Strategic Decision-Making During Cyber Conflict : The SingHealth Case

Baram, Gil; Sommer, Udi

2019

Baram, G., & Sommer, U. (2019). Strategic Decision-Making During Cyber Conflict : The SingHealth Case [RSIS Commentaries, No. 182]. RSIS Commentaries. Singapore: Nanyang Technological University.

https://hdl.handle.net/10356/104473

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 182 – 17 September 2019

Strategic Decision-Making During Cyber Conflict: The SingHealth Case

By Gil Baram & Udi Sommer

SYNOPSIS

Cyber technology enables countries to act covertly. Furthermore, it is not always easy to identify who is behind a given attack. So, what leads countries that were victims of cyberattacks to reveal the incidents?

COMMENTARY

IT IS always not easy to identify the perpetrator of a cyber attack. Once the victim of a cyber offensive has identified the attack and decided to use a public strategy, it has two major options: firstly to reveal the attack and attribute it to the alleged attacker; or secondly reveal only the fact that the attack had occurred, without attribution.

In the current political and technical landscape, it is important to consider cyberattacks in the wider strategic context. In certain geopolitical situations, it is in the victim's interests to reveal the aggressive actions of its adversary. This might look at first like the victim admitting to its vulnerabilities. Yet, in a long-term cost-benefit analysis, sometimes it is better to 'call out' the aggressor as flouting international laws and norms than to keep quiet.

Naming & Shaming Strategy

For one, the victim is trying to say: 'I know what you (the attacker) are up to and now so does everyone else.' This is a Naming and Shaming strategy, which means publicly identifying perpetrators that are 'doing wrong' and undermining international law and the rules-based order.

Another consideration is the need to avoid public humiliation. The victim can decide to disclose the attack in order to avoid humiliation and degradation, which will most likely

accompany the publication of the attack by the attacker or by a third party. In a post-Snowden reality, secrecy is difficult.

The general public is more aware of state activities, and has the means to publicise them, for instance via social media. So, getting ahead of the news cycle is often better than trying to avoid it altogether. Costs associated with hiding an incident, may easily supersede those of immediate transparency.

Another goal may be showing strength in front of an international audience by warning the attacker from taking future actions. By disclosing the attack and accusing the attacker, the victim conveys a message that he has identified the attack and may intend to retaliate. Plus, he has the technical knowhow to identify the attack and point out the entity behind it.

Attribution is a function of capacity, so demonstrating defensive capability can signal general technological competence that may hint at a complementary offensive know-how. It seems that revealing the attack has its advantages. Now the question is why not attribute it publicly?

Motivations Not to reveal Attacker

Assuming that the victim has identified the attacker, there are two main reasons why the victim would not want to reveal the attacker's identity in public:

The first is safety of intelligence sources.

The desire to avoid exposing intelligence and sources is an important reason for not moving forward with making the attacker’s identity public. This is even more acute in cyberspace because it is difficult to identify the attacker only by using technical tools.

Therefore, it is often necessary to use intelligence of various kinds, such as advanced technological and even human resources to obtain the necessary information. These sources are considered highly important and valuable for the country's intelligence services, and therefore it is essential to protect their safety and covertness.

The second is preventing escalation.

There may be differences in the existing technological capabilities and power of the victim and the attacker. If this is the case, the victim may choose not to publicise the attack in order to avoid the chance that the exposure will lead to open confrontation. Not revealing the identity of the attacker allows the victim to refrain from the obligation to respond, and thereby contain the attack and prevent undesirable escalation.

Although at first glance, revealing the attack might be perceived as exposing the country's weakness, we identify several considerations with positive implications, which could lead the country to decide to reveal the attack. The question is why do states act that way and in the pursuit of which advantages.

And more specifically, what led the authorities in Singapore to reveal the attack and to carry out such an extensive public inquiry but consistently not mention the identity of the attacker?

The SingHealth Case

In the SingHealth case, it seems that although the head of Cyber Security Agency of Singapore (CSA) estimated a nation-state was behind the attack and many security analysts even estimated certain countries, Singapore took caution not to reveal the identity of the attacker in public.

The decision to make the attack public, nonetheless, is likely based on two main considerations: The first derived from the theft of personal information that is critical for the daily life of citizens. As E-Government is well developed and most activities that are essential to the daily lives of Singapore's citizens take place online, there was a concern that the attacker might want to use the data to gain access to additional information concerning the citizens.

The second consideration for exposing the attack without attributing it might be the concern of public humiliation. If the attacker or a third party exposed the attack before the Singaporean authorities did, it could damage the reputation of the administration. Under such circumstances, it would appear that not only did the administration fail to protect its citizens, but it also made an attempt to conceal it.

Speaking at a press conference on 20 July 2018, Chief Executive of the CSA, David Koh, confirmed that: "We have determined that this is a deliberate, targeted and well-planned cyberattack, not the work of casual hackers or criminal gangs… beyond this I apologise we are not able to reveal more because of operational security reasons."

It seems that for national security reasons the CSA most probably wanted to keep its intelligence resources safe and did not reveal any information that could jeopardise their integrity. While experts pointed fingers at some nations, authorities remained tight-lipped.

One explanation for this is the need to avoid escalation. Singapore has close trade and economic relationships with many countries, although differences occur from time to time. The will of Singapore not to take any steps that could risk such relationships and escalate the situation seems to be one reason why Singapore chose not to reveal the identity of the attacker.

Gil Baram is an Adjunct Research Fellow with the Centre of Excellence for National Security (CENS), a unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Udi Sommer is Senior Lecturer (Associate Professor), Department of Political Science at Tel Aviv University.