Informative Document

13/2013 24th April 2013

Mª José Caro Bejarano

SOME REFLECTIONS ON CYBERWAR

This document has been translated by a Translation and Interpreting Degree student doing work experience, CRISTINA STOLPOVSCHIH, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.

SOME REFLECTIONS ON CYBERWAR

Abstract:

The recent cyber-attacks on South Korea are the basis for considering the possibility of facing a cyberwar or whether cyber conflict is simply used as an additional mechanism to conventional conflict. Public-private collaboration is needed to face cyber conflict, as many of the targeted resources are owned or managed by the private sector.

Keywords:

Cyberwar, cyber-attack, cyber conflict.

SOME REFLECTIONS ON CYBERWAR

One of the cases of risk contemplated in the eighth edition of the Global Risks Report (Global Risks 2013) presented last January by the World Economic Forum (WEF[1]) is at the centre of a constellation of technological and geopolitical risks that vary from terrorism to cyber-attacks and the failure of global governance. This case is called "digital uncontrolled fire in a hyper connected world" about the massive disinformation extending via Internet. This risk examines how hyper connection could allow a digital fire that creates chaos in the real world. This case considers the challenge presented by the wrong use of an open and easily accessible system as the Internet and the greatest danger of misguided attempts to avoid such results.

Last week, President Barack Obama convened 15 main U.S. financial leaders to the White House to discuss what its government believes to be the more penetrating, more persistent and less manageable threats – the cyber-risks.

Unlike the nuclear threat, where some governments actually faced other governments, now "the financial sector, companies and their knowledge is a new battlefield."

In this new world, cyber conflicts are a reality, but no one has written the rules about how the responsibility between the government and the private sector should be managed.

Unlike the typical national security crises, the private sector controls most of the resources that can decisively resolve the cyber conflicts. The Government maintains the general responsibility of the national cyber defence; however, it has not developed doctrines of response. There is some limitation in public administration due to its internal processes, competing interests and lack of experience in solving issues of national security, in collaboration with the private sector.

A group of prominent cyber strategists performed a simulation illustrating how quickly a cyber conflict could escalate from initial tensions into something more serious. The meeting[2] demonstrated how often the administration of government and the private sector fail to communicate effectively, or to act jointly to deal with a threat to national security that can only be dominated together.

[1] See www.weforum.org. Global Risks 2013, eight edition.

[2] The simulation was convened by the Atlantic Council and the private enterprise SAIC.

The simulation consisted of a DDoS or distributed denial of service on U.S. financial institutions launched earlier this year. These attacks followed the scheme of the attacks produced last summer that used a malicious code to erase data from around 30,000 computers from the Saudi Aramco company.

This cyber simulation allowed collecting, following the development of a fictional situation, a number of conclusions and recommendations to react to a situation of this sort.

Among the conclusions, its highlighted that, although all too often, the government wants to solve the cyber conflicts by itself, as it does in most national security crises, in this type of scenario the collaboration with the private sector is essential. In fact, there are few cyber conflicts in the last 25 years that have been resolved decisively by governments, according to Jason Healey, director of the Atlantic Council Cyberstatecraft Initiative.

To resolve most cyber crises, it is necessary to combine the agility and the experience of the private sector, which in addition, also usually, has access to the means to do so. The government lacks these virtues, although it knows the general context of the attack and it has huge resources of espionage and funding, and it controls the levers of traditional economic, diplomatic and military powers.

These past months have shown that such discussions are not theoretical. Obama's message to the financial sector was clear: *Before things get even more serious, the government and the private companies together should do more to prepare for the inevitable future cyber conflicts*.[3]

Moreover, the study of recent cyber-attacks on South Korea highlights four truths about cyber conflicts, once they have been analysed. The implications of three of them are obvious, the fourth is not so yet: 1) cyber conflicts are detrimental, 2) but are far from the war, 3) cyber conflicts are increasingly easier to predict and the nation responsible for them is often perfectly obvious, 4) however, to stop this kind of asymmetric attacks, sometimes a traditional approach must be used.

The cyber conflicts analysed are the ones that took place in March 2013. On that time, the South Korean teams of financial, energy and media sectors suffered a sophisticated attack that affected the ATMs and websites offline. Initially the attacks seemed to be a typical denial of service, in which the networks were flooded by the traffic, which turned them out of service.

[3] For more information see the article *Seeking to Avert Cyber War* by Frederick Kempe, President and CEO of the Atlantic Council.

At first, even the large DDoS attacks are easy to launch, as the criminal groups are able to get the necessary capacity by simply renting it for hours, and therefore, do not need the so-called cyber-warriors. At a second stage, it was noted that the attacks had a more interesting and dangerous component, since the data of the computers attacked with the erasure of their hard disk was destroyed.

Despite that, this disruption was not a long lasting one neither of a lethal nature since the systems recovered in some days and even hours. And this is, in fact, the cyber conflicts rule, not the exception.

The study carried out by the Atlantic Council and the Cyber Conflict Studies Association on the history of the cyber conflict, has not found a single case in which someone has been killed by a cyber conflict. Cyber conflicts may be relatively easy to implement, but is also quite easy to recover from them. The affected resources can be replaced quickly. The inconveniences are unquestionable. As such, the conflicts involve many inconveniences but they can rarely be considered as terrorism and much less as war.

The second truth contradicts the idea that cyber-attacks are unpredictable. The attacks on South Korea are just the latest in a series that dates back to 2009, a trend that became not only entirely foreseeable, but predictable.

In the history of cyber conflict there is a strong link between the geopolitical crises in the real world and the subsequent cyber-attacks. For example, whenever there is a dispute between the fishing boats from China and other claimant of the disputed islands, there is expected to be a hacking or a patriotic piracy coming from China. Consequently, as soon as North Korea renounced the armistice with South Korea in mid-March, some have already raised the alarm about the probability of cyber-attacks.

The attacks were predictable due to the reactions of North Korea, and the international community should count on that nation as the main one responsible for them, unless there is exculpatory evidence. This connection cannot be demonstrated, but the truth is that cyber conflict does not have to be different from other mysteries of national security.

When the Cheonan, a South Korean corvette, was sunk in 2010, with the loss of 46 lives, it also failed to prove that North Korea was the one responsible, but the authorship of the explosion was clear enough. The attack, as the later artillery fire on a South Korean island in which two marines and two civilians died, helps to feed the new determination of China to reprimand and, with a bit of luck, restrict its ally rebel.

This points to the fourth truth. When it comes to avoiding that the regime of Kim Jong Un lunges with cyber-attacks, the path should not start in Pyongyang, but in Beijing.

This is not the first response of most of the cyber community, whose first instinct is to find technical answers. Technicians can help to defend against future disruptions, but they will not help with the underlying behaviour of North Korea.

The international community will also find some new cyber-power mechanisms to reduce the intensity of the crises. North Korea is simply too isolated, with only a weak connection in the cyberspace. Fortunately, there is no need to look for new cyber solutions since the cyber conflicts cannot be resolved isolated from the underlying dynamic of the national security.

Indeed, the international community hasn't a cyber problem with North Korea; it simply has a problem with North Korea. Cyber attacks are just one facet of this larger dilemma. The Chinese leadership is already becoming increasingly publically frustrated with the attitude of Kim Jong Un. And any new provocation put, even more, the Chinese leadership in an uncomfortable situation. According to Jason Healey, *the Director of the Cyber Statecraft Initiative at the Atlantic Council*[4]*,* the diplomats from South Korea and the United States must add every new interruption to the list of outrages that Beijing has to respond and do not treat each one as a separate issue.

However, China and others may try to divert attention by claiming that there is insufficient evidence of the authorship of North Korea. United States and South Korea should not treat the cyber issue as something different and respond in the same way they did after the sinking of the Cheonan. Then, a group of international experts examined the evidence and issued a documented report with the irrefutable proof that "made known to North Korea and to the international community that even the most undercover attack leaves evidence."

A committee, duly selected by the United Nations or by the governments involved, should also examine the forensic evidence and the national security context to draw conclusions about which group or nation is responsible. As with the Cheonan report, there will still be detractors, but a public and complete adjustment of accounts will bring the necessary clarity and it will help set the benchmark for the new international standards.

[4] For more information see the article *To Stop North Korean Cyber Attacks, Start in Beijing* by Jason Healey, Director of the Cyber Statecraft Initiative at the Atlantic Council.

North Korean cyber-attacks have not caused casualties or serious disruptions yet. However, North Korea has learned to press with their military confrontations, the cyber-attacks will get worse and someday they could cross the thresholds. The international community should treat the cyber-attacks as it would do it with any other use of force by North Korea and it should pressure the Chinese government to curb its rebellious neighbour.

Mº José Caro Bejarano
Analyst in the IEEE