilities and improve preparedness:

- **NIS2 Directive** – sets baseline cybersecurity risk-management and incident-reporting requirements for organisations in critical sectors.
- **Cyber Resilience Act** – establishes cybersecurity requirements for digital products sold in the EU.
- **Cybersecurity Act** – creates an EU certification framework for Information and Communications Technology (ICT) products and services.
- **ENISA (EU Agency for Cybersecurity)** – provides technical expertise, guidance and coordination among national cybersecurity authorities.

Crisis response – detecting and managing cyber incidents

Operational cooperation structures help detect, manage and recover from cyber incidents:

- **CSIRTs Network** – operational cooperation between national incident-response teams.
- **EU-CyCLONe** – strategic coordination among national authorities during large-scale cyber incidents.
- **CERT-EU** – incident response team protecting EU institutions and agencies.
- **Cyber Solidarity Act** – establishes EU cyber detection and response infrastructure, including security operations centres, regional cyber hubs, a cybersecurity reserve and emergency response mechanisms.

Deterrence – responding to malicious cyber activity

The EU uses diplomatic, legal and security tools to impose costs on attackers:

- **European Cybercrime Centre (EC3) at Europol** coordinates cybercrime investigations across member states.
- **Cyber Diplomacy Toolbox (within the European External Action Service (EEAS))** – diplomatic measures including public attribution and **cyber sanctions** against individuals and entities responsible for cyberattacks.
- **EU INTCEN (at the EEAS)** – provides strategic intelligence analysis supporting EU external action.
- **Member state offensive cyber capabilities** – increasingly recognised in EU defence discussions as part of broader deterrence.

Cross-level coordination

Several mechanisms link these layers of the EU cyber architecture:

- **EU Cyber Crisis Blueprint** – playbook for responding to large-scale cyber crises.
- **Joint Cyber Unit** – coordination platform connecting EU institutions, member states and partners.
- **Integrated Political Crisis Response (IPCR)** – political crisis coordination mechanism at EU level.

behaviour of determined cyber criminals, especially if they are backed by states. But if done right, they can raise the costs of malicious activity by constraining financial flows, exposing hostile actors and disrupting the networks that enable cyber operations.

Starting in 2015, the US has developed an extensive cyber-related sanctions practice, applying it against state intelligence officers, criminal groups and the financial and technical enablers that support them.[5] In 2017, the EU adopted the EU Cyber Diplomacy Toolbox, a framework under the EU's Common Foreign and Security Policy that enables the Union and its member states to respond collectively to malicious cyber activities through diplomatic, political, economic and legal measures. It is integrated into the EU's wider cyber security architecture (see box), and includes tools such as diplomatic demarches, public attribution, capacity building and restrictive measures. Within this framework, the EU created, in 2019, its dedicated cyber sanctions regime allowing for restrictive measures against individuals or entities responsible for cyberattacks.[6] After Brexit, the UK developed its own autonomous sanctions framework, under which cyber-related designations have been introduced since 2020.[7] While EU-British cooperation on sanctions in general has remained strong, collaboration on cyber sanctions has been intensified, e.g. in the framework of annual UK-EU Cyber Dialogues starting in 2023.

STATE OF PLAY

The EU's cyber sanctions framework: Potential and constraints

The EU's cyber sanctions regime is intended "to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States".[8] It applies to cyberattacks and attempted attacks with significant harm for critical infrastructure, services and administrations.[9] The regime allows for targeted measures, including travel bans and asset freezes against individuals and entities. Unlike most EU sanctions regimes, which are country-specific, the cyber framework applies globally. In principle, this horizontal design gives the EU flexibility to act wherever threats emerge.

However, since the adoption of the regime, only 17 individuals and four entities have been designated despite the large number of cyber incidents. These listings include actors linked to Russian, Chinese and North Korean operations and have concentrated primarily on individual perpetrators and state-linked operatives rather than systematically targeting the technical and financial infrastructure that enables cyber operations.[10] This limits their effectiveness as those individuals usually act under the direction and protection of foreign states and within complex enabling ecosystems.

A main reason for the low number of listings are difficulties with attribution, i.e. the technical, legal and political assignment of individual responsibility for cyberattacks which is a precondition for designations. Attribution is the prerogative of member states, but those have varying technical and intelligence capabilities, making the identification of originators and proving malicious intent difficult for some. This leads to an incoherent and sometimes contradictory attribution policy across the EU.[11] Many member states are also reluctant to share sensitive intelligence, leading to information gaps between member states and at the EU level.[12] As a result, there is a heavier reliance on open-source evidence for designations, which is often not as extensive and detailed. This makes it harder to design smart sanctions that are built on a thorough understanding of targeted actors' techniques and their motivations and that can also be successfully defended in court. This in turn makes it more difficult to get member states to agree to EU sanctions.

Many member states are also reluctant to share sensitive intelligence, leading to information gaps between member states and at the EU level.

For a designation to go ahead there needs to be unanimous agreement among the 27 EU member states in the Council. As a result, sanctions decisions are based on political compromise, which often comes at the expense of clarity, detail and strategy. Moreover, arduous consensus building delays designations, which usually come several years after cyber incidents take place, reducing the deterrent and signalling value of sanctions. For example, following cyberattacks on Estonia in 2020, the EU only imposed sanctions against the Russian operatives who perpetrated them in 2025.[13]

EU listings are accompanied by only sparse public communication. This makes accompanying legal action more difficult than, for example, in the US, where more detailed information on hostile actors in designations such as timelines, infrastructures and methods facilitates indictments.[14] Moreover, limited explanation of designations and technical advisories limit the ability of the private sector to understand and support the measures. Especially ICT companies and financial institutions are indispensable in providing technical attribution, threat intelligence, monitoring financial flows and the impact of sanctions, and helping with enforcement and public exposure of malicious actors. While public authorities and law enforcement in the EU already collaborate closely with firms, there is no single entry point across member states for the private sector, which limits effective public-private information sharing in the EU. This is exacerbated by limited information exchange between member states. Strong data protection laws in the EU are a guarantor for civil liberties, but they also limit what companies and governments can share with each other in relation to cyber threats. At the same

time, the EU and its member states rely heavily on large foreign ICT companies – most of them from the US – for threat intelligence and enforcement. While their scale and expertise makes their collaboration crucial, they also entrench dependencies.

The EU also relies on strong international cooperation as well as intelligence and expertise from allied third countries, including the UK and the Five Eyes alliance.[15] EU cyber sanctions have often followed ones put in place by allies, especially the US and UK. But intelligence coordination with these countries mainly runs through member states rather than the EU level, further complicating EU information pooling to build cases for sanctioning.

Altogether, evidence for the effectiveness of existing EU cyber sanctions is sparse. Data on the freezing of assets under the EU cyber sanctions regime is minimal and there is little evidence of significant disruption of malicious cyber actors and their ecosystems.[16] At the same time, EU cyber sanctions have demonstrated the EU's resolve not to leave foreign cyberattacks unanswered, while reinforcing its diplomatic posture and its commitment to upholding norms of responsible state behaviour in cyberspace. To raise the cost for cyber threat actors and their protectors and increase deterrence, an increasing number of EU countries, such as Germany and Italy,[17] are considering more offensive cyber action for which EU member states hold varying capabilities.[18] In its Defence White Paper, the EU has acknowledged the need for offensive cyber capabilities as a complement to other tools of deterrence and suggested creating a voluntary support scheme for offensive cyber capabilities among member states.[19]

The UK's cyber sanctions framework: Agility and operational integration

Sanctions are a core foreign and security policy instrument in the UK. British cyber sanctions apply globally like the EU regime, but their scope is broader, targeting not only cyber activity that threatens national security and critical infrastructure but also economic prosperity, allowing for more flexible deployment. Moreover, the framework is more operational than the EU's one as it defines more clearly the technical effects and harms of cyber activity. So far, the UK has designated around 82 individuals and 13 entities under the cyber sanctions regime since it entered into force in 2020, more than four times as many as the EU. While also sanctioning hostile actors directly, listings have focused more on their enabling ecosystems than EU designations, actions such as against Media Land, a Russian bulletproof hosting provider[20] being a case in point.[21]

Sanctions decisions are taken directly by the Foreign, Commonwealth and Development Office (FCDO), allowing faster and more agile implementation of sanctions than in the EU. This makes the UK more responsive to evolving cyber threats and facilitates the coordination of sanctions with other measures, such as law enforcement, public exposure, diplomatic signalling and offensive cyber capabilities. Using a mix of tools, the UK has sought to create sustained campaigns with a consistent narrative, which can significantly increase the pressure on hostile cyber actors and their ecosystems and degrade their activities over time, especially when coordinated with partners. An example has been the case of the cybercrime group LockBit, where sanctioning, exposure and coordinated disruption by law enforcement of the UK and several countries undermined credibility and fractured its ecosystem.[22]

The impact of UK sanctions is amplified by a longstanding, close collaboration with the private sector.

The impact of UK sanctions is amplified by a longstanding, close collaboration with the private sector, for example through information-sharing and collaborative threat analysis. Designations are more detailed than in the EU, providing important context for businesses. Moreover, the UK government has invested in developing public–private partnerships to amplify exposure, improve enforcement and exchange threat intelligence, technicalities about designations and information about the impact of sanctions.[23]

Close diplomatic, police and especially intelligence collaboration with international partners has been at the core of the British approach to cyber sanctions. For example, the UK's potent Government Communications Headquarters (GCHQ) intelligence service is closely integrated in the Five Eyes alliance. Its members have coordinated more quickly and efficiently and have issued simultaneous designations, such as against Media Land in November 2025.[24] At the same time, trust, information-sharing practices and strategic alignment in the Five Eyes alliance have come under pressure during the second Trump administration.[25]

To increase deterrence, the UK can, in select cases, rely on well-developed offensive cyber capacities, which are openly integrated into its national security strategy and could serve as a reference point for less developed offensive cyber practices in the EU.

EU-UK cooperation on cyber sanctions: Strong links, untapped potential

At the policy level, EU-UK cooperation on cyber sanctions has largely been informal, with regular exchanges between the FCDO and the EEAS and EU member states. Since 2023 this has been complemented by the formal EU-UK Cyber Dialogue, which meets once a year.[26] Cooperation has been more structured in the area of law enforcement, notably through the EU-UK Trade and Cooperation Agreement and operational cooperation in the framework of Europol's European Cybercrime Centre.

EU and UK cyber sanctions have occasionally aligned in practice, including actions against Russian GRU operatives, Chinese actors linked to the Microsoft Exchange hack and North Korean cyber operators involved in the 2017 WannaCry attack. However, coordination has largely taken the form of sequenced or parallel listings rather than formally synchronised designations.

Given that the EU must coordinate among 27 member states, it often cannot move at the same pace as the UK and other partners. This makes it difficult to synchronise sanctions measures across jurisdictions. Even when partners identify the same threat actors, the EU may require significantly more time to assemble evidence, secure political agreement and prepare listings. Simultaneous sanctions designations are therefore often unrealistic.

The difficulty of sharing sensitive intelligence and cyber threat information between the EU and the UK is another structural constraint. Intelligence sharing between governments remains constrained by classification rules, national security considerations and the limited availability of secure channels for exchanging highly sensitive information. These barriers can complicate efforts by the EU and the UK to rapidly agree on targets or develop coordinated sanctions packages. Altogether, while cooperation between the two sides is already close, there is significant potential to deepen it if appropriate reforms are undertaken.

RECOMMENDATIONS

1. **Strengthen Europe's autonomous cyber threat intelligence capacity**

   The EU and its member states should invest more in their own cyber threat intelligence and analytical capabilities. Disparities in national capacities could be reduced by ENISA stepping up support for member states with weaker forensic and cyber-threat-analysis capabilities through technical guidance, peer reviews, exercises and operational cooperation. This could facilitate and accelerate attribution across member states and, subsequently, the introduction of EU cyber sanctions. Moreover, it would increase the EU's autonomy in reacting to cyber threats but also benefit trusted partners like the UK, who could rely on better and more timely EU intelligence and deterrence.

2. **Reinforce coordination in attribution policy and intelligence sharing**

   The EU should strengthen its capacity to coordinate the attribution of cyberattacks in order to allow for more timely and effective cyber sanctions. To overcome fragmentation across member states, the EU should therefore tighten the legal criteria for attribution and work towards greater convergence in evidentiary standards. Moreover, member states should expand structured mechanisms for the confidential exchange of forensic and intelligence information related to cyber incidents. In parallel, EU INTCEN and the EU Joint Cyber Unit should be strengthened to improve the exchange of threat intelligence and forensic information among member states and to better coordinate EU attribution policy. This could facilitate and accelerate collective attribution decisions and support more robust cyber sanctions listings. More systematic and secure information-sharing and Cyber Threat Intelligence (CTI) capacity should also be established between the EU, the UK and other trusted international partners, to facilitate collaboration on designations, law enforcement and diplomacy.

3. **Consider qualified majority voting and coalitions of the willing**

   Ideally, the EU would allow qualified majority voting (QMV) in the Council for the adoption of cyber sanctions. This could accelerate the decision-making process, facilitate agreement on a greater number of designations and allow for clearer, more detailed and strategic sanctions. In case of deadlock in the Council, EU member states should consider greater use of coalitions of the willing, including with the UK and other trusted partners, with respect to public attribution, offensive cyber actions and other measures where responsibility is not clearly located at the EU level. This could help to reduce the time lag between cyber incidents and responding to them.

4. **Expand exposure and attribution as a complementary disruption tool**

   When listings are delayed or impractical, the EU and the UK should publicly expose hostile cyber actors, their techniques and enabling infrastructure – ideally in collaboration with international partners. Public messaging sh[]ould be coordinated between the UK and the EU or as many EU member states as possible. Exposure should be paired with operational guidance to the private sector (e.g., indicators of compromise, mitigation steps) which can amplify signalling and disruption. Exposure could then still be followed up by listings once evidentiary thresholds and unanimity for sanctions in the Council are met. This sequencing could allow for a quicker response and a greater deterrence-based impact.

5. **Target the ecosystems of hostile cyber actors more**

   While direct sanctions against cyber attackers and operatives send important signals, taken alone they tend to be less effective in changing behaviour. The EU should therefore focus its sanctions and other measures more on broader ecosystems that sustain malicious cyber activity, including facilitators, front companies, infrastructure providers and financial channels such as crypto-related actors involved in laundering proceeds or enabling hostile operations. This can help to disrupt malicious operations and raise their cost. To do so, cyber sanctions could also be combined more with tools to counter illicit finance networks, for example sanctions in other regimes like the EU's Russia framework.

6. **Strengthen collaboration with the private sector and reduce dependencies**

   Both sides should strengthen their structured cooperation with relevant private companies, especially trusted cybersecurity firms and digital infrastructure providers. The EU and its member states should reinforce intelligence-sharing frameworks between public authorities and law enforcement on the one hand and the private sector on the other, while harmonising approaches as much as possible across the Union. Ideally, there would be a single entry point for companies for their public sector collaboration on cyberattacks. To facilitate the exchange of sensitive information, the EU should also simplify data protection rules while maintaining high standards. To reduce excessive dependencies on large foreign technology platforms, the EU should, wherever this can be achieved, strive to diversify in terms of the partners that it cooperates with but without limiting the quality, quantity and rapid availability of shared information. It should increase European digital autonomy by facilitating the development of more European digital champions with policies that help to improve digital innovation ecosystems and alleviate the scale-up gap.

7. **Build campaigns around strategic narratives**

   The EU should move from isolated listings more towards sustained campaigns that combine sanctions with other measures, such as public exposure, attribution, law enforcement, diplomatic instruments and, if appropriate, offensive cyber capabilities. More developed UK practice in this respect can provide some lessons learnt. To facilitate campaigns across the EU, coordination across different domains at the EU level and among member states should be strengthened, including between foreign ministries, intelligence services, law enforcement and cyber agencies. Moreover, the EU and the UK should coordinate campaigns as much as possible based on a coherent narrative. Even if the EU moves more slowly on designations, common public messaging telling a coherent story can amplify signalling and deterrence.

8. **Strengthen early warning and strategic coordination on cyber sanctions**

   The EU and the UK should reinforce mechanisms for early information-sharing and strategic coordination on cyber sanctions between the EEAS and the FCDO. Regular exchanges on planned measures, potential targets and priorities would help ensure that actions are complementary and sequenced effectively. While differences in decision-making timelines mean that simultaneous designations will often remain difficult, greater advance awareness of each other's plans can improve overall coordination and maximise the strategic impact of sanctions and other measures.

DISCLAIMER

This EPC Policy Brief has been financially supported by the UK Mission to the European Union.

The support the European Policy Centre receives for its ongoing operations, or specifically for its publications, does not constitute an endorsement of their contents, which reflect the views of the authors only. Supporters and partners cannot be held responsible for any use that may be made of the information contained therein.

ABOUT THE AUTHOR

Dr. Philipp Lausberg is a Senior Policy Analyst in the European Political Economy Programme at the European Policy Centre and leads the EPC's EU sanctions project.

NOTES

[1] The Five Eyes intelligence-sharing alliance comprises five Anglophone countries: the United States, the United Kingdom, Canada, Australia, and New Zealand.

[2] ENISA (2025), ENISA Threat Landscape 2025.

[3] Hurel, Louise Marie and Mott, Gareth (2025), Rethinking Cyber Deterrence in a Multipolar World, Royal United Services Institute for Defence and Security Studies (RUSI), August 2025.

[4] Miadzvetskaya, Yuliya (2024), EU sanctions in response to cyber-attacks as crime-based emergency measures, Computer Law & Security Review, Volume 54, September 2024.

[5] Bartlett, Jason and Ophel, Megan (2021), Sanctions by the Numbers: Spotlight on Cyber Sanctions, Centre for a New American Security, 4 May 2021.

[6] Council of the European Union (2019), Cyber-attacks: Council is now able to impose sanctions, press release, 17 May 2019.

[7] The relevant legal basis is the Cyber (Sanctions) (EU Exit) Regulations 2020, adopted under the Sanctions and Anti-Money Laundering Act 2018.

[8] Council of the European Union (2019), Council decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Council Decision (CFSP) 2019/797, Paragraph 7.

[9] The whole list includes: Critical infrastructure, services necessary for the maintenance of essential social and economic activities, critical state functions, the storage or processing of classified information, government emergency response teams, attacks carried out against EU institutions, bodies, offices, agencies, delegations in third countries and Common Security and Defence Policy (CSDP) missions and operations.

[10] European Commission, EU Sanctions Map: Cyber Attacks, accessed: 15 March 2026.

[11] Ivan, Paul (2019), Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox, European Policy Centre, 18 March 2019.

[12] This is, for example, because the collected evidence and intelligence might contain information that would reveal capabilities, techniques and methods that a state in question possesses. Moreover, by publicly disclosing information about a cyber operation, a state takes the risk that other malicious actors might feel emboldened to reuse or exploit similar vulnerabilities to perpetrate further cyber operations. See: Bendiek, Annegret and Schulze, Matthias (2021), Attribution: A Major Challenge for EU Cyber Sanctions, Stiftung Wissenschaft und Politik, 16.12.2021.

[13] In Cyber News (2025), EU Sanctions Three Russian Agents for Cyberattacks Against Estonia, 2 February 2025.

[14] Saiz Erausquin, Gonzalo (2025), RUSI Cyber Sanctions Taskforce: Countering State-Backed Cyber, Threats, Royal United Services Institute for Defence and Security Studies (RUSI), 28 October 2025.

[15] For example, the attempted cyberattack against the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague in 2018 — conducted by operatives of Russia's military intelligence service (GRU) — was uncovered and disrupted only after UK authorities provided intelligence that helped Dutch security services identify and intercept the attackers before the operation could be carried out. See: Bendiek, Annegret and Schulze, Matthias (2021), Attribution: A Major Challenge for EU Cyber Sanctions, Stiftung Wissenschaft und Politik, 16.12.2021.

[16] Saiz Erausquin, Gonzalo (2025), RUSI Cyber Sanctions Taskforce: Countering State-Backed Cyber, Threats, Royal United Services Institute for Defence and Security Studies (RUSI), 28 October 2025.

[17] Victor Jack and Laura Kayali (2025), Europe thinks the unthinkable: Retaliating against Russia, Politico, 27 November 2025.

[18] Skingsley, Juliet (2023), Offensive Cyber Operations, States' perceptions of their utility and risks, Chatham House, September 2023.

[19] European Commission (2025), Joint White Paper for European Defence Readiness 2030, Brussels, 19.3.2025.

[20] Bulletproof hosting (BPH) is technical infrastructure service provided by an internet hosting service that is resilient to complaints of illicit activities, which serves criminal actors as a basic building block for streamlining various cyberattacks.

[21] Foreign, Commonwealth and Development Office (FCDO), UK Sancitons List; Cyber, accessed: 15 March 2026.

[22] National Crime Agency (2024), LockBit leader unmasked and sanctioned, 7 May 2024.

[23] Jarvis, Dan and UK Home Office (2024), Building partnerships to protect the UK from cyber crime, Arlington, October 2024.

[24] Foreign, Commonwealth & Development Office (2025), UK smashes Russian cybercrime networks responsible for attacks on UK businesses, 19 November 2025.

[25] Giles, Keir and Sipher, John (2025), Allies Assess What Intelligence They Can Still Share With Trump, Foreign Policy, 27 February 2025.

[26] European External Action Service (2023), Cyber: EU and UK launch Cyber Dialogue, 14 December 2023.

With the strategic support of King Baudouin Foundation
Working together for a better society