THE OXFORD STATEMENT ON INTERNATIONAL LAW PROTECTIONS AGAINST FOREIGN ELECTORAL INTERFERENCE THROUGH DIGITAL MEANS

We, the undersigned public international lawyers, have watched with growing concern reports of cyber incidents targeting electoral processes around the world, including allegations of foreign state and state-sponsored interference. We also note that the COVID-19 pandemic raises additional challenges to ensuring the integrity of such processes.

Whereas:

Two prior Oxford Statements have described the rules and principles of international law governing cyber operations that threaten two areas of pressing global importance, namely the safeguarding of the health care sector and global vaccine research;

International law protects electoral processes, and efforts to interfere, including by digital means, with a state’s choice of its political leaders or other matters on which it has free choice, contravene basic principles of the international order;

The Charter of the United Nations (UN) establishes sovereign equality and each state’s political independence as a bedrock element of the international system; the United Nations General Assembly has affirmed that no State “has the right to intervene directly or indirectly, for any reason whatever, in the internal or external affairs of any other state”; and the International Court of Justice has stated that every sovereign State has the right “to conduct its affairs without outside interference”;

Article 25 of the International Covenant on Civil and Political Rights declares that “[e]very citizen shall have the right and the opportunity, without … unreasonable restrictions [t]o take part in the conduct of public affairs, directly or through freely chosen representatives; [and t]o vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;” and electoral interference can infringe human rights protected under the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples’ Rights, the American Convention on Human Rights, and the European Convention on Human Rights;

Other international instruments, such as the Paris Call for Trust and Security in Cyberspace (2018), have called on all stakeholders to “[s]trengthen their capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities”;

All efforts by states and others to prevent such malign interferences should be consistent with international law;

The International Law Commission’s 2001 Articles on State Responsibility establishes that a state is responsible for the conduct of its organs or officials, as well as for conduct carried out by persons or groups acting on the instructions of, or under the direction or control of, the state;

In line with the UN Guiding Principles on Business and Human Rights, online intermediaries and digital media companies should “conduct due diligence to ensure that their products, policies and practices … do not interfere with human rights”, as recognised in the April 2020 Joint Declaration on Freedom of Expression and Elections in the Digital Age, adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression.
As states and other stakeholders learn more about the ways in which foreign cyber actions can adversely affect domestic electoral processes and how best to address such harms, international law can be further clarified and strengthened by state practice that becomes accepted as customary international law.

We affirm that all states are bound to act in accordance with the rules and principles identified below.

**Applicability**

1. International law applies to cyber operations by states, including those that have adverse consequences for the electoral processes of other states.
   a. “Electoral processes” refer but are not limited to processes for selecting or electing individuals for public office, referenda, and plebiscites. These include:
      i. Balloting: registering, casting, tabulating, or assuring the integrity of a ballot including voter registries, ballot security and integrity protocols, voting machines, and paper ballots;
      ii. Verifying: systems used for reporting, recording, verifying and auditing votes and results of an election;
      iii. Informing: public or private systems that provide an electorate with procedural information about how to participate in an electoral process, as well as substantive information, of whatever origin, related to an electoral process, including information on individuals or groups participating in electoral processes, such as candidates for elective office, political parties, or organizations.

2. Adverse consequences, in the electoral context, include actions, processes or events that intervene in the conduct of an electoral process or undermine public confidence in the official results or the process itself. These actions include but are not limited to intrusions into digital systems or networks that cast doubt on the integrity of election data, such as votes and voter registers, as well as cyber operations against individuals and entities involved in the election.

**Duty to Refrain**

2. A state must refrain from conducting, authorising or endorsing cyber operations that have adverse consequences for electoral processes in other states. States must refrain from, *inter alia*,
   a. Interfering, by digital or other means, with electoral processes with respect to balloting or verifying the results of an election;
   b. Conducting cyber operations that adversely impact the electorate’s ability to participate in electoral processes, to obtain public, accurate and timely information thereon, or that undermine public confidence in the integrity of electoral processes.
   c. Conducting operations that violate the right to privacy, freedom of expression, thought, association, and participation in electoral processes.

**Duty Not to Render Assistance**

3. A state must not render assistance to cyber operations that it knows will likely have adverse consequences for electoral processes in other states.

**Due Diligence**

4. a. When a state is or should be aware of a cyber operation that emanates from its territory or infrastructure under its jurisdiction or control, and that may have adverse consequences
for electoral processes abroad, that state must take all feasible measures to prevent, stop and mitigate any harms threatened or generated by the operation.

b. To discharge this obligation, states may, to the extent feasible, be required to, *inter alia*, investigate, prosecute or sanction those responsible, take measures to prevent or thwart operations spreading misleading or inaccurate information, and/or assist and cooperate with other states in preventing, ending, or mitigating the adverse consequences of foreign cyber operations affecting electoral processes.

c. The measures taken to discharge a state’s obligations should be carried out in full compliance with other rules of international law.

**Obligation to Protect Against Foreign Electoral Interference**

5. States have an obligation to protect and ensure their own electoral processes from interference by other states. To discharge this obligation, states may be required to put in place electoral security measures, such as legislation and backup systems, as well as to secure the availability of public, timely and accurate information on electoral processes. Any restrictive measures taken by states that interfere with human rights must be in accordance with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.

6. These rules and principles are without prejudice to other applicable international rules and ongoing processes.