Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **28 March 2018**

Public Authority: Foreign and Commonwealth Office

Decision (including any steps ordered)

1. The complainant has requested information in relation to the number, nature, and effects of cyber attacks on the Foreign and Commonwealth Office. The department relied on the exclusions at sections 24(2) and 31(3) as its basis for neither confirming nor denying whether it held information within the scope of the request.

2. The Commissioner's decision is that:

   - The Foreign and Commonwealth Office was not entitled to neither confirm nor deny holding information within scope of the first part of the request.[1]

   - The Foreign and Commonwealth Office was entitled to neither confirm nor deny whether it held information within the scope of the second part of the request.[2]

3. The Commissioner requires the public authority to take the following steps to ensure compliance with the legislation.

   - Confirm or deny whether it holds information within the scope of the first part of the request.

4. The Foreign and Commonwealth Office must take these steps within 35 calendar days of the date of this decision notice. Failure to comply may

[1] The Commissioner has highlighted this as Part 1 of the request in the main body of this notice.

[2] The Commissioner has highlighted this as Part 2 of the request in the main body of this notice.

result in the Commissioner making written certification of this fact to the High Court pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Request and response

5. On 3 November 2016 the complainant wrote to the Foreign and Commonwealth Office (FCO) and requested information in the following terms:

6. "I write with a request for information about cyber attacks on the department….

   Please disclose the number of recorded cyber attacks in 2015;

   Please disclose the number of recorded cyber attacks to date in 2016;

   For 2016, please provide:

   A month-by-month breakdown;

   The number of successful attacks – i.e. where there was a breach;

   In the cases of a breach, please disclose:

   the nature of the attack (DDOS, phishing etc),

   the nature of the breach,

   how many individuals' information were affected,

   whether any classified information was affected,

   what organisations or individual/s are suspected to known to have made the attack."

7. The FCO responded on 14 December 2016. It neither confirmed nor denied holding information within the description specified in the request by virtue of the provisions in section 24(2) (National security) and section 31(3) (Law enforcement) FOIA.

8. Following an internal review the FCO wrote to the complainant on 16 January 2017. The original decision to rely on sections 24(2) and 31(3) was upheld.

Scope of the case

9. The complainant contacted the Commissioner on 17 January 2017 to complain about the way his request for information had been handled. The Commissioner has referred to his submissions at the relevant parts of her analysis below.

10. The scope of the Commissioner's investigation therefore was to determine whether the public authority was entitled to neither confirm nor deny holding information within the scope of the request on the basis of sections 24(2) and 31(3) FOIA.

Reasons for decision

11. For ease of reference, the Commissioner has divided the request into two parts. Part 1 covers the first part of the request for the number of recorded cyber attacks in 2015 and 2016. Part 2 covers the second part of the request for details about cyber attacks for 2016 including the number of attacks broken down by month, the nature, and the effects of those attacks.

Section 24(2)

12. Section 24 partly states:

> 1. Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purposes of safeguarding national security.
>
> 2. The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purposes of safeguarding national security

13. By virtue of section 24(3) FOIA a certificate signed by a Government Minister certifying that exemption from section 1(1)(b), or from section 1(1)(a) and (b), is, or at any time was, required for the purpose of safeguarding national security shall be conclusive evidence of that fact[3].

14. For the avoidance of doubt, the FCO has not issued a certificate pursuant to section 24(3) in this case.

[3] Subject to section 60 FOIA – Appeals against national security certificate

Section 31(3)

15. The FCO has relied on this exclusion on the basis that confirming or denying whether it holds information within the scope of the request would be likely to prejudice the prevention or detection of crime.

16. The relevant provisions in section 31 state:

    1. Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice

    a. The prevention or detection of crime……..

    3. The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

17. The FCO's submission to the Commissioner in support of reliance on both exclusions is summarised below.

18. Section 24(2) was applied because confirming or denying whether information is held within the scope of the request would be likely to assist malicious actors in undertaking cyber attacks against the department's ICT systems. Section 31(3) was applied because confirming or denying whether information is held would be likely to assist malicious actors in the pursuance of criminal acts. Any confirmation or denial could help malicious actors deduce if their attacks had gone undetected or not.

19. The FCO pointed out that it and other government departments hold a wide range of sensitive information on their ICT systems that is of interest to a variety of malicious actors with criminal intent, including the intent to compromise the UK's national security. This includes financial and commercial information, information about departmental assets, and personal data belonging to staff and service users. In the FCO's case it also includes political reporting, information shared with allies and information about the UK's national position on key foreign policy issues.

20. It stated that it is aware a wide number of malicious actors make frequent attempts to attack government systems for a variety of criminal purposes, including purposes which would prejudice national security. Some may be more sophisticated/professional than others, but there are certainly some who will keep detailed information relating to attempted attacks in order to "fine tune" their strategy. While their key targets may be those departments which they feel will hold the most useful/sensitive information, they will attempt attacks across the board.

A successful attempt on one department's systems could provide an inroad to others, especially as many departments are linked via a secure network.

21. Requests to government departments on cyber attacks are often round robins such as the request in this case. Therefore, if departments do not adopt a neither confirm nor deny stance (NCND) consistently malicious actors would have the opportunity to build up a picture of, and focus their attention on, those departments which are potentially more vulnerable in this regard.

22. In response to a comment by the complainant, the FCO argued that the fact that a Denial of Service (DOS) attack on the Ministry of Justice's (MOJ) website was made public does not mean that all cyber attacks against government infrastructure should be confirmed or denied. Websites such as the MOJ's are public facing, and the results of a DOS attack are apparent because the service becomes unavailable to the public. Internal department ICT systems are clearly not public facing. Therefore, if departments do not confirm or deny they hold information about attacks on internal networks, malicious actors are less likely to know whether such attacks have been successful or not.

23. With respect to the balance of the public interest, the FCO acknowledged the public interest in being confident that departments are able to adequately protect their systems from hostile attack. However, given the amount and sensitivity of much of the data held on those systems, it is also clearly in the public interest that it does not release information that could increase the threat of such attacks occurring or being successful, prejudice the ability to prevent or detect such attacks, or to apprehend those responsible.

24. For the above reasons, the FCO submitted that neither confirming nor denying whether information is held within the scope of the request is required for the purpose of safeguarding national security. It further submitted that confirming or denying whether information is held within the scope of the request would be likely to prejudice the prevention or detection of crime.

Complainant's position

25. The complainant's position is reproduced below.

26. "The neither confirm nor deny response itself is untenable. It is clear that the FCO does record cyber attacks. The Government has previously spoken about the many thousands of attacks on departments each month and other departments have previously confirmed attacks,

including: http://news.sky.com/story/cyber-attack-on-ministry-of-justice-website-10417630

27. To be clear: the request is for * numbers of attacks * numbers of successful attacks and in those cases the type of attacks etc. There is a compelling public interest in disclosure of information capable of informing people how many attacks there have been and how many have been successful or not. Transparency allows the public to scrutinise whether the millions of pounds of public money being spent on secure systems is adequate and provides sufficiently robust protection for data held by the FCO. Only recently the Government announced that £1.9 billion of public money is being spent on cyber security. This alone provides a compelling justification for transparency surrounding this issue.

28. It must also be pointed out that transparency will increase public confidence in Government security.

29. None of the information requested would help hackers. It doesn't reveal the hacks they used to penetrate the systems. It simply reveals how many attacks have been successful and how many people were affected etc.

    There is a compelling and legitimate public interest in knowing how secure the FCO's systems are. Information concerning Britons relies on the FCO having resilient systems and it is paramount that the public is able to obtain basic information about how secure those systems are. It must be pointed out that the numbers are capable of demonstrating how many attacks have failed. This shows that public money the FCO has spent on secure systems has been well spent and, as mentioned, improves confidence in the FCO."

Commissioner's position

30. Including this complaint, the complainant submitted complaints against 13 departments in total pursuant to the same request under consideration in this case. In addition to the FCO's submissions in this case, the Commissioner has received a confidential submission from the Cabinet Office in support of reliance on NCND by 11 of the departments including the FCO. The remaining two departments have not relied on NCND.

31. For the avoidance of doubt, the Commissioner has considered all of the submissions received in this case including the complainant's above.

32. The duty imposed on public authorities to either confirm or deny whether they hold information of the description requested by an

applicant is enshrined in section 1(1)(a) FOIA (commonly referred to as the duty to confirm or deny).

33. Part II of the FOIA contains a number of exclusions from the duty to confirm or deny. Sections 24(2) and 31(3) FOIA are two of those exclusions from the duty to confirm or deny.

34. Broadly speaking, a public authority may withhold information on the basis of section 24(1) FOIA if it considers that placing the information in the public domain would leave the United Kingdom (UK) vulnerable to a national security threat. Section 24(2) is available to a public authority if it considers that an exemption from the duty to confirm or deny is required for the purposes of safeguarding national security. In other words, if it considers that complying with the duty in section 1(1)(a) would leave the UK vulnerable to a national security threat.

35. A public authority may withhold information on the basis of section 31(1)(a) if its disclosure would be likely to prejudice the prevention or detection of crime. Section 31(3) is available to a public authority if it considers that compliance with the duty in section 1(1)(a) would be likely to prejudice the prevention or detection of crime.

36. Clearly, exclusions from the duty to confirm or deny and exemptions from compliance with the requirement in section 1(1)(b)[4] cannot be relied on simultaneously in response to the same request.

37. With respect to the meaning of national security, the Commissioner endorses the Information Tribunal's summary of the House of Lords observations in Secretary of State for the Home Department v Rehman [2001] UKHL 47. The Tribunal summarised the House of Lords observations on the meaning of national security as follows:

- National security means the security of the UK and its people.
- The interests of national security are not limited to actions by an individual which are targeted at the UK, its system of government or its people.
- The protection of democracy and the legal and constitutional systems of the state are part of national security as well as military defence.
- Action against a foreign state may be capable indirectly of affecting the security of the UK.

[4] To release requested information to an applicant.

- Reciprocal cooperation between the UK and other States in combating international terrorism is capable of promoting the UK's national security.

38. The exclusion in section 24(2) applies where neither confirming nor denying whether information is held within the scope of a request is "required for the purposes of safeguarding national security." The Commissioner considers this to mean that the exclusion can be applied where it is necessary to in order to safeguard national security. However, it is not sufficient for the information sought simply to relate to national security. In the Commissioner's view, there must be a clear basis for arguing that confirming or denying whether the information is held would have an adverse effect on national security. This however does not mean that it is necessary to demonstrate that confirming or denying whether the information is held would lead to a direct or immediate threat to the UK. Support for this view is taken from the Rehman case especially from the following observation by Lord Lynn:

    "To require the matters in question to be capable of resulting 'directly' in a threat to national security limits too tightly the discretion of the executive in deciding how the interests of the state, including not merely military defence but democracy, the legal and constitutional systems of the state need to be protected. I accept that there must be a real possibility of an adverse effect on the United Kingdom for what is done by the individual under inquiry but I do not accept that it has to be direct or immediate."

39. Clearly therefore, the question for the Commissioner with respect to the application of section 24(2) is whether there is sufficient basis for arguing that confirming or denying information is held within the scope of the request would have an adverse effect on national security. However, the causal effect does not have to be immediate or direct.

40. The Commissioner shares the view that revealing details of a particular cyber incident or attack especially in order to assure service users that it has been identified and that work is ongoing to rectify it does not in itself make an NCND response untenable. She does not consider that this undermines FCO's argument for relying on NCND in order to protect its ICT networks especially internal networks against threats and attacks which may not always be apparent to the public. Having said that, there is sufficient information in the public domain in the Commissioner's view which at least suggests that as a government department, it is more probable than not that it has been the subject of cyber attacks. For example, on 1 November 2016 the Chancellor of the Exchequer published the National Cyber Security Strategy 2016-2021 which contains the following statement: "We regularly see attempts by states and state-sponsored groups to penetrate UK networks for political,

diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors."[5] Furthermore, in a speech given at the Billington Cyber Security Summit on 13 September 2016 by the Chief Executive of the National Cyber Security Centre (NCSC) he stated, "….last year we detected twice as many national security level cyber incidents – 200 per month – than we did the year before."[6]

41. Therefore, in the Commissioner's view the prejudicial effect of issuing a response which effectively confirms or denies whether there were recorded incidents of cyber attacks at the FCO in 2015 and 2016 would be minimal. Revelatory public pronouncements at such high levels of government undermine the view that confirming or denying whether these attacks occurred would have an adverse effect on national security. The Commissioner has also considered the confidential submission by the Cabinet Office and has concluded that it supports her position in the circumstances of this case. She has explained the rationale for this conclusion in a confidential annex.

42. However, the Commissioner considers that the FCO's response to the second part of the request for a detailed breakdown of the number of cyber attacks, the nature, and effects of the attacks is likely to be more useful to malicious actors. Confirming or denying whether information is held in relation to this part of the request would reveal something about the way cyber attacks are recorded including whether or not certain details about the nature and effects of attacks are held. A confirmation that information is held for example may give an indication to the success or otherwise of an attack. A denial on the other hand may indicate vulnerabilities in the system or that a particular type of attack was unsuccessful. The Commissioner recognises that terrorists and other malicious actors can be highly motivated and may go to great lengths to gather intelligence. Therefore, although seemingly harmless, confirming or denying whether information such as a monthly breakdown of the number of recorded cyber attacks, the nature, and effects of those attacks is held, may assist malicious actors when pieced together with existing or prospectively available information whether gathered lawfully or not.

---

[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[6] https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

43. The Commissioner has therefore concluded that the FCO was not entitled to rely on section 24(2) with respect to Part 1 of the request but was entitled to engage same with respect to Part 2 of the request.

44. Having found that the FCO was entitled to engage section 24(2) in relation to Part 2 of the request, the Commissioner is not obliged to consider whether it was entitled to rely on section 31(3) with respect to same. However, in the circumstances of this case, the Commissioner has gone on to consider whether the FCO was entitled to rely on section 31(3) in relation to both Parts 1 and 2 of the request.

45. The question for the Commissioner with respect to the application of section 31(3) is whether confirming or denying information is held within the scope of the request would be likely to prejudice the prevention or detection of crime.

46. In view of her findings in relation to the application of section 24(2), the Commissioner has no hesitation concluding that confirming or denying whether information is held in relation to a monthly breakdown of the number of cyber attacks, the nature, and effects of the attacks, would pose a real and significant risk of prejudice to the prevention or detection of crime. The FCO was therefore entitled to engage section 31(3) with respect to Part 2 of the request.

47. For the same reasons previously set out above, the Commissioner has also concluded that confirming or denying whether the FCO holds the number of recorded cyber attacks for 2015 and 2016 would not pose a real and significant risk of prejudice to the prevention or detection of crime. Therefore, the FCO was not entitled to rely on section 31(3) with respect to Part 1 of the request.

Public interest test

48. The Commissioner next considered whether in all the circumstances of the case the public interest in maintaining the exclusions of the duty to confirm or deny outweighs the public interest in disclosing whether it holds information within the scope of Part 2 of the request. Having found that sections 24(2) and 31(3) were not engaged with respect to Part 1 of the request, there is no requirement for her to conduct a public interest test.

49. The complainant has correctly pointed out that given the amounts spent by the government on cyber security there is a public interest in knowing how robust the systems in place are. In the Commissioner's view, confirming or denying whether information is held would only provide limited insight in that regard. However, this limited benefit would clearly be outweighed by the damage such confirmation or denial

is ultimately likely to cause to national security and more widely, the prevention or detection of crime. The complainant is right to point out that transparency would increase public confidence in government ICT systems and that this would be in the public interest. However, this must be balanced against the stronger public interest in not undermining confidence in government ICT systems by revealing information which would be useful to malicious actors intent on causing criminal damage to the UK and its institutions.

50. Therefore, the Commissioner has concluded that in all the circumstances of the case the public interest in maintaining the exclusions at sections 24(2) and 31(3) outweighs the public interest in confirming or denying whether any information is held with respect to Part 2 of the request.

Right of appeal

51. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 1234504
    Fax: 0870 739 5836
    Email: GRC@hmcts.gsi.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

52. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

53. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Gerrard Tracey
Principal Adviser
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF