An International Attribution Mechanism for Cyber Operations

האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

Dan Efrony

HU CyberLaw

מרכז המחקר להגנת הסייבר
CYBER SECURITY RESEARCH CENTER

The Backdrop

- Intensified hostile cyber activities/a tense geopolitical climate
- Major legal questions are debated and pose significant obstacles.
- Failure to establish binding legal framework in cyberspace and failure to attribute responsibility result in..
- Lack of accountability – prerequisite element to ensure security & stability.
- The challenge – establishing international attribution mechanism- a vicious circle?

Current Mechanisms in int'l Law

The Agency/Mechanism

- **IAEA –** International Atomic Energy Agency
- **OPCW-** The Organization for Prohibition of Chemical Weapons
- **CTBTO -** The Comprehensive Nuclear Test Ban Treaty Organization.
- **PSI -** The Proliferation Security Initiative.

Characteristics

- Verification by fact-finding, On Site Inspection, reporting to the UNSC and the State Parties
- Verification by fact- finding, Technical Assistance VisitV (equivocal to OSI), reporting to the State Parties.
- Attribution of responsibility, including three-layers of verification regime. **Not operational.**
- Law – enforcement cooperation.

The Relevancy to Cyberspace

- The IAEA and the OPCW:
  - Function as a verification regime with no authority to attribute responsibility.
  - In cyberspace, there are no international rules to verify compliance with, and even if there is such rules, attribution is the more necessary element.
- The CTBTO:
  - May provide evidence, most notably, forensic evidence, which is independent, objective, accurate, and sufficient to attribute responsibility to a violation of international law.
  - It is not operational and seemingly, not going to be due to the precondition set by the convention. In general, such a concept may be relevant to cyberspace, depending on its feasibility to cyberspace and…. the willing of the leading States.
- The PSI
  - Is a joint statement of States to cooperate in enforcing specific rules of international law. Such an initiative may be relevant to cyberspace if found agreed rules or norms to comply with.

Proposed mechanisms of attribution

The Agency/Mechanism	Characteristics
The Atlantic Council – Multilateral Cyber Attribution and Adjudication Council (MCAAC).	States and Non-State actors . consensus-driven attribution, along with limited judiciary authority, reporting to the UNSC, ICJ.
The Microsoft's Proposal	States and Non-State actors. Verifying compliance with norms. Technical attribution based on credibility/legitimacy.
The RAND's proposal- A Global Cyber Attribution Consortium	Stateless attribution. Publicly attributing responsibility. Its authority based on reputation and legitimacy.

Initial Insights

All three proposals preclude the possibility of having a new consensual convention.

Consequently, the attribution is mostly, confined to technological attribution and isn't sufficient to attribute responsibility.

Non-State Actors, specifically, the PS and academia should have a significant role in establishing the legal framework in cyberspace.

However, States should lead the process as they are the "legislators" of the International law and in the receiving-end of enforcing it.

The British AG: "States have responsibility to be clear about how international law obligation bind us"

As the consensus driven approach isn't practical, it might be the time to turn to alternative approach

Initiating a non-consensual convention or CDI (Cyber Domain initiative)addressing the legal and political challenges of establish practical convention.

THANK YOU