Global Affairs Canada / Affaires mondiales Canada

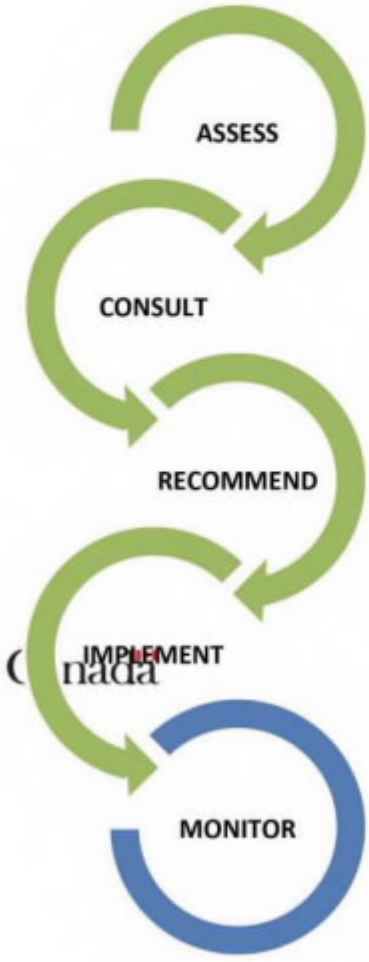
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Government of Canada's Framework for Public Attribution of Responsibility for Malicious Cyber Activity

CHAPEAU:

The purpose of this framework is to outline the process for the Government of Canada (GC) to decide whether to publicly attribute a malicious cyber act directed at the cyber networks and systems of Canada or our allies by a responsible state or actor.

The framework includes a five step process for public attribution of a malicious act(s) to a responsible state or actor.



Assess

Identify the occurrence of malicious cyber act(s) and the responsible actor(s). This would typically involve technical/intelligence assessments, information from partner(s) or other sources.

Consult

Discuss within GC and with allies whether a public attribution should be made, with consideration of the domestic and international impacts.

Recommend

Provide a recommendation to the Minister of Foreign Affairs on whether to attribute and what type of statement should be made.

Implement

Carry out the decision by the Minister of Foreign Affairs in collaboration with relevant stakeholders.

Monitor

If a statement is made, monitor and evaluate the effectiveness of and responses to the statement. If a statement is not made, monitor the malicious activity and reassess.

[APG]

Global Affairs Canada / Affaires mondiales Canada

UNCLASSIFIED//FOR OFFICIAL USE ONLY

OVERVIEW:

1. The purpose of this framework is to outline the process for the Government of Canada (GC) to decide whether to publicly attribute to a responsible state or actor for a malicious cyber act or acts directed at the cyber networks and/or systems of Canada or our allies.

2. Canada would publicly attribute to highlight behaviour that is prohibited under international law or otherwise unacceptable under non-binding international norms or deemed a threat to the public safety, national security, economic prosperity and/or interests of Canada. Additionally, the attribution can show solidarity with victims and allies and warn Canadian citizens and businesses so they can better protect themselves and their personal data, intellectual property, or proprietary information.

3. It is in Canada's interest to deter malicious acts in cyberspace. Public attribution is one option in a range of possible responses for the Government of Canada. It is important that adversaries know that they will face consequences for engaging in malicious cyber activities against Canada and its interests.

SCOPE:

4. For the purpose of this framework, a malicious cyber act directed at the cyber networks and systems of importance to Canada or our allies is defined as any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any digital information and/or the infrastructure on which it resides[1] that is deemed unacceptable under international norms or a threat to the public safety, national security, economic prosperity and/or interests of Canada.

5. This framework applies only to the decision-making process for public attribution. The process for technical attribution, decisions on other options for response to malicious cyber acts, decisions on defensive and active cyber operations, malicious activity of domestic origin with no foreign policy implications, and the use of cyber and digital tools for disinformation campaigns are out of scope for this framework.

6. This framework is focused on malicious acts in cyberspace that are below the threshold of the threat or use of force under international law. The framework applies to malicious cyber acts that are internationally wrongful acts as well as acts that are not unlawful but have significant impacts to the public safety, national security, economic prosperity and/or interests of Canada.

Canada

7. Malicious acts are analyzed in terms of international legal obligations, and more broadly in relation to international understandings of appropriate State behaviour in cyberspace, notably the voluntary norms developed by the UN Group of Governmental Experts.

8. An important consideration is to distinguish between technical attribution, legal attribution and public attribution:

[1] This derives from the Canadian Centre for Cyber Security's Glossary definition for cyber incident

[APG]

a. **Technical attribution** is the assessment undertaken by CSE, in consultation with CSIS and other relevant stakeholders when required, to determine to a reasonable level of certainty that a malicious act can be attributed to a State or non-state actor.

b. **Legal attribution** involves analysis of whether the malicious cyber act(s) constitute internationally wrongful acts(s), and whether the required legal nexus for responsibility of a State is established, directly or through its proxies.

c. **Public attribution (or political attribution)** is the political decision to publicly inform the responsible State and/or the broader public that the Government of Canada blames it for unacceptable malicious cyber activity. Both the technical and legal attributions can be key considerations for any decision to publicly attribute.

INTERNATIONAL EFFORTS:

9. This framework also provides a roadmap for engaging in cooperative public attribution with partners. Participating in cooperative statements will help Canada to build better responses to malicious cyber acts, strengthen our partnerships, reinforce and shape the development of international law, establish interoperable mechanisms and fortify the collective deterrence impact of likeminded countries.

10. Responsible state behaviour in cyberspace and the use of public attribution is an international issue. Canada must work together with our likeminded allies and partners towards collective cyber deterrence and responses to impose consequences upon malicious cyber actors, as was agreed at the 2018 G7 Foreign Ministers Meeting[2].

11. Canada continues to promote responsible state behaviour in cyberspace as well as cooperative attribution and collective cyber defense initiatives through a range of international fora including the United Nations (UN), North Atlantic Treaty Organization (NATO), Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), ASEAN Regional Forum (ARF) and G7.

Canada

[2] 2018 G7 Foreign Ministers' Communique: 42. We reaffirm our commitment to contribute to international cooperative action by working together to develop measures aimed at preventing, deterring, discouraging and countering malicious cyber acts and thus strengthen our collective resolve to deter malicious cyber actors by imposing costs in a timely manner.

[APG]

PROCESS:

12. The process for public attribution of a malicious cyber act to a responsible state or actor has five steps: Assess, Consult, Recommend, Implement and Monitor.

Assess

13. This framework is triggered when a malicious cyber act (Triggering Event) has, or is occurring, that has a:

    a. significant impact[3] to the public safety, national security, economic prosperity and/or interests of Canada, or

    b. significant impact to the public safety, national security, economic prosperity and/or interests of a partner country.

14. As soon as appropriate after a Triggering Event, relevant GC stakeholders shall be informed of the malicious activity.

15. A technical assessment will be completed by CSE, in consultation with CSIS, and/or other relevant departments or agencies or partners, to confirm the occurrence and impact of the triggering event. Regardless of the source of information, the assessment will require CSE's technical expertise, in consultation with CSIS, to confirm.

16. GAC will organize and inform a group of relevant GC stakeholders for consultation. Although, as an informal group, any relevant stakeholder can initiate.

17. GAC will approach allies and likeminded partners, where appropriate, to share information on the Triggering Event. The central points of contact with foreign states on Canada's official position are directly with GAC foreign ministry counterparts, with all relevant GC stakeholders ensuring a single message when engaging their counterparts.

18. GAC will coordinate a strategic assessment on the impact of the Triggering Event on Canada. The strategic assessment will require input from affected departments and agencies and other relevant stakeholders assessing their areas of responsibility (e.g. Public Safety for impacts to domestic interests and GAC for a legal assessment).

19. Decision is taken by the group of relevant GC stakeholders to initiate consultations regarding a public attribution.

[3] Determining the threshold of significant impact will be achieved through discussion on a case-by-case basis.

[APG]

Global Affairs Canada / Affaires mondiales Canada

UNCLASSIFIED//FOR OFFICIAL USE ONLY

CONSULT

20. Following the decision to undertake a consultation, GAC will develop a strategic assessment of the foreign policy considerations, objective of a public attribution, and the implications of such a statement. Public Safety will lead a process of the development of a strategic assessment of the impacts to domestic interests.

21. Concurrently, GAC will coordinate a consultation with relevant GC stakeholders, including the GC communications community, on the potential implications on their respective mandates and programs.

22. At this time, relevant GC stakeholders are responsible for briefing their senior officials, including Ministers when necessary. All relevant GC stakeholders, coordinated by GAC, will share their respective assessments to be used in briefing their senior officials.

23. Considerations for the strategic assessment and consultation will include:

    a. What is the level of confidence in the identification of the malicious actor?

    b. Has there been a violation of national and/or international law or a lack of respect for non-binding norms?

        i. In some cases, the malicious act(s) may not constitute a violation of international law, but may be otherwise unacceptable for Canada. The decision to publicly attribute is ultimately a political decision.

    c. What is the strategic assessment on the impact to public safety and domestic interests?

        i. Public Safety and other relevant GC stakeholders will provide their assessment of the implications for public safety and other domestic interests that include, but are not limited to, impacts on people, businesses, critical infrastructure, institutions, systems, and services.

        ii. Would the Canadian public benefit from an increased understanding of the threats they face?

Canada

    d. What is the foreign policy impact of a public attribution (e.g. geopolitical and bilateral)?

        i. There are a range of potential international fora that could be impacted by a public attribution, including discussions on responsible state behaviour in cyberspace and the development of rules-based international order.

        ii. Would a public attribution have a deterrent impact and/or help reinforce and shape the development of international law and norms consistent with Canadian positions and interests?

[APG]

e. Will other partners engage in a cooperative attribution?

f. What type of statement would be the best response? Relevant GC stakeholders, including communications, will be consulted on the type of statement.

i. A statement to publicly attribute can take a variety of forms, such as:

- Political Statement – Ministerial or departmental statement, such as a press release or press conference, to publicly attribute a malicious act(s) to the responsible State.
- Technical Statement – either a technical CSE cyber bulletin to inform Canadians of the threat or a discrete statement by CSE identifying that unacceptable malicious cyber activity has taken place.

ii. Bilateral and multilateral options for non-public statements to give notice to the responsible State (i.e. direct engagement using diplomatic channels).

24. GAC will continue engagement with partners and likeminded countries, including the potential for a cooperative attribution.

25. GAC will coordinate a signals check with senior national security committees to ensure that all views are taken into account and better coordinate timing for briefing senior officials.

Recommend

26. GAC will develop response recommendations to the Minister of Foreign Affairs following the consultative process.

27. GAC will coordinate the Government's decision. These decisions will not be made unilaterally and will build on the consultative process. In reaching the decision, the Minister of Foreign Affairs will, as appropriate, consult the Prime Minister, the Minister of Public Safety, and other Ministers.

28. The recommendations will include whether Canada should make a public attribution and if so, how and by whom the statement will be delivered. The default process will be for the Minister of Foreign Affairs to make the public attribution and GAC to lead the coordination.

29. If after the consultative process, the public statement is referred to a different Minister for delivery, then that Minister's department or agency will lead the coordination of the statement's dissemination.

Implement

30. Following a decision by the Minister of Foreign Affairs, GAC will inform the relevant GC stakeholders of the Government's decision. These stakeholders will be responsible for ensuring that their senior officials are briefed.

[APG]

31. If the Government decides not to make a public attribution, the group of relevant GC stakeholders will:

    a. Continuously monitor the activity;

    b. Continuously reconsider the need for a public attribution as the event develops and refer the matter to the Minister of Foreign Affairs as appropriate;

    c. Review and consider additional mechanisms that could be implemented; and,

    d. GAC to conduct outreach to partners and likeminded countries

32. If the Government decides to make a public attribution, the group of relevant GC stakeholders will:

    a. Develop talking points and common briefing material, to be coordinated by the lead department;

    b. Seek the support of partners and likeminded countries;

    c. Consult the GC communications community (e.g. develop media lines); and,

    d. Remain responsible for advanced notification of affected entities under their mandate

33. In addition to a public attribution, the GC can explore measures to educate Canadians on the threat and ways to improve safety and security in cyberspace.

Monitor

34. Following a public attribution , the group of relevant GC stakeholders will monitor the impact of the statement, including but not limited to:

    a. Responses by the responsible State or actor(s), partners and likeminded countries and other countries;

    b. The effect of the attribution, as assessed by diplomatic, security and intelligence sources;

    c. Effect of the attribution on the public safety, national security, economic prosperity and/or interests of Canada;

    d. The effect of the attribution in the strengthening and shaping of international law and the rules-based international order more broadly; and,

    e. Whether the attribution had a deterrent effect.

35. Considering these assessments, GAC will conduct a lessons learned and update the framework when required.

[APG]

36. GAC will coordinate engagement with partners and likeminded countries to share assessments and lessons learned.

37. GAC will regularly review and update this framework.

Canada

[APG]