



THE PUTIN TAX

Estimating the Economic Cost of
Russian Hostile Activity Against
the United Kingdom

GRAEME DOWNIE MP

With Dr Dominic Reed

OCTOBER 2026

Table of Contents

Foreword – Tom Keatinge, RUSI	2
Findings and Recommendations.....	3
Executive Summary	4
What is the Putin Tax?	5
Methodology	6
Limitations	8
What was found: Attribution, Costs and Limits.....	9
Royal Mail and the LockBit attack	10
The NHS Advanced Attack	11
The Viasat Attack	11
London Arson Attacks.....	11
JLR: The Costliest Cyber-attack in British History	13
Government Information	14
Industry Information: CyberCube	14
Extrapolated Costs	15
What is Known.....	15
Layer One: Proven Losses	15
Layer Two: Russia-linked Cyber Activity	15
Layer Three: Economy-wide exposure	16
Layer Four: The Infrastructure Multiplier & Subsea cables	17
A Working Estimate	20
What the Putin Tax Could Pay For	20
What We Don't Know	21
Conclusion and Recommendations	22
Bibliography.....	23

Foreword – Tom Keatinge, RUSI

Tom Keatinge, Director of the Centre for Finance & Security at the Royal United Services Institute (RUSI)

Russia's threat to the United Kingdom rightly commands considerable attention.

Much debate focuses on the government's response, including sanctions to constrain Moscow's ability to sustain its illegal war in Ukraine and its aggression towards the UK and its allies.

Yet another question receives less scrutiny: what are Russia's hostile actions already costing the UK economy?

This welcome report by Graeme Downie MP addresses that gap. Framing this burden as a 'Putin Tax', it highlights costs borne by British businesses, public services and taxpayers through disruption, recovery and investment in resilience.

At the Centre for Finance & Security at RUSI, our work examines exactly this intersection of finance and security. We warmly welcome this contribution to understanding those connections.

The economic consequences of hostile activity must inform the government's assessment of the threat, its response and the resources it commits.

Measuring these costs is difficult: attribution is complex, information fragmented and consequences extend beyond immediate damage.

This report assembles available evidence while highlighting what remains unknown.

With government finances under pressure, it should prompt a systematic effort to measure this burden, raise awareness with the private sector and explain its significance to the public.

Understanding the price Britain already pays is essential to protecting its future.

Findings and Recommendations

KEY FINDINGS

- This report is the first attempt to measure the economic burden of Russian hostile activity.
- The annual "Putin Tax" costs the UK at least £2-2.5bn per year.
- Confirmed attacks alone have generated an estimated £1.6bn–£2.1bn in economic losses.
- Government has identified attacks but often cannot say what they cost the country.
- The current and future cost of hostile activity originating in Russia is likely to be vastly higher.

RECOMMENDATIONS

- The UK Government publish an annual report to Parliament setting out the estimated economic cost of hostile foreign-state activity to the United Kingdom with increased attribution to specific states where possible.
- The National Cyber Security Centre publish annual assessments of significant hostile-state cyber activity, including attribution and estimated economic impacts wherever operationally possible.
- The Ministry of Defence develop and publish a methodology for assessing the economic costs of physical hostile activity directed at UK people, businesses, infrastructure and interests.
- The UK Government should launch a national public awareness campaign on hostile-state threats, cyber resilience and national preparedness.



Executive Summary

Russia's hostile activity against the United Kingdom imposes a significant economic burden that is rarely measured and poorly understood.

This report introduces the concept of the "**Putin Tax**": the cost borne by British taxpayers, businesses and public services as a result of Russian cyber-attacks, sabotage, critical infrastructure threats and other forms of hostile-state activity.

Drawing on Parliamentary Questions, government evidence, National Cyber Security Centre data, industry analysis and publicly reported incidents, the report finds a striking lack of government assessment of the wider economic consequences of these attacks.

The report examines a series of case studies, including attacks affecting Royal Mail, NHS suppliers, communications infrastructure and major British businesses.

These examples demonstrate how hostile-state activity can inflict substantial economic damage, disrupt essential services and undermine economic resilience even outside periods of conventional conflict.

They also illustrate how economic harm is increasingly being used alongside traditional military and diplomatic tools as part of Russia's wider strategy against Western states.

The report combines the costs of known incidents, estimates of Russia-linked cyber activity, wider economic losses from cybercrime and Britain's exposure through critical infrastructure.

The evidence shows:

- **£2bn-£2.5bn** estimated annual cost of the "Putin Tax" to the United Kingdom.
- **300+** Russia-linked cyber incidents affecting UK companies identified since 2022.
- **75%** of significant cyber incidents affecting critical national infrastructure are linked to hostile states.
- There is a 5% chance that the UK will experience **a single attack by a hostile power that would cost a UK company £3.3 billion**, over 1.5 times the cost of the JLR attack.
- **£250m-£500m** annual economic exposure from damage to subsea communications cables.

The UK lacks a consistent framework for measuring the economic impact of hostile-state activity. In many cases, government departments are unable to estimate the costs arising from major incidents, leaving Parliament and the public without a clear picture of the financial consequences.

The report argues that hostile-state activity should be treated not only as a national security threat, but also as a material economic risk. Better measurement would enable government to identify trends, prioritise resources, evaluate interventions and strengthen accountability.

The report concludes that hostile Russian activity is imposing a measurable and growing cost on the British economy. The true figure is likely to be higher, as attribution challenges, under-reporting and gaps in government data mean many costs remain unquantified, including resilience spending, insurance premiums, investment decisions and wider productivity losses.

Britain is already paying a Putin Tax.

Government should begin systematically measuring these costs, publish regular assessments of the economic impact of hostile-state activity, and ensure that policymakers, businesses and the public better understand the financial consequences of ongoing Russian aggression.

Far from being solely a national security challenge, Russian hostile activity represents a significant and recurring economic cost that British taxpayers and businesses are already paying every year.

Graeme Downie MP
October 2026

What is the Putin Tax?

The Putin Tax describes the economic burden imposed on the UK through hostile Russian activity. These costs include physical attacks, cyber-attacks, resilience spending, security upgrades, infrastructure protection, business losses and wider economic disruption.

Throughout this report, the phrase Putin Tax is used deliberately because it describes a cost that can be ascribed to Russian-based actions that already exist, are rarely recognised, yet have a day-to-day effect on every British taxpayer.

When people think about taxation, they think about something visible. They think about deductions from their wages or bills that arrive in the post. The burden imposed by hostile Russian activity does not appear in the same way. It is not listed on a payslip, and it is not collected by HM Revenue and Customs. Yet it is paid, nonetheless.

It is paid when businesses are forced to spend millions recovering from cyber-attacks rather than investing in growth. It is paid when public bodies divert resources into security and resilience measures. It is paid when disruption affects productivity, delays services or increases costs throughout the economy. It is paid through police investigations into illegal activity. For example, it has been evidenced that **the cost of the police investigation alone after drone disruption over RAF Lakenheath in November 2024 was over £600k.**¹

When we first began examining the issue, there was an assumption that some part of government must already be tracking these costs.

After all, government routinely publishes cost estimates of fraud, economic crime, flooding and a wide variety of other risks facing the country.

However, very quickly it became apparent this assumption was wrong.

Government departments collect information about incidents. Security agencies collect information about threats. Businesses collect information about their losses. Insurers collect information about claims. Analysts collect information about trends. Yet nowhere are these strands brought together into a single assessment of what hostile-state activity is costing the nation. We also found that attribution was very difficult as, unlike other allied governments, the UK has been reluctant to the point of refusal to ever attribute attacks to a specific hostile nation.

The result is a curious situation. Few people today would dispute that Russia poses a serious threat to Britain and its allies. Intelligence agencies warn repeatedly about cyber activity. Ministers speak regularly about attacks against critical infrastructure. Parliamentary committees have devoted considerable attention to questions of resilience, energy security and national preparedness. The danger is widely recognised. What remains poorly understood is the economic burden already being placed on the UK by these attacks.

This report seeks to establish what is currently known, identify costs that can be measured and which cannot. It seeks to understand what information government possesses and, equally important, what information it does not possess.

Most importantly, this report makes the case that hostile-state activity should be treated like any other significant economic risk facing the country. It should be assessed and reported, transparently and with an action plan to prevent or deter such activity.

The concept of the Putin Tax therefore serves two purposes. It describes the cumulative burden already being imposed upon Britain by hostile Russian activity. But it also highlights the fact that this burden currently sits in a blind spot between national security and economic policy.

¹ UK Parliament, Written Question UIN 19664: Military Bases: Unmanned Air Systems, tabled by Graeme Downie MP, 16 July 2026, answered by Louise Sandher-Jones MP on 2 September 2026, available at: <https://questions-statements.parliament.uk/written-questions/detail/2026-07-16/19664> (accessed 1 October 2026).

Methodology

This report uses official attribution, law enforcement attribution and credible intelligence assessments in determining specific Russian hostile activity.

The purpose of this research is to establish the most robust assessment possible using the information and resources presently available, identify the areas in which reliable estimates can be produced, and highlight the significant gaps that still exist. A conservative estimate, quantifying the *minimum* cost to taxpayers, is advanced.

From the outset, this project faced a fundamental challenge in accessing reliable data on the cost of hostile state action. To address that challenge, evidence was sought from those organisations most directly involved in measuring risk and estimating economic losses.

Discussions were held with industry specialists including CyberCube, one of the world's leading cyber-risk analytics firms, whose work on economic modelling and systemic risk is widely used across financial markets and the insurance sector.

These discussions proved invaluable because they highlighted the limitations of existing datasets and reinforced a point that emerged repeatedly throughout this research, that while individual incidents can often be measured, there is currently no comprehensive mechanism for estimating the cumulative economic burden.

CyberCube advised that historical loss data, while useful, is often insufficient to answer the central question posed by this report. Attribution remains difficult, many incidents are under-reported, and the wider economic consequences are rarely captured in a consistent way. Furthermore, it misses the harm that would be caused by escalatory aggression that targets key technologies. They suggested the most promising approach involved combining known incidents with catastrophe modelling and wider economic exposure analysis.

This insight influenced the structure of the report. Rather than relying solely on retrospective analysis, it seeks to combine evidence about known incidents with a broader assessment of Britain's exposure to future hostile-state activity. The purpose is not simply to ask what Russian activity has cost Britain in the past, but to understand what it may cost Britain in the future if current trends continue.

Unless otherwise stated, the report includes both hostile activity directly attributed to the Russian state and incidents attributed to Russia-based or Russia-linked actors, including criminal and proxy networks operating from Russian territory, where there is credible evidence that such activity contributes to the wider threat environment originating from Russia.

Alongside industry evidence, information disclosed by government has been extensively drawn upon in response to targeted questions submitted during this research. These questions, placed before several government departments, sought information relating to cyber-attacks, hostile-state activity, critical infrastructure, drone incursions and the costs associated with specific incidents. In several cases, the responses confirmed that no economic estimate existed. In others, they revealed important operational information.

The report also relies heavily upon research commissioned by the Department for Science, Innovation and Technology (DSIT) into the economic impact of cyber-attacks. This remains the most comprehensive publicly available attempt to quantify cyber-related losses across the UK economy and provides important estimates relating to annual cyber costs, intellectual property theft and fraud associated with data breaches.

Additional evidence was obtained from the House of Commons Library, parliamentary committee inquiries, ministerial statements, parliamentary debates and publicly available reporting.

Throughout the report, incidents have been assessed according to three broad levels of confidence regarding attribution.

1. Incidents formally attributed by the UK Government or allied governments.
2. Incidents linked by law enforcement or intelligence agencies to criminal organisations operating from Russia.
3. Incidents where a credible body of evidence exists linking activity to Russian interests, even where formal government attribution has not been made.

The report also distinguishes between three separate categories of cost.

- Direct costs include property damage, remediation expenditure and recovery costs.
- Indirect costs include lost productivity, supply-chain disruption and commercial losses.
- Strategic costs include resilience spending, infrastructure protection, cyber-security investment and wider measures introduced in response to the threat environment.

One of the clearest findings of this project is that direct costs are often measurable but indirect and strategic costs, which may ultimately be much larger, are rarely measured in any consistent way.

The absence of those figures should not be mistaken for an absence of economic impact. On the contrary, it is evidence of the very problem this report exposes, that not enough attribution is undertaken nor enough measurement of economic impacts of foreign-state attacks on the UK and our economy.

Limitations

This report is an independent, desk-based effort to estimate the economic burden imposed on the UK by hostile activity linked to Russia. It is important to acknowledge the limitations in producing this report, which affect both the research process itself and the resulting conclusions.

This research was conducted within the office of a Member of the UK Parliament and undertaken principally by a single postdoctoral researcher. Parliamentary offices have limited resource and capacity, and do not possess dedicated analytical teams, access to classified intelligence or any budget for research.

The analysis in this report relies upon publicly available information, parliamentary material and library briefings, stakeholder views, media reporting and industry research.

Much hostile-state activity is not publicly reported. Many incidents are never disclosed by the affected organisations, while others are only partially reported due to commercial sensitivities, ongoing investigations or national security considerations. The evidence available in the public domain is unlikely to capture the full scale of hostile activity directed towards the UK.

Attribution remains a significant challenge. This report seeks to rely on incidents where attribution has been established by law enforcement, government bodies or reputable cybersecurity organisations. However, it is not always possible to determine the precise relationship between criminal groups, proxy actors and the Russian state. The report distinguishes, where possible, between directly attributed state activity, and activity which originates from Russian-linked criminal networks.

It is inherently difficult to quantify the economic impact of hostile activity. While some incidents have resulted in publicly reported financial losses, many costs remain indirect or dispersed across the economy. These could include lost productivity, increased security spend, delays to investment decisions, disruption to public services, loss of trust between the business and the consumer, and wider economic effects that are rarely measured consistently.

This report does not seek to produce a definitive, comprehensive estimate of the total economic cost of Russian hostile activity. It assembles available evidence, identifies known costs and develops an indicative estimate based on publicly accessible information. The figures presented should be understood as illustrative – a floor – and subject to revision as additional data becomes available.

Finally, the principal finding of this research is that the UK Government does not currently publish a comprehensive assessment of the economic costs of hostile-state activity. Given this, independent researchers are required to piece together information from multiple sources.

The limitations identified reflect not only the constraints of this report, but the wider challenge of measuring a phenomenon that is not yet systematically assessed by government.

What was found: Attribution, Costs and Limits

One of the most striking conclusions to emerge from this research is that Britain's understanding of hostile-state activity has advanced considerably faster than its understanding of the economic costs that activity imposes.

Over recent years, Parliament, the intelligence community, Government departments and security organisations have repeatedly warned about the breadth of Russian hostile activity directed against the UK and its allies.

The Intelligence and Security Committee of Parliament's Russia Report described Russian influence activity in the UK as "the new normal" and highlighted the breadth of Russian cyber, intelligence and influence operations directed against Western Democracies.²

The UK Government's own Resilience Action Plan refers explicitly to a growing number of Russian "sub-threshold attacks" and highlights increasing concerns regarding critical infrastructure, economic security and resilience.³

In GCHQ's first Annual Lecture in May 2026, its Director, Anne Keast-Butler, set out the scale of that activity in stark terms:

"Russia is scaling up its daily hybrid activity against the UK and Europe, stretching from the seabed to cyberspace — relentlessly targeting critical infrastructure, democratic processes, supply chains and public trust."

— Anne Keast-Butler, Director GCHQ, GCHQ Annual Lecture, Bletchley Park, 27 May 2026.⁴

The issue, therefore, is not whether the activity exists but how much it costs. That distinction is important because much of the activity discussed throughout this report falls below an arbitrary and poorly defined threshold traditionally associated with conflict.

These attacks are often described as 'sub-threshold'. Yet for those affected, the consequences rarely feel sub-threshold. A business forced to spend millions recovering from a cyber-attack does not experience a sub-threshold cost. A patient whose treatment is delayed because critical systems are offline does not experience a sub-threshold disruption. An employer forced to suspend production for weeks as a result of malicious cyber activity does not experience a sub-threshold consequence.

Indeed, the term 'sub-threshold' holds within its definition a reason not to act. That is unhelpful if the threat to the UK and its economy is as severe as laid out by government and agencies.

When this research was started, it was anticipated that there would be significant challenges associated with attribution. In a limited number of cases attribution was relatively strong, but the costs were unknown. In others, costs could be estimated but attribution remained contested. In most cases, both attribution and economic impacts remained incomplete. The examples below illustrate both the evidence currently available and the considerable gaps that remain.

² Intelligence and Security Committee of Parliament, Russia (HC 632, The Stationery Office, 2020). https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf [Accessed 2 Oct. 2026], p.15

³ Cabinet Office, *The UK Government Resilience Action Plan: 2026 Implementation Report*, 2026. Available at:

<https://www.gov.uk/government/publications/the-uk-government-resilience-action-plan-2026-implementation-report/the-uk-government-resilience-action-plan-2026-implementation-report-html> [Accessed 2 October 2026]

⁴ Anne Keast-Butler, "GCHQ Annual Lecture 2026 - as delivered," speech delivered at Bletchley Park, 27 May 2026, Government Communications Headquarters (GCHQ), <https://www.gchq.gov.uk/speech/gchq-annual-lecture-2026-as-delivered> [Accessed: 2 October 2026]

Royal Mail and the LockBit attack

- Ransomware attack against Royal Mail by the Russia-linked LockBit group in January 2023.
- Disrupted international export services and affected businesses across the country dependent upon Royal Mail's international operations.
- Attribution was linked to the LockBit ransomware organisation, a group disrupted by the National Crime Agency, the Federal Bureau of Investigation and international partners.⁵
- LockBit was widely regarded by law-enforcement agencies as operating from Russia and became one of the world's most prolific ransomware organisations before its disruption.⁶

To understand the economic consequences of the attack, government ministers were asked what estimate had been made of the costs imposed on both Royal Mail and British businesses. The UK Government's response, in full, was as follows:

"We do not routinely comment on costs of individual cyber-attacks. Royal Mail's parent company, International Distributions Services (IDS), has publicly reported spending £10 million on remediation and systems resilience improvements following the incident affecting Royal Mail in 2023.

We know that cyber-attacks can have serious consequences for businesses, with independent research finding that the average cost of a significant cyber incident is almost £195,000. The Government works closely with industry and relevant authorities to support resilience against cyber threats and to ensure risks are appropriately managed."

— Kate Dearden MP, Minister in the Department for Business, Innovation, Science and Trade, written answer to PQ 19662, 2 September 2026.⁷

The £10 million figure tells us what the attack cost Royal Mail but does not tell us what it cost exporters unable to fulfil orders, businesses forced to seek alternative logistics arrangements or lost commercial opportunities.

Even in one of the best-documented incidents considered during this research, only a partial picture of the economic consequences exists. The direct costs are visible, but the wider economic costs are not.

The answer also confirms that government does not assess what individual cyber-attacks cost. Yet in the same answer, government points to its own benchmark: the average significant cyber incident costs a UK business almost £195,000. That figure creates a way to put a floor under the wider burden, and it is used in Chapter 2.

⁵ National Crime Agency, *The NCA announces the disruption of LockBit with Operation Cronos*. National Crime Agency, 2024. <https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos> [Accessed 2 Oct. 2026].

⁶ National Crime Agency, *LockBit leader unmasked and sanctioned*, 7 May 2025

. Available at: <https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned> [Accessed 5 October 2026]

⁷ G. Downie, 'Royal Mail: Cybercrime', Written Question UIN 19662, answered by K. Dearden, Department for Business, Innovation, Science and Trade, 2 September 2026. Available at: <https://questions-statements.parliament.uk/written-questions/detail/2026-07-16/19662> [Accessed 5 October 2026]

The NHS Advanced Attack

- Ransomware attack affecting Advanced Computer Software in August 2022.
- Disrupted NHS 111 services and urgent treatment centres.⁸
- Illustrated how a cyber-attack affecting a private supplier can affect public services and taxpayers.

Because of the scale of the disruption, government was asked what estimate had been made of the wider economic impact. The response was simple:

"No data is held on the total economic impact of the 2022 LockBit attack on NHS 111 and other patient services."

— James Frith MP, Parliamentary Under-Secretary of State for Health and Social Care, 7 September 2026.⁹

A substantial cyber incident disrupted healthcare services, affected thousands of appointments and imposed real costs on public services, yet no estimate existed concerning the broader economic consequences.

The incident later resulted in a £3.07 million penalty imposed by the Information Commissioner's Office in connection with security failings associated with the attack, which represents only a portion of the likely economic burden.¹⁰

The Viasat Attack

- Cyber-attack against Viasat which provides broadband service to Ukraine in February 2022.
- Formally attributed to Russia by the UK and international partners.¹¹
- Formed part of wider activity immediately preceding Russia's full-scale invasion of Ukraine.¹²

The attack disrupted satellite communications infrastructure used across Europe and has frequently been cited as one of the clearest examples of state-sponsored cyber activity integrated into military operations.

Despite the breadth and audacity of this attack, again information on the financial implications was scant and there remains no accepted estimate concerning the economic consequences for the UK. This is an important finding as, while government may know who carried out an attack, that does not mean it could have estimated the costs.

London Arson Attacks

- Russian-linked actors carried out an arson attack on industrial units in Leyton, East London in March 2024.
- Warehouse was linked to aid for Ukraine.
- According to Counter Terrorism Police, the attack caused approximately £1 million in direct damage.¹³
- Financial losses appear modest but demonstrate measurable economic harm from Russian action.

⁸ Dan Milmo, 'NHS ransomware attack: what happened and how bad is it?', *The Guardian*, 11 August 2022. Available at:

<https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it> [Accessed 3 October 2026]

⁹ G. Downie, 'Cybercrime', Written Question UIN 19663, answered by J. Frith, Department of Health and Social Care, 7 September 2026. Available at: <https://questions-statements.parliament.uk/written-questions/detail/2026-07-16/19663/> [Accessed 5 October 2026].

¹⁰ Information Commissioner's Office, *Software provider fined £3m following 2022 ransomware attack*. Information Commissioner's Office, 2025. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/software-provider-fined-3m-following-2022-ransomware-attack/> [Accessed 2 Oct. 2026]

¹¹ BBC News, *UK blames Russia for satellite internet hack at start of war*. BBC News, 10 May 2022. <https://www.bbc.co.uk/news/technology-61396331> [Accessed 2 Oct. 2026].

¹² Foreign, Commonwealth & Development Office, *Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion*. GOV.UK, 10 May 2022. <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion> [Accessed 2 Oct. 2026].

¹³ Counter Terrorism Policing, *Men who organised Russia-backed arson at London warehouse jailed*. Counter Terrorism Policing, 24 October 2025. <https://www.counterterrorism.police.uk/news/men-who-organised-russia-backed-arson-at-london-warehouse-jailed/> [Accessed 2 Oct. 2026].

This attack shows that hostile-state activity is not confined to cyberspace, as is clear from increasing disruption to our airport networks and subsea cable infrastructure.

Once again, while single impact costs were provided, the wider impacts were not. Policing activity, intelligence resources, security responses and broader business disruption remain difficult to quantify.

These attacks were similar to those seen in Estonia in September 2026 which were quickly attributed and highlighted by the Estonian Government.¹⁴

¹⁴ Jon Henley, 'Estonia blames Russia for arson attack on drone maker supplying Ukraine', *The Guardian*, 29 September 2026.
<https://www.theguardian.com/world/2026/sep/29/estonia-blames-russia-arson-attack-drone-maker-ukraine> [Accessed 2 Oct. 2026].

JLR: The Costliest Cyber-attack in British History

- Cyber-attack on carmaker in August/September 2025.
- Most economically significant single incident so far attributed to Russia, although not by the UK Government.
- Broader economic impact was estimated at between £1.6 billion and £2.1 billion.¹⁵

For many years, cyber-attacks were discussed principally as an information technology problem, but the JLR attack shows major cyber incidents can rapidly become economically significant.

An investigation by the New York Times reported that investigators from the Federal Bureau of Investigation, the National Crime Agency, the NCSC and industry concluded the attack originated from a Russian-linked group.¹⁶

Production was halted for five weeks, and the attack imposed an estimated £1.9 billion hit on the British economy, affecting a company supporting around 120,000 jobs through its wider British supply chain.¹⁷

The damage was visible in the national accounts. When official growth figures for the third quarter of 2025 were published, The Guardian's headline read:

"UK economy grew by just 0.1% in third quarter after hit from JLR cyber-attack"

— The Guardian, 13 November 2025.¹⁸

The significance of this incident lies not only in attribution but in scale, demonstrating that a single cyber-attack can generate economic consequences previously associated only with major industrial disruption.

Taken individually, the incidents discussed above may appear disconnected, but each incident created costs for businesses, public services, infrastructure operators or taxpayers.

What links them together is that they form part of a broader pattern of hostile-state activity that repeatedly generates economic consequences while remaining below the threshold of conventional conflict. These are only some of the attacks that are known about and in the public domain. The hidden costs will likely be much larger if investigated and quantified more thoroughly.

¹⁵ Cyber Monitoring Centre, *Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025*, 22 October 2025, <https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rover-cyber-incident-october-2025/> [Accessed 2 Oct. 2026]; BBC News, 'JLR hack "is costliest cyber attack in UK history", experts say', BBC News, 22 October 2025. <https://www.bbc.co.uk/news/articles/cy9pdld4y81o> [Accessed 2 Oct. 2026]

¹⁶ Adam Goldman, Jane Bradley, Dustin Volz and Michael Schwartz, 'A \$2.5 Billion Whodunit: The Hack That Dented the U.K. Economy', *The New York Times*, 26 June 2026. <https://www.nytimes.com/2026/06/26/world/europe/jaguar-russia-hack.html> [Accessed 2 Oct. 2026].

¹⁷ Goldman et al, 'A \$2.5 Billion Whodunit'.

¹⁸ Heather Stewart, 'UK economy grew by just 0.1% in third quarter after hit from JLR cyber-attack', *The Guardian*, 13 November 2025. <https://www.theguardian.com/business/2025/nov/13/uk-economy-grew-by-just-01-in-third-quarter-amid-jlr-cyber-attack-hit> [Accessed 2 Oct. 2026].

Government Information

Alongside the case studies above, our Parliamentary Questions produced some of the strongest official evidence available concerning the wider threat environment.

When government was asked about cyber-attacks originating from Russia, China and Iran, ministers disclosed information supplied by the National Cyber Security Centre, noting:

"In the latest reporting year, the NCSC received 1,727 incident reports, resulting in 429 incidents requiring NCSC support, of which 204 were assessed as nationally significant.

Between June 2025 and May 2026, the NCSC managed more than 200 incidents affecting organisations within the UK's critical national infrastructure and supporting ecosystem, around 75% of which were assessed as linked to state actors."

— Uma Kumaran MP, Foreign Office Minister, 9 September 2026.¹⁹

These official statistics demonstrate that hostile-state activity is already affecting systems at the heart of the British economy. They are also consistent with wider government warnings that hostile states are increasingly targeting the systems upon which Britain's essential services depend.²⁰

Industry Information: CyberCube

The same conclusion emerged from our engagement with industry.

CyberCube, the world's leading cyber risk analytics company, identified more than 300 Russia-linked cyber-attacks against British companies since 2022. By their own reckoning, this was likely a significant undercount given the difficulties in attributing incidents.

Academic and industry research points towards a similar conclusion. Work undertaken by Dr Tom Johansmeyer argues that large single-company cyber losses do not necessarily capture the wider secondary and tertiary economic impacts associated with cyber catastrophes affecting multiple organisations.

This uncertainty reflects the reality that the costs of hostile-state activity are often dispersed throughout the wider economy and not the result of a single action that happens in one particular place at one point in time.

Taken together, the evidence uncovered during this project points toward a clear conclusion, with clear evidence that hostile-state activity imposes economic costs, but no one measuring these costs systematically.

That challenge forms the basis of the next chapter, which will examine what the available evidence can show about the wider scale of Britain's exposure, and what that may reveal about the true scale of the Putin Tax.

¹⁹ Graeme Downie, 'Cybersecurity', Written Question UIN 27124, answered by Uma Kumaran, Foreign, Commonwealth and Development Office, 9 September 2026. <https://questions-statements.parliament.uk/written-questions/detail/2026-09-03/27124> [Accessed 2 Oct. 2026]

²⁰ National Cyber Security Centre, *UK and Allies urge critical sectors to improve defences against Russian intelligence targeting* (2026). <https://www.ncsc.gov.uk/news/uk-and-allies-urge-critical-sectors-to-improve-defences-against-russian-intelligence-targeting> [Accessed 2 Oct 2026].

Extrapolated Costs

This chapter builds progressively from the evidence available, explaining exactly what can be known and what remains uncertain.

What is Known

Three broad findings emerge from the evidence that has been assembled:

- Individual incidents can generate very substantial economic costs, running from millions of pounds to, in the case of JLR, billions, but that the potential for even larger damage should be thought of as a very realistic possibility. The identifiable figures are set out under layer one below.
- Government itself recognises hostile-state cyber activity at scale.²¹
- Government research suggests cyber-attacks impose substantial costs, estimated at £14.7 billion annually.
 - This includes between £1 billion and £8.5 billion from intellectual property theft and £755 million from fraud linked to organisational breaches.²²

Taken together, these findings leave little doubt that hostile-state activity imposes economic costs that can be measured in the tens of billions.

Layer One: Proven Losses

The most conservative approach is to focus only on losses for which identifiable figures already exist for three very specific instances. Using the incidents discussed in the previous chapter produces the following known losses:

Incident	Identified cost
Royal Mail – remediation and resilience costs	c. £10 million
Leyton arson attack – direct damage	c. £1 million
JLR cyber-attack – economic losses	c. £1.6bn–£2.1bn
Minimum identifiable burden	£1.61bn–£2.11bn

This is the minimum identifiable burden based only on just three incidents where meaningful public estimates exist. This also excludes supply chain losses, infrastructure protection costs, general resilience investments and aviation disruption, among other factors. It is a floor, not a ceiling.

Layer Two: Russia-linked Cyber Activity

The next question is whether there is evidence that Russian-linked activity occurs at a scale capable of generating wider economic losses. Here, engagement with CyberCube was particularly important.

CyberCube advised that its incident databases contained more than 300 incidents where the threat actor was known and connected to Russia.

The significance of this figure lies in what it suggests about volume. The JLR attack demonstrates that individual events can produce losses measured in billions.

CyberCube's data suggests that such incidents are not isolated examples occurring in a vacuum. Rather, they exist within a larger ecosystem of Russia-linked cyber activity and occur at a significant scale.

CyberCube's own estimations were based on significant caveats which means that the true number of Russian attacks is likely significantly larger, namely:

²¹ Royal United Services Institute, *Hostile States Behind 75% of Cyber Attacks on UK Infrastructure* - NCSC CEO. RUSI, 17 June 2026.

<https://www.rusi.org/news-and-comment/rusi-news/hostile-states-behind-75percent-cyber-attacks-uk-infrastructure-ncsc-ceo> [Accessed 2 Oct. 2026].

²² Department for Science, Innovation and Technology, *Summary of research on the economic impact of cyber-attacks*. GOV.UK, 12 November 2025. <https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk/summary-of-research-on-the-economic-impact-of-cyber-attacks> [Accessed 2 Oct. 2026].

1. That a significant share of attacks in their database had no reliable attribution.
2. That many businesses will not report a cyber-attack and so will not be considered.
3. That non-British headquartered businesses were not included.

The UK Government's own figures allow the rough figure of 300 cases to be given a baseline value. In its answer on the Royal Mail attack, the government cited independent research putting the average cost of a significant cyber incident at almost £195,000.

Applied to CyberCube's more than 300 Russia-linked incidents, that implies a baseline of around £58.5 million, before any major event is counted. A single incident of JLR's scale costs around 30 times that entire baseline.

This shows how heavily the total burden depends on a small number of severe attacks, and why the baseline should be treated as a floor.

The implication is that the £1.6–£2.1 billion identified in the previous section almost certainly understates the wider burden. The likely significant undercount of cases by CyberCube further increases this likelihood.

More significantly still, CyberCube estimates that there is a 5% chance that the UK will experience a single attack in a given year by a hostile threat actor that would cost a UK company \$4.4 billion (£3.3 billion). This is over 1.5 times the cost of the JLR attack.

Taken together, these figures make for difficult reading. They represent the first reliable figures indicating the scale of the Russian threat and provide an indication of the direct cost of an attack.

Layer Three: Economy-wide exposure

A broader approach begins with the UK Government's estimate of the country's annual cyber burden. As noted, research commissioned by DSIT estimates overall annual cyber losses to UK businesses of approximately £14.7 billion, some 0.5% of total GDP.²³

IBM's X-Force Threat Intelligence Index notes that the UK is the most targeted European nation for cyber-attacks.²⁴

In April 2026, the head of the NCSC reported that the UK is now experiencing four 'nationally significant' cyber-attacks per week.²⁵

This built on earlier comments by UK Security Minister, Dan Jarvis, who acknowledged that the 200 'nationally significant' attacks on the UK in 2025 were more than double the year before.²⁶ 43% of British businesses reported a cyber breach or attack in 2025.²⁷

Of course, not all losses can be attributed to Russia, but it is possible to estimate that a significant number are.

There is good evidence that suggests Russian cyber-attacks on the UK and other NATO states are growing, with an in-year increase of 25% in 2025 alone, and the UK the second most targeted region after the US.²⁸

The NCSC itself designates Russia as 'one of the world's most prolific cyber actors' with 'a significant and enduring threat to the UK'.²⁹

As noted in response to a parliamentary question, three-quarters of incidents affecting Critical National Infrastructure are linked to hostile state actors.³⁰

²³ Department for Science, Innovation and Technology, *Summary of research*.

²⁴ IBM, *X-Force Threat Intelligence Index 2026*. IBM, 2026. <https://www.ibm.com/reports/threat-intelligence> [Accessed 2 Oct. 2026].

²⁵ Emma Burrows, 'UK faces cyberattacks from Russia, Iran, and China, warns NCSC head', *Associated Press News*, 22 April 2026. <https://apnews.com/article/russia-iran-china-uk-cyber-defense-5fcdc5eaf14b2d016c2575bbdab47c39> [Accessed 2 Oct. 2026].

²⁶ Dan Jarvis, *Security Minister's speech to CYBERUK 2026*. Cabinet Office, GOV.UK, 22 April 2026. <https://www.gov.uk/government/speeches/security-ministers-speech-to-cyberuk-2026> [Accessed 2 Oct. 2026].

²⁷ Department for Science, Innovation and Technology, *Summary of research*.

²⁸ Dan Milmo, 'Russian cyber-attacks against Nato states up by 25% in a year, analysis finds', *The Guardian*, 16 October 2025. <https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds> [Accessed 2 Oct. 2026].

²⁹ National Cyber Security Centre, *NCSC Annual Review 2023: Threats and risks. Case study: Russia - an acute and chronic cyber threat* (NCSC, 2023). <https://www.ncsc.gov.uk/collection/annual-review-2023/threats-risks/case-study-russia> [Accessed 2 Oct 2026].

³⁰ G. Downie, 'Cybersecurity', *Written Question UIN 27124, answered by U. Kumaran*, 9 September 2026.

Typically, the hostile states in question are Russia, China, Iran and North Korea, but according to Matthew Prince, CEO of Cloudflare, a cybersecurity firm which provides protection for a fifth of the internet, there is significant evidence that Russia uses Iran as a proxy for some of its attacks, further increasing their share.³¹

The threat is now so pronounced that CEOs of prominent National Infrastructure companies will now receive intelligence briefings on the specific Russian threat.³²

Even when attacks come from cyber-attackers elsewhere, they have often leased the ransomware used from Russian sources.³³

Accordingly, there is reason to surmise that Russia may be responsible for a significant portion of the attacks committed by hostile states. On that basis, even if only a modest share of Britain's overall cyber losses were attributable to hostile Russian activity, the resulting figures would be substantial:

- 10% of annual UK cyber losses = £1.47 billion.
- 15% of annual UK cyber losses = £2.21 billion.
- 20% of annual UK cyber losses = £2.94 billion.

These calculations demonstrate how rapidly costs increase as disruption grows. Using the most conservative figure that Russia-based activity could be responsible for 10% of UK cyber losses of £1.47 billion per year, in addition to the average cost of proven attacks since 2022, the cost to the British state begins to look increasingly significant.

Layer Four: The Infrastructure Multiplier & Subsea cables

A cyber-only estimate underestimates the broader threat picture.

The Government's own Resilience Action Plan Implementation Report highlights increasing concern regarding Russian unconventional activity and the need to strengthen UK resilience in infrastructure, public services and economic security.³⁴

Similarly, the Joint Committee on the National Security Strategy's report on subsea cables warned that Britain's economy relies heavily on infrastructure vulnerable to disruption. The Committee highlighted that subsea cables carry approximately 99% of the UK's international data traffic and supports around \$1.5 trillion of global cross-border trading every day.

It concluded that even low-level deniable attacks could be economically damaging while remaining difficult to attribute and prevent.³⁵

The Government has also acknowledged heightened concern regarding Russian activity around subsea infrastructure. In 2026, ministers announced plans to strengthen protections for undersea internet cables,

³¹ Ali Lyon, "'Sower of chaos' - Russia behind UK cyberattacks, says Cloudflare boss", *City A.M.*, 30 October 2025. <https://www.cityam.com/sower-of-chaos-russia-behind-uk-cyberattacks-says-cloudflare-boss/> [Accessed 2 Oct 2026].

³² Cabinet Office and Ministry of Defence, *CEOs from sensitive sectors to receive briefings on Russia threats* (2026). <https://www.gov.uk/government/news/ceos-from-sensitive-sectors-to-receive-briefings-on-russia-threats> [Accessed 2 Oct 2026].

³³ Theo Leggett, 'The cost of cyber hacking on UK business is greater than it seems', *BBC News*, Internet edition. 6 October 2025. <https://www.bbc.co.uk/news/articles/c5ye8zj5l4jo> [Accessed 2 Oct 2026].

³⁴ Cabinet Office, *The UK Government Resilience Action Plan: 2026 Implementation Report* (2026). <https://www.gov.uk/government/publications/the-uk-government-resilience-action-plan-2026-implementation-report/the-uk-government-resilience-action-plan-2026-implementation-report-html> [Accessed 2 Oct 2026].

³⁵ Joint Committee on the National Security Strategy, *Subsea telecommunications cables: resilience and crisis preparedness* (HC 723, HL 179, 2025). <https://committees.parliament.uk/publications/49566/documents/264088/default/> [Accessed 2 Oct 2026], p.1.

noting that approximately £1.4 trillion of daily UK transactions rely upon the subsea cable system.³⁶ £65bn of UK economic activity relies on these cables.³⁷

That demonstrates the scale of Britain's exposure. Even limited disruption affecting systems of this kind could generate economic consequences significantly larger than those observed in many of the individual incidents examined earlier.

Subsea cables are one of the few areas of hostile-state exposure where a credible per-incident cost already exists in the public domain.

The International Cable Protection Committee (ICPC), the global body representing cable owners, operators and suppliers, reports that dragged anchors account for around 30% of cable faults each year, amounting to roughly 60 faults globally.

It puts the cost of repair at between £500,000 and £1 million per incident for telecommunications cables, and between £10 million and £100 million per incident for power cables.³⁸

Two points follow. The first is that these are repair costs alone. They do not include the economic consequences of the outage itself, the disruption to data traffic, payments and energy transmission that the Joint Committee identified.

The second is that the £100 million figure describes a severe incident affecting power infrastructure, not a routine telecommunications fault. We therefore work from the middle and upper part of the ICPC's power-cable range, £50 million to £100 million per significant incident, rather than from its ceiling.

The question is how many such incidents a year it is reasonable to assume. The Baltic Sea provides an empirical and reasonable comparison. At least 11 subsea cables were damaged or cut in the Baltic Sea in the fifteen months to January 2025 – a rate of almost 9 a year, in a single European sea under sustained Russian pressure.³⁹

Britain is subject to that same pressure. In April 2026, the UK Government revealed that Russian specialist submarines operated by GUGI, Moscow's deep-sea warfare directorate, were attempting to surveil critical undersea infrastructure in and around British waters.⁴⁰ The then Defence Secretary addressed the point directly: "we see you, we see your activity over our cables and pipelines."⁴¹

In September 2026, British, American and Norwegian forces disrupted a Russian operation near Svalbard in which GUGI submersibles were rehearsing the deployment of a capability designed to disable subsea cables without leaving evidence of attribution.⁴²

Verinea Codrean of EUROATLAS told LBC that the significance lay in the shift from surveillance to rehearsal: "what's significant is not just that Russian vessels were operating near critical infrastructure, they were

³⁶ Department for Science, Innovation and Technology, *Plan to toughen protections for subsea internet cables amid heightened Russian activity* (2026). <https://www.gov.uk/government/news/plan-to-toughen-protections-for-subsea-internet-cables-amid-heightened-russian-activity> [Accessed 2 Oct 2026].

³⁷ UK Government, *National Security Strategy 2025* (Cabinet Office, 2025), Available at: https://assets.publishing.service.gov.uk/media/685ab0da72588f418862075c/E03360428_National_Security_Strategy_Accessible.pdf [Accessed 5 October 2026] p.23.

³⁸ International Cable Protection Committee, *Damage to Submarine Cables from Dragged Anchors* (2025). <https://www.iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/> [Accessed 2 Oct 2026].

³⁹ France 24, 'At least 11 Baltic cables have been damaged in 15 months, NATO to up its guard', *France 24*, Internet edition. 28 January 2025. <https://www.france24.com/en/video/20250128-at-least-11-baltic-cables-have-been-damaged-in-15-months-prompting-nato-to-up-its-guard> [Accessed 2 Oct 2026].

⁴⁰ Ministry of Defence, *UK exposes covert Russian submarine operation in and around UK waters* (2026). <https://www.gov.uk/government/news/uk-exposes-covert-russian-submarine-operation-in-and-around-uk-waters> [Accessed 2 Oct 2026].

⁴¹ Ministry of Defence, *UK exposes covert Russian submarine operation*.

⁴² S. McFarlane and G. Slattery, 'EXCLUSIVE: NATO allies foil Russian subsea cable sabotage plot', *Reuters*, Internet edition. 10 September 2026. <https://www.reuters.com/world/europe/nato-allies-foil-russian-subsea-cable-sabotage-plot-2026-09-10/> [Accessed 2 Oct 2026].

rehearsing how to disable that infrastructure.” She warned that the UK remains exposed to a coordinated attack across multiple cables at once.⁴³

Government is already planning on that basis. On 30 September 2026, the UK and Ireland jointly conducted Eastern Pearl, the first exercise of its kind, simulating disruption to multiple cables beneath the Irish Sea.⁴⁴

Applying the ICPC’s per-incident costs to the rate already observed in the Baltic produces a working range for subsea exposure:

£250m–£500m
a year

Five significant incidents a year at £50–100 million each – the rate already observed in the Baltic, applied to UK-relevant infrastructure.

This is an exposure range, not a measured loss, and we set it out as such. The ICPC itself notes that most cable damage results from poor seamanship or equipment failure rather than hostile action.

We include it because the alternative, recording Britain’s subsea exposure as zero, which is the practical effect of there being no government estimate at all, is demonstrably wrong.

The same logic applies to airport resilience. Ministers confirmed that no formal estimate had been made concerning the costs associated with drone incursions affecting airports.⁴⁵

Yet it is entirely reasonable to conclude that there must be economic cost of airport runways being disrupted by drone incursions or threats.

Direct contact with Airports UK confirmed that no such information was available, although in this case on security grounds.⁴⁶

However, independent estimates of the 2018 Gatwick disruption placed losses at between £50 million and £70 million.⁴⁷

⁴³ E.J. Ward, ‘Russia rehearsing attacks that could cripple Britain’s internet and financial system’, *LBC*, Internet edition. 14 September 2026. https://www.lbc.co.uk/article/russia-undersea-cable-attacks-britain-internet-economy-sabotage-5HjdhMM_2/ [Accessed 2 Oct 2026].

⁴⁴ Department of Culture, Communications and Sport, *Major Ireland-UK Emergency Exercise to Strengthen Subsea Telecoms Resilience* (2026). <https://www.gov.ie/en/department-of-culture-communications-and-sport/press-releases/major-ireland-uk-emergency-exercise-to-strengthen-subsea-telecoms-resilience/> [Accessed 2 Oct 2026]

⁴⁵ G. Downie, ‘Airports: Unmanned Air Systems’, Written Question UIN 19666, answered by K. Mather, Department for Transport, 7 September 2026. <https://questions-statements.parliament.uk/written-questions/detail/2026-07-16/19666> [Accessed 2 Oct 2026].

⁴⁶ Private correspondence with AirportsUK, 21 September 2026, confirming that information regarding the effects of cyber or other attacks was considered sensitive and could not be shared.

⁴⁷ S. Calder, ‘Gatwick drone disruption cost over £50m’, *The Independent*, Internet edition. 22 January 2019. <https://www.independent.co.uk/travel/news-and-advice/gatwick-drone-airport-cost-easyjet-runway-security-passenger-cancellation-a8739841.html> [Accessed 2 Oct 2026].

A Working Estimate

The evidence presented above, with the limitations outlined, but with the measurable economic cost of even the limited Russian-based, reasonably attributable and even measured at its most conservative, provides the basis for an estimate of what The Putin Tax costs the UK each year.

With the information presented, any figure below £2 billion annually is difficult to reconcile with identifiable losses already exceeding £1.6 billion, the scale of hostile-state cyber activity identified by the NCSC, CyberCube's Russia-linked incident database and government research showing annual cyber losses of £14.7 billion.

Based on our information, the minimum annual economic burden imposed by Russian hostile activity **is between £2 billion and £2.5 billion per year**.

It is the first attempt to establish an evidence-based estimate of the Putin Tax.

£2bn–£2.5bn
a year

Our working estimate of the annual economic burden imposed on the United Kingdom by Russian hostile activity – the Putin Tax.

These figures illustrate the scale of the economic burden imposed through a combination of security expenditure, resilience investment, business losses, infrastructure protection and wider economic disruption.

What the Putin Tax Could Pay For

The scale of the burden becomes clearer when it is set against the cost of frontline public services. Even at the lower end of our estimate, £2 billion a year would pay the starting salaries of around 62,000 newly qualified nurses. At the upper end, £2.5 billion would pay the starting salaries of around 78,000 nurses, 73,000 teachers or 78,000 police constables.

This is the cost to UK public services of Russia-based aggression.

Equivalent starting salaries	At £2bn a year	At £2.5bn a year
Newly qualified nurses (£32,073)	c. 62,000	c. 78,000
Newly qualified teachers (£34,069)	c. 59,000	c. 73,000
Police constables (£32,256)	c. 62,000	c. 78,000

Illustrative. Based on 2026/27 starting salaries in England, excluding employer on-costs. Sources: NHS Employers; National Education Union; LBC (15 July 2026).

What We Don't Know

Nobody in government is currently bringing this information together. Instead, a patchwork quilt of information was found, spread across Whitehall, regulators, security agencies, infrastructure operators, insurers and private companies. Each organisation possesses only part of the picture.

That is significant because the evidence gathered throughout this report points towards a burden that is already substantial. The case studies examined in Chapter 1 identify losses running into billions of pounds and hostile states are linked to most significant incidents affecting Critical National Infrastructure.

And yet government cannot tell Parliament what the overall figure is. When asked about the economic consequences of the ransomware attack affecting NHS services, ministers confirmed that no estimate existed.

When asked about the costs associated with airport disruption and drone incursions, ministers confirmed that no estimate existed.

When asked about cyber-attacks originating from hostile states, government could provide operational statistics but not economic assessments.

In most areas of public policy, this would be regarded as unusual. The costs of flooding are measured or estimated because flood defences cost money. The costs of fraud are measured because anti-fraud activity costs money. Hostile-state activity increasingly affects critical infrastructure, public services and the wider economy. Yet no equivalent effort has been made to understand its cumulative financial impact.

Indeed, some of the most significant burdens identified during this research are likely among the hardest to quantify.

Britain is investing increasing resources in cyber security, infrastructure protection, resilience planning, maritime monitoring and emergency preparedness.

The UK Government has acknowledged growing concerns regarding Russian activity and has introduced additional measures to protect subsea telecommunications infrastructure and wider critical systems.

These activities carry costs even where no successful attack occurs. They are the price of operating in a more hostile environment.

By the time they appear in annual accounts, insurance claims, resilience budgets, delayed investment decisions and disrupted services, the burden is already being borne by taxpayers, businesses and consumers.

The evidence assembled in this report shows that the Putin Tax is real, the economic burden is real, and it must be properly assessed.

Conclusion and Recommendations

Over the course of this research, evidence was found of cyber-attacks, sabotage, disruption affecting public services, attacks against major employers and growing concern regarding critical infrastructure.

Up to £2.1bn in identifiable losses was found, evidence of substantial hostile-state activity affecting critical systems and growing public expenditure on resilience and preparedness. What was not found was a department capable of bringing those costs together into a single assessment.

The estimate in this report represents an essential, single, preliminary assessment of the economic burden imposed by Russian hostile activity. It is the first parliamentary effort to quantify the Putin Tax.

Our conclusion, ultimately, is straightforward. The Putin Tax is already paid by British taxpayers, by businesses through disrupted trade and higher security costs. It is paid by public services through recovery costs and resilience spending. It is paid by taxpayers through the growing resources required to protect critical infrastructure and respond to hostile activity.

This report should therefore not be treated as the end of the conversation, but the beginning of one. An open and honest conversation between the UK Government and the British public, who have a right to know the costs imposed upon them by an increasingly hostile adversary.

The challenge now is not proving that the Putin Tax exists but ensuring that Britain starts measuring it.

Our findings have led to the following four recommendations.

RECOMMENDATIONS

1. The UK Government should publish an annual report to Parliament setting out the estimated economic cost of hostile foreign-state activity to the United Kingdom.
2. The National Cyber Security Centre should publish annual assessments of significant hostile-state cyber activity, including attribution and estimated economic impacts wherever operationally possible.
3. The Ministry of Defence should develop and publish a methodology for assessing the economic costs of physical hostile activity directed at UK people, businesses, infrastructure and interests.
4. The UK Government should launch a national public awareness campaign on hostile-state threats, cyber resilience and national preparedness.

Bibliography

- BBC News, [UK blames Russia for satellite internet hack at start of war](https://www.bbc.co.uk/news/technology-61396331). BBC News, 10 May 2022. <https://www.bbc.co.uk/news/technology-61396331> [Accessed 2 Oct. 2026].
- BBC News, [JLR hack “is costliest cyber-attack in UK history”, experts say](https://www.bbc.co.uk/news/articles/cy9pdl4y81o). BBC News, 22 October 2025. <https://www.bbc.co.uk/news/articles/cy9pdl4y81o> [Accessed 2 Oct. 2026].
- Burrows, E., 'UK faces cyberattacks from Russia, Iran, and China, warns NCSC head'. *Associated Press News*, 22 April 2026. <https://apnews.com/article/russia-iran-china-uk-cyber-defense-5fcdc5eaf14b2d016c2575bbdab47c39> [Accessed 2 Oct. 2026].
- Cabinet Office and Ministry of Defence, CEOs from sensitive sectors to receive briefings on Russia threats. 2026. <https://www.gov.uk/government/news/ceos-from-sensitive-sectors-to-receive-briefings-on-russia-threats> [Accessed 2 Oct 2026].
- Cabinet Office, The UK Government Resilience Action Plan: 2026 Implementation Report, 2026. <https://www.gov.uk/government/publications/the-uk-government-resilience-action-plan-2026-implementation-report/the-uk-government-resilience-action-plan-2026-implementation-report-html> [Accessed 2 Oct 2026].
- Calder, S., 'Gatwick drone disruption cost over £50m', *The Independent*, Internet edition. 22 January 2019. <https://www.independent.co.uk/travel/news-and-advice/gatwick-drone-airport-cost-easyjet-runway-security-passenger-cancellation-a8739841.html> [Accessed 2 Oct 2026].
- Counter Terrorism Policing, *Men who organised Russia-backed arson at London warehouse jailed*. Counter Terrorism Policing, 24 October 2025. <https://www.counterterrorism.police.uk/news/men-who-organised-russia-backed-arson-at-london-warehouse-jailed/> [Accessed 2 Oct. 2026].
- Cyber Monitoring Centre, *Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025*. 22 October 2025. <https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/> [Accessed 2 Oct. 2026].
- CyberCube. *Follow-Up Briefing to the Office of Graeme Downie MP*. September 2026. Confidential industry briefing.
- Department for Science, Innovation and Technology. *Independent Research on the Economic Impact of Cyber Attacks on the UK*. London: DSIT, 2025. Available at: <https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk>
- Department for Science, Innovation and Technology, *Plan to toughen protections for subsea internet cables amid heightened Russian activity*, 2026. <https://www.gov.uk/government/news/plan-to-toughen-protections-for-subsea-internet-cables-amid-heightened-russian-activity> [Accessed 2 Oct 2026].
- Department of Culture, Communications and Sport, *Major Ireland-UK Emergency Exercise to Strengthen Subsea Telecoms Resilience*, 2026. <https://www.gov.ie/en/department-of-culture-communications-and-sport/press-releases/major-ireland-uk-emergency-exercise-to-strengthen-subsea-telecoms-resilience/> [Accessed 2 Oct 2026].
- Downie, G., 'Airports: Unmanned Air Systems', Written Question UIN 19666, answered by Mather, K., Department for Transport, 7 September 2026. <https://questions-statements.parliament.uk/written-questions/detail/2026-07-16/19666> [Accessed 2 Oct 2026].
- Downie, G., 'Cybercrime', Written Question UIN 19663, answered by Frith, J., Department of Health and Social Care, 7 September 2026. Available at: <https://questions-statements.parliament.uk/written-questions/detail/2026-07-16/19663/> [Accessed 5 October 2026].
- Downie, G., 'Cybersecurity', Written Question UIN 27124, answered by Kumaran, U., Foreign, Commonwealth and Development Office, 9 September 2026. <https://questions-statements.parliament.uk/written-questions/detail/2026-09-03/27124> [Accessed 2 Oct. 2026].
- Downie, G., 'Royal Mail: Cybercrime', Written Question UIN 19662, answered by Dearden, K., Department for Business, Innovation, Science and Trade, 2 September 2026. Available at: <https://questions-statements.parliament.uk/written-questions/detail/2026-07-16/19662> [Accessed 5 October 2026].
- Earendel Associates. *Ukraine & Russia: “Conversations Not Speeches” – Vacuum of Governance in Kyiv as Russia Accelerates Disruption in Europe*. September 2026.
- Foreign, Commonwealth & Development Office, *Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion*. GOV.UK, 10 May 2022. <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion> [Accessed 2 Oct. 2026].
- France 24, 'At least 11 Baltic cables have been damaged in 15 months, NATO to up its guard', France 24, Internet edition. 28 January 2025. <https://www.france24.com/en/video/20250128-at-least-11-baltic-cables-have-been-damaged-in-15-months-prompting-nato-to-up-its-guard> [Accessed 2 Oct 2026].
- Goldman, A., Bradley, J., Volz, D. and Schwirtz, M., *A \$2.5 Billion Whodunit: The Hack That Dented the U.K. Economy*. The New York Times, 26 June 2026. <https://www.nytimes.com/2026/06/26/world/europe/jaguar-russia-hack.html> [Accessed 2 Oct. 2026].
- Henley, J., *Estonia blames Russia for arson attack on drone maker supplying Ukraine*. The Guardian, 29 September 2026. <https://www.theguardian.com/world/2026/sep/29/estonia-blames-russia-arson-attack-drone-maker-ukraine> [Accessed 2 Oct. 2026].
- Horne, Richard., *Hostile States Linked to Three-Quarters of Cyber Attacks Affecting UK Critical Systems*. Royal United Services Institute Annual Security Lecture, June 2026. Available at: <https://www.rusi.org/news-and-comment/rusi-news/hostile-states-behind-75percent-cyber-attacks-uk-infrastructure-ncsc-ceo>
- House of Commons Library. *Countering Russian Influence in the UK*. Research Briefing CBP-9472, 13 March 2025. Available at: <https://commonslibrary.parliament.uk/research-briefings/cbp-9472/>
- House of Commons Library. Correspondence and research assistance provided to the Office of Graeme Downie MP, August-September 2026.
- IBM, X-Force Threat Intelligence Index 2026. IBM, 2026. <https://www.ibm.com/reports/threat-intelligence> [Accessed 2 Oct. 2026].
- Information Commissioner's Office. *Software Provider Fined £3 Million Following 2022 Ransomware Attack*. Available at: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/software-provider-fined-3m-following-2022-ransomware-attack/>
- Intelligence and Security Committee of Parliament, *Russia (HC 632)*. The Stationery Office, 2020. https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf [Accessed 2 Oct. 2026]

- Jarvis, D., *Security Minister's speech to CYBERUK 2026*. Cabinet Office, GOV.UK, 22 April 2026.
<https://www.gov.uk/government/speeches/security-ministers-speech-to-cyberuk-2026> [Accessed 2 Oct. 2026].
- Johansmeyer, Tom. "Cyber Catastrophe Losses and Economic Measurement Methodology." *Journal of Strategic Competition*. Available at: <https://strategiccompetition.org/index.php/josc/article/view/22/3>
- Johansmeyer, Tom. *The Cost of NotPetya to Russia*. Irregular Warfare Initiative. Available at: <https://www.irregularwarfare.org/notpetya-cost-russia/>
- Johansmeyer, Tom. *NotPetya, Ukraine and the Limits of Economic Impact from Cyber Attacks*. Available at: <https://theloop.ecpr.eu/notpetya-ukraine-and-the-limits-of-economic-impact-from-cyber-attacks/>
- Joint Committee on the National Security Strategy, Subsea telecommunications cables: resilience and crisis preparedness (HC 723, HL 179, 2025). <https://committees.parliament.uk/publications/49566/documents/264088/default/> [Accessed 2 Oct 2026].
- Keast-Butler, Anne. 'GCHQ Annual Lecture 2026 - as delivered'. Bletchley Park, 27 May 2026. Available at: <https://www.gchq.gov.uk/speech/gchq-annual-lecture-2026-as-delivered>. Accessed 2 October 2026.
- LBC. "Police Officers in England and Wales to Receive 3.5% Pay Rise." 15 July 2026. Available at: <https://www.lbc.co.uk/news/uk/police-officers-in-england-and-wales-to-receive-35-pay-boost/>
- Ward, E.J., 'Russia rehearsing attacks that could cripple Britain's internet and financial system', LBC, Internet edition. 14 September 2026.
https://www.lbc.co.uk/article/russia-undersea-cable-attacks-britain-internet-economy-sabotage-5HjdHMM_2/ [Accessed 2 Oct 2026].
- Leggett, T., 'The cost of cyber hacking on UK business is greater than it seems', *BBC News, Internet edition*. 6 October 2025.
<https://www.bbc.co.uk/news/articles/c5ye8zj5l4jo> [Accessed 2 Oct 2026].
- Lyon, A., 'Sower of chaos' - Russia behind UK cyberattacks, says Cloudflare boss', *City A.M.*, 30 October 2025.
<https://www.cityam.com/sower-of-chaos-russia-behind-uk-cyberattacks-says-cloudflare-boss/> [Accessed 2 Oct 2026].
- Milmo, Dan. 'NHS ransomware attack: what happened and how bad is it?'. *The Guardian*, 11 August 2022. Available at: <https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it> [Accessed 5 October 2026]
- Milmo, D., 'Russian cyber-attacks against Nato states up by 25% in a year, analysis finds'. *The Guardian*, 16 October 2025.
<https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds> [Accessed 2 Oct. 2026].
- Ministry of Defence, UK exposes covert Russian submarine operation in and around UK waters, 2026.
<https://www.gov.uk/government/news/uk-exposes-covert-russian-submarine-operation-in-and-around-uk-waters> [Accessed 2 Oct 2026]
- National Crime Agency, *LockBit leader unmasked and sanctioned*, 7 May 2024. Available at: <https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned> [Accessed 5 October 2026]
- National Crime Agency, *The NCA announces the disruption of LockBit with Operation Cronos*. National Crime Agency, 2024.
<https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos> [Accessed 2 Oct. 2026].
- National Cyber Security Centre, NCSC Annual Review 2023: Threats and risks. Case study: Russia - an acute and chronic cyber threat. NCSC, 2023. <https://www.ncsc.gov.uk/collection/annual-review-2023/threats-risks/case-study-russia> [Accessed 2/10/2026].
- National Cyber Security Centre. *Annual Review 2025*. London: NCSC, 2025. Available at: <https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf>
- National Cyber Security Centre, UK and Allies urge critical sectors to improve defences against Russian intelligence targeting, 2026.
<https://www.ncsc.gov.uk/news/uk-and-allies-urge-critical-sectors-to-improve-defences-against-russian-intelligence-targeting> [Accessed 2 Oct 2026].
- National Education Union. *Pay Scales – England*. Available at: <https://neu.org.uk/advice/your-rights-work/pay-advice/pay-scales/pay-scales-england>
- NHS Employers. *Pay Scales for 2026/27*. Available at: <https://www.nhsemployers.org/articles/pay-scales-202627>
- Parliamentary Questions submitted by Graeme Downie MP relating to hostile-state cyber activity, the NHS Advanced ransomware attack, airport drone incursions, Royal Mail, Russia-linked cyber activity and National Cyber Security Centre incident reporting. Answered July-September 2026.
- Private correspondence with AirportsUK, 21 September 2026.
- McFarlane, S. and Slattery, G., 'EXCLUSIVE: NATO allies foil Russian subsea cable sabotage plot', Reuters, Internet edition. 10 September 2026. <https://www.reuters.com/world/europe/nato-allies-foil-russian-subsea-cable-sabotage-plot-2026-09-10/> [Accessed 2 Oct 2026].
- Royal United Services Institute, *Hostile States Behind 75% of Cyber Attacks on UK Infrastructure - NCSC CEO*. RUSI, 17 June 2026.
<https://www.rusi.org/news-and-comment/rusi-news/hostile-states-behind-75percent-cyber-attacks-uk-infrastructure-ncsc-ceo> [Accessed 2 Oct. 2026].
- Stewart, H., 'UK economy grew by just 0.1% in third quarter after hit from JLR cyber-attack'. *The Guardian*, 13 November 2025.
<https://www.theguardian.com/business/2025/nov/13/uk-economy-grew-by-just-01-in-third-quarter-amid-jlr-cyber-attack-hit> [Accessed 2 Oct. 2026].
- Written evidence submitted by Graeme Downie MP to the Defence Committee inquiry *Defence in the High North*. Available at: <https://committees.parliament.uk/writtenevidence/164281/html/>
- UK Defence Journal. Reporting on JLR, Russian hostile activity, the High North and critical infrastructure resilience. Available at: <https://ukdefencejournal.org.uk/britain-now-in-conflict-with-russia-warns-mp/> and related articles.
- UK Government, National Security Strategy 2025. Cabinet Office, 2025. Available at: https://assets.publishing.service.gov.uk/media/685ab0da72588f418862075c/E03360428_National_Security_Strategy_Accessible.pdf [Accessed 5 October 2026].

About CyberCube

CyberCube is the leading provider of software-as-a-service cyber risk analytics to quantify cyber risk in financial terms. CyberCube leverages data, analytics, artificial intelligence, and human resources to serve insurance institutions globally. The CyberCube platform was established in 2015 within Symantec and has operated as a standalone company since 2018. With offices in San Francisco, New York, London, and Tallinn, Estonia, the team is committed to helping organizations and society build resilience to cyber risk. For more information, please visit www.cybcube.com or email info@cybcube.com.