IMPROVING TRANSPARENCY

INTERNATIONAL LAW AND STATE CYBER OPERATIONS

STATE AND STATE-SPONSORED CYBER-OPERATIONS ARE ON THE RISE

According to the U.S. Council on Foreign Relations, since 2005, 33 States have been publicly associated with one or more cyber-operations

2005 → present

2019

In 2019, there were at least 76 State or State-sponsored cyber operations.

States agree that international law applies to state cyber-operations

- See, for example,
  - UNGA Resolution 266 (2019)
  - ASEAN-US Leaders' Statement on Cybersecurity Cooperation (2018)
  - EU Statement (2018)
  - UN Group of Governmental Experts, First Committee, UN General Assembly (2015)

BUT … WE STILL KNOW VERY LITTLE ABOUT *HOW* INTERNATIONAL LAW APPLIES

Most State have remained silent on the application of international law

Those States that have offered views exhibit key differences over

- which international legal regimes apply in the cyber context;
- how to interpret those regimes all agree do apply; and
- how to attribute responsibility for internationally wrongful behavior in cyberspace.

Some States have begun to offer "official views" on how international law applies in the cyber context:

- US (2012, 2015, 2016), UK (2018), France (2019), Estonia (2019) Netherlands (2019) Australia (2019), Iran (2020), Finland (2020), Germany (2021)
- UNGA has called for more such national statements via the ongoing GGE

But . . . these statements remain in the minority (and non-state actor views like the Tallinn Manuals are useful, but not authoritative).

State Silence remains the dominant position

THE *IMPROVING TRANSPARENCY* INITIATIVE AT THE OAS

1. Identify areas of convergence in State understanding of which rules of IL apply and how they do so

2. Identify divergent views on what international laws apply or how they do so.

3. Limit risks of inadvertent escalation or conflict due differing State understanding of IL's application

4. Afford the OAS and its Member States a voice in global conversations about international law's application.

THE PROJECT

A questionnaire featuring ten questions was sent to OAS Member States

Nine responses received

Two States directed the committee to prior statements or outside pending work: Brazil and the USA	Seven were substantive: Bolivia, Chile, Costa Rica, Ecuador, Guatemala, Guyana, Peru

WHAT STATE RESPONSES REVEALED

States that responded shared a dedication to the rule of law, including an interest in the role international law can play in regulating State behavior in cyberspace.

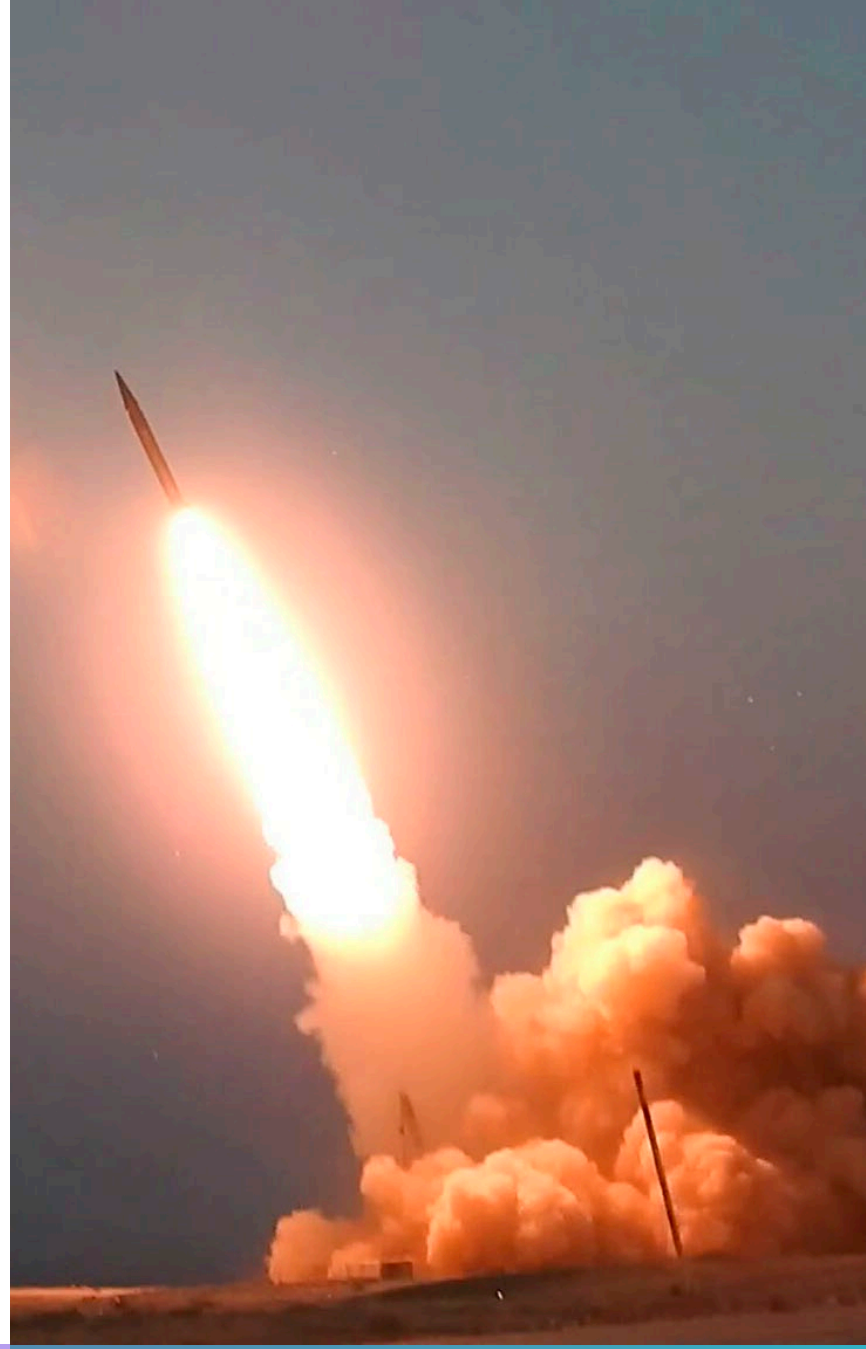
States revealed a lack of capacity both technically and legally to respond to cyber threats

DO EXISTING FIELDS OF INTERNATIONAL LAW APPLY TO CYBERSPACE? IF YES, ARE THERE EXCEPTIONS?

- Most States emphasized existing international law's application
- Some States highlighted particular fields of international law as especially relevant
  - Peru and the United States flagged international human rights law
  - Bolivia focused on the *jus ad bellum* and the *jus in bello apply*
- Guatemala and Guyana expressed positive support for IL's application. Yet, both offered caveats indicating that the novelty of cyberspace made its application challenging or in need of further elaboration

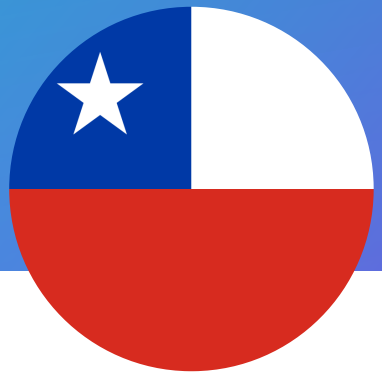
WHAT QUALIFIES AS A USE OF FORCE?

- Most (but not all) States appear to accept the application of international law on the use of force (e.g., the *jus ad bellum*) to their cyber operations.
- Bolivia, Chile, Guatemala, Peru, and the United States are all clear that both the prohibition on the use of force and the inherent right of self-defense in response to an "armed attack" may be triggered by cyber operations alone
- Guyana's response expressed doubts about the applicability of the *jus ad bellum* to cyber operations alone
- Most responding States continue to find power in drawing the relevant thresholds by analogizing cyber operations to kinetic or other past operations that did (or did not) qualify as a use of force or armed attack.



WHAT CONSTITUTES STATE RESPONSIBILITY?



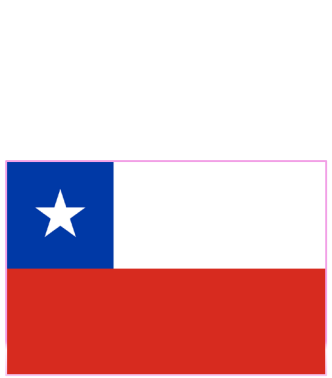



- States expressed general concerns about the difficulty of attribution in cyberspace
- Peru indicated that if states have the capacity to control a nonstate actor who commits a cyberattack that could give rise to the attack being attributed to the state
- Bolivia stressed the corollary that states should not bear responsibility for non state actors outside of their control or beyond their technological capacity
- Chile, Guyana, and Peru cited Article 8 of the Articles of State Responsibility -- “The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct”

UNDER IHL, WHAT HARM MUST OCCUR FOR SOMETHING TO QUALIFY AS "AN ATTACK?"

- Responses generally reveal support for the applicability of IHL generally as well as the idea that cyber operations can constitute an attack in that context.
- Responses were mixed, however, with respect to whether a cyber operation could qualify as an "attack" under IHL if it fails to cause death, injury, or direct physical harm

- Chile, Peru, and the United States took the position that an ”attack” must cause death, injury, or direct physical harm.
- Guatemala and Ecuador opined that “attacks” could result in functionality losses rather than death, injury, or destruction of property.
- Bolivia and Guyana’s responses were equivocal







More dialogue needed on how proximate death/destruction must be to functionality losses

IS AN OPERATION THAT TARGETS CIVILIAN DATA PROTECTED BY IHL?

- No State endorsed civilian data alone as subject to the principle of distinction in armed conflict.
- Chile acknowledged civilian data might warrant distinction if an operation targeting data exclusively would have knock-on effects in terms of affecting a civilian population
- Guyana similarly focused on effects rather than the label to attach to civilian data

DUE DILIGENCE

- Chile, Ecuador, Guatemala, Guyana, and Peru all took the position that the due diligence is a part of the international law that States must apply in cyberspace
- Bolivia opined that a State may not be held responsible for a cyberattack when it lacks technological infrastructure to control a non-State actor without commenting on the legal status of due diligence
- In the June 2020 Chatham House discussion, several Member States expressed support for due diligence as an (important) rule of international law in the cyber context.
    - However, one Member State expressed hesitation given the risk of non-compliance that might occur for States unable to adequately respond to cyberthreats because of a lack of technical capacity.

A NEED FOR NEW PERSPECTIVES?

- Ecuador and Guyana indicated that there may be a need for new international law in the cyber context
- At least one participant called for developing a distinctly Latin American perspective on the international governance and legal framework of cyberspace- noting how most ideas on international law in cyberspace have been developed by European States, or scholars from the Global North

CHALLENGES TO FURTHER TRANSPARENCY ON IHL'S APPLICATION IN CYBERSPACE

- Capacity issues - technical, legal and internal
  - A lack of technical capacity to identify perpetrators means that states may be unable to invoke Int'l Law due to absence of a known State actor.
  - A lack of governmental expertise (or resources) on cyber-related issues as well as how international law manifests in the cyber context
- Political issues –
  - More internal coordination required
  - Desire to preserve operational flexibility;
  - Avoiding entanglements in great power politics

THE FUTURE?

- The OAS Juridical Committee plans to continue working on international law's application in cyberspace
- 2021 - Mariana Salazar Albornoz takes up the topic as the new Rapporteur