Clingendael
Netherlands Institute of International Relations

Policy Brief

Sico van der Meer

JUNE 2020

How states could respond to non-state cyber-attackers

Dealing with non-state actors in cyberspace is a challenge for states experiencing large-scale cyber-attacks launched by such actors. Especially since more and more state actors seem to be hiding behind so-called independently operating non-state actors, it is important to get more clarity on how states could respond to such actors. This Policy Brief briefly explores some policy options that are available.

The majority of cyber-attacks in the world are launched by non-state actors, especially criminals looking for money. Most of these cyber-attacks are far from advanced and have relatively little societal consequences. Yet, state actors increasingly also seem to hire non-state actors to launch more severe cyber-attacks with potentially damaging effects for societies abroad.[1] While effectively responding to state-launched cyber-attacks is already a complicated task, this becomes even more difficult when states hide behind non-state actors.

How could states respond to non-state cyber-attackers, especially those aiming for large-scale operations harming their societies? This Policy Brief will briefly explore the problems in dealing with non-state cyber-attackers and will offer some policy options that are available. The benefits and risks of the policy options will be discussed as well, especially from a viewpoint of escalation risks.

Non-state actors in cyberspace

Although a large majority of the massive number of daily cyber-attacks are conducted by non-state actors, the common perception used to be that non-state actors may be responsible for the large majority of cyber-attacks, but that state actors are the biggest cyber-threat. Only states could mobilise the necessary funds to invest in the large-scale and long-term work needed to create the cyber-attacks that could cause actual large-scale harm to societies abroad.[2]

Yet, in the last few years more and more attention has been given to a hybrid kind of actor in cyberspace: states which use non-state actors for their cyber operations. The relationships between these ‘cyber proxies’ or ‘cyber mercenaries’ and the state’s officials they cooperate with vary widely, yet they have one thing in common: states ordering cyber-operations from non-state actors can even more easily

[1] Tim Maurer, *Cyber mercenaries: The state, hackers, and power*, Cambridge University Press, 2018.

[2] For example : Adam Segal, *The hacked world order. How nations fight, trade, maneuver, and manipulate in the digital age*, Public Affairs, 2nd edition, 2017, p. 31.

circumvent attribution and the potential consequences involved.[3]

While the attribution problem and consequently the ease with which to deny any involvement is one of the 'benefits' of cyber-attacks in general, hiring non-state actors improves this 'cloak of invisibility' for states even more; if the cyber-attack could be attributed at all, state officials could still deny any knowledge of the activities by a so-called independently operating actor, thus making it even harder for victims to take countermeasures.

Due diligence

While states have various tools available to respond to large-scale cyber-attacks conducted by state actors[4], there is less clarity on effectively dealing with non-state cyber-attackers. This is partly due to the lack of agreement in international relations on the concept of 'due diligence' in cyberspace.

Due diligence means an obligation for states to take measures to ensure that their territories are not used by any actor to harm other states.[5] If a state fails to meet its due diligence obligations, a victim state may resort, when appropriate, to countermeasures such as legal procedures or self-defence. Yet, in the cyber domain this concept is less clear compared to, for example, terrorists operating from a certain territory. In cyberspace, there are no borders at all; hackers in a certain country may well use servers and other digital infrastructure in other countries for their operations.

In 2015, the United Nations Group of Governmental Experts dealing with international cyber security issues acknowledged that due diligence is applicable in cyberspace, but opinions on the implications and implementation of the concept differ.[6]

Various states are hesitant about practically applying the principle of due diligence to cyber activities because of the corresponding obligations that it would impose on them; especially highly connected countries, which are more vulnerable to having cyber infrastructure on their territory being used by malicious actors, fear that they will bear the heaviest burden of due diligence and therefore prevent agreement on the issue in international forums such as the United Nations.[7] This does not mean that a victim state cannot use the due diligence principle to request another state to put an end to malicious cyber activity being conducted from its territory, yet it is somewhat unclear what it practically means under international law if the state does not act upon that request.

Policy options

Nevertheless, states have various policy tools available to respond to large-scale cyber-attacks which are convincingly attributed to non-state actors. Large-scale cyber-attacks are attacks which could have an actual societal impact by damaging or undermining national interests. The use of the term 'large-scale' is important here, because small-scale cyber-attacks such as common and extensive cyber-crime activities are a different category which should not automatically be dealt with using the same policy tools.

Below, seven policy options to respond to non-state cyber-attackers are identified.

[3] Tim Maurer, *Cyber mercenaries*, p. 3-8.

[4] Sico van der Meer, 'State-level responses to massive cyber-attacks: a policy toolbox', Clingendael Policy Brief, December 2018.

[5] Michael N. Schmitt, 'In defense of due diligence in cyberspace', *Yale Law Journal Forum*, Vol. 125 (2015), pp. 68-81.

[6] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Document A/70/174, 22 July 2015, paragraph 13h.

[7] Sico van der Meer, 'Could the Coronavirus Crisis Strengthen Due Diligence in Cyberspace?', *Net Politics*, 12 May 2020.

Option 1: Requesting host state to take action

When there is convincing evidence that a cyber-attack by a non-state actor has been or is being conducted from the territory of a certain state, the first and most simple option is to request this 'host' state to take measures against the actor. In many instances, this state would consequently take action to end the malicious activities and prevent future ones by the non-state actor. A request for action can be done at a technical assistance level (for example involving Computer Emergency Response Team experts) or at a diplomatic or even political level.

A benefit of requesting a state to take action to halt cyber-attacks from its territory is that such a request is non-accusatory (it does not automatically accuse the state of any involvement in the cyber-attack) and thus bears little risk of escalation.

Option 2: Capacity-building

If the 'host' state is willing, but is not able to take effective measures against the non-state cyber-attacker, a logical policy option is to assist the state in doing so. This could be done by short-term action, for example by sending some technical or police experts to act against the non-state actor specifically, and/or by starting a long-term capacity-building process to assist the country in also preventing similar malicious cyber-activities in the future.

Option 3: Diplomatic action

If the 'host' state is doing little or nothing after the request for assistance, while it should be able to do so, a diplomatic protest may be a viable option. This can be done by a diplomatic statement which could be delivered confidentially, but also publicly. In addition to a diplomatic statement, diplomatic protests could be strengthened by expelling some diplomats or other officials representing the state.

This kind of diplomatic retaliation may be damaging to the international reputation of the host state to a certain extent, because it shows that the state is not willing to act against malicious non-state actors, and consequently may even raise suspicion that it somehow facilitates those actors.

Option 4: Legal measures

Legal measures to end the malicious cyber-activities of the non-state actor (and to deter any future similar activities) could be used as well. Indicting the organisation or individuals involved sends a clear, public signal that the cyber-attackers have been identified and will face repercussions.

Yet, indictments will generally occur at a national level, for example under national criminal law. Unfortunately, this also implies that legal measures are often of a symbolic nature, because indicted individuals can generally only be arrested if they visit the country in which they are indicted (or any ally thereof). Moreover, the non-state organisation behind the cyber-attack might simply change its identity to evade legal repercussions.

Public mentioning of any state involvement in a legal procedure against a non-state actor could have an effect of 'naming and shaming' and deter further cyber-attacks to some extent. Theoretically, one could also imagine legal procedures against the state that is not willing to effectively halt the non-state actor's internationally harmful activities, for example via the International Court of Justice or the International Criminal Court, but in most cases that does not seem to be a proportional and/or feasible option.

Option 5: Sanctions

Sanctions could also be used to target the non-state actor and/or the state that is not taking effective action against this actor. Sanctions could, for example, involve blacklisting the individuals involved in or accommodating the cyber-attack, thus limiting their possibilities to travel abroad and/or to conduct international financial transactions.

Economic sanctions targeted at the host state may prohibit certain economic transactions with the country, for example the import or export of certain goods or (financial) services. Retaliation (and deterrence) by imposing sanctions might definitely have an effect, especially when the sanctioned country strongly depends on the sanctioned imports and/or exports. Yet, it should always be made clear what needs to be done to end the sanctions in order to enhance an actual change of behaviour.

Option 6: Retaliation in cyberspace

Going further than diplomatic options, a victim state could also use the principle of due diligence to respond to a large-scale cyber-attack by retaliating with a counter-attack. The most obvious option is to retaliate with a cyber-attack as well. It may seem logical to launch a cyber-attack to damage the computers of the non-state actor so that it will not be able to do more harm. Yet, the actor could easily accept the loss, acquire new computers and continue its malicious activities. It may be more effective to intrude into the computer system without damaging it, to inquire into working methods and to sabotage the activities as much (and as invisibly) as possible, for example by quickly patching the vulnerabilities which the hackers are seen to be targeting.

Another, more far-reaching option would be a cyber-attack against the state which is deemed to be capable but unwilling to act against the non-state actor. One could think of paralysing certain governmental digital infrastructures to signal that cyber-attacks from its territory, even if conducted by (semi-)non-state actors, will not be tolerated. However, this entails some escalation risks, which will be analysed below.

Option 7: Conventional military retaliation

A final and most robust policy option is retaliation through conventional military means, for example through a proportional strike against a specific location related to the non-state actor behind the cyber-attack or the state from which it operates. Military retaliation may send a crystal-clear message that cyber-attacks are not tolerated – thus deterring any potential cyber-attacker in the near future. Yet, it entails the risk of triggering a military response from the other side as well and could therefore start a dangerous process of escalation.

This policy option only seems likely to be considered in the case of more destructive cyber-attacks with actual physical damage and/or victims being involved, and/or if the country involved is a militarily much less powerful state so that any escalation is considered less dangerous. As far as is known, there has only been one example of conventional military action against a non-state cyber-aggressor, and not as retaliation but as pre-emption: in 2019, Israeli fighter aircraft bombed a building in Gaza, according to the Israeli air force because in that building Hamas hackers were preparing a cyber-attack against Israeli targets.[8]

Benefits and risks

An important consideration with regard to these policy options is the balance between the potential benefits and risks of each option.

The benefits of all options are similar: responding to a large-scale cyber-attack is meant to hold cyber-attackers accountable, to signal that their activities and involvement are well known and will not be tolerated. Another element is deterrence: punishing the attackers could deter them, as well as

[8] Lily Hay Newman, 'What Israel's Strike on Hamas Hackers Means For Cyberwar', *Wired*, 6 May 2020.

any other adversaries deliberating launching similar activities, from any further attacks.

The risks involved vary per policy option. In general, however, one could argue that the more convincingly a cyber-attack can be attributed, the less risks the countermeasures bring. This is because the more convincing the public evidence is, the harder it is for the cyber-attacking actor (and its supporting state) to deny everything and to respond with retaliation as well. This also implies that if one of the stronger policy responses is chosen, especially retaliatory measures, a great deal of public evidence should be provided to prevent international condemnation of the response. Such international condemnation risks switching the original victim into a new role of an aggressor and may result in a country's reputation being damaged, and consequently in economic losses and political isolation.

Furthermore, the response option chosen should always be proportional. Sometimes the signal alone may be enough to deter further attacks. Especially for the last three policy options (sanctions, retaliation in cyberspace and conventional military retaliation) it is important to prevent collateral damage because that could result in international condemnation as well.

The main risk of any of the policy options described is that the opponent (the non-state actor itself and/or its supporting state) may respond to the countermeasure in a hostile manner, especially if it wants to strengthen its denial of the original cyber-attack. Thus, retaliation against the cyber-attack may result in a further escalation and may actually cause more problems than it solves. Only the first two options (requesting assistance and capacity-building) entail hardly any risk of a hostile response.

Concluding remarks

Dealing with non-state actors in cyberspace is a challenge for states experiencing large-scale cyber-attacks from such actors. Especially since more and more state actors seem to be hiding behind so-called independently operating non-state actors, it is useful to get more clarity on how states can deal with such actors.

As described above, states have several policy options available to respond to a cyber-attack attributed to a non-state actor (really non-state or actually supported by a state). These options are: 1) Requesting the host state to take action; 3) Capacity building to assist the host-state in taking action; 3) Diplomatic action; 4) Legal measures; 5) Sanctions; 6) Retaliation in cyberspace; and 6) Conventional military retaliation.

Yet, especially the last two policy options should be used with restraint, because they contain a risk of escalation in case the state hosting (and/or supporting) the non-state actor would retaliate against the retaliation as well. Additionally, any response to a cyber-attack should, of course, be proportional.

As a last remark, the concept of due diligence could be useful in dealing with non-state actors in cyberspace, yet so far there is too little unanimity in the international community on how this legal concept actually applies in cyberspace. Renewed diplomatic efforts to reach consensus on this issue is desirable, preferably within the United Nations via the UN Group of Governmental Experts or the UN Open Ended Working Group which are currently deliberating on international cyber security issues.

About the Clingendael Institute
Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Newsletter

About the author

Sico van der Meer is a Research Fellow at the Clingendael Institute as well as a Doctoral Candidate at Eindhoven University of Technology.