Clingendael
Netherlands Institute of International Relations

Policy Brief

Sico van der Meer

DECEMBER 2018

# State-level responses to massive cyber-attacks: a policy toolbox

While cyber-attacks are becoming a rather common phenomenon in international relations nowadays, states are still looking for the best way to respond to massive cyber-attacks targeting their society. This Policy Brief concisely explores the policy instruments available to states experiencing a large-scale cyber-attack, as well as the potential effects and risks of these tools.

How can states respond to massive cyber-attacks targeting their society? Even though cyber-attacks have become a rather omnipresent phenomenon in international relations, there is still no clear answer to this question. Many ways of responding have been explored, but none of them have proved unconditionally effective in retaliating against a large-scale cyber-attack so that further attacks will be deterred.[1] Some states, for example the United States (US), are currently focussing on offensive cyber operations to prevent cyber-attacks before they even occur[2], or on deterring them by openly suggesting retaliation with substantial – even nuclear – counter-attacks.[3] Other states, that are more cautious concerning the escalatory effect of such approaches, have chosen to focus on diplomatic responses, such as the member states of the European Union which developed a so-called ‘Cyber Diplomatic Toolbox’ focussing on deterring cyber-attackers with the prospect of political and economic sanctions.[4]

This Policy Brief concisely explores the policy instruments available to states experiencing a massive cyber-attack, as well as the potential effects and risks of these tools. A distinction will be made between diplomatic and non-diplomatic responses, and the effectiveness of both types of tools will be weighed as well. Examples of the actual use of the instruments will be particularly found in US policies, because this state has been most active in (publicly) experimenting with the various tools in searching for effective means of retaliation against and the deterrence of large-scale cyber-attacks.

[1] For some examples of cases between 2007 and 2014, see: Sico van der Meer, Foreign policy responses to international cyber-attacks: Some lessons learned, Clingendael Policy Brief, September 2015.

[2] David E. Sanger, ‘Pentagon puts cyberwarriors on the offensive, increasing the risk of conflict’, New York Times, 17 June 2018.

[3] David E. Sanger & William H. Broad, ‘Pentagon suggests countering devastating cyberattacks with nuclear arms’, New York Times, 17 June 2018.

[4] ‘Cyber-attacks: EU ready to respond with a range of measures, including sanctions’, Press release 357/17, European Council, 19 June 2017.

## The attribution problem

Before discussing the policy tools themselves, it is essential to point to a fundamental issue with regard to cyber-attacks: attribution.[5] Without the ability to identify an attacker, effectively responding (let alone retaliating) is hard. Obtaining complete certainty concerning the source of an attack is often difficult in the cyber realm; traces can be wiped quite effectively, or even be manipulated, seemingly pointing to an innocent third party. Examples of such false-flag operations are the cyber-attack on the French broadcaster TV5 in 2015 and on the opening ceremony of the Olympic Games in 2018.[6] This complication entails the risk that any means of retaliation may subsequently appear to have been targeted at an innocent party. Moreover, detailed investigations into the attack may take so much time that the 'momentum' for an effective response may have already passed – ideally, an attacker is retaliated against immediately, and not after several months.

In the past few years the technical possibilities of cyber forensics have developed rapidly, and indisputable attribution seems to become increasingly feasible. Nevertheless, even if compelling evidence on the cyber-attacker is found by investigators, it may not always be possible to bring this into the open without harming the future use of the intelligence instruments that were used. Especially if the accused party publicly denies any involvement (for example, claiming that the accusation is completely false or that it must have been a false-flag operation), retaliating without making public detailed evidence may risk an escalation as well as international condemnation of the retaliatory action.

Effectively responding to large-scale cyber-attacks therefore starts with investing in cyber forensic capabilities. Without any convincing evidence as to who has conducted a cyber-attack, effectively responding will become difficult. Cyber forensic capabilities can be developed at a national level, but also at a multinational level, for example through regional (security) organisations. Close cooperation with the private cyber security sector will definitely be helpful as well; public-private cooperation may be an effective way of combining multiple sources for evidence gathering.

## Diplomatic responses

Once the perpetrator of a cyber-attack has become known – which in the case of massive cyber-attacks are generally states or state-sponsored entities – states have various options to respond. First of all, there is the 'diplomatic toolbox'. This toolbox offers various diplomatic responses, all with their own merits and disadvantages.

A key element of these diplomatic options is 'signalling': showing the cyber-attackers that their activities and involvement are well known and will not be tolerated.[7] This is particularly important in the cyber domain, because conducting cyber-attacks is often considered as being almost risk-free: cyber-attacks are relatively cheap and easy while, because of difficulties in attribution, involvement can always be denied. Therefore, the exposure of the cyber-attackers, and thus removing their 'cloak of invisibility', is an important first step in holding cyber-attackers accountable. Another element is retaliation, or in other words: punishing the attackers in order to deter them from any further attacks.

[5] Neil C. Rowe, 'The attribution of cyber warfare', in: James A. Green (ed.), Cyber warfare. A multidisciplinary analysis, Routledge, 2015, pp. 61-72.

[6] Gordon Corera, 'How France's TV5 was almost destroyed by Russian hackers', BBC News, 10 October 2016; Chris Bing, 'Winter Olympics hack shows how advanced groups can fake attribution', Cyberscoop, 26 February 2018.

[7] Sico van der Meer, 'Signalling as a foreign policy instrument to deter cyber aggression by state actors', Clingendael Policy Brief, December 2015.

An overview of possible diplomatic ‘tools’ is presented below:

*Tool 1: Acquiescence and strengthening cyber security*

The first option is the least complicated one, although maybe not very realistic in the case of a massive cyber-attack: doing nothing directly towards the attacker, but simply acknowledging that the cyber security measures in this case were not adequate, communicating that lessons have been learned and that the cyber security of the targeted networks have been improved and will receive more and continuing attention.

The merit of this option is that it prevents any escalation; no-one can complain about being retaliated against for something it denies having done. The inherent risk is, though, that the attacker will consider this response as an invitation to continue its malicious cyber activities on an even larger scale. If there are no negative consequences involved, why not even bring these activities to a higher level? Deterrence by denial, as raising the barriers for potential enemies is often called, is only effective if it actually changes the cost-benefit analysis of these enemies.[8] Yet, they might consider it worthwhile to simply increase their efforts to surpass the improved cyber security measures.

An example of such a response was the initial US policy after the cyber-attack against the US Office of Personnel Management (OPM) in 2015, in which the personal details of more than 21 million current and former US government employees and their partners were stolen. The US government publicly acknowledged the inadequate cyber security of the OPM and focussed on improving it; although traces of the cyber-attack led to China, no visible action was taken against the hackers involved. Only in 2017 was one Chinese person arrested because of involvement in the cyber theft.[9]

*Tool 2: Diplomatic protests*

Another option to respond to a massive cyber-attack is diplomatic protests. This can be done in various ways. First of all, it can be done by a diplomatic statement, communicated to the state allegedly conducting or facilitating the cyber-attack. The statement could be delivered under diplomatic confidentiality, but it could also be made public. This can be done by a public statement, but also by requesting a statement of condemnation from a multilateral organisation, for example a regional organisation such as the Organisation for Security and Cooperation in Europe (OSCE) or a universal organisation such as the United Nations. In addition to a diplomatic statement, diplomatic protests could be strengthened by expelling some diplomats or other officials representing the accused state.

This kind of diplomatic retaliation may be damaging to the international reputation of the accused state to a certain extent and may well show that the attacked state is able to identify cyber-attackers, thereby removing their ‘cloak of invisibility’. On the other hand, diplomatic protests will not be very harmful to the attacking state. From that perspective, it will probably not deter this state – or any other potential cyber adversary – from conducting similar cyber-attacks. This is why diplomatic protests can be considered as a largely symbolic response. Yet, the positive side is that there is hardly any risk of an escalation. The other state may publicly deny any involvement in the cyber-attack and maybe expel some diplomats as well, but that is all of the escalation that could reasonably be expected.

An example of this diplomatic tool being used is the response of the US government in 2016 by expelling 35 Russian diplomats

[8] Sico van der Meer, ‘Deterrence of cyber-attacks in international relations: denial, retaliation and signalling’, International Affairs Forum, Vol. 2 (2017) 85-90,

[9] Evan Perez, ‘FBI arrests Chinese national connected to malware used in OPM data breach’, CNN Politics, 24 August 2017.

after alleged Russian cyber-attacks against political organisations, and leaking stolen information or using it (mixed with fake information) in social media campaigns to influence the US presidential elections. Two Russian semi-diplomatic locations were forced to close as well, and a few sanctions against Russian intelligence services were announced.[10]

*Tool 3: Legal measures*

Legal measures are in the 'diplomatic toolbox' as well. Indicting organisations or individuals involved in a cyber-attack sends a clear, public signal that the cyber-attackers have been identified and will face repercussions. Combined with some international reputational damage involved, these measures may also have some deterrent effect.

Indictments will generally occur at a national level, for example under national criminal law. Involving international judicial organisations such as the International Court of Justice or the International Criminal Court currently seems to be a little far-fetched (but not impossible). Yet, this also implies that legal measures are often of a symbolic nature. Indicted individuals can generally only be arrested if they visit the country in which they are indicted (or any ally) and certain organisations might just change their identity to evade legal repercussions.

Moreover, legal measures entail some risks. First, they may result in court cases in which sensitive intelligence operations have to be exposed in order to provide the judicial evidence. Exposing intelligence methods may well be more damaging than advantageous. Second, the state behind the cyber-attack could retaliate with legal measures as well – for example, indicting companies doing business in that country with falsified accusations.

The US has used this tool on various occasions, for example in 2014, when five officers of the Chinese People's Liberation Army were indicted in a charge of the massive theft of intellectual property from several US companies via cyber espionage.[11] A recent example is the indictment of seven officers from the Russian military intelligence agency, the GRU, in October 2018.[12] So far, all of the indicted persons are yet to appear before court.

*Tool 4: Political & economic sanctions*

Another diplomatic tool is sanctioning. Political sanctions could, for example, involve blacklisting the persons and organisations involved in the cyber-attack, limiting their possibilities to travel abroad and/or to conduct international financial transactions. Economic sanctions may prohibit certain economic transactions with the country behind the cyber-attack, for example the import or export of certain goods or (financial) services.

Retaliation by imposing sanctions might definitely have some deterrent value, especially for countries that strongly depend on such imports and/or exports. However, once the sanctions are in place the sanctioned state has little reason to change its behaviour as long as there are no clear guidelines on how to have these sanctions removed. How and when should it prove that it has stopped any misbehaviour so that the sanctions can be lifted? Even more important is the risk that the sanctioned state could retaliate with countersanctions – which may especially have a major impact if there is a great deal of (economic) interaction between the two states concerned. One could question whether the potential economic damage of such a 'sanctions war' is worth the deterrent effect with regard to cyber-attacks.

[10] David E. Sanger, 'Obama Strikes Back at Russia for Election Hacking', New York Times, 29 December 2016.

[11] 'US charges five Chinese military hackers for cyber espionage against US corporations and a labor organization for commercial advantage', Press Release, US Department of Justice, 19 May 2014.

[12] Ellen Nakashima, Michael Birnbaum & William Booth, 'US and its allies target Russian cyber spies with indictments, public shaming', Washington Post, 4 October 2018.

The US has used this instrument on several occasions, for example in March 2018 when it blacklisted several Russian organisations and individuals because of their involvement in several cyber-attacks (varying from the manipulation of the US presidential elections to the disruptive global NotPetya cyber-attack).[13] Yet, the list of sanctioned entities and individuals is relatively short and one may question whether Russian cyber-attacks will be effectively deterred by this move. In order to be effective, one may assume that sanctions have to be imposed on a somewhat larger scale.

## Beyond diplomacy

Apart from the diplomatic measures described above, states have some additional options to respond to large-scale cyber-attacks. These options, which generally require the involvement of the security services and/or the armed forces, tend to focus on the retaliation part more than the signalling part of responses. The aim of such retaliation is to vigorously deter the cyber-attackers from any similar activities.

As with the diplomatic possibilities, these non-diplomatic options all come with their own merits and disadvantages. The following is an overview of the possible 'tools' beyond diplomacy:

*Tool 5: Retaliation in cyberspace*

Going further than diplomatic activities, a state could also respond to a large-scale cyber-attack by retaliating with a counter-attack. The most obvious option to retaliate in this way is striking back in the same dimension that the offender has used: cyberspace. Preferably, a counter-cyber-attack, for example paralyzing some governmental cyber infrastructures, would clearly signal that cyber-attacks will be attributed and retaliated against, but without starting a cycle of escalation into a tit-for-tat spiral of cyber-attacks.

From that perspective, a counter-attack in the cyber domain should be proportional and not cause too much damage (let alone actual victims) in order to be effective; the signal alone may be enough to deter further attacks. Yet, this is also the main risk of this 'tool'; the opponent may retaliate against the counter-attack as well, especially if it wants to strengthen its denial of the original cyber-attack. Thus, a retaliation may result in a further escalation and may actually cause more problems than it solves.

Even more, the international community may condemn a counter-attack when evidence of the attribution of the original cyber-attack cannot be made (completely) public because of the need to protect the intelligence methods used, thus switching the original victim into a new role of an aggressor with all the negative implications that this implies. Last but not least, unexpected collateral damage caused by the cyber-attack (as happened, for example, with the Stuxnet[14] and the Wannacry[15] cyber-attacks) may result in international condemnation as well.

As far as is known, there are no examples, as yet, of *openly* retaliating against a cyber-attack by a counter-cyber-attack. Yet, this tool is closely linked to the next one: Covert Retaliation in Cyberspace, of which various examples have been made public. One may expect that, in practice, retaliatory cyber-attacks may already have taken place without having been made public.

*Tool 6: Covert retaliation in cyberspace*

A slightly different option to respond to a large-scale cyber-attack is covert retaliation in cyberspace. Instead of publicly launching a counter-cyber-attack, with the risk of escalation and international condemnation, this can be done covertly. Ideally, only

[13] 'Treasury sanctions Russian cyber actors for interference with the 2016 US elections and malicious cyber-attacks', Press Release, US Department of the Treasury, 15 March 2018.

[14] Vivian Yeo, 'Stuxnet infections spread to 115 countries', ZDNet, 9 August 2010.

[15] Damien Gayle a.o., 'NHS seeks to recover from global cyber-attack as security concerns resurface', The Guardian, 13 May 2017.

the original attacker will realize what the counter-attack involves, thus deterring future attacks. Nevertheless, a certain announcement may be helpful; a state may for example issue a statement after a large-scale cyber-attack that the perpetrators have been identified and will be retaliated against in an appropriate manner that only they will know. This may have a deterrent effect on any potential cyber-attacker.

Covert retaliation has the benefit that it may prevent any escalation; any future cyber incident in the state that is being counter-attacked may be part of the retaliation, but may have other causes as well; the opponent may ideally doubt everything. As long as it cannot prove what is a covert cyber-attack and what is not, it is hard to openly condemn anything. Yet, an escalation is not completely excluded. The state may respond with even more (covert) cyber-operations as retaliation against perceived covert counter-attacks – even when they were not counter-attacks at all – thus causing a cycle of escalation as well.

An example of this tool being used by the US was the response to the Sony hack of 2014, which US President Obama considered as an attack by North Korea against the freedom of speech in the US. Obama stated that the US would "respond in a place and time and manner that we choose."[16] Soon afterwards, North Korea accused the US of cyber-attacks putting down the Internet in the country twice; the US did not admit or deny any involvement.[17]

*Tool 7: Military retaliation*

A final policy option to respond to a massive cyber-attack is retaliation through conventional military means, for example a proportional strike against a specific location related to the perpetrators of the cyber-attack. One may assume that in this instance convincing evidence on the attribution of the cyber-attack has to be made public in order to prevent any backlash by an international condemnation of the retaliatory attack.

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 bears the risk of triggering a military response from the other side as well and thus could start a dangerous process of escalation.

This option only seems to be likely to be considered in the case of more destructive cyber-attacks with actual physical damage and/or victims involved, and/or if the country involved is a militarily much less powerful state so that an escalation is considered less dangerous. Nevertheless, there will always be a risk that the international community will deem the counter-attack to be disproportional, especially if collateral damage is involved. International condemnation may result in a country's reputation being damaged, and consequently in economic losses and political isolation.

Although a military alliance like NATO has stated that a massive cyber-attack could trigger a collective (conventional) military response, and the US administration of President Trump has suggested that such cyber-attacks could be retaliated against by conventional or even nuclear military strikes, it is currently not clear how such a response would look like in practice.[18] So far, no examples are known of actual (publicly visible) military retaliation against cyber-attacks.

## Important considerations

The overview above shows that states confronted with a massive cyber-attack have several tools available to respond, varying from silent acquiescence and diplomatic protests to counter-attacks by cyber or conventional military means. These tools all have their own benefits and disadvantages,

[16] Steve Holland & Matt Spetalnick, 'Obama vows US response to North Korea over Sony cyber-attack', Reuters, 19 December 2014.

[17] 'Sony hack: North Korea blames President Obama for internet outage', BBC World, 27 December 2014.

[18] 'Massive cyber-attack could trigger NATO response: Stoltenberg', Reuters, 15 June 2016.

mostly to be found in a mix between credibly deterring the cyber-attacker from any new attacks and the risk of an escalation into more problems.

It is obvious that any tool available can only be used after a thorough deliberation of the pros and cons, preferably at a national interdepartmental or interagency level. Before choosing any tool to respond to a large-scale cyber-attack, credible attribution is crucial. Responding to a wrong, innocent actor because of incorrect attribution will only create more problems. From that perspective, the availability of good cyber attribution capabilities and an effective interdepartmental and/or interagency cooperation within the cyber domain may already function as a first effective deterrent against large-scale cyber-attacks. Yet, deterrence only works if the opponent realizes the potential costs it may face. This means that a state should be relatively open concerning its capabilities, which in turn creates a dilemma because too much openness may give opponents insights into how to avoid these capabilities.

Especially for relatively smaller states, it may be desirable not to respond unilaterally, but to seek cooperation with allies, for example via regional frameworks like the EU or military alliances like NATO. This also depends on the response option that is chosen; silent acquiescence and strengthening cyber security means can be done unilaterally much more easily than other options.

It should be emphasized that responding to massive cyber-attacks is also experimental. Large-scale cyber-attacks are a relatively new phenomenon in international relations and there is currently little experience in what are the most feasible ways of responding. Moreover, the international legal framework in which cyber-attacks and counter-measures have to be considered is not crystal-clear either, even though initiatives like the Tallinn Manual offer some useful guidance to international lawyers.[19]

Last but not least, it should be prevented that, in the longer term, the use of (covert) cyber-attacks by states against other states may become a de facto accepted norm. Such a development is dangerous and would contribute to more instability and insecurity in the international system. One may even question whether cyber deterrence can actually be achieved at all, except perhaps at a very high cost, because effective retaliation entails major risks. In the long term, international cooperation and norm-setting seem to be more viable in preventing large-scale cyber-attacks than a cycle of attacks and counter-attacks escalating into yet higher levels of cyber destruction.[20]

[19] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edition, Cambridge University Press, 2017.

[20] Sico van der Meer, 'Enhancing international cyber security. A key role for diplomacy', Security and Human Rights, Vol. 26 (2015) 193-205.

**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

## About the author

**Sico van der Meer** is a Research Fellow at the Clingendael Institute. His research focusses on non-conventional weapons like Weapons of Mass Destruction and cyber weapons from a strategic policy perspective.