Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Appendix to Interview Summary: House of Commons Administration (Hedi Touati and Benoît Dicaire)*

Hedi Touati, Deputy Director of Information Technology ("**IT**") Security, and Benoît Dicaire, Chief Information Officer, were interviewed by Commission Counsel on September 17, 2024. The interview took place in a secure environment and included references to classified information. This summary discloses information that, in the opinion of the Commissioner, would not be injurious to the vital interests of Canada or its allies, national defence or national security.

Notes to readers:

- Commission Counsel have provided explanatory notes in square brackets to assist the reader.
- This Appendix should be read with the unclassified interview summary from September 3, 2024.

1. Organization of the House of Commons Digital Services

[1] Mr. Dicaire is the Chief Information Officer for Digital Services and Real Estate at the House of Commons ("**Digital Services**").

[2] Mr. Touati was appointed Deputy Director, IT Security, for the House of Commons in 2019. In 2021, his position reported to the Chief Technology Officer. Mr. Dicaire stated that in 2023, Digital Services underwent an internal restructuring. The position of Chief Technology Officer was abolished, resulting in the Deputy Director of IT Security reporting directly to the Chief Information Officer [Mr. Dicaire]. Mr. Dicaire explained that the purpose of this restructuring was to enable Digital Services to deal with growing

* Translation

threats and continue to fulfill their mandate effectively. The position of Assistant Director has also been upgraded to Director level (Chief Information Security Officer).

2. Classified Intelligence and Cybersecurity

[3] Mr. Dicaire explained that the House of Commons Sergeant-at-Arms has a direct relationship with the Canadian Security Intelligence Service ("**CSIS**"). Digital Services and the Canadian Centre for Cyber Security ("**CCC**") have a Memorandum of Understanding ("**MOU**") governing information sharing. Mr. Dicaire added that the Sergeant-at-Arms and Digital Services exchange information on a regular basis. Mr. Dicaire indicated that the information sharing processes, both between the Sergeant-at-Arms and Digital Services, and between Digital Services and the CCC, were efficient

[4] Mr. Touati explained that House of Commons Digital Services receive classified intelligence at varying frequency, depending on cybersecurity incidents and potential threats. This information sharing fosters cooperation between intelligence agencies and the House of Commons. Classified intelligence is transmitted verbally, in meetings held in sensitive compartmented information facilities ("**SCIFs**").

[5] Mr. Touati added that the sharing of intelligence with a lower classification (such as Protected B intelligence) is more frequent, and takes place by e-mail. This intelligence most often concerns technical matters for operational purposes.

[6] Mr. Touati indicated that he holds a Top Secret security clearance. He specified that this level of classification does not allow him access to classified information in SCIFs beyond the Top Secret level. He indicated that, due to its specific mandate, the House of Commons Administration was not a traditional partner of intelligence and security agencies in this area.

[7] Mr. Touati said that Digital Services' access to intelligence is based on the "need to know" principle and is consistent with its mandate to protect the House of Commons and users of its IT infrastructure from cyber threats. Mr. Touati added that Digital Services

does not have the mandate, tools or resources to process and operationalize highly classified intelligence. Also, actions they might take on their own based on this type of intelligence could imperil the investigations of national security agencies, as well as their sources.

[8] According to Mr. Touati, the information received, mainly of a technical nature, is sufficient to enable the House of Commons to determine whether the measures it is putting in place are mitigating the risks. It also allows House of Commons staff to understand the contribution they can make to help defend the House of Commons more effectively against threats. Mr. Touati emphasized that a better understanding of the means employed by malign actors helps to broaden House of Commons' counter-threat activities. An understanding of the broader context in which these threats are deployed is also useful for parliamentary monitoring and business continuity purposes.

[9] Mr. Touati noted that the sharing of information between government agencies and Digital Services is collaborative: the information Digital Services receive enables them to counter and investigate threats to House information systems, while the information they pass on to government agencies informs their own investigations.

[10] Mr. Touati pointed out that, as part of these exchanges, Digital Services cannot share MPs' information without their prior consent. There is no employment relationship between the House of Commons and MPs, who are independent of the House and retain control over their own data.

3. ATP31 Cyberattack targeting Parliamentarians

[11] Commission counsel asked the House of Commons officials about the chronology of events entitled *Email Tracking Link Campaign Targeting Canadian Parliamentarians*, prepared by the Communications Security Establishment[1].

[1] [CAN.SUM.000027.001]

[12] Mr. Touati confirmed that he was the House of Commons representative referred to as "Director, IT Security" in this timeline. However, he clarified that the title was inaccurate, as he was in fact Deputy Director, IT Security at the time.

[13] Mr. Touati asserted that he was the House of Commons representative who participated in the classified briefing of February 17, 2021, which also included representatives from the CCC and CSIS. During this briefing, Mr. Touati was informed that government agencies suspected that a malign hacking group with suspected links to the People's Republic of China, known as APT31, was responsible for the activities detected in January 2021 targeting parliamentarians' e-mail accounts. He was also briefed on the tactics and historical targets of this malign actor. Mr. Touati explained that he was familiar with the malign actor identified in the briefing. It was a well-known player in the world of cybersecurity, under other monikers as well.

[14] For his part, Mr. Touati shared technical information concerning the House of Commons' information systems with CCC and CSIS representatives. He explained that there was no information indicating that the House of Commons protection system had not functioned properly, and that it had not blocked activities targeting parliamentarians. In addition, these activities targeted MPs' public e-mail addresses, which are generally not used on their personal devices and are traditionally managed by their staff. Thus, had the cyberattack succeeded, no sensitive information about MPs would have been collected.

[15] Mr. Touati explained that his risk assessment of the cyber attack was not affected by the classified briefing of February 17, 2021. The information received did not contradict Digital Services' assessment that the cyber attack had failed. Given these circumstances, Mr. Touati was not alarmed by the classified briefing he had just received. In his view, the attack was nothing out of the ordinary. The House of Commons is frequently targeted by malign cyber actors.

[16] Mr. Touati nevertheless asked his team to conduct additional checks to ensure that nothing was missed, notably by going back and broadening the scope of the checks already carried out. Mr. Touati described this as an exercise in due diligence. Following these steps, the initial diagnosis of the cyber attack remained unchanged. Mr. Touati indicated that, to date, he had no information that would lead to the conclusion that the cyber attack had compromised parliamentarians' information.

[17] The subsequent meetings listed in the chronology served to continue this exchange of information between Mr. Touati's team and the CCC. Mr. Touati indicated that the chronology generally seemed to reflect the frequency of the meetings in which he took part.

4. Changes in Cybersecurity

[18] Mr. Dicaire highlighted two changes underway in the area of cybersecurity. First, as part of the renewal of the MOU with the CCC currently being negotiated, the focus is on improving collaborative processes to counter cyber threats of a higher degree of severity. This new protocol will aim to improve the responsiveness of the House of Commons, as well as collaboration and interaction between the two entities in cases requiring a rapid response.

[19] Second, Mr. Dicaire expressed a desire for CCC to improve the content of its technical bulletins to Digital Services in terms of recommendations. In his view, the recommendations shared in the bulletins are very technical. More context would assist him in fulfilling his mandate of ensuring business continuity for Parliament.

[20] Since about mid-2023, Mr. Dicaire has noticed a growing willingness on the part of government agencies to share more information. By way of example, Mr. Dicaire alluded to the Ministerial Directives on Threats to the Security of Canada Directed at Parliament and Parliamentarians, and to the information provided by Global Affairs Canada regarding the *Spamouflage* campaign that targeted parliamentarians in the late summer of 2023.