Clingendael
Netherlands Institute of International Relations

Policy Brief

Sico van der Meer

DECEMBER 2015

Signalling as a foreign policy instrument to deter cyber aggression by state actors

Signalling might be an effective foreign policy instrument to change the cost-benefit calculations of states engaging in or sponsoring cyber aggression activities. While especially cyber espionage and cyber sabotage are currently considered to be cheap, almost non-risk activities, the instrument of signalling may make them less anonymous and risk-free. Yet, the effectiveness of the instrument is difficult to measure.

Cyber aggression – be it espionage, sabotage or even warfare – among state actors is an increasing threat to international security and stability. Due to a lack of commonly accepted international rules or norms in the cyber security area, individual states are looking for the best way to deal with the threat.[1] One of the most effective methods in this regard is to deter cyber threats, preferably before the actual aggression starts or escalates.[2] One potential foreign policy instrument that might be considered useful for cyber deterrence is the concept of signalling: informing any state that is conducting or sponsoring cyber aggression that this (hidden) activity is being monitored and that it may be met with retaliation.

Signalling in international relations

The foreign policy instrument of signalling is regularly used to deter aggression, especially during military tensions in the geopolitical realm. It consists of giving a signal to an adversary to express knowledge as well as discontent about certain behaviour of this adversary. Thus the actor in question may be convinced to stop the signalled behaviour, realizing that any continuation will be noticed and potentially result in retaliation.[3] Especially during the Cold War, signalling was frequently used by the United States and the Soviet Union to deter military behaviour that might lead to an escalation between them. If, for example, one of both states was secretly trying to violate any arms control treaty, the other one would simply notify that the violation had been detected, which was

1 Tobias Feakin, *Developing a proportionate response to a cyber incident*, Cyber Brief, Council on Foreign Relations, August 2015.

2 Sico van der Meer, 'Deterrence as a security concept against cyber threats', in: Frans-Paul van der Putten, Minke Meijnders & Jan Rood (eds.), *Deterrence as a security concept against non-traditional threats. Clingendael Monitor 2015*, 2015, pp. 38-43.

3 Ahmer Tarar and Bahar Leventoglu, *Bargaining and Signaling in International Crises*, Research Paper prepared for the United States National Science Foundation, 2008.

often enough to bring the cheating to an end.[4]

Signalling in international security issues is a tool aimed at psychological effects. Generally, it is as simple as just communicating that the behaviour of the adversary is known and is deemed undesirable. This can be done in private, only known between the two adversaries, or in public, which makes the instrument more like 'naming and shaming'.

To be an effective instrument, the signalling must convince the adversary that continuing the activity in question may result in countermeasures by the signalling actor. This implies that effective signalling entails the (indirect) threat of potential retaliation as well. In this way the cost-benefit calculation behind the signalled behaviour is influenced – continuing will be more costly than was (assumingly) expected before the signal was received.

Signalling and cyber security

Especially the aspect of influencing cost-benefit calculations could be an important contribution of signalling to international cyber security. Cyber aggression instruments, especially if applied for espionage but also for military and/or sabotage purposes, are generally considered as almost 'cost free'. Cyber aggression instruments are often effective, while being cheap to use. Moreover, because of difficult attribution, the anonymity of the user is to some extent guaranteed. Signalling, however, could change this cost calculation. If applied successfully, signalling could remove the perceived anonymity of the cyber aggressor and could show him that continuing its behaviour will initiate countermeasures.

Although signalling is often done in private, between two influential officials or politicians, doing it in public may have even more of an effect. Public naming and shaming could have negative consequences for the adversary state's reputation, with potential repercussions in the political and economic realm.

When using the instrument of signalling it may be less necessary to provide 100% convincing evidence compared to (public) legal or military countermeasures. Signalling as a foreign policy instrument could thus contribute to increasing the threshold for state-conducted or state-sponsored cyber aggression.

To support the signalling instrument, retaliation options must be on the table as well. Without the risk of being retaliated against, the cyber aggressor will less easily be impressed by signalling efforts. In the cyber domain, the retaliation option will generally consist of legal measures, economic sanctions, or the (covert) use of cyber operations. Conventional military retaliation seems far-fetched for cyber espionage and sabotage, as long as the cyber aggression has not caused actual physical harm.

Signalling will not be able to completely stop cyber aggression by state actors, but it could definitely raise the costs of what has been considered as a relatively low-risk, asymmetric strategy so far. Moreover, the instrument of signalling provides foreign policy makers with an extra escalation level, with only psychological effects, before the next level of actual retaliation. Such an extra 'mild' escalation level could contribute to international stability.

Difficulties in the cyber security realm

Although the foreign policy instrument of signalling appears to be an interesting contribution to limit international cyber aggression by state actors, some difficulties should be taken into account as well.

First of all, signalling in the cyber domain requires a nuanced approach because of the difficulties in reliable attribution,

4 Mason Rice, Jonathan Butts, and Sujeet Shenoi, 'A signaling framework to deter aggression in cyberspace', *International Journal of Critical Infrastructure Protection*, Vol. 4, 2011, pp. 57-65.

and consequently the mysterious nature of cyber aggressors, their intentions and targets. Signalling is only effective if the right adversary is shown that his activities are being monitored and are disapproved of, while in cyberspace adversaries may be cloaked as someone else and their intentions with certain activities may be different from what they may seem at first sight. Caution in not signalling too easily is always crucial, but in the cyber realm maybe even more so.

Second, in the cyber domain many more adversaries may be active than in a conventional military confrontation. The political, cultural, and ideological values of these cyber aggressors may vary considerably. These differences may influence the adversary's perception of the defender's signals, potentially leading to misinterpretation and miscalculation. For example: signals that may be too ambiguous for one adversary may be considered too offending for another adversary. This, in turn, entails a risk of causing an escalation of tensions instead of the de-escalation that was intended with the instrument of signalling.

Moreover, the retaliation options that should back the effect of the signalling instrument may lack credibility as far as the cyber aggressor is concerned. While signalling in itself regularly does not require the release of convincing evidence to prove the allegations, further steps like imposing sanctions or legal measures do. Providing such evidence may comprise sensitive information on the intelligence tools with which the evidence was gathered. This knowledge may be used by the adversary to make future cyber operations even more difficult to attribute, thus making the deterrent effect of the retaliation options meaningless.

Last but not least, the threat of retaliation which ideally should be on the table to make signalling more effective, in itself brings a risk of escalating tensions. Imposing sanctions or starting legal procedures may backfire if the adversary state will also retaliate, for example by sanctioning or indicting companies from the signalling state as well. Threatening retaliation by (covert) cyber operations may have a deterring effect in the short term, but risks a vicious circle of escalating tit-for-tat actions in the long term.[5] The instrument of signalling may thus bring a risk of escalation, but one could argue that any response to cyber aggression may bring that risk; even not responding at all, because that will invite the adversary to increase its aggressive activities.

Past cases: some lessons learned

To assess the usefulness of signalling with regard to international cyber security, it would be useful to evaluate past cases. The problem here is that signalling is most often conducted via non-public channels, by officials (be it diplomats, military or intelligence officers, or politicians) towards their counterparts in the – suspected – adversary state. How often this is happening and how effective it is, is thus hard to evaluate.

From this perspective, it is interesting to note that acts of cyber aggression are often also kept secret by the victims. Especially private companies generally prefer to keep them secret to prevent further harm like reputation damage, legal measures by angry customers, or imitation by other actors in cyberspace who are drawn to the apparent weakness of the company's cyber security. Even states sometimes seem to prefer to keep cyber-attacks from abroad as an internal affair, seemingly to prevent any escalation, reputation damage or imitation attacks.[6]

Few cases of diplomatic signalling in cyber security have become public. Here three of these cases are briefly discussed: Estonia signalling to Russia in 2007, the United States signalling to China in 2014, and the United States signalling to North Korea in 2014-2015. Of course, more cases could be thought of, but these three cases

5 Sico van der Meer & Frans-Paul van der Putten, *US deterrence against Chinese cyber espionage. The danger of proliferating covert cyber operations*, Clingendael Policy Brief, September 2015.

6 Sico van der Meer, *Foreign policy responses to international cyber-attacks. Some lessons learned,* Clingendael Policy Brief, September 2015.

offer good examples of the difficulties involved in using the signalling instrument in international cyber security issues.

Estonia-Russia, 2007

In April 2007 Estonia experienced a cyber sabotage attack, targeting large parts of the country's digital infrastructure. A wave of so-called Distributed Denial of Service (DDoS) attacks shut down the websites of banks, media, ministries and political parties, thereby suggesting an attempt to paralyze Estonia's society.

While the technical defence against the cyber-attack was being dealt with by the governmental Computer Emergency Response Team (CERT), the Minister of Foreign Affairs, Urmas Paet, used the instrument of signalling shortly after the start of the cyber-attack. He publicly stated that the cyber-attacks "have been made from IP addresses of concrete computers and individuals from Russian government organs including the administration of the President of the Russian Federation."[7] The accusation linked the cyber-attack to the relocation of a Soviet-era war memorial in Tallinn which in the previous days had caused tensions in Estonian-Russian diplomatic relations, as well as riots by members of the Russian minority in Estonia. The public accusation was probably meant to show Russia that Estonia had evidence of its involvement, hoping that public accusation would force Moscow to limit its role. However, no retaliation measures were communicated.

If the public accusation was indeed meant as signalling and thus to deter the cyber adversary from continuing the attack, it did not have any visible effect. Russia simply denied the allegation and warned Estonia against making accusations without any evidence. Moreover, Russia used the public accusation as an argument not to help in any way in the aftermath of the cyber-attack. Russia refused to cooperate with the Estonian authorities in investigating the case.[8]

One could argue that the rapid signalling did have a deterrent effect to some extent, because Estonia has not experienced a similar cyber-attack since 2007. However, it is always difficult to analyse why events did *not* happen, because there could be countless reasons for this, for example the lack of motives for adversaries to launch a similar cyber-attack.

U.S.-China, 2014

In May 2014, the U.S. Department of Justice indicted five Chinese military officers for the large-scale cyber theft of trade secrets from several large U.S. companies. The officers were blamed for job losses, plant closures and billions of dollars in damage for the companies in question due to lost research and development costs.

Publicly naming the five, and providing detailed evidence of their cyber espionage in a 48-page indictment, was a perfect example of signalling. It is unlikely that the officers will ever be brought to trial in the U.S., because there is no extradition treaty with China.[9] The indictment was only meant to show China that the U.S. government was aware of the Chinese state involvement in commercial cyber espionage, and that it would no longer be tolerated.

The effect, however, was not positive. Although China could not deny the accusations outright because of the detailed evidence provided, it furiously blamed the U.S. for being the biggest cyber spying state in the world. Moreover, China ended the few cooperation mechanisms it had with the U.S. (mainly a diplomatic working group aimed at dialogue on cyber security) and even threatened further retaliation for the indictment.[10]

7 Cited in: Kertu Ruus, 'Cyber War I: Estonia attacked from Russia', *European Affairs*, Vol. 9, No. 1-2, Winter/Spring 2008.

8 Ruus, 'Cyber War I'.

9 Devlin Barrett & Siobhan Gorman, 'U.S. Charges Five in Chinese Army With Hacking', *Wall Street Journal*, 19 May 2014.

10 Ting Shi & Michael Riley, 'China Halts Cybersecurity Cooperation After U.S. Spying Charges', *Bloomberg Business*, 20 May 2014.

As far as is known, the Chinese government did not decrease its involvement in massive cyber espionage towards U.S. companies and (state) organisations. Among U.S. policy makers involved in this signalling operation, it was considered to be an experiment which had failed with no positive but only negative effects. Although one could argue that cultural differences played a role here, because in Chinese culture public accusations are considered to be very rude behaviour, various preceding non-public signalling efforts did not have any effect either.[11]

U.S.-North Korea, 2014-2015

The U.S. company Sony Pictures Entertainment experienced a major cyber-attack in 2014. Hackers released many confidential data stolen from the company's computers and implanted a software programme designed to erase all data from the company's network. The hackers first demanded financial compensation to stop their attack, while releasing more stolen information step-by-step. Later the hackers changed their demands and required the cancellation of the planned release of the feature film 'The Interview', a comedy about the assassination of the North Korean leader Kim Jong-Un. They also threatened cinemas which would show the film with terrorist attacks. Sony responded by cancelling the release, after which the hackers indeed ended their cyber-attack.

The U.S. government dealt with the cyber-attack on the private company as a national security matter because it considered the demand for the cancellation of a feature film to be an attack on the freedom of expression and thus the way of life in the U.S.[12] The Federal Bureau of Investigation (FBI) publicly stated that it had evidence (but refused to publish it) that the North Korean government was involved in the cyber-attack. Shortly thereafter, the U.S. enforced some (rather limited) economic sanctions against a few North Korean entities. Although the sanctions would not severely hurt the North Korean government, they were meant as a signal that this kind of cyber-attack would not be tolerated. The White House publicly stated: "We take seriously North Korea's attack that aimed to create destructive financial effects on a U.S. company and to threaten artists and other individuals with the goal of restricting their right to free expression."[13] In the same period, North Korea suffered from internet outages, but the U.S. government refused to comment whether this was caused by any covert retaliatory activity.[14]

North Korea has always denied any involvement in the Sony hack, and it is hard to see what effects this signalling operation has had so far.

These three cases show several difficulties in applying the foreign policy instrument of signalling towards cyber adversaries. In these examples signalling was used to show an adversary that was involved in cyber sabotage or espionage that this had been discovered and was not appreciated. In two cases, the adversary denied the signalled accusations, making use of the attribution problems in cyberspace. In the first two examples, the signalling did not have any positive effects, only negative ones (hampering cooperation and dialogue). In the last example, it is not known whether North Korea learned any lesson from the U.S. signalling, but at least no negative effects have been seen as yet. If one has to acknowledge anything positive in all three cases, it was that further escalation did not occur.

It is difficult to analyse why the signalling effort had little positive effects in these cases. One could for example argue that the communicated retaliating options could have been more powerful, but this would only

11 Interview with an official of the U.S. Department of Homeland Security who was involved in the operation, April 2015.

12 'Sony hack: White House views attack as security issue', *BBC World*, 19 December 2014.

13 Carol E. Lee and Jay Solomon, 'U.S. targets North Korea in Retaliation for Sony Hack', *Wall Street Journal*, 3 January 2015.

14 Dan Roberts, 'Obama imposes new sanctions against North Korea in response to Sony hack', *Guardian*, 2 January 2015.

be speculation (and might have caused an escalation). The signalling effort may also have come too late, during or after the cyber aggression had already escalated instead of (shortly) before this.

On the other hand, it is possible to argue that the signalling efforts in these cases had a positive, though hard to define, result: at least the adversaries did not increase their cyber aggression. This assumption, however, shows a key problem with any prevention or deterrence policy: is the absence of something undesirable caused by the prevention or deterrent efforts, or would it be absent anyway? The only conclusion that can be drawn based on these three cases is that the concept of signalling seems to be useful in the cyber security realm, but that it is difficult to measure whether its application has been effective.

Conclusions & Recommendations

Signalling might be an effective foreign policy instrument to change the cost-benefit calculations of states engaging in or sponsoring cyber aggression activities. While especially cyber espionage and cyber sabotage are currently considered to be cheap, almost non-risk activities, the instrument of signalling may make them less anonymous and risk-free.

Signalling, or 'naming and shaming', may make states conducting or sponsoring cyber aggression aware that these activities are being thoroughly followed and may result in retaliation. Public signalling may also damage the international reputation of a state, with potential political and economic consequences. Moreover, the instrument of signalling provides foreign policy makers with an extra escalation level, with only psychological effects, before the next level of retaliatory activities. Such an extra, but to some extent risk-free escalation level could be an important contribution to international stability.

Nevertheless, effective signalling in the cyber realm encounters some difficulties. First of all, the deterrent effect of signalling is most effective if combined with credible retaliation options. However, for retaliation – for example, via legal measures, sanctions, or (covert) counter-activities – generally precise evidence has to be provided. Because of the often difficult attribution in cyberspace and the reluctance of intelligence services to damage future cyber intelligence operations by disclosing too much of their methods, retaliation options based on credible evidence may be difficult to apply. States can quite easily deny the signalled behaviour, as was seen in the cases described above (although the knowledge that their activities are being monitored may in itself already have some deterrent value). More investments in improving cyber attribution are required to strengthen the credibility of retaliation options. Moreover, retaliation must follow as soon as the adversary continues its signalled behaviour, which bears the risk of a vicious cycle of escalation.

Even despite these difficulties in effective signalling, more experiments with the instrument are advisable in the international cyber security arena. Little experience has been made public so far, although one cannot exclude that non-public cases of signalling have been successful. As long as there are no generally accepted rules and norms of state behaviour in the international cyber policy domain, signalling could provide a useful extra tool for foreign policy makers dealing with cyber aggression by state actors.

About Clingendael

Clingendael is the Netherlands Institute of International Relations. We operate as a think-tank, as well as a diplomatic academy, and always maintain a strong international perspective. Our objective is to explore the continuously changing global environment in order to identify and analyse emerging political and social developments for the benefit of government and the general public.

www.clingendael.nl

About the author

Sico van der Meer is a Research Fellow at the Clingendael Institute, specializing in international cyber security issues as well as the non-proliferation and disarmament of Weapons of Mass Destruction.