Hacking Back and International Law: An Irreconcilable Pair?

Henning Lahmann 2020-07-16T12:11:23

Imagine you‘re at the onset of a global pandemic, and one of the nation‘s leading hospitals falls victim to a debilitating cyberattack, crippling its medical infrastructure for days. This is exactly what happened to Brno University Hospital on March 13, then home to one of the largest COVID-19 testing facilities in the Czech Republic. Now imagine further that your national security authorities identify a command and control server through which the attackers execute the malicious cyber operation, which would end immediately if you were to hack “back” into that system to render it inoperative (this part is fiction). Technically, that would be feasible. Alas, you realise that the server is located abroad. Shouldn’t you be allowed to go ahead and heroically save the nation?

A Definite No to Active Cyber Defence Legislation

Enter the Social Democrats: No, you shouldn’t. On July 10, Der Spiegel reported that the Grand Coalition‘s junior partner had finally buried the longstanding efforts to legislate the so-called hack back, or “active cyber defence”, a law that would have allowed a yet-to-be-designated domestic security agency to carry out cyber operations for defensive purposes on foreign territory. Explaining the decision, party leader Saskia Esken cited doubts regarding the conformity of such policy with international law.

But what are those doubts? After all, in Switzerland, such a law has been in force since 2017 (Article 37(1) Federal Intelligence Service Law). In Germany, the debate mainly focused on constitutional questions, in particular as to which public authority should obtain the mandate to carry out hack backs. From the standpoint of international law, this issue is of course immaterial. Irrespective of which domestic agency acts, it is always Germany that is the accountable legal entity. Two opinions by the Scientific Services of the Bundestag, from 2018 and 2019, respectively, noted in passing that in relation to Germany’s obligations under international law, active cyber defence measures would most likely violate the prohibition of the use of force pursuant to Article 2(4) UN Charter unless they could be justified as an act of self-defence against an armed attack by another state in accordance with Article 51 UN Charter. However, most cyber operations – both the original attack by the foreign actor and the active cyber defence measure – will probably not reach the use-of-force threshold. The more likely scenario is that malicious cyber conduct against German interests will at most amount to an unlawful intervention or simply violate Germany’s sovereignty, even though the status of sovereignty as a standalone rule under customary international law is still unsettled.

In that case, an active cyber defence measure would not need to meet the requirements of self-defence but might be justified as a countermeasure. The latter is a customary remedy that permits otherwise unlawful conduct by a state in response to a violation of its rights by the targeted state with the aim to induce that state to comply with its international obligations (Article 49(1) ILC Articles on State Responsibility). More to the point, if a hospital in Germany was attacked through cyberspace by a foreign state, Germany would be permitted to hack back in order to thwart or terminate the malicious cyber operation. To be sure, again, should the consequences of such an active cyber defence measure be so severe that the conduct reaches the threshold of a use of force – for instance by causing physical destruction or even injury and death in the target state – the hack back could only be justified as self-defence.

The Problem of Attributing Cyber Operations

While this legal construction seems straightforward enough, both self-defence and countermeasures are only permitted as remedies against the state that is responsible for the malicious cyber operation. This means that in order for the hack back to be justified, the cyber operation it is directed against must be attributed to the state where the targeted server is located. As hinted at by Esken, it is this aspect that ultimately led the Social Democrats to oppose the proposed legislation; because due to the technical characteristics of IT infrastructures, attribution of cyber operations remains a vexing challenge. It generally involves a three-step process: first, identification of the system that is used to carry out the operation; second, identification of the person that operates the system; and finally, linking this person to the state in accordance with the customary rules on attribution as laid down in Articles 4 to 11 ILC Articles on State Responsibility.

Now, contrary to still widely held belief, it is not the case that attribution of cyber operations is never possible. In fact, over the past few years, official, public statements of attribution have become an increasingly common phenomenon. Just consider the recent announcement by German law enforcement agencies to indict a member of the Russian intelligence agency GRU for hacking into the networks of the Bundestag in 2015. But this example also shows that confident attribution with a sufficient degree of evidence takes time – time that is likely not available in the emergency scenarios that serve as the rationale for legislating active cyber defence, such as cyberattacks against a hospital's IT infrastructure. If a state's security agencies go ahead anyway and shut down a server on foreign soil but it subsequently turns out that the target state was in fact not responsible for the attack, the defending state is responsible for a violation of its international obligations; international law knows no exonerating circumstances for a mistake of fact ("Erlaubnistatbestandsirrtum"). Given this impasse, a state will often, if not most of the time be barred from invoking either countermeasures or self-defence to justify hacking back.

Necessity to the Rescue?

However, there is another potential way to preclude the wrongfulness of active cyber defence conduct that appears to suit the described legal and factual intricacies: necessity. Recognised as customary international law, necessity may be invoked if the conduct in question is “the only way for the State to safeguard an essential interest against a grave and imminent peril” and “does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole” (Article 25 ILC Articles on State Responsibility). Rather intriguingly, necessity focuses entirely on the threat itself and ignores the question of its possible cause or source, so there is no need to attribute the malicious cyber operation to a state. That aside, the requirements for a successful invocation of necessity are (deliberately) high. Whereas it seems reasonable to argue that at least a state’s critical infrastructures, which includes medical facilities, can be considered “essential interests”, and that attacking them through cyber means constitutes “a grave and imminent peril”, past pleas of necessity in proceedings before international courts and tribunals frequently failed to discharge the need to show that the chosen emergency measure was indeed the “only way” to safeguard the interest. Furthermore, there is of course a real possibility that the server affected by the active cyber defence measure is itself indispensable for critical functions, so disabling it runs the risk of impairing an essential interest in the target state, rendering the hack back unlawful.

More crucially, like all norms derived from the legal-theoretical concept of the state of exception, the customary plea of necessity legitimates the invoking state to act outside its normatively expected performance. This means that by definition, it must be limited to genuinely exceptional, unforeseen circumstances. Resorting to it too frequently is bound to normalise the exception and thus gradually erode the regular operation of the legal system. Given the steady increase of cybersecurity incidents and adversarial behaviour in cyberspace, malicious conduct can hardly be considered “unforeseen”. Therefore, necessity as based in customary international law should not be used as the default legal basis for active cyber defence legislation.

An (Unlikely) Path Ahead

As this brief analysis has shown, the reluctance to legislate active cyber defence is indeed sensible. While hack backs may not be *per se* contrary to standing international law, the legal hurdles will likely prove insurmountable in practice. In light of the persistent problem of timely attribution, the only path to preclude the wrongfulness of such conduct will often be the customary state of necessity, a wobbly and vague justification simply not suited as the legal basis for a legislative act with potentially momentous foreign policy implications. As it appears unlikely that last week’s decision by the Social Democrats was the last time we’ll hear about plans to put active cyber defence into law, one possible path ahead would be the codification of an international treaty that enacts context-specific rules for defensive conduct in cyber emergency situations. Although international law knows examples of such special emergency regimes, the prospect of states agreeing on such a treaty is of

course highly unlikely given the current sorry state of international cooperation. For the time being, then, hacking back is hardly consistent with international law.
