An International Attribution Mechanism[1] – Is it required? Is it practical?

Dan Efrony

A strategy of silence or ambiguity that has been adopted by states active in cyberspace has created a vicious cycle. While serving their interests in maintaining operational latitude, it renders a significant obstacle in establishing accountability that requires a binding legal framework and an efficient enforcement mechanism, both have not been formulated yet and can't be shaped under conditions of ambiguity. Obviously, lack of accountability leads to intensifying damaging cyber operations. Moreover, even if the international community reaches a consensus about binding international law in cyberspace, it will not be enough to fully ensure compliance, given the unique characteristics of cyber technology. Put bluntly, the incentive is too high to resist the temptation. Ultimately, cyberspace's greatest strength allowing anonymous and secured cross-borders operations is simultaneously its greatest weakness, making it very difficult to attribute a full responsibility for such operations to a specific state.

Hence, it has become more urgent to overcome that weakness and establish an international and credible mechanism to assign the responsibility for damaging cyber operations to the offender, be it a state, a group or an individual who act on behalf of a state. It may look as putting the cart before the horses, but it isn't, given the universal norms included in the UN Charter and other norms of states' behavior which had already been consensually affirmed by the UN-GGE 2013 and 2015 and adopted by resolutions of the UN- General Assembly. Tough these norms are non-

[1] The focus of such a mechanism is to increase accountability among states through the attribution of state or state sponsored cyberoperations.

binding they may legitimate counter actions to deter and restrain the intensifying destructive cyber operations, once a credible attribution has been made.

Such a mechanism might be an important element in shaping states practice in accordance with universal values and norms, even more so, a catalyst to overcome the political obstacles and accomplish the articulation of binding international law to cyberspace.

How that mechanism would look like is an open question. We have examined four existing international mechanisms: 1) The International Atomic Energy Agency (IAEA). 2) The OPCW Inspection Mechanism. 3) The Comprehensive Nuclear Test Ban Treaty (CTBT) 4) The Proliferation Security Initiative (PSI) and three proposed models for an international attribution mechanism in cyberspace. 1) The Multilateral Cyber Attribution and Adjudication Council (MCAAC) proposed by the Atlantic Council 2) Microsoft's Proposal to establish an international mechanism to verify compliance with norms. 3) A Global Cyber Attribution Consortium (GCAC) proposed by Rand Institution.

Technical findings (technical attribution) is mostly not enough to attribute the responsibility to a state. Almost always the attribution process relies on all source information on a state level, even then, the degree of certainty might be high, and in its utmost "almost certainly". Thus, to succeed in the attribution process, a significant cooperation with relevant capable states and cyber security companies is crucial. States are also indispensable in establishing another vital component of accountability, that of binding international rules in cyberspace. As many relevant states as possible, involved in the process and leading it, that will significantly increase the odds of success.