[redacted]

---------- Forwarded message ---------
From: [redacted]@ipac.global>
Date: Thu, Apr 25, 2024 at 5:41 AM
Subject: URGENT AND CONFIDENTIAL: PRC SPONSORED CYBER ATTACK BRIEFING FROM IPAC
To: [redacted]@ipac.global>, [redacted]@ipac.global>, [redacted]@ipac.global>

Urgent letter from Executive Director Luke de Pulford
CONFIDENTIAL

Dear Canadian Members of IPAC,

You are receiving this confidential email because you were targeted by a Chinese state-sponsored hacking group in January 2021. IPAC Canada Co-Chairs John McKay MP and Garnett Genuis MP have requested that we write to those who were unable to attend the urgent security briefing yesterday.

The group concerned is known as APT31 (Advanced Persistent Threat 31). IPAC learned about this attack from an unsealed indictment released by the United States Department of Justice on 25th of March. The indictment said that the attackers had sent "over 1000 emails to over 400 unique accounts associated with IPAC". The full indictment can be read here. Subsequent to this, some IPAC members wrote to Secretary Blinken to protest that the FBI had not warned politicians of this attack. The FBI responded to this letter revealing that they had indeed told the respective governments of the targeted legislators in 2022. At this point, the IPAC Secretariat was still unaware of the precise identities of the legislators targeted.

The FBI met with the IPAC Secretariat last week and agreed to take IPAC's distribution list of email addresses and cross-check those emails with the FBI database of those targeted. We now have the results of this exercise. 122 email addresses in the IPAC database match the FBI database. This means the FBI has confirmed that at least 122 members o IPAC were targeted by APT31 in January 2021. **You are receiving this email because your email address was in that list.**

Pixel Reconnaissance Attacks
The emails that you received were all from the domain "nropnews.com". There were various email addresses and names of fake journalists attached to this domain. This kind of attack is known as pixel reconnaissance. It works by embedding a tracking pixel in a photograph or image. When the receiver opens the email, the tracking pixel is able to send back some limited information to whoever has sent the email. This information includes the recipient's IP address, the time, and the frequency of email opening, and some limited device data like the operating system used by the recipient.

Part of a Progressive Attack
In itself, a pixel reconnaissance email does limited damage, and should not be understood as a successful hack. However, in the hands of APT31, a pixel recons targeting programme should be understood as the first stage in a progressive cyber attack. It is important to emphasise here that at least 2 members of IPAC were compromised in mid-2021 subsequent to APT31 pixel reconnaissance emails. The FBI has confirmed in writing that the APT31 targeting in January 2021 should be seen as the beginning of a progressive attack.

Sovereignty Concerns

The FBI made clear that they were prevented from informing legislators around the world directly by their own rules regarding sovereignty. For this reason, in 2022, when they learned of the attack, the FBI issued Foreign Dissemination Requests (FDRs) to every government with impacted legislators. To our knowledge, only 2 of those governments informed their legislators.

Responsibility to Disclose
Having received this information from the FBI we believe that IPAC has a responsibility to disclose it to you. However, the correspondence from the FBI is marked sensitive and cannot be forwarded. That said, if legislators would like to see this correspondence, they are advised to make contact with Executive Director Luke de Pulford on Signal @[redacted] or on WhatsApp +44 [redacted].

Summary
1. You were targeted by a Chinese state-sponsored hacking group in 2021, the first stage in what would normally be a progressive attack.
2. The FBI informed your government when they learned about the attack in 2022.
3. Many governments chose not to disclose the attack to their MPs and this seems to be the case in Canada.

Additional Security Measures
There are certain steps you can take to improve defences against future cyber attacks. For example, you can turn off automatic image loading in your emails, you can download some useful security plug-ins for your browsers which block pixel trackers, and of course you can enable two factor authentication (2FA) for all of your accounts which, though simple, remains one of the most effective defences against email hacking attempts. I attached to this email a cyber security guide that we developed for politicians which has detailed instructions on each of these measures.

We anticipate that Members in Canada will wish to discuss this matter in Parliament. Though we do not yet know what precise form that will take, it may be useful to know what other legislators in various countries have been calling for subsequent to learning that they were targeted;
1. The United States and the United Kingdom have formally attributed this attack to the Chinese state. Legislators in other countries will be calling upon their governments to do the same.
2. The United States and the United Kingdom imposed targeted sanctions upon several individuals associated with the APT31 group, other affected legislators will be calling upon their government to do the same.
3. Parliamentarians in other countries are very concerned that their governments decided not to disclose the attack to them and will be seeking assurances that in the event of a future state sponsored attack they will be informed immediately.
4. Parliamentarians in other countries will also be calling for increased cyber security support.

We recognise that this news is somewhat disturbing. If you would like any more details or to discuss any other issues related to this attack, please do not hesitate to reach out. We take this opportunity to note that parliamentarians of all parties in many different countries were targeted in this attack. The attack was upon IPAC as a whole and our response to this attack must be one of resolute unity in defence of our shared values, transcending partisan divisions.

As ever,
Luke

[redacted]