Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **28 March 2018**

Public Authority: Ministry of Defence

Decision (including any steps ordered)

1. The complainant has requested information in relation to the number, nature, and effects of cyber attacks. The public authority refused to disclose the information held within the scope of the request on the basis of the exemptions at sections 31(1)(a), 24(1), 26(1)(a) and (b) FOIA.

2. The Commissioner's decision is that the public authority was entitled to rely on the exemption at section 24(1) as the basis for withholding the information held within the scope of the request.

3. No steps are required.

Request and response

4. On 3 November 2016 the complainant wrote to the public authority and requested information in the following terms:

   "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."

5. The public authority responded on 23 November 2016. It stated that following an initial search for the information requested, it had determined that it held information within the scope of the request. It however concluded that the information requested was exempt on the basis of sections 24(1) (National Security), 26(1)(a) and (b) (Defence) and 31(1)(a) (Law Enforcement) FOIA.

6. Following an internal review the public authority wrote to the complainant on 23 January 2017. It upheld the original decision.

Scope of the case

7. The complainant contacted the Commissioner on 24 January 2017 in order 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

8. The scope of the investigation therefore was to determine whether the public authority was entitled to rely on the exemptions at sections 24(1), 26(1)(a) and (b) and 31(1)(a). The public authority has provided additional confidential submissions in respect of the application of another provision in the FOIA.

Reasons for decision

Section 24(1)

9. The Commissioner has first considered whether the public authority was entitled to rely on this exemption which was applied to the information held within the scope of the request.

10. Section 24(1) 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 purpose 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 purpose of safeguarding national security.
>
> (3) A certificate signed by a Minister of the Crown 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, subject to section 60, be conclusive evidence of that fact.
>
> (4) A certificate under subsection (3) may identify the information to which it applies by means of a general description and may be expressed to have prospective effect."

Complainant's submissions

11. The complainant has submitted the following arguments in support of his view that the requested information ought to be disclosed.

12. "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, how many people were affected and the type of attacks etc. It gives nothing away that would compromise security."

13. "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 MOD. 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."

14. "There is a compelling and legitimate public interest in knowing how secure the MOD's systems are. The security of data concerning Britons and issues affecting Britons depends on the MOD 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 MOD has spent on secure systems has been well spent and, as mentioned, improves confidence in the MOD."

Public authority's submissions

15. The public authority's submission in support of reliance on this exemption is summarised below.

16. It pointed out that it processes data on a vast range of subjects on its systems that is of interest to a variety of threat actors ranging from criminals to hostile intelligence services. This includes sensitive personal data of staff, weapons systems data, intelligence data and sensitive commercial information.

17. The public authority therefore submitted that to provide information about the specific number of cyber attacks against its IT systems would provide useful intelligence to those who may have malicious intent. It may also assist them in the use of an effective form of software against its IT systems and may also be motivational to those who might have previously targeted the systems using such software. Individuals would be able to deduce how successful it is in detecting attacks and indicate how robust its defences were against attacks. It would also expose that attacks had probably gone unnoticed which in turn could suggest vulnerability especially if one adversary had mounted numerous attacks way above the amount it had detected. On the other hand if an adversary considered that the number of attacks were extremely low, it may encourage them to produce more resilient software, less susceptible to detection.

18. The public authority further argued that were it to provide the level of details in the latter parts of the request, this could infer that its IT systems had proved vulnerable to a certain type of malicious attack. Even if, in reality, this is the wrong inference to draw, it would be seen as useful intelligence to those who may have malicious intent to target its systems.

19. The public authority also considered whether the public interest in maintaining the exemption outweighs the public interest in disclosing the information in scope. Its submission on the balance of the public interest is summarised below.

20. The public authority acknowledged that releasing the information in scope would increase public understanding and meet the inherent public interest in transparency about the level of IT security employed by government departments. More so, given that the Secretary of State has announced the levels of public money to be invested in cyber defence.[1]

21. It however argued that the public interest in maintaining the exemption far outweighed that in disclosure. It submitted that there was a strong public interest in not releasing information which would be seen as useful intelligence to those with malicious intent and would assist them in the use of an effective form of software against its IT systems.

22. It also submitted that there was a strong public interest in not releasing information which would enable individuals to deduce how successful it is in detecting attacks and indicate how robust its defences were against attacks. It was not in the public interest for an adversary to have details of the level of protection employed by the public authority.

Is the exemption engaged?

23. The Commissioner has first considered whether the exemption at section 24(1) was engaged.

24. In broad terms a public authority may rely on section 24(1) if it considers that releasing the information requested would make the UK's institutions and/or its citizens more vulnerable to a national security threat. There is no definition of national security. However, the Commissioner is guided by the Information Tribunal's[2] interpretation of the House of Lords observations in relation to the meaning of national security in Secretary of State for the Home Department v Rehman [2001] UKHL 47. The Tribunal summarised the Lords' observations 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.

[1] https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre

[2] In Norman Baker v the Information Commissioner and the Cabinet Office EA/2006/0045

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

25. The exemption applies where withholding the information requested is "required for the purposes of safeguarding national security". The Commissioner considers this to mean that the exemption can be applied where it is reasonably 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 disclosure would have an adverse effect on national security.

26. This however does not mean that it is necessary to demonstrate that disclosing the requested information would lead to a direct or immediate threat to the UK. Support for this approach 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."

27. The Commissioner can certainly appreciate why information held in relation to the request for cyber attacks statistics would appear relatively harmless or of very limited use to those with malicious intent. Conversely, she can understand why information held in relation to the nature of the cyber attacks would be very useful intelligence to those with malicious intent. Nevertheless, the test is whether withholding the information in scope is reasonably necessary for the purposes of safeguarding national security. There is no requirement on the public authority to show that disclosure would lead to a direct or immediate threat to the UK.

28. She has carefully considered the public authority's written submissions and the explanation subsequently provided verbally. She is particularly mindful of the fact that the public authority will have in its possession,

some of the country's most sensitive information which in the wrong hands could do very serious damage to national security. This fact alone undoubtedly makes it a high value target for hackers and other actors with similar malicious intent. She accepts the view that releasing the number of recorded cyber attacks, the number of successful attacks, and the number of individuals affected for the relevant period could indicate how robust the public authority's defences were, and also the number of attacks that had probably gone unnoticed. It is not inconceivable that malicious actors could be able to deduce how successful the public authority is in detecting attacks from the statistical information released pursuant to this request when pieced together with existing or prospectively available information whether gathered lawfully or not. In the Commissioner's view, this makes withholding the statistical information reasonably necessary in order to safeguard national security.

29. Furthermore, she is persuaded that information regarding the nature and effects of the cyber attacks would be useful to malicious actors. For example, it could reveal whether a specific type of attack has a high or low success rate. Therefore, in the Commissioner's view, this also makes withholding information in relation to the nature and effects of cyber attacks reasonably necessary in order to safeguard national security.

Balance of the public interest

30. The exemption at section 24(1) is qualified by the public interest test set out in section 2(2)(b) FOIA. Therefore, the Commissioner must determine whether in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosure.

31. The Commissioner considers that the complainant has made a reasonable case for releasing the information in the public interest. She accepts that there is a public interest in being able to assess the extent to which the significant sums of money spent and budgeted on cyber security is having an impact. However, she does not consider that it is possible to extrapolate anything conclusive in this regard from the limited amount of information in scope. Nevertheless, she considers that the information held by the public authority would provide a snapshot (albeit limited in relation to this specific public interest) of the robustness or otherwise of the public authority's defences against cyber attacks.

32. The Commissioner must however balance this public interest against the significant public interest in safeguarding national security. She has already set out why she considers that protecting the information held

by the public authority is reasonably necessary for safeguarding national security.

33. For the same reasons, she accepts the public authority's submissions that the public interest in maintaining the exemption is significantly weightier than the public interest in disclosure.

34. The Commissioner therefore finds that the public authority was entitled to rely on the exemption at section 24(1).

35. Consequently, she has not considered the applicability of the remaining exemptions.

Right of appeal

36. 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

37. 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.

38. 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