An Argument for Assumed Extra-territorial Consent During Cybercrime Investigations

Joshua I. James
UCD Digital Forensic Investigation Research Group
KNPU International Cybercrime Research Center

During cybercrime investigations it's common to find that a suspect has used technology in a country outside of the territorial jurisdiction of Law Enforcement investigating the case. The suspects themselves may also be located outside of the territory of the investigating group. A country may be able to claim jurisdiction over a suspect or device that is located outside of their territory [1], however, foreign Law Enforcement would not have jurisdiction within the territorial jurisdiction of another country unless explicitly granted. This means that if a suspect or digital device is located in another territory, the investigating country may need to request assistance from the country that has territorial jurisdiction. This request could be in the form of mutual legal assistance requests, international communication channels such as INTERPOL and United Nations networks, through a personal contact within the country of interest, etc.

It appears to be increasingly common that Law Enforcement will use personal contacts to quickly begin the investigation process in the country of interest and request data be preserved, while at the same time making an official request for cooperation through official channels. This is simply because official channels are currently far too slow to deal with many types of cybercrime that rely on preserving data before the records are overwritten or deleted; a problem that has been communicated by Law Enforcement for over a decade.

For similar reasons, Law Enforcement in many countries commonly access data stored on servers in countries outside of their jurisdiction. When and how they access this data is usually not well defined because law too, in most – if not all – countries, is failing to keep up with changes in cross-border digital crime. However, a recent work by the NATO Cooperative Cyber Defence Centre of Excellence – *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn Manual) – attempted to explicitly state some of these issues and their practical implications, albeit in the context of Cyber Warfare.

In the Tallinn Manual the expert group considered issues of jurisdiction applied to cyber infrastructure. Of these considerations, they claim that "...States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure" [2] with some exceptions. Further, Rule 1 paragraph 8 stipulates that:

> A State may consent to cyber operations conducted from its territory or to remote cybercrime operations involving cyber infrastructure that is located on its territory.

VFAC Review. no. 25, pp. 7-8, July 2013

In this rule, the expert group gives the explicit example that a State may not have the technical ability to handle a situation within their territory, and thus may give permission for another State to conduct cyber activities within their jurisdiction.

Much of the discussion on sovereignty, jurisdiction and control stipulate the scope of control a State possesses; however, Rule 5 specifies the obligation of the State to other states. Specifically that "the principle of sovereign equality entails an obligation of all States to respect the territorial sovereignty of other States". The expert group elaborates with Rule 5 paragraph 3 claiming that:

> The obligation to respect the sovereignty of another State... implies that a State may not 'allow knowingly its territory to be used for acts contrary to the rights of other States'.

Rule 5 paragraph 3 has interesting implications in cyber space. For example, the infrastructure of many different countries may be used in an attack against a single victim. Because of this rule, each country whose infrastructure was involved is obliged to not allow these attacks to continue once they are aware of such attacks. A State, however, is not necessarily obliged to actively look for attacks against other countries from its infrastructure.

In other words, if an attack is made from (or through) State A to State B, and State B makes State A aware of the attack, then State A is normally obliged to help in stopping – and presumably helping to investigate – the attack on State B, if possible.

The Tallinn Manual goes on with Rule 7 stating that an attack originating from a State is not proof of a State's involvement, but "... is an indication that the Sate in question is associated with the operation". However, instead of assuming that the State could be guilty, in this work we propose to assume the innocence of the state whose infrastructure is being used in an attack.

Let's assume State B is affected by a cyber attack apparently originating from State A. State B then attempts to make State A aware of the attack. There is essentially one of three responses that State B will receive from State A: Response to collaborate, Response to not collaborate, or no response. In the case of no response if there is an assumption of innocence of State A, then State B may also assume that State A – being obliged to help – cannot stop the attacks because of lack of technical ability, resources, etc. In this way, consent to conduct remote cyber investigations on infrastructure within State A could potentially also be assumed.

In this way, when requests for assistance are made between States, if one State does not, or cannot, respond to the request, then cyber investigations can continue. Under this assumption, countries with intention to collaborate but limited investigation capacity, convoluted political and/or communication processes, or just no infrastructure will gain increased capacity to fight abuses of their infrastructure from countries that have more resources.

By assuming innocence of a state, at least four current problem areas can be improved. First, by assuming a State's consent for remote investigation upon no reply to international assistance requests, this will lead to a reduction in delay during cross-border investigations for all involved countries despite weaknesses in bureaucratic official request channels. Second, such an assumption will force States to take a more active role in explicitly denying requests, if so desired,

rather than just ignoring official requests, which is a waste of time and resources for everyone involved. Third, depending on the reason for the denial, such an explicit denial to investigate attacks against other countries would be slightly more conclusive proof of State A's intention to attack, or allow attacks, on State B, and could potentially help where attack attribution is concerned. And finally, such an assumption may also hold where mutual legal assistance currently – and oftentimes – breaks down; when dual criminality does not exist between two countries [3].

Essentially, if an attack on Country B occurs from infrastructure in Country A, Country A will either want to help stop the attack or not. By assuming that Country A does want to help but is simply unable to, this forces Country A to be explicit about their stance on the situation while at the same time ensuring that international cybercrime investigations can be conducted in a timely manner.

Bibliography

1. Malanczuk, P. (1997). Akehursts modern introduction to international law (7th ed.). Routledge.

2. Schmitt, M. N. (Ed.). (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

3. Harley, B. (2010). A Global Convention on Cybercrime?. Retrieved from http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/