



| Brief |

Cyber Threats to UK Elections

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Government, Cybersecurity, Geopolitical

June 25, 2024

Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on June 21, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Brief | Cyber Threats to UK Elections

Executive Summary

When the United Kingdom (UK) holds its general election on July 4, 2024, Prime Minister Rishi Sunak's Conservative Party is very likely to lose its majority to the main opposition: the Labour Party led by Keir Starmer. Recent polling indicates that, should Labour win, the Conservatives may not even be the largest opposition party, with the upstart Reform UK party threatening to further reduce its share of voters. Nevertheless, Conservatives will be campaigning in an attempt to prevent the loss of seats, while Labour will primarily be campaigning to win as many seats as possible to avoid the need to form a coalition with other parties. The 2024 UK elections are also taking place during a period of massive weaponization of cyberspace for covert, as well as overt, digital influence and intimidation campaigns. Many of the cyber instances ZeroFox discovered (including the propagation of deepfakes, tactical disclosure of "technically legitimate" half-truths in malinformation campaigns, and stealthy-yet-mass-scale disinformation campaigns) are at least partially designed to influence voter behavior to narrow the margin of a Labour victory or a Conservative defeat. ZeroFox discovered geopolitical and financially motivated data breaches and distributed denial-of-service (DDoS) attacks conducted by so-called "hacktivists" tied to the election as well.

| Cyber Campaigns Inspired by Domestic Politics

The UK has a plurality voting system—meaning that the candidate that wins the most votes gets that seat. This tends to benefit establishment parties like the Conservative and Labour parties, which have “heartlands” and a floor of support that prevents smaller parties from winning seats. This system also benefits parties like the Scottish Nationalist Party (SNP), which does not have nationwide appeal but has historically had concentrated support in specific areas of Scotland.

- The system does not benefit parties that have shallower but more widespread appeal like the Green Party, with policies that may be popular but which struggles to build seat totals.
- The upstart Reform UK party and its previous iterations have traditionally had similar struggles, since voters in support of its policies may decide voting for the Conservative Party is a better value. However, this election could see Reform UK become the main opposition party, which would open it up to more widespread appeal for future elections.

This could incentivize threat actors to target elections wherein multiple parties are running candidates or the election is particularly close, because influencing even a small group of voters could shift the outcome. Threat actors could seek to exacerbate domestic UK political divisions regarding the primary electoral issues, including:

- Economic issues like the cost of living and inflation—where the perception is that both have been higher than in the rest of the European Union (EU) since Brexit, while the wider UK economy has grown less;
- Crime, notably violent knife attacks;
- Continued high immigration, despite Brexit assurances that it would decrease;
- Support for Israel, which has the potential to see some support for both the major parties move towards more fringe parties;
- Taxes, including raising some to fund initiatives like the clean energy transition and the National Health Service (NHS), while also lowering others to ease the high cost of living; and
- Healthcare, where the NHS has been plagued by work stoppages and lengthy wait times.

The threat to the UK elections from misinformation and disinformation is likely to be high and could affect the election outcomes. The UK's 66 million-strong internet user base presents a conspicuous target for cyber-based campaigns. As was the case in the 2019 elections,¹ the greatest disinformation threat comes from contesting political parties within the country. There have been targeted political ads, intensified by higher campaign spending limits and artificial intelligence (AI).

- In 2019, Britain's Conservative Party faced criticism from the Twitter (now X) community for misleading the public by temporarily renaming one of its accounts "factcheckUK" during the first election debate of the season.²
- In April 2023, Labour Party strategists ran an ad accusing Prime Minister Rishi Sunak of not supporting the jailing of child abusers, prompting calls for Keir Starmer to apologize and retract it. The party released yet another ad blaming Sunak for nearly 1,000 adults avoiding prison since 2010, despite their gun-related convictions.³ The motivation for these sorts of misleading ads is to limit support for Sunak with voters concerned with violent crime.
- In October 2023, an audio clip went viral on social media that purportedly showed opposition leader Keir Starmer verbally abusing his staff. It was debunked as AI-generated by both private-sector and British government analyses.⁴ The motivation for this AI-generated content was likely to siphon support from Starmer towards other left-of-center political parties like the Liberal Democrats, thus limiting his party's majority in Parliament.

¹ [hXXps://edition.cnn\[.\]com/2019/11/20/media/uk-election-debate-disinformation-intl-ge19-gbr/index.html](https://edition.cnn.com/2019/11/20/media/uk-election-debate-disinformation-intl-ge19-gbr/index.html)

² [hXXps://www.nytimes\[.\]com/2019/11/20/world/europe/factcheck-uk-conservative-party.html](https://www.nytimes.com/2019/11/20/world/europe/factcheck-uk-conservative-party.html)

³

[hXXps://www.theguardian\[.\]com/politics/2023/apr/07/labour-defends-ad-claiming-sunak-doesnt-think-child-sex-abusers-should-be-jailed](https://www.theguardian.com/politics/2023/apr/07/labour-defends-ad-claiming-sunak-doesnt-think-child-sex-abusers-should-be-jailed)

⁴ [hXXps://www.politico\[.\]eu/article/uk-keir-starmer-labour-party-deepfake-ai-politics-elections/](https://www.politico.eu/article/uk-keir-starmer-labour-party-deepfake-ai-politics-elections/)



X account posting a clip of the deep-fake audio of Keir Starmer

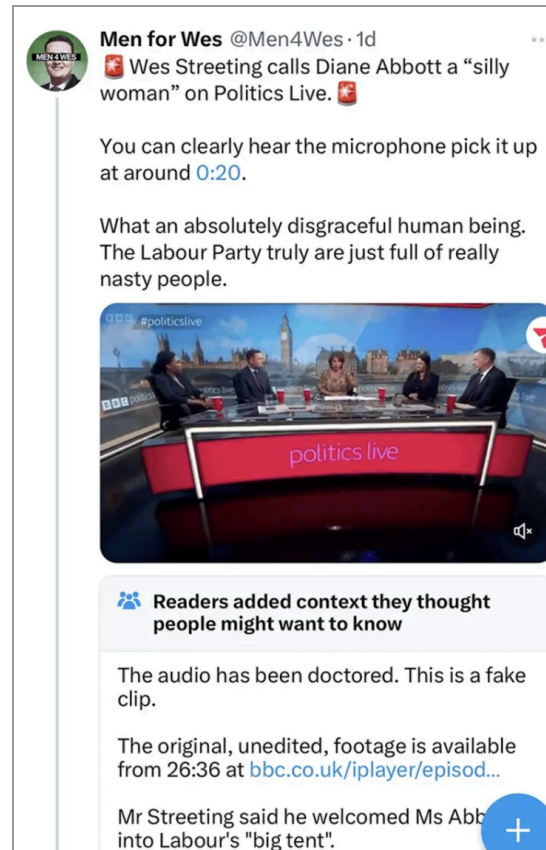
Source:

[hXXps://www.bloomberg\[.\]com/news/articles/2024-03-15/battle-with-x-over-starmer-deepfake-highlights-uk-election-worry](https://www.bloomberg.com/news/articles/2024-03-15/battle-with-x-over-starmer-deepfake-highlights-uk-election-worry)

The UK election faces high risk from social media-based misinformation campaigns. These campaigns can influence voter opinions. With most of the UK population active on social media and having significant screen time, the target audience can be continuously engaged.

- A network of X accounts disseminated a manipulated video of Labour Party's Wes Streeting seemingly insulting former Shadow Home Secretary Diane Abbott. The video, which was doctored and shared widely, misrepresented Streeting's actual words.⁵ Again, the intention of this malinformation is to limit support for Labour.
- Abbott is a relatively controversial Labour Party member supported most by the left-leaning side of the party; malinformation suggesting the Labour Party is mistreating her could see Abbott supporters opt not to vote for Labour and instead cast their ballots for more left-leaning parties.

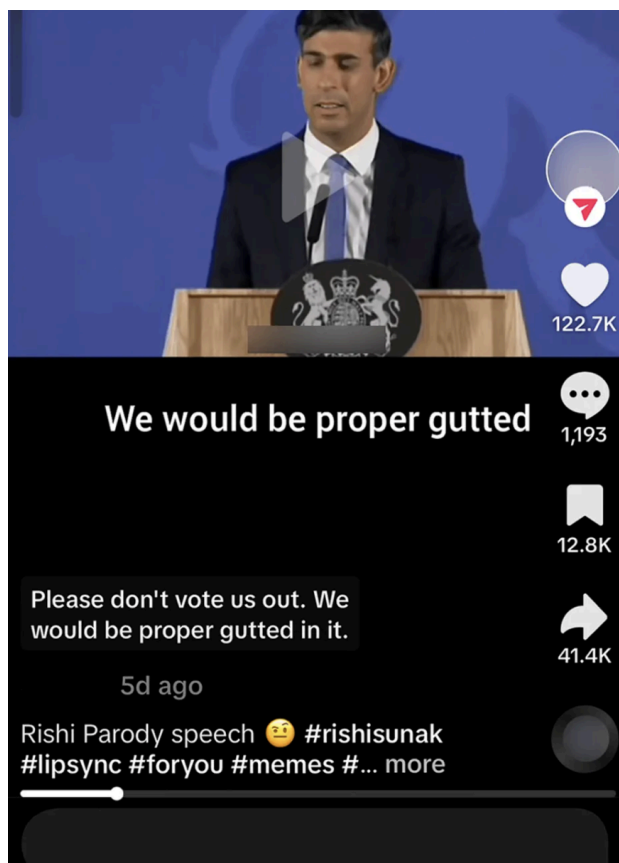
⁵ [hXXps://www.bbc\[.\]com/news/articles/cg33x9jm02ko](https://www.bbc.com/news/articles/cg33x9jm02ko)

**X account sharing doctored video of Wes Streeting insulting Diane Abbott**

Source: [hXXps://www.bbc\[.\]co\[.\]uk/news/articles/cg33x9jm02ko](https://www.bbc.com/news/articles/cg33x9jm02ko)

- Satirical AI-generated clips depict Prime Minister Sunak pleading not to vote out his party alongside unverified statements about Conservative spending, including allegations Sunak sent funds to his associates.⁶ This disinformation is likely designed to further reduce support for the Conservative Party. While it could benefit the Labour Party, it could also be advantageous to the Reform UK Party, a more right-leaning political party in the UK competing for conservative voters in the general elections.

⁶ [hXXps://www.bbc\[.\]com/news/articles/c1ww6vz1l81o](https://www.bbc.com/news/articles/c1ww6vz1l81o)

**Doctored TikTok video of Rishi Sunak asking to not vote out his party**

Source: [hXXps://www.bbc\[.\]co\[.\]uk/news/articles/c1ww6vz1l81o](https://www.bbc.co.uk/news/articles/c1ww6vz1l81o)

| Foreign Cyber Influence Operations

Election Interference

ZeroFox assesses that foreign threat actors pose a significant risk in the upcoming UK elections, potentially influencing public opinion via multiple avenues—including distributing disinformation campaigns, hacking voter databases, or attempting to disrupt voting processes. The UK's Joint Committee on the National Security Strategy has alerted Prime Minister Sunak to the need for stronger measures against foreign interference in the upcoming general election⁷; China, Russia, and Iran are identified as likely perpetrators of cyberattacks during this time.

⁷

[hXXps://www.forbes\[.\]com/sites/emmawoollacott/2024/05/28/uk-security-committee-warns-pm-about-foreign-election-interference/](https://www.forbes.com/sites/emmawoollacott/2024/05/28/uk-security-committee-warns-pm-about-foreign-election-interference/)

- In 2019, Britain's main political parties faced consecutive cyberattacks aimed at disrupting their websites just weeks before a national election.⁸ Following warnings from security agencies about potential interference from Russia and other countries, both the Labour and Conservative parties were targeted. The Labour Party repelled a sophisticated cyberattack without compromising data, but subsequent attacks followed—including one on the Conservative Party's website, highlighting ongoing cybersecurity concerns ahead of the election.

Russia

Following a cyberattack during the 2015 British general election, the hacking of the U.S. Democratic Party's emails as part of an alleged campaign by Russia to help Donald Trump win the 2016 U.S. presidential election, and a rise in clandestine online activity by the Russians across the UK at that time, UK political parties asked for help from the security agencies to protect their online data in 2017.⁹

- In 2023, the UK government accused Russia's Federal Security Service (FSB) of orchestrating a prolonged hacking campaign targeting politicians, civil servants, journalists, and non-governmental organizations (NGOs).¹⁰ Through the hacking group Star Blizzard, the FSB allegedly stole data used to interfere in British politics, including the 2019 election. Government officials highlighted the FSB's role in selectively leaking and amplifying information to undermine trust in politics both domestically and in allied nations.
- In the run-up to the 2024 elections, the UK has issued a warning about targeted spear phishing campaigns by cyber actors from Russia and Iran. Throughout 2022, campaigns conducted by groups like SEABORGIUM and APT42 (TA453) targeted specific sectors such as academia, defense, government, NGOs, and individuals

⁸ [hXXps://www.reuters\[.\]com/article/idUSKBN1XM19H/](https://www.reuters.com/article/idUSKBN1XM19H/)

⁹

[hXXps://www.independent\[.\]co\[.\]uk/news/uk/politics/uk-general-election-russia-hacked-cyber-attack-a7580076.h
tml](https://www.independent.co.uk/news/uk/politics/uk-general-election-russia-hacked-cyber-attack-a7580076.html)

¹⁰

[hXXps://www.forbes\[.\]com/sites/emmawoollacott/2023/12/07/uk-government-accuses-russia-of-election-interfere
nce-through-long-lasting-cyber-attack/](https://www.forbes.com/sites/emmawoollacott/2023/12/07/uk-government-accuses-russia-of-election-interference-through-long-lasting-cyber-attack/)

(including politicians, journalists, and activists) for information gathering.¹¹ The information gathered could then be used in Russian-backed misinformation campaigns.

The incentive for Russian threat actors to influence voter behavior in the UK elections is high.

- Russia would likely benefit from a narrow election victory for Labour. A strong opposition would make passing laws regarding taxes, spending, immigration, and relations with the EU more difficult.
- However, both the Labour Party and the Conservatives are relatively united in their support for Ukraine. Reform UK does not have a clear position on aid to Ukraine, but it is a largely Eurosceptic party—meaning it does not support close UK ties with the EU. Its political allies across the EU, like Hungary’s Viktor Orban or France’s Marine Le Pen, have advocated for closer relations with Russia in the past.
- In the event of a Labour Party win, if Reform UK overtakes the Conservatives as the leading opposition party—or the Conservatives adopt Reform UK policies—it could impact Labour’s ability to govern, including financial and military support for Ukraine.

China

In August 2023, the UK Electoral Commission disclosed a data breach dating back to August 2021 that was initially detected in October 2022.¹² The breach involved unauthorized access to voter data, including email and electoral registers, affecting approximately 40 million people.¹³ Investigations led by the UK’s National Cyber Security Centre (NCSC) attributed the attack to a China-backed threat actor.

- In March 2024, the UK government sanctioned two Chinese individuals allegedly associated with China state-affiliated cyber espionage group APT31. The individuals were accused of conducting "malicious" cyber campaigns against members of Parliament and the Electoral Commission.¹⁴

¹¹

[hXXps://www.ncsc.gov.uk/news/uk-cyber-experts-warn-of-targeted-phishing-attacks-from-actors-based-in-russia-and-iran](https://www.ncsc.gov.uk/news/uk-cyber-experts-warn-of-targeted-phishing-attacks-from-actors-based-in-russia-and-iran)

¹² [hXXps://www.infosecurity-magazine.com/news/uk-blames-china-for-2021-electoral/](https://www.infosecurity-magazine.com/news/uk-blames-china-for-2021-electoral/)

¹³

[hXXps://timesofindia.indiatimes.com/gadgets-news/uk-electoral-commission-hack-exposed-data-of-40-million-voters/articleshow/102576780.cms](https://timesofindia.indiatimes.com/gadgets-news/uk-electoral-commission-hack-exposed-data-of-40-million-voters/articleshow/102576780.cms)

¹⁴ [hXXps://www.bbc.com/news/uk-politics-68654533](https://www.bbc.com/news/uk-politics-68654533)

- While the illicitly-obtained personal information of UK citizens is unlikely to be leveraged to directly influence the results of the 2024 UK general elections, access to sensitive communications between political figures and policy decisions could be of significant value to adversarial nation-state entities.

These events are likely part of broader Chinese strategic initiatives to gather information, exert strategic influence, demonstrate cyber capabilities, undermine Western institutions, and conduct targeted punitive measures in response to recent political disagreements.

Iran

Iran has been accused of orchestrating a series of cyberattacks targeting critical parts of the UK's national infrastructure in 2018.¹⁵ The UK Post Office and local government networks were among those hit in coordinated attacks, resulting in the theft of personal details of thousands of employees. Expert analysis linked the attacks to a group associated with the Iranian Revolutionary Guard, which also targeted the Parliamentary network in 2017, compromising the data of over 10,000 individuals.

Disinformation

ZeroFox assesses there is a medium-high threat of foreign disinformation campaigns influencing the UK elections. Although not likely to directly disrupt the voting processes, these campaigns push geopolitical propaganda and disinformation that are likely to influence voter opinion—and possibly turnout. Chinese, Russian, and other foreign nation-based misinformation has been identified on social media and digital platforms ahead of the elections.

- In 2022, UK-funded research revealed the Kremlin's sophisticated disinformation tactics via a troll factory targeting politicians and audiences across a number of countries, including the UK, South Africa, and India. The campaign aimed to sway opinion on Russia's war in Ukraine, fostering support for Russia and recruiting sympathizers through deceptive online narratives.¹⁶

¹⁵ [hXXps://news.sky\[.\]com/story/iran-conducted-major-cyber-assault-on-key-uk-infrastructure-11676686](https://news.sky.com/story/iran-conducted-major-cyber-assault-on-key-uk-infrastructure-11676686)

¹⁶

[hXXps://www\[.\]gov\[.\]uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda](https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda)

- In 2019, the UK's NCSC identified Star Blizzard (a group likely associated with Centre 18 of Russia's Federal Security Targeting) conducting spear-phishing attacks against UK parliamentarians from multiple political parties from 2015 to 2019.¹⁷ The attacks were likely designed to steal information on UK policy towards Russia.

In addition to social media campaigns, threat actors are likely to deploy other tools to propagate misinformation. In March 2024, a content farm was found impersonating over 60 prominent English-language U.S. and UK media outlets, including *Reuters* and *The Washington Post*.¹⁸ Adversaries are likely to use such services to further enhance their misinformation campaigns—possibly by using information stolen from UK parliamentarians during the 2015–2019 period on their impersonation websites.

Malinformation

In the years leading up to the 2024 elections, UK authorities have identified several data breaches affecting UK voters. Threat actors could then use the stolen data for malinformation—deliberate false information with harmful intent—campaigns in the upcoming elections.

- Compromised data from UK military personnel, voter records, and politicians' details can be used to spread malinformation.
- This could involve creating fabricated stories or altering leaked information to incite division, undermine trust in institutions, or manipulate public perception for political or ideological gain. Malinformation tactics might include selectively releasing data to create misleading narratives or using stolen credentials to impersonate individuals for malicious purposes, amplifying the impact of the breaches beyond mere dis/misinformation to actively harm individuals or organizations.

In May 2024, personal information of undisclosed UK military personnel was accessed through a Ministry of Defence payroll system.¹⁹ The compromised data includes names, bank details of current and some former armed forces members, and in rare cases, personal addresses.

¹⁷ [hXXps://www.ncsc\[.\]gov\[.\]uk/news/uk-and-allies-expose-cyber-campaign-attempted-political-interference](https://www.ncsc.gov.uk/news/uk-and-allies-expose-cyber-campaign-attempted-political-interference)

¹⁸

[hXXps://www.bleepingcomputer\[.\]com/news/security/content-farm-impersonates-60-plus-major-news-outlets-like-bbc-cnn-cnbc/](https://www.bleepingcomputer.com/news/security/content-farm-impersonates-60-plus-major-news-outlets-like-bbc-cnn-cnbc/)

¹⁹ [hXXps://www.bbc\[.\]com/news/uk-68966497](https://www.bbc.com/news/uk-68966497)

- At the time, UK authorities suggested the data was accessed by Chinese-backed threat actors to identify which armed services members could be exploited over their finances.²⁰

Many British, French, and European parliament politicians' email addresses and other details are reportedly available on dark web markets.²¹ The exposed data includes passwords, dates of birth, addresses, and social media accounts.

- On January 14, 2024, "Garuda From Cyber" (pro-Palestine hackers from Indonesia) announced on their channel that they had leaked information from the UK Parliament. According to the post, the group's leader "RENZOSPLEENZ" personally hacked the website parliament[.]uk. Garuda From Cyber shared a sample from the database as proof of the supposed attack. The allegedly leaked information from this data package is likely not the same as that from APT31, a China state-affiliated actor that was almost certainly responsible for targeting UK parliamentarians' emails in 2021.

Hacktivism

Hackers across the world will likely target the upcoming UK elections to disrupt proceedings, steal sensitive data, conduct DDoS or ransomware attacks paralyzing key systems, carry out phishing schemes targeting officials and participants, or make political statements. These attacks are intended to cause disruption and inconvenience, as well as bring the electoral process into disrepute.

- In January 2024, a hacker group called Anonymous Sudan claimed responsibility for an unsuccessful cyberattack on the London Internet Exchange (LINX), citing Britain's support of Israel as the motive. In retaliation for the UK's airstrikes on Iranian-backed Houthi rebels in Yemen and its "unconditional" support of Israel, the group also targeted Legal and General (one of the largest insurance companies in the UK) with a

²⁰

<https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity>

²¹ <https://www.securityweek.com/information-of-hundreds-of-european-politicians-found-on-dark-web/>

cyberattack. These airstrikes were conducted in response to the Houthi rebels' use of drones and missiles to attack shipping off the coast of Yemen.²²

- Pro-Russia hackers are targeting operational technology (OT) devices in North American and European water and wastewater systems, dams, energy, and food and agriculture sectors. These attacks primarily use unsophisticated techniques to manipulate industrial control systems (ICS) equipment, causing nuisance effects. However, investigations have revealed that these actors possess the capability to employ more advanced techniques that could pose physical threats to insecure and misconfigured OT environments.²³

Hacker groups were observed conducting DDoS attacks on European political parties in the lead-up to the EU elections. ZeroFox assesses that hackers could similarly target the UK elections to launch DDoS attacks against political parties to gain attention for their cause. These attacks aim to disrupt political activities and create widespread awareness of the hackers' agenda.

- In early June 2024, pro-Russian hacker group "NoName57(16)" announced its plans to penalize the EU for opposing the invasion of Ukraine, collaborating with seven other organizations and additional anonymous teams. Another Moscow-affiliated cyber group, HackNet, claimed responsibility for the attack on its Telegram channel. Targets included the European Court of Auditors and the Dutch Reformed Political Party.
- Pro-Russian hacker groups launched significant DDoS attacks on political websites in the Netherlands. The initial attack reached a peak of 115 million requests per hour, with one site receiving 73,000 requests per second for four hours. The second attack inflicted a disruption of 44 million requests per hour and a peak of 52,000 requests per second on a single target.²⁴

²²

[hXXps://www.csoononline\[.\]com/article/1291724/london-internet-attack-highlights-confusing-wide-ranging-hackivism-movement.html](https://www.csoononline.com/article/1291724/london-internet-attack-highlights-confusing-wide-ranging-hackivism-movement.html)

²³ [hXXps://www.techrepublic\[.\]com/article/pro-russia-hackers-target-operational-technology/](https://www.techrepublic.com/article/pro-russia-hackers-target-operational-technology/)

²⁴

[hXXps://phishingtackle\[.\]com/articles/ddos-attacks-hit-european-governments-on-the-first-day-of-the-eu-elections/](https://phishingtackle.com/articles/ddos-attacks-hit-european-governments-on-the-first-day-of-the-eu-elections/)

| Conclusion

The 2024 UK elections are taking place during a period of increased digitization and heightened geopolitical tension. Although the winning political party is very likely predetermined, there has very likely been an increase in cyber incidents compared to previous elections that were closer. The UK's parliamentary system gives several major political parties competing across the country incentive to contest every seat, which increasingly means utilizing deceptive cyber tactics. Foreign-backed threat actors also have impetus to divide voters, while even those disinterested in the outcome see the election as an opportunity to access voter data that they can later weaponize.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%