Clingendael
Netherlands Institute of International Relations

Policy Brief

Sico van der Meer & Frans Paul van der Putten

SEPTEMBER 2015

US Deterrence against Chinese Cyber Espionage

The Danger of Proliferating Covert Cyber Operations

Only a few months before two recent cyber attacks against the United States Office of Personnel Management were discovered, the US government had announced that it would retaliate against major cyber attacks. How will the US respond to the OPM attacks, for which it seems to hold China responsible? This Policy Brief discusses various options for deterring similar cyber attacks in the future. It concludes that covert cyber attacks against China appear to be the most likely US response. However, this Policy Brief also notes that such a course of action would be detrimental to international stability. Countries such as the Netherlands, which to an important degree depend on the United States for security, should urge Washington to refrain from seeking cyber deterrence through retaliation as long as the United States itself conducts similar cyber-espionage operations against China and other nations. Instead, those countries should work with the United States towards establishing norms that halt the proliferation of state-sponsored espionage and covert cyber operations across borders. Only with such norms in place can a strategy of deterrence against state-sponsored cyber attacks be effective.

1. Introduction

Two recent cyber attacks against the United States Office of Personnel Management (OPM) have put the US government in an awkward position. Only a few months before these attacks were made public in June 2015, US Defense Secretary Ash Carter announced an updated cyber strategy, according to which the United States would retaliate against major cyber attacks, either with cyber tools or by other means.[1] The OPM cyber attack is the first test case of this cyber strategy: how to respond to such attacks in the absence of clear and indisputable

1 See Phil Stewart, 'Pentagon's New Cyber Strategy Cites U.S. Ability to Retaliate', *Reuters.com*, 23 April 2015, available at http://www.reuters.com/article/2015/04/23/us-usa-pentagon-cyber-idUSKBN0NE0AS20150423 and *The DOD Cyber Strategy*, US Department of Defense, April 2015, p. 11 and p. 25, available at http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

evidence, and, hence, without running the risk of escalation of a tense relationship because of misplaced retaliation? More importantly, if the attacks can be traced indisputably to Chinese (governmental) origins, what kind of retaliation would then be adequate, acceptable and balanced, as well as establish a credible deterrent against future cyber attacks?

2. Deterring Cyber Attacks

The cyber attacks against the OPM resulted in the theft of personal information of more than 20 million Americans, mostly current and former officials of the US federal government. The American Federation of Government Employees believes that "the hackers are now in possession of all personnel data for every federal employee".[2] These data include names, addresses, birth dates, job and pay histories, and insurance and pension information. In most cases, the information stolen from the OPM derived from application forms of individuals who had applied for non-sensitive, public trust or national security positions since 2000, either as federal government employees or as contractors. In 1.1 million instances, the stolen data included the applicants' fingerprints.[3] According to *The New York Times*, the Obama administration believes that the Chinese government is behind this instance of cyber espionage, which it regards as being of such a large scale and serious nature that retaliation is required.[4] If this is the case, the attack would present a clear challenge to the Pentagon's cyber strategy.

It is very difficult to see whether and what kind of retaliation would be appropriate, especially if this is to achieve the purpose of deterring potential future attacks.

To what extent and in what ways the United States is capable of deterring large-scale cyber attacks is important not only for the United States itself, but also for US allies. As indicated by the Clingendael Institute in its recent report on deterrence against non-traditional security threats,[5] the means for countries smaller than the United States to deter major cyber attacks are limited. This applies to both deterrence by retaliation and deterrence by denial. Many US allies therefore depend to a considerable degree on the United States to deter large-scale cyber attacks on themselves.

The two OPM hacks differ from many other cyber attacks, in the sense that they were neither aimed at stealing commercial or military data, nor at inflicting direct damage. In fact, it is not very clear what they were aimed at. Until it is known definitively who stole these data, it is hard to determine the motive for the attacks. According to *The New York Times*, US officials are convinced that the attack was carried out or sponsored by the Chinese authorities, even though they have not formally accused China. Still, on one occasion, Director of National Intelligence James Clapper did publicly refer to 'China' as the perpetrator. Speaking at a conference, Clapper said China was the "leading suspect" in the attacks, and that, given the difficulty of the intrusion, "you have to kind of salute the Chinese for what they did."[6] Interestingly, the US government makes a distinction between intelligence operations for national security purposes and government sponsored cyber-espionage for

2 See Ken Dilanian, 'Union: Hackers Have Personnel Data on Every Federal Employee', *AP.org*, 12 June 2015, http://bigstory.ap.org/article/af77f567a4b74f128a4869031dc9add9/union-hackers-have-personnel-data-every-federal-employee.

3 Kristin Finklea, 'Cyber Intrusion into US Office of Personnel Management: In Brief', Washington, DC: Congressional Research Service, 17 July 2015.

4 See David E. Sanger, 'U.S. Decides to Retaliate Against China's Hacking'. In: *The New York Times*, 31 July 2015, available at: http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0.

5 Frans Paul van der Putten, Minke Meijnders and Jan Rood, Deterrence as a Security Threat Against Non-Traditional Threats; Clingendael Monitor 2015. The Hague: The Clingendael Institute, June 2015, available at: http://www.clingendael.nl/pub/2015/clingendael_monitor_2015_en/2_deterrence_as_a_security_concept_against_non_traditional_threats/.

6 Sanger, 'U.S. Decides to Retaliate Against China's Hacking'.

commercial gain.[7] The United States has (at least implicitly) acknowledged to be doing the first, which it calls legitimate, and has accused China of doing also the second, which it considers illegitimate.[8] The OPM hacks seem to fit the first category more than the second. Indeed, Michael Hayden, former director of both the NSA and the CIA said in an interview with *The Wall Street Journal* that "the current story is" the Chinese Ministry of Public Security was responsible for the OPM hacks and that "those [OPM] records are a legitimate foreign intelligence target. If I, as director of the CIA or NSA, would have had the opportunity to grab the equivalent in the Chinese system, I would not have thought twice, I would not have asked permission".[9]

Whether China is actually responsible cannot be determined on the basis of publicly available information. Should the Chinese government indeed have acquired personal data on a large number of US officials, this could provide Beijing with the possibility of stealing further information from government agencies through the use of false identities, or at least with an improved ability to monitor actions by the US federal bureaucracy. And if detection of the OPM hacks was planned, they could even have been Chinese retaliation for US cyber-espionage operations in China, such as those outlined in documents leaked by former contractor Edward Snowden.[10] In other words, the OPM hacks could have been partly aimed at deterring the United States from continuing its own cyber attacks against China.

As is well known, attribution is a fundamental issue with regard to cyber attacks. Without the ability to identify an attacker, deterrence is not possible. Obtaining complete certainty about the source of a cyber attack is often impossible.[11] And even if compelling evidence is found by US investigators, it may not be possible to bring this into the open without harming the future use of American intelligence instruments or sources. In the OPM case, US officials seem to believe that China is behind the cyber theft, but they have not disclosed any details on what they know about the attacker's identity. By retaliating against China, the United States risks escalation, as well as international condemnation of the retaliatory action.

3. Options for Retaliation

How could the United States respond to the recent cyber attacks against the OPM, for which it accuses China (although not formally)? The US cyber strategy states that the United States will retaliate against major cyber attacks, either with cyber tools or by other means. With no response to the cyber attack against the OPM, the credibility – and thus the deterrence function – of the cyber strategy may thus be damaged. The following overview discusses the main policy options that are relevant for retaliating and deterring major cyber attacks by foreign states, including their risk of escalation.

7 Shane Harris, 'Team Obama Knows China Is Behind the OPM Hack. Why Won't They Say So?'. In: *The Daily Beast*, 20 July 2015, available at: http://www.thedailybeast.com/articles/2015/07/20/team-obama-knows-china-is-behind-the-opm-hack-why-won-t-they-say-so.html.

8 David E. Sanger, 'With Spy Charges, U.S. Draws a Line That Few Others Recognize'. In: *The New York Times*, 19 May 2014, available at: http://www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html.

9 Jack Goldsmith, 'The United States' Feckless Cyber Deterrence Policy', *Lawfareblog.com*, 1 August 2015, available at: https://www.lawfareblog.com/united-states-feckless-cyber-deterrence-policy and 'Michael Hayden Says U.S. Is Easy Prey for Hackers'. In: *The Wall Street Journal*, 21 June 2015, available at: http://www.wsj.com/articles/michael-hayden-says-u-s-is-easy-prey-for-hackers-1434924058.

10 See David E. Sanger and Nicole Perlroth, 'N.S.A. Breached Chinese Servers Seen as Security Threat'. In: *The New York Times*, 22 March 2015, available at: http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

11 See Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks'. In: *Journal of Strategic Studies*, 38 (2015) 1-2, p. 4–37.

Option 1: Passive Deterrence

The first option is the least complicated, although it is not very realistic in the current situation: doing nothing directly towards China. The United States could simply acknowledge that its cyber security measures in this case were not adequate, but also communicate that lessons have been learned and that its security systems have been improved and will receive on-going attention. This option prevents any escalation; China cannot accuse the United States of retaliating against something that it wrongly blames China for without any evidence.

Improving cyber security measures acts as a so-called passive deterrent; raising the costs of any future cyber intrusions may lower the chance that they will occur. The risk, however, is that China (or whoever was responsible for the OPM attacks) will consider this response to be an invitation to continue its cyber-espionage activities on an even larger scale. If no negative consequences are involved, why not even raise these activities to a higher level? Deterrence by denial – as raising the barriers for potential enemies is often called – is only effective if it changes the costs–benefits calculus of these enemies. In this case, the attackers might consider it worthwhile increasing their efforts to surpass the improved cyber security measures.

Option 2: Diplomatic Protests

A largely symbolic response with hardly any risk of escalation could be diplomatic protests. Additionally, some Chinese officials could be expelled from the United States. China, however, may do the same in response. Although this kind of retaliation may damage China's international reputation to some extent, these actions would not be very harmful to China. This harmlessness in turn perfectly indicates the negative side of this policy option: it would probably not deter China – or any other cyber enemy – from continuing similar cyber attacks.

Option 3: Legal Measures

Legal action against Chinese organizations or individuals is another option. The United States has used this tool before: in 2014, five officers of the Chinese People's Liberation Army were indicted on the charge of theft of intellectual property from US-based companies via cyber espionage. As with diplomatic protests, however, legal measures are mostly of a symbolic nature. Indicted individuals can only be arrested when they visit the United States or a US ally, and organizations might just change their identity. Moreover, this option entails the risk that such a legal track could result in a court case in which the United States is forced to expose sensitive intelligence operations in order to provide the evidence. This would hurt more than it merits. Moreover, China might retaliate by starting 'symbolic' indictments of US organizations and individuals as well – US companies doing business in China could be especially vulnerable targets. Similar to option 2, this option may to some extent be damaging to China's reputation and suggest the United States' ability to identify cyber attackers; it is doubtful, however, whether this will have a deterring effect.

Option 4: Economic Sanctions

After the US government blamed North Korea for active involvement in the hacking of Sony Pictures Entertainment in 2014, it retaliated by strengthening existing economic sanctions against the North Korean regime. Such economic retaliation might have some value as a deterrent, especially for countries like China with an economy that is highly dependent on exports. However, once the sanctions are installed or strengthened, the sanctioned state has little reason to change its behaviour unless there are guidelines on how to ease or get rid of the sanctions. Far more important in the Chinese case is that the US economy is heavily dependent on interaction with China. If China was to retaliate with economic counter-sanctions, this would significantly hurt the United States as well, and one could question whether such economic damage would outweigh the deterrent effect regarding cyber attacks.

Option 5: Retaliation in Cyberspace

The threat of serious retaliation has proved to be an effective deterrent in history. By retaliating, the United States would show that future cyber intrusions of this scale will not be tolerated. The most obvious option regarding retaliation is to strike back in the

same dimension that the offender used – that is, cyberspace. The United States could, for example, try to steal and publish information from the Chinese government. A cyber attack to indicate that certain cyber infrastructures of the Chinese government could be paralyzed would also be an option, showing that the United States is capable of, and will not refrain from, starting offensive cyber operations in many ways. However, a serious risk emerges here of starting a cycle of escalation.

Option 6: Military Retaliation

An almost unrealistic option is retaliation through conventional military means, such as a strike against a specific location that is related to Chinese cyber forces. Such an action would probably trigger a military response from the Chinese and could culminate in a dangerous process of escalation. This option seems likely to be considered only in the case of more destructive cyber attacks, and/or if the country involved is less powerful than China.

Option 7: Covert Retaliation in Cyberspace

A final option is the use of covert retaliation in cyberspace. It is the invisibility, and therefore unpredictability, of covert retaliation that might deter China – *if* it attacked the OPM in the first place – from conducting similar cyber attacks. On the other hand, this option still carries with it the risk of escalation; China might respond with covert operations against US targets, or with retaliatory actions in other domains, such as hurting the United States economically.

All of these options are to some extent problematic, almost all of them carry a risk of escalation, and none of them may be truly effective in deterring future cyber attacks. Yet if no action is taken, the credibility of the US cyber security strategy diminishes. Although the United States has not formally accused China, the fact that major Western media believe that the US government thinks that China is the perpetrator already raises questions regarding the feasibility of deterring Chinese cyber attacks. In this context, Washington might decide that covert retaliation through cyber means is the most appropriate type of response. One of the possible targets mentioned in *The New York Times*' report involves undermining the Chinese government's ability to censor the use of the internet by Chinese citizens. Adam Segal of the Council of Foreign Relations outlined three possibilities for such a retaliatory act: expose information to embarrass the Chinese authorities; allow Chinese citizens to access blocked foreign websites; or undermine restrictions on domestic flows of information on the internet.[12] Of course, a combination of two or three of these options could also be possible.

4. Repercussions of US Retaliation against China

A major US cyber operation aimed at threatening key interests of the Chinese government, even if covert and well calibrated, could have serious consequences. In the short term, it would carry the risk of provoking Chinese counter-attacks that would destabilize the already complex Sino–US relationship. In addition to the existing risk of an (inadvertent) military incident in the South or East China Sea, further insecurity and volatility would result from even a limited and covert cyber conflict. Moreover, if other countries observe that the United States is likely to be conducting covert cyber operations against China as a retaliatory measure, in the longer run the use of covert cyber attacks by states against other states may become a *de facto* accepted norm. Both developments are dangerous and would contribute to less stability and more insecurity in the international system. While it is questionable whether cyber deterrence can actually be achieved in this instance, except perhaps at a very high cost, it seems clear that retaliation carries major risks. This makes it more difficult for the United States to act, thereby undermining the credibility and effectiveness of its cyber security strategy.

12 See Adam Segal, 'Retaliating Against China's Great Firewall', *Council on Foreign Relations*, 3 August 2015, available at: http://blogs.cfr.org/cyber/2015/08/03/retaliating-against-chinas-great-firewall/.

A more credible strategy of cyber deterrence, which could be extended to US allies and thus strengthen the alliance system, would result from a greater focus on how the United States deals with the issues of attribution and norms. At the moment, either the US government has no reliable evidence that China is behind the OPM thefts, or it does have such evidence but it cannot disclose this without damaging the intelligence instruments with which the evidence was collected. In the latter case, the United States should at least say so and build up a track record of making credible statements on suspected cyber attackers, which should be supported by publicly available evidence as soon as possible. Moreover, if the US government no longer promoted the notion that foreign intelligence-gathering for national security purposes is legitimate (and at least scaled down its intelligence operations against foreign governments), it would become easier to take action in instances such as the OPM breach. While the danger of escalation would still be there, this would open the way for the United States to take overt rather than covert measures against China (assuming that the Chinese government is indeed responsible and that the United States has evidence of this).

At first sight, the costs of such a course of action may seem high, given the benefits that Western intelligence communities have long enjoyed because of their superior technological and financial resources. Yet the United States and its allies should ask themselves whether, in a world in which cyber attacks and cyber espionage are becoming ever more damaging and within closer reach of new actors, their national security interests are better served by a proliferation of state-sponsored espionage and covert cyber operations, or by norms that aim at limiting such activities.

5. Conclusion

The OPM case perfectly shows the problems that are involved in deterring large-scale, anonymous cyber attacks. Although various options for retaliation are available, none of them is perfect. They all carry the risk of escalation or, if not, they have too little value as a deterrent. For the US government, a covert cyber operation against China may appear to be the most attractive option, and this may therefore be the most likely course of action that Washington is currently contemplating or preparing. Yet beyond the obvious danger of escalation into a Sino–US conflict, there is also the risk that covert retaliation against foreign governments that are suspected of being behind cyber attacks becomes a norm in international relations.

The fact that even the United States, the leading major power, finds it hard to respond to a major breach of its cyber security shows that less powerful states will have even more problems in deterring and retaliating against cyber attacks. Countries such as the Netherlands, which to an important degree depend on the United States for their security, should urge Washington to refrain from seeking cyber deterrence through retaliation as long as the United States itself conducts similar cyber-espionage operations against China and other nations. Instead, these countries should work with the United States towards establishing norms that halt the proliferation of state-sponsored espionage and covert cyber operations across borders. Only with such norms in place can a strategy of deterrence against state-sponsored cyber attacks be effective.

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 authors

Sico van der Meer is a Research Fellow at the Clingendael Institute, specialising in international cyber security issues, as well as the non-proliferation and disarmament of weapons of mass destruction.

Frans Paul van der Putten is a Senior Research Fellow at the Clingendael Institute. His work relates to security, geopolitics and China's rise as a great power.