Clingendael
Netherlands Institute of International Relations

Policy Brief

Sico van der Meer

SEPTEMBER 2015

Foreign Policy Responses to International Cyber-attacks

Some Lessons Learned

How could foreign policy instruments be helpful in responding to major cyber-attacks? This policy brief provides a first exploration of this topic by investigating five cases of international cyber-attacks which had a great deal of societal impact. What role did foreign policy instruments play in the responses to these cyber-attacks, and how can we evaluate their role in hindsight? The policy brief concludes that, although cyber technicians will always be in the lead when a massive cyber-attack occurs, foreign policy instruments such as diplomatic communication, warnings, and sanctions could contribute to limiting the damage of a cyber-attack as well.

Introduction

Responding to major international cyber-attacks is generally considered a task for cyber technicians: they have to end the attack by protecting the targeted networks and to try to collect evidence on the identity, methods and aims of the attackers. While acknowledging that the technical level is indeed crucial, foreign policy could play an important (supporting) role as well in responding to major international cyber-attacks. Nearly all cyber-attacks originate from abroad, and foreign policy may be helpful in sending important signals to the attacker. In what way could foreign policy tools be helpful to respond to cyber-attacks?

This policy brief provides a rudimentary exploration of this topic by investigating five cases of major international cyber-attacks: Estonia 2007, Saudi Arabia 2012, the United States 2012, South Korea 2013, and the United States 2014. What were the foreign policy responses to these cyber-attacks, and how can we evaluate them in hindsight? These five cases have been chosen because they were 'big' given their societal impact, while not being part of a more classic military operation (such as the cyber-attack on Georgia in 2008, which coincided with a Russian conventional military attack).

Analysing cyber-attacks and responses by countries is a challenge in view of the secrecy concerning (the effectiveness of) countermeasures. Governments do not want to provide (possible) enemies with insights into their cyber defence policies. Moreover, they do not want to be too precise about potential responses to cyber-attacks in order to prevent setting red lines that, if crossed, might oblige them to act, with an undesired

escalation as a result. Given this sensitivity and secrecy, it is not surprising that little academic literature has been published on this subject. Interviews with diplomats involved also proved hard to arrange. The analysis provided here is thus primarily based on information that is available in the public domain, mainly media reports. Considering these facts, and the posture of the governments involved in the five cases in not bringing their response policies into the open, this policy brief can give no more than a glimpse into the foreign policy activities involved. These limitations notwithstanding, the information available provides a basis for some lessons learned that may help in formulating foreign policy responses to the relatively new phenomenon of cyber-attacks against a country.

Estonia 2007

In April 2007 Estonia experienced a cyber-attack targeting large parts of the country's cyber infrastructure. This cyber-attack – shutting down the websites of ministries, banks, media, and political parties, thereby suggesting an attempt to paralyze Estonia's society – consisted of a wave of so-called Distributed Denial of Service (DDoS) attacks, by which public websites suddenly receive tens of thousands of visits, thus disabling them by overcrowding the bandwidths for the servers running the sites. Although the attacks came from all over the world, Estonian officials and computer security experts claimed that, particularly in the early phase, some attackers were identified by their internet addresses, many of which were Russian, and some of them could be traced back to Russian state institutions.[1] Even while considering that Estonia is a highly cyber-dependent country where, for example, 97 percent of all bank transactions are conducted online, the attack was not able to effectively paralyze the country. It caused economic damage and annoyance, but nothing more.[2]

The governmental response to the cyber-attack was mainly executed by the Computer Emergency Response Team (CERT), linked to the Ministry of Economic Affairs and Communications. The CERT reacted especially by closing down the websites under attack for foreign internet traffic, in an attempt to keep them accessible to domestic users. The CERT received assistance and intelligence from cyber security experts from various European countries in order to restore the normal cyber network situation, and additional assistance was provided by NATO CERTs and the European Network and Information Security Agency (ENISA) of the European Union.[3]

The role of the Estonian Ministry of Foreign Affairs in the response was limited, according to the public information that is available. Interesting, however, was a public statement by the Minister of Foreign Affairs, Urmas Paet, shortly after the start of the cyber-attack. He claimed 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".[4] The accusation linked the cyber-attack to the relocation of a Soviet-era war memorial in Tallinn which had caused tensions in diplomatic relations between Estonia and Russia during the preceding days, as well as riots by members of the Russian minority in Estonia. The public accusation, probably meant to force Russia to end its involvement by focussing international attention on Moscow's role, did not have much effect. Russia simply denied the accusation and

1 Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia'. In: *The Guardian*, 17 May 2007.

2 Andrzej Kozlowski, 'Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan'. In: *International Scientific Forum Proceedings*, 3 (2013), p. 236-246.

3 Stephen Herzog, 'Revisiting the Estonian Cyber-attacks. Digital Threats and Multinational Responses'. In: *Journal of Strategic Security* 4 (2011) 2, p. 49-60.

4 Cited in: Kertu Ruus, 'Cyber War I: Estonia Attacked from Russia'. In: *European Affairs* 9 (2008) 1-2.

warned Estonia against making accusations without any evidence – and thus pointing at the problem of the attribution of cyber-attacks; formal Russian involvement was almost impossible to prove. The attacking IP addresses that Estonia tracked down to the Russian government could well have been hijacked 'zombie' computers. Moreover, the public accusation by the Minister of Foreign Affairs gave Russia an argument for not helping in any way in the aftermath of the cyber-attack. Russia refused to cooperate with the Estonian authorities in investigating the case. When various attackers within the jurisdiction of the Russian Federation were identified, the Estonian State Prosecutor made a formal investigative assistance request, which was rejected by Moscow with the argument that procedural problems prevented cooperation.[5]

The Estonian Ministry of Foreign Affairs furthermore played a role in raising the cyber-attack issue with its diplomatic and political network in the European Union and NATO, in collaboration with the Ministry of Defence and the Office of the President.[6] These activities were mostly effective in the longer term, for example by increasing attention for cyber security in these fora, as well as significant investments in the NATO Cooperative Cyber Defence Centre of Excellence in Estonia in later years.

Saudi Arabia 2012

Saudi Arabia experienced a cyber-attack in August 2012. Actually, the attack was targeted towards one specific company only, but also the biggest company in the country: the state oil company Saudi Aramco. More than 30,000 computers were damaged by the attack, not only in Saudi Arabia but also in foreign offices like the ones in The Hague and Houston.[7] The hardware of about 85 percent of the company's computer devices was said to be disrupted.[8] The cyber-attack appeared to be aimed at disrupting oil and gas production in Saudi Arabia and oil exports to the rest of the world; if successful, this would not only have severely damaged the Saudi economy, but could have created global economic disturbance as well. However, the attack failed to actually disrupt the flow of Saudi oil and gas. Saudi Aramco claimed that the huge damage was limited to office computers and did not affect systems being used for technical operations.

The cyber-attack made use of a computer virus known as 'Shamoon' and a group of hackers, until then unknown, claimed responsibility, blaming Saudi Arabia for "crimes and atrocities" in countries like Syria and Bahrain. In the months prior to the cyber-attack, Saudi Arabia had supported rebel groups in Syria and had sent troops into Bahrain to back its rulers, fellow Sunni Muslims, against Shiite-led protesters.

As far as can be reconstructed from open sources, the Saudi Ministry of Foreign Affairs was not directly involved in the response to the cyber-attack. Saudi Aramco itself led the way in countering the cyber-attack. The company shut down its internal network for more than a week in order to stop the spread of the virus and to restore or replace all infected computers. Next to the state-owned company itself, it was the Ministry of Interior which dealt with the cyber-attack at the governmental level; the cyber-attack was apparently considered to be a domestic affair, even though the Ministry of Interior issued a statement during a press conference that the attack originated from several other countries (while declining to identify these countries).[9] The Ministry of Interior especially assisted Saudi Aramco in investigating the

5 Ruus, 'Cyber War I: Estonia Attacked from Russia'.
6 Traynor, 'Russia Accused of Unleashing Cyberwar to disable Estonia'.
7 Christopher Bronk and Eneken Tikk-Ringas, *Hack or attack? Shamoon and the Evolution of Cyber Conflict*, Working Paper, James A. Baker III Institute for Public Policy, Rice University, 1 February 2013.
8 'Saudi Aramco Investigating Origins of Shamoon Virus Following Attack'. In: *Al Arabiya*, 12 September 2012.
9 Wael Mahdi, 'Saudi Arabia says Aramco Cyberattack came from Foreign States', *Bloomberg*, 9 December 2012.

origin and damaging effects of the attack.[10] The results of this investigation have never been made public. Although some experts and media speculated that the government of Iran was the actual perpetrator of the cyber-attack, neither Saudi Aramco nor the Ministry of Interior have ever openly blamed any country.[11] It is conceivable that the Saudi government deliberately tried to deal with the cyber-attack as a domestic issue and to give it as little publicity as possible in order to limit the damage to its state company's reputation, as well as to prevent any potential further escalation by the cyber-attacker.

United States 2012

Only one month after the cyber-attack in Saudi Arabia, in September 2012 the United States experienced a major cyber-attack as well. According to some media, this was "the biggest cyber-attack in history".[12] Although that claim may be questionable, the attack definitely caused some nuisance in the United States. A DDoS attack, directing huge amounts of internet traffic at a website to make it crash, was launched against the websites of six of the nation's leading banks. Although this did not affect the computer networks of the banks themselves, the websites suffered day-long slowdowns and were sporadically not accessible to the attacked banks' customers. This caused frustration more than economic damage, but if the attacks would have been more sophisticated and would have lasted longer, one could speculate that they might have caused more economic damage.[13] An Islamist cyber-fighters group claimed responsibility for the cyber-attack, but various experts and politicians considered that the attack was too complicated to be executed by a non-state actor. Fingers were almost immediately pointed at Iran, which was assumed to be seeking revenge in this way for the US-led economic sanctions against the country as well as the Stuxnet cyber-attack on Iran's nuclear installations some years earlier, for which Tehran also blamed the US.[14]

The cyber-attack was mainly dealt with by the targeted banks themselves, in cooperation with cyber security companies hired by them – the banks are reported to have spent tens of millions of dollars to cope with the attack.[15] They were assisted, however, by experts from various ministries and governmental agencies, such as the Department of Homeland Security, the State Department, the National Security Agency and the Cyber Command of the US Armed Forces. According to some media reports, the Obama administration considered but ultimately rejected an option to hack into the adversary's network – assumed to be in Iran – and crush the problem at its source. Also considered but rejected was a diplomatic instrument: delivering a formal warning to Iran through diplomatic channels. Both options are reported to have been rejected out of fears that they could escalate hostilities to undesired levels.[16]

The governmental actors involved instead chose a response that was partly diplomatic, and partly technical. The diplomatic channels of the State Department were used to appeal for assistance to 120 countries, asking them to remove identified malicious computer codes from the servers around the world that were being used as springboards for the attacks. Christopher Painter, the State Department's coordinator for cyber issues,

10 Mahdi, 'Saudi Arabia says Aramco Cyberattack came from Foreign States'; 'Aramco says Cyberattack was Aimed at Production'. In: *The New York Times*, 9 December 2012.
11 Bronk and Tikk-Ringas, *Hack or attack? Shamoon and the Evolution of Cyber Conflict*.
12 David Goldman, 'Major Banks hit with Biggest Cyberattacks in History', *CNN Money*, 27 September 2012.
13 Nicole Perlroth, 'Attacks on 6 banks Frustrate Customers'. In: *The New York Times*, 30 September 2012.
14 Goldman, 'Major Banks hit with Biggest Cyberattacks in History'.
15 Ellen Nakashima, 'U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks'. In: *The Washington Post*, 11 April 2014.
16 Nakashima, 'U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks'; Ellen Nakashima, 'U.S. Response to Bank Cyberattacks Reflects Diplomatic Caution, Vexes Bank Industry'. In: *The Washington Post*, 27 April 2013.

said in a later interview: "The pitch was, 'We're making a request of you, and we would really like your help. You have just as much of an interest in taking action because these are compromised machines. Please do what you can to mitigate this threat'."[17] It was not only the diplomats of the State Department who raised the issue with their counterparts around the world; the cyber technicians of the Department of Homeland Security also contacted their foreign counterparts with the same request. Although this multinational mobilization did not end the cyber-attacks, it diminished their effects considerably and gave the cyber technicians within the banks and their hired cyber-security consultants more room to lessen the consequences of the attack as well.[18]

South Korea 2013

South Korea regularly experiences cyber-attacks, generally attributed to North Korea – according to some sources North Korea carries out several cyber-attacks (large and small) every day against its southern neighbour.[19] In March 2013, the largest cyber-attack so far was carried out against South Korea. Malware called 'DarkSeoul' appeared to be specifically designed to evade some of South Korea's most popular antivirus programmes and to render computers unusable. The attack was targeted at paralyzing three major banks and three national television broadcasting stations. In particular the effects of the attack on the banks had a serious impact: ATMs, payment terminals and mobile banking systems throughout the country stopped functioning. The effect on the media was less visible, because TV broadcasts were not affected; the attack only created chaos in the offices of the television networks. The cyber-attack incapacitated some 48,000 computers and caused approximately 800 billion Won (600 million Euro) of economic damage.[20] Although most damaged computer networks had already been restored after one or two days, the malware attacks went on for several more weeks, without however causing much more disruption.

No responsibility for the cyber-attack was claimed, but it was generally assumed that North Korea was behind it. The attack came shortly after North Korea had reacted furiously to tightened United Nations Security Council sanctions in response to its latest nuclear test. A week before the attack the government in Pyongyang accused the United States and South Korea of conducting cyber-attacks against North Korea, which was probably meant to make the cyber-attack on South Korea seem like a retaliatory attack. Initially, the source of the cyber-attack was linked to an IP address in China, but both the Korea Communications Commission and the Chinese Ministry of Foreign Affairs stated that hackers from other countries could have routed their attack through this address to obscure their identity. Later it was reported that the trace could indeed be followed back from this Chinese IP address to a North Korean one.[21]

While the targeted banks and broadcasting stations primarily dealt with restoring their computer networks themselves, the governmental response to the cyber-attack was executed by various ministries and governmental organisations. An emergency security meeting was convened by the Minister of Defence, and the military raised their alert against cyber-attacks. The Ministry of Defence was also involved with press communications. The Ministry refused to

17 Quoted in: Nakashima, 'U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks'.

18 Nakashima, 'U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks'; Nakashima, 'U.S. Response to Bank Cyberattacks Reflects Diplomatic Caution, Vexes Bank Industry'.

19 Alex Hern, 'North Korean "Cyberwarfare" Said to have Cost South Korea £500m'. In: *The Guardian*, 16 October 2013.

20 Nicole Perlroth and David E. Sanger, 'Cyberattacks Seem Meant to Destroy, Not Just Disrupt'. In: *The New York Times*, 28 March 2013; 'South Korea Blames North for Bank and TV Cyber-attacks', *BBC News*, 10 April 2013; Hern, 'North Korean "Cyberwarfare" Said to have Cost South Korea £500m'.

21 'China IP address Link to South Korea Cyber-attack', *BBC News*, 21 March 2013; 'South Korea Blames North for Bank and TV Cyber-attacks'.

accuse anyone of the cyber-attack; the official statement read: "We cannot rule out the possibility of North Korean involvement, but we don't want to jump to a conclusion."[22] Police teams were sent to affected sites, especially to prevent chaos because of paralysed ATMs and payment terminals. The civil Korea Communications Commission asked government agencies and companies to triple the number of people monitoring for possible hacking attacks on their computer networks as well, while the Office of the President established a governmental task force, led by the Ministry of Science, ICT and Future Planning, to investigate the cyber-attack and its effects. This governmental task force would later conclude that most of the evidence that could be found pointed towards North Korea. It discovered traces of IP addresses based in North Korea preparing the attacks for months and implanting malware inside the banks' computer networks.[23] In media reports no mention was made of any foreign policy activities regarding the cyber-attack; apparently the government tried to deal with the cyber-attack within the domestic context in order to prevent a further escalation with its long-time enemy in the North.

United States 2014

The US company Sony Pictures Entertainment was the target of a major cyber-attack in 2014. Hackers, operating under the name *Guardians of Peace*, had presumably been active in the company's network for months and in November 2014 they released many confidential data stolen from the company's computers – varying from financial data to embarrassing e-mails sent by top managers. They also implanted a software program designed to erase all data from the computer servers. The hackers demanded financial compensation to stop their attack, while releasing more stolen information step-by-step. In December, however, 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 planned to show the film with terrorist attacks. Sony responded by cancelling the release of the film, after which the hackers indeed ended their cyber-attack.[24]

Although the cyber-attack on Sony was initially not regarded as a massive attack with a major societal impact, the US government stepped in after the demand to cancel the release of 'The Interview'. The government announced that it now regarded the hacking as a serious national security matter, because, as the Secretary of Homeland Security stated: "The cyber-attack against Sony Pictures Entertainment was not just an attack against a company and its employees. It was also an attack on our freedom of expression and way of life."[25] President Obama openly called Sony's decision to cancel the film "a mistake" (Sony later distributed the film to a limited number of cinemas and published it online).[26]

Although many media linked the cyber-attack to North Korea – which had previously officially protested against the film – the US government initially refused to name any country which was potentially involved. A few days after the cancellation of the film, however, the Federal Bureau of Investigation (FBI) formally stated that it had evidence that

22 Cited in: Choe Sang-Hun, 'Computer Networks in South Korea are Paralyzed in Cyberattacks'. In: *The New York Times*, 20 March 2013. See also: Tania Branigan, 'South Korea on Alert for Cyber-attacks after Major Network Goes Down'. In: *The Guardian*, 20 March 2013.

23 Choi He-suk, 'Seoul Blames Pyongyang for Cyber-attacks'. In: *Korea Herald*, 10 April 2013; Jeyup S. Kwaak, '"Dark Seoul" Behind some Cyberattacks in South Korea. In: *The Wall Street Journal*, 27 June 2013.

24 Ben Child, 'Hackers Demand Sony Cancel Release of Kim Jong-un-baiting Comedy'. In: *The Guardian*, 9 December 2014.

25 'Sony Hack: White House Views Attack as Security Issue', *BBC World*, 19 December 2014; Statement by Secretary Johnson on Cyber-attack on Sony Pictures Entertainment, Department of Homeland Security, 19 December 2014.

26 'Obama Pledges Proportional Response to Sony Hack'. In: *The New York Times*, 19 December 2014.

the North Korean government was involved in the cyber-attack. North Korea has always denied any involvement.

According to media reports, the US government was looking for a retaliatory action of a symbolic nature to show North Korea (and other states) that cyber-attacks on US companies will not be tolerated, while at the same time preventing any international escalation.[27] Retaliation came, a few weeks later, with some rather limited economic sanctions against North Korean entities. According to the Treasury Secretary these sanctions were meant to defend US businesses and citizens from "attempts to undermine our values or threaten the national security of the United States".[28] A statement from the White House added: "We take seriously North Korea's attack that aimed to create destructive financial effects on a US company and to threaten artists and other individuals with the goal of restricting their right to free expression."[29] In the same period, North Korea suffered from internet outages, but the US government refused to comment whether this was caused by any covert US retaliatory action.[30]

Conclusion

This brief analysis of five major cyber-attacks in recent years indicates that governmental responses to cyber-attacks vary widely. In Saudi Arabia and South Korea the cyber-attack was more or less treated as a domestic affair, with no foreign policy instruments involved. Only in the Estonian and US cases were diplomats from the Ministry of Foreign Affairs directly involved, as far as can be found in open sources.

An important foreign policy instrument being deployed was the use of diplomatic channels to request assistance from other countries. Especially US diplomats in 2012 contacted their counterparts with a very focussed question, requesting that malicious computer codes be removed from specific servers in each country that was approached. This diplomatic effort, combined with the cyber technicians of the Department of Homeland Security, who also contacted their foreign counterparts with the same request, had an effect almost directly; the cyber-attack was weakened every time a country cleaned servers which the attackers were using. In the Estonian case the diplomatic request for help was a little less focussed; most of the direct cyber assistance from abroad was involved through the network of the cyber experts in the Estonian Computer Emergency Response Team. The diplomatic channels were particularly useful for agenda-setting in the somewhat longer term.

In 2012 the United States also considered, but rejected, another foreign policy instrument: delivering a formal warning to Iran through diplomatic channels. This option was rejected because of the lack of convincing evidence for a formal accusation and the risk of causing an undesired escalation. From this perspective, the diplomatic warning option was somewhat similar to what the Minister of Foreign Affairs in Estonia did after the cyber-attack on his country had started: he publicly blamed Russia, presumably in the hope that this country would end its involvement as soon as it was openly accused. This public accusation did not have any positive effect, however. Russia simply denied that it was responsible and refused any cooperation when Estonia wished to prosecute identified Russian individuals involved in the cyber-attack. It is difficult to say whether the public accusation had any negative effects (Russia might have refused to cooperate in the prosecution anyway), but the lack of any positive effects seems rather obvious.

In 2014 the US deployed the foreign policy instrument of economic sanctions against North Korea, which was publicly blamed by the US government as being guilty of the cyber-attack against Sony. Limited economic sanctions were meant to send a

27 Danny Yadron, Devlin Barrett and Julian E. Barnes, 'U.S. Struggles for Response to Sony Hack'. In: *The Wall Street Journal*, 18 December 2014.

28 Carol E. Lee and Jay Solomon, 'U.S. Targets North Korea in Retaliation for Sony Hack'. In: *The Wall Street Journal*, 3 January 2015.

29 Lee and Solomon, 'U.S. targets North Korea in Retaliation for Sony Hack'.

30 Dan Roberts, 'Obama Imposes New Sanctions Against North Korea in Response to Sony Hack'. In: *The Guardian*, 2 January 2015.

signal to North Korea (and potential other cyber-attackers) that similar attacks would not be tolerated. Economic sanctions were thus used as a deterrent by retaliation. It should nevertheless be emphasized that public accusations and retaliations may only be effective (and not cause an escalation) if the sanctioning state is more powerful than the sanctioned party. As was seen in the Estonian case, where the accused state is more powerful than the accusing state, proactive blaming (and/or retaliating) may not always be the best option.

In general, foreign policy responses to cyber-attacks seem to be most effective in the domain of requesting international assistance, as long as the requests are focussed and aimed at direct actions. Moreover, foreign policy tools can be useful after the cyber-attack: by diplomatic warnings and (economic) sanctions signals can be sent that similar attacks will not be tolerated; in this way the foreign policy tools are not directly used to respond to the cyber-attack at hand, but instead as a deterrent to prevent more of these attacks.

Overall, foreign policy can mainly be regarded as supporting instead of leading. Based on the experiences analysed here, the initial response to a massive cyber-attack is probably best coordinated by the more technical cyber experts, often organized in a specialized governmental agency like a CERT. Diplomats could play an important supporting role, which of course requires excellent communication channels with the coordinating cyber experts. The more intergovernmental cooperation and communication, the more effective the response to any cyber-attack will be.

More research could be helpful to determine under which circumstances and at what stage during a cyber-incident foreign policy instruments can be most effectively employed to put pressure on a suspected adversary, to request assistance from other countries, or to seek redress through the appropriate international fora. Furthermore, it would be interesting to explore how such diplomatic communications could be strengthened by basing them on references to existing norms of responsible behaviour and obligations as established in international law. Last but not least, while this policy brief focuses on *responses* to cyber-attacks, more research into foreign policy instruments that could help in *preventing* cyber-attacks could definitely be useful as well.

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. His main research topics are cyber security, and the non-proliferation and disarmament of Weapons of Mass Destruction. He graduated from the Radboud University Nijmegen in 1999 with a Master's degree in History. Before joining the Clingendael Institute, he worked as a journalist and as a Fellow of a think tank on civil-military relations.