IDEAS IN FOCUS

INTERNATIONAL LAW IN CYBERSPACE MATTERS: THIS IS HOW AND WHY

François Delerue[*]
May 2019

What can a government do if its transportation system, energy grid or another critical infrastructure system is disabled for an extended time due to a cyberattack, causing disruptions, economic losses and, potentially, human casualties? Is a military response justified or would it constitute a violation of international law? These and many other questions about *if* and *how* existing international law applies to cyberspace have preoccupied legal advisors and scholars. While specific answers always need to be provided on a case-by-case basis following a thorough legal analysis, there are a number of standard steps that are involved in the process of applying international law to a cyber operation, from the determination of who may be behind it to the adoption of unilateral measures aimed at the responsible party.

The flowchart illustrates this process to help anyone concerned with the application of international law navigate the different norms of international law and understand the logical process of their implementation. It presents the diversity of possible legal outcomes stemming from a cyber operation and illustrates that designating the operation as a use of force and a cyber armed attack - invoking a response of self-defence - is only one option among several, and neither applicable nor suitable in the vast majority of cases. Importantly, the flowchart focuses on peacetime and does not include the law of armed conflict. Indeed, the law of armed conflict, also referred to as the international humanitarian law, is applicable only when an armed conflict, either of international (between two or more states) or non-international (involving non-state actors) character occurs.

Step 1. Attribution of a cyber operation

Under international law, the attribution process aims to determine whether the cyber operation can be attributed to a state and, more precisely, whether the behaviour of the individual or the group responsible for the cyber operation can be attributed to a state. In other words, the first step is to identify the state culprit.[2]

According to the *Articles on Responsibility of States for Internationally Wrongful Acts* adopted by the International Law Commission in 2001,[3] which reflect the norms of customary international law on state responsibility, two situations are possible. First, an act or omission is attributable to a state if it is conducted by its organs (Article 4), persons or entities exercising elements of governmental authority (Article 5) or organs placed at the disposal of the state by another state (Article 6) (**Step 1a**). For instance, the army or intelligence services are organs of the state, so cyber operations attributed to these organs are attributable to that state. An example of an entity exercising elements of governmental authority can be found in the case of a private cybersecurity company hired by a state to perform general cyberdefence on its behalf.

[*] The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author(s).
[2] This process must be distinguished from other assignations of attribution, notably the public attribution, which is the political decision of a state to name the actor responsible for a cyber operation.
[3] Articles on Responsibility of States for Internationally Wrongful Acts (adopted by the International Law Commission at its 53rd session in 2001, annexed to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol I)/Corr4).

Step 1

Attribution

IS A CYBER OPERATION ATTRIBUTABLE TO A STATE?

1a Act of the state

- organ of the state
- entities empowered to exercise elements of the governmental authority
- organs placed at the disposal of the state

1b Act conducted on behalf of the state

- non-state actor acting under the instructions, direction or control of the state
- absence or default of the state
- context of mob violence, insurrections and civil wars
- act endorsed by the state

Step 2

Lawfulness

IS THE STATE RESPONSIBLE FOR AN INTERNATIONALLY WRONGFUL ACTS, SUCH AS... 2a

- threat or use of force
- violation of state sovereignty
- violation of the principle of non-intervention
- violation of other norms of international law

IN CASE OF THE USE OF FORCE, DOES IT AMOUNT TO AN ARMED ATTACK?

ARE THERE CIRCUMSTANCES PRECLUDING OR ATTENUATING THE WRONGFULNESS OF UNLAWFUL CYBER OPERATIONS? 2b

- force majeure
- distress
- consent
- necessity
- countermeasures
- self-defence

lawful act

Step 3

Responsibility

the victim state is entitled to invoke the responsibility of the responsible state

WHAT ARE THE RESPONSES AVAILABLE TO THE VICTIM STATE?

UN Security Council

interantional tribunal or court

Step 4

Unilateral measures

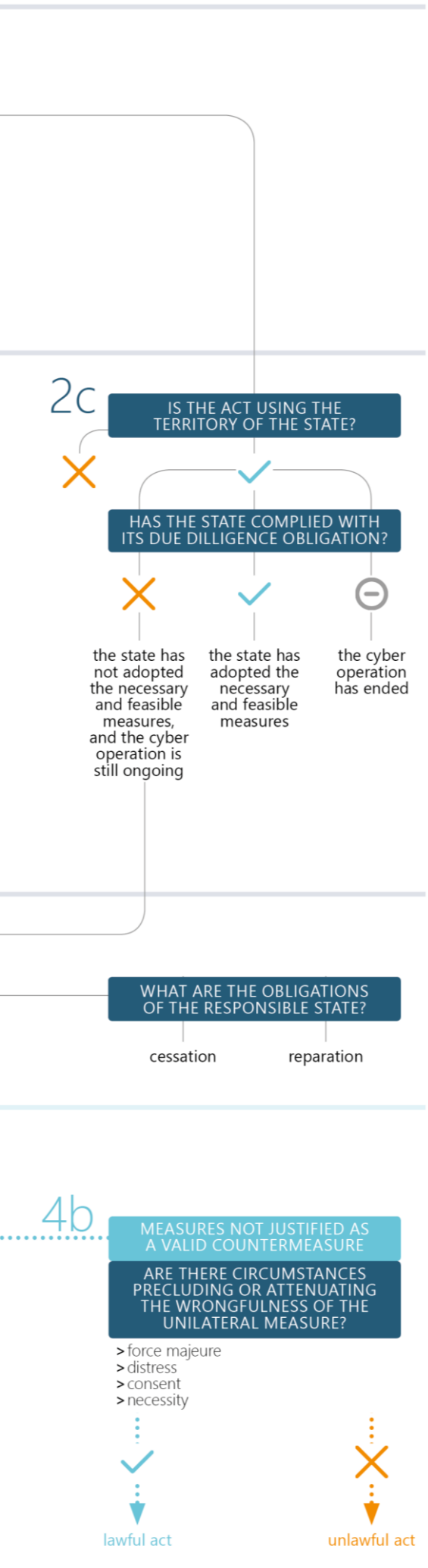
unilateral measures

4a

SELF-DEFENCE
lawful act

COUNTER-MEASURES
lawful act

MEASURES OF RETORSION
lawful act



Second, the conduct of a non-state actor is attributable to a state if it is conducted under the state's instructions, direction or control (Article 8), carried out in the absence or default of the official authorities (Article 9), conducted by an insurrectional or other movement (Article 10) or acknowledged and adopted by a state as its own (Article 11) (**Step 1b**). Importantly, in these cases, the attribution to the state of each act of the concerned non-state actor will be assessed separately, as opposed to step 1a in which every act of the concerned actor is automatically attributed to the state. A good example of an act conducted under a state's instructions, direction or control would be the case of a state giving instruction to a group of hackers to conduct a Distributed Denial of Service attack against a specified target.

It is only if the cyber operation fulfils one of these categories that it can be attributed to a state.

Step 2. Assessing the wrongfulness of the cyber operation

The second step aims to determine whether a cyber operation attributed to a state constitutes an internationally wrongful act of that state (**Step 2a**). Cyber operations between states are not *per se* prohibited by international law and generally constitute unfriendly or hostile acts. Despite the absence of a general prohibition on cyber operations, the conduct of a cyber operation may lead to a violation of specific norms of international law, such as state sovereignty, the principle of non-intervention, human rights or the prohibition of the threat or use of force (Article 2, paragraph 4, of the Charter of the United Nations). Moreover, certain instances of the use of cyber force may constitute an armed attack. As a matter of fact, what qualifies as an armed attack in cyberspace is one of the most debated issues among legal scholars.

The wrongfulness of an action that would otherwise constitute a breach of an international obligation of the responsible state can be precluded if the operation is perpetrated in some specific circumstances (*force majeure*, distress, consent, necessity, countermeasures or self-defence) (**Step 2b**). Indeed, the cyber operation may itself constitute a reaction to a previous wrongful act, which may not be of cyber character, and thus be justified either as a countermeasure or a measure of self-defence.

Alternatively, in some cases, even if a cyber operation is not attributed to a state, that state may be still held responsible according to the principle of due diligence (**Step 2c**). This principle imposes a duty on states not to allow their territory to be used for the launch or the transit of cyber operations targeting another state. The principle of due diligence is an obligation of conduct and not one of result. A state will incur responsibility not because it did not achieve the expected result but because it manifestly failed to take the necessary but feasible measures to prevent the act from happening despite being under an obligation to do so. For instance, a state that has taken no steps to mitigate an attack originating from its territory may be still held accountable under the international law. The attribution of the act does not matter; it can be perpetrated by a state or a non-state actor. In that perspective, due diligence may constitute an interesting palliative to the problem of attribution.

Step 3. State responsibility

The state injured by a cyber operation sponsored by another state may be entitled to invoke the responsibility of the sponsoring state and to seek reparations for the damage caused. The wrongdoing state bears an obligation of cessation and non-repetition of the wrongful act, as well as an obligation of reparation of the caused injury. The obligation to make full reparation of the injury resulting from an internationally wrongful act may take three forms, which are: restitution (reestablishing the status quo ante), compensation (payment of a sum in lieu of restitution), and satisfaction (e.g. apology, expression of regret, or acknowledgement of the breach).

To illustrate, we can take the example of a state responsible for malware that targeted the banking system of another state, which amounted to a violation of the territorial sovereignty of the targeted state and caused important economic loss. First, if the cyber operations have a continuous character, the responsible state has an obligation to cease them. Second, it has an obligation not to repeat the wrongful behavior. Third, it has an obligation to repair the economic loss resulting from its cyber operations, which would take the form of compensation in this case.

Step 4. Responses available for the victim state

International law imposes an obligation on states to settle their international disputes by peaceful means. The victim state may decide to appeal to the UN Security Council or an international tribunal or court. However, a central, compulsory judicial and enforcement mechanism may not always be available. Therefore, self-help measures constitute an important means for the enforcement of international law. The victim state of an unlawful cyber operation may have recourse to extrajudicial measures to compel the wrongdoing state to fulfil its obligations, namely measures of retorsion, countermeasures and self-defence (**Step 4a**).

A state targeted by a cyber operation constituting an armed attack has the right to resort to self-defence, using either cyber operations or other forms of force such as kinetic force. The vast majority of cyber operations do not qualify as a use of force and, *a fortiori*, an armed attack. Consequently, in such cases, the victim state does not have a right to self-defence and thus cannot respond with kinetic force. Countermeasures are unlawful measures adopted by a state against another state in reaction to that state's wrongful act. As a consequence, the wrongfulness of the actions adopted as countermeasures is precluded. Measures of retorsion are lawful but unfriendly.

In some circumstances, the wrongfulness of the reaction of a state to a cyber operation, which is not justified as a countermeasure or measure of self-defence, may be excused by another circumstance precluding wrongfulness (*force majeure*, distress, consent or necessity) (**Step 4b**). The most likely scenario would be the case in which the wrongful reaction is justified by the plea of necessity, which is to say that it constitutes the only means for the state to safeguard an essential interest against a grave and imminent peril.

Dr François Delerue is a researcher in cyber defence and international law at the Institute for Strategic Studies, French Military School (IRSEM).

EU CYBER DIRECT

This project is funded by the European Union.