Foreign Interference Research Group 'EOM'
for Global Affairs Canada

Governmental views on and action against foreign interference in information environment activities in the context of foreign interference

1 Research interest

Asking how the fourteen countries in question view foreign interference in information environment, this section seeks to identify existing common ground and leads towards potentially internationally agreeable legal or political measures. To do that, this section maps political measures and opinions the countries have taken or expressed on information influence activities in the context of foreign interference.

Rather than analysing any country policies, their relevance or effectivity, the scope of mapping is to make the very diversity of action, objectives and measures, visible. Combined with the conceptual and legal analysis (Chapters I and III, respectively), we believe, political analysis will help to create comprehensive understanding of actual and potential action to be considered.

To discover governmental measures against foreign informational interference activities, the clusters of sources of explicit policies, principal themes, and focus areas, are investigated. This inquiry will include planned lines of action and measures already taken. Of explicit policies where concerns of information influence activities or foreign interference may have been addressed, various national security policy and strategy documents are potential choices and sources. In addition, governments may have expressed and addressed their national concerns in international fora, at the United Nations or in regional organizations.[1]

Though having analysed ca. 130 national documents and online sources, listed below, our analyses is not to offer an exhaustive or historically comprehensive but wide enough and account to illustrate and contextualize contemporary political thinking and measures taken against foreign interference in informational environment.[2]

2 Key findings

Influence and interference

Many countries explicitly seek to exercise influence in world affairs.[3] Some state objectives may appear more modest, but they still want to have a say or influence on their issues or areas of interest, for example gender equality or countering global warming.[4] Influence is an elementary part of international affairs: countries exercise and seek to exercise influence over each other to promote their immediate political

---

[1] Documents to determine governmental action against foreign interference, when applicable, include parliamentary inquiries, national security strategies or doctrines, national military strategies or doctrines, national cyber, digital or information security strategies or doctrines, strategies and plans to protect critical infrastructure and vital societal functions and services, including electoral processes, submissions to the United Nations, regional declarations, submissions and action, and national position statements.

[2] The analysis does not explicitly or implicitly assess or refer to the relevance, feasibility or implementation of the mentioned policies, strategies, lines of action or individual measures.

[3] For example, AU (The Department of the Prime Minister and Cabinet (2016)); FR (Premier Ministre (2015). *French National Digital Security Strategy*); RU(Ministry of Foreign Affairs of the Russian Federation (2013). *Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020*); UK (HM Government (2015). *National Security Strategy and Strategic Defence and Security Review 2015*), US (The White House (2018). *National Cyber Strategy of the United States of America*).

[4]

objectives and (allegedly) long-term national interests. All deliberate activities, operations, have or intend to have influence on either the perceptions or behaviour of people or the course of political, societal or technical events.[5]

Seeking influence is thus not necessarily controversial state actively unless and until it breaches the principles and letter of international law, most notably the principles of non-intervention, equal sovereignty of states and peaceful settlement of disputes. The most compelling and widest 'black letter' then can be found in the United Nations Charter.[6]

Foreign interference, interference and intervention are legal and political interpretations of certain state activities where various payloads are being used in manner inconsistent with either national or international law.

National concerns differ

Despite the 1998 and 2004 Russian warnings how information and disinformation can be used against national, state and private citizen interests, many countries started to pay attention to malign information influence activities only in mid-2010's. Triggered by particular, close-proximity experiences, national concerns of malign information influence and foreign interference are contingent. Often, political or geographical proximity, alternatively, distance, to the superpowers of China, Russia or the United States condition and maintain some views.

There are several contested issues in the use of information influence activities which may breach international law, for example by constituting forbidden intervention or interference in internal or external affairs of another country, violating sovereignty, or disregarding the right of self-determination. What is common is political emphasis of sovereignty, self-determination and the sanctity of *domaine réservé*. Legal interpretations of the concepts and some state and cyberspace activities vary and may be assessed case-by-case.

---

[5] See, for example UK military doctrinal definition of the notion 'cyber': "[T]o operate and project power in and from cyberspace to influence the behaviour of people or the course of events (Ministry of Defence (2016). *Cyber Primer* (2nd edition), p. 1).

[6] United Nations (1945). *Charter of the United Nations*, art 2(7), also International Court of Justice (1986), Reports 1986, p. 14, paras. 202-204 (Nicaragua v. United States case).

According to the analysed countries, such activities target democratic processes, especially elections and electoral processes,[7] political decision-making,[8] public opinion,[9] willingness to defend the country,[10] social order,[11] the cohesion of national fabric and heritage[12] or use the Internet and disinformation for terrorist or violent extremist purposes. [13]

Spectrum of governmental measures

In general, state measures to prevent or respond to malign information influence range from

- Legal and regulative frameworks to e.g. ban, limit, penalise or direct state, private sector or individual human activities[14]
- Establishment of authorities and mandates to strengthen or establish potent agency[15]
- Restrictions on the collection, dissemination or publication of information[16]

---

[7] For example, G7 ("Charlevoix commitment on defending democracy from foreign threats"); AU (Department of Foreign Affairs and Trade (2021). *Australia's International Cyber and Critical Tech Engagement Strategy*); CA (Government of Canada (2020). "Combatting foreign interference"; FR (Secrétariat général de la défense et de la sécurité nationale (2018). *Revue stratégique de cyberdéfense*); DE (The Federal Government (2021). "On the Application of International Law in Cyberspace"; JP (The Government of Japan (2018). *Cybersecurity Strategy*); NL (Ministry of Security and Justice (2018). *National Cyber Security Agenda*); NZ (Department of the Prime Minister and Cabinet (2019). *New Zealand's Cyber Security Strategy*); SE (Ministry of Justice (2021). "Regleringsbrev för budgetåret 2022 avseende Myndigheten för psykologiskt försvar"; UK (HM Government (2021). *National Cyber Strategy 2022*); US (The White House (2021). *Interim National Security Strategy Guidance*).

[8] For example, AU (Australian Security Intelligence Organisation (2021). "Director-General's Annual Threat Assessment"); FR (Ministère des Armées (2019). "International Law applied to operations in cyberspace"); IT (Presidenza del consiglio dei ministri. Sistema di informazione per la sicurezza della repubblica (2017). *Relazione sulla politica dell'informazione per la sicurezza*); SE (Direktinvesteringsutredningen (2021). *Granskning av utländska direktinvesteringar*).

[9] For example, IT (Presidenza del consiglio dei ministri. Sistema di informazione per la sicurezza della repubblica (2017). *Relazione sulla politica dell'informazione per la sicurezza*); JP (Ministry of Defence (2018). *National Defense Program Guidelines for FY 2019 and beyond*); RU (Group of Governmental Experts (2004). "Contribution by the governmental expert of the Russian Federation to the work of the United Nations Group of Governmental Experts on International Information Security); ZA

[10] SE (Swedish Psychological Defence Agency (2022). "Our mission").

[11] NL (Ministry of Security and Justice (2011). *The National Cyber Security Strategy* and (2018). *National Cyber Security Agenda*); NZ (Department of the Prime Minister and Cabinet (2017). "Briefing to Incoming Minister responsible for cyber security policy).

[12] For example, RU (The Kremlin (2000/2008). *Doctrine of Information Security of the Russian Federation*); SG (Ministry of Home Affairs (2021). "Second Reading of Foreign Interference (Countermeasures) Bill).

[13] For example, AU (Department of Defence (2016). *Defence White Paper*); BRICS (*X BRICS Summit Johannesburg Declaration*); *Christchurch Call to eliminate terrorist and violent extremist content online* (NZ, FR, AU, CA, DE, IT, JP, NL, SE, UK, US); RU (Ministry of Foreign Affairs of the Russian Federation (2013). *Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020* and (2021) *Fundamentals of the state policy of the Russian Federation in the field of international information security*); UK (HM Government (2015). *National Security Strategy*); US ("National position of the United States of America (2016)").

[14] See Chapter II for detailed legal analysis.

[15] For example, AU (Counter Foreign Interference Taskforce); CA (Security and Intelligence Threats to Elections); Fr (*Le service de vigilance et de protection contre les ingérences numériques étrangères*); SE (Swedish Psychological Defence Agency).

[16] For example, *Christchurch Call to eliminate terrorist and violent extremist content online* (NZ, FR, AU, CA, DE, IT, JP, NL, SE, UK, US); SG (*Foreign Interference (Countermeasures) Bill*); ZA ("Regulations issued in terms of Section 27(2) () of the Disaster Management Act 2002").

- Multi-stakeholder cooperation to enable wide spectrum of responsibility and action[17]
- Citizen awareness and public education to strengthen societal resilience and media literacy[18]
- Targeted or general guidance on resisting or countering informational influence[19]
- Targeted or general guidance on enhancing information and cybersecurity[20]
- Military doctrinal and capacity development to enhance military defence or response capacity[21]
- Direct effect-creating operations to influence the behaviour of persons or groups of person or course of events[22]
- Promoting international cooperation[23].

Conceptual clarity

Without explicitly attributing to any particular state, state positions and doctrinal practice, as well as linguistic and operational logic, point to a taxonomy which helps to clear, distinguish and contextualize the notions or concepts of influence, interference and various (types of) operations.

As noted, influence is a commonly used mean to achieve political objectives. For wielding influence, an objective for many, if not all states, governments can deploy various instruments *inter alia* alliances, preferential treatments, posturing, coercion, sanctions, or cyber-physical or informational activities. In the context of information environment, the core domain of the study, what may be determined as foreign interference contrary to international law can be take place by or through various vectors, for example, cyberoperations, cyber-enabled operations, information operations or traditional military operations. Each vector, and type of operation, can contain various payloads such as the typically in the cyber-informational environment employed malware, disinformation and narrative shaping.

Though in colloquial language so considered, influence and interference/intervention are not types of operations. Influence is at the same time an intermediate level objective and means to a higher political end.

Relevance of opinion

Superpower and other influential state constellation (e.g. G7, BRICS) opinions and practise rather constitute a minority than majority view in terms of sovereign nations. The differences in political (domestic and international) and operational ambitions and the available resources make a universal and top-down approach difficult and perhaps even detrimental to be achieved. These states are not 'swing states' or 'middle ground countries' to, by influence, inevitably end up in either of the vocal camps.

---

[17] For example, AU (*Australia's International Cyber and Critical Tech Engagement Strategy*); NZ (*New Zealand's Cyber Security Strategy* (2011, 2015, 2019)), UK (*National Cyber Strategy* (2021)).

[18] Citizen awareness and public education are lines of action taken in all national cyber security strategies.

[19] For example, SE (*Countering information influence activities: A handbook for communicators*); UK National Cyber Security Centre.

[20] For example, CA (*Cyber Security Guide for Campaign Teams & Cyber Security Guidance for Elections Authorities*); UK (National Cyber Security Centre); US (Department of Homeland Security).

[21] For example, FR (*Élements publics de doctrine militaire de lute informatique d'influence (L2I)*); NL (*An Integrated International Security Strategy 2018-2022*); RU (*Doctrine of Information Security of the Russian Federation* (2000/2008 & 2016); UK (*National Cyber Strategy 2022)*; US (*National Cyber Strategy of the United States of America*).

[22] For example, the UK against ISIS; the US against (Russian) 'Internet Research Agency' troll farm.

[23] For example, NZ (Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online); RU (*Fundamentals of the state policy of the Russian Federation in the field of international information security*); US (*National Cyber Strategy of the United States of America; Interim National Security Strategy Guidance*).

Similarly, whether international measures should follow or derive from certain domestic practices, should be openly and critically examined since state practice tends to emphasize strong sovereignty and the interests of the powerful over international obligations.

International ways forward

As seen from our empirical analysis, capturing influence under an umbrella normative instrument on influence is not feasible or desirable. Instead, common normative ground should be sought by determining what constitutes interference by information influence activities. The above-mentioned areas of concern and troublesome information influence activities may serve as a point of departure. Instead of seeking normative measures against information and disinformation, attention should be put on usage of them.

Yet, the diversity of concerns and policy preferences serves also as a 'health warning.' Whereas liberal democracies want to emphasize on election interference/election security, authoritarian states may want to counter, 'balance' or steer negotiations towards public moral and national heritage. Similarly, countering terrorist use of the Internet may slide into imposing excessive content controls.[24]

[24] Such trade-offs and shifts have taken place in the UN GGE discussion on the use and development of information and telecommunications, especially between international obligations and sovereignty and human rights and sovereignty.