2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Covert or not Covert: National Strategies During Cyber Conflict

Gil Baram
School of Political Science
Tel Aviv University
Tel-Aviv, Israel
gilbaram@tauex.tau.ac.il

Udi Sommer
School of Political Science
Tel Aviv University
Tel-Aviv, Israel
http://people.socsci.tau.ac.il/mu/udis

Abstract: Anonymity is considered to be a key characteristic of cyber conflict. Indeed, existing accounts in the literature focus on the advantages of the non-disclosure of cyber attacks. Such focus inspires the expectation that countries would opt to maintain covertness. This hypothesis is rejected in an empirical investigation we conducted on victims' strategies during cyber conflict: in numerous cases, victim states choose to publicly reveal the fact that they had been attacked. These counterintuitive findings are important empirically, but even more so theoretically. They motivate an investigation into the decision to forsake covertness. What does actually motivate states to move into the international arena and publicly expose a cyber attack?

The goal of this paper is to understand why and under which geopolitical circumstances countries choose to give up the advantages of anonymity. Whether they wish to Name and Shame opponents for ignoring international norms or whether they try to avoid public humiliation, victims of cyber attacks occasionally reveal the fact that they had been attacked. There is tension between such motivations and the will to protect intelligence sources and the incentives to prevent escalation if an attack is revealed, even more so if the attacker is exposed. Indeed, we find that sunk costs, counter-escalation risks and the need to signal resolve—while critical in motivating victims to keep cyber attacks secret—may not suffice under such specific circumstances. By focusing on the victim's side, we draw inspiration from data on real-world cyber attacks in order to place cyber operations in the larger context of secrecy and covert actions in the international arena. In so doing, the aim is to advance the use of empirical data

* This research was supported by a research grant from the Blavatnik Interdisciplinary Cyber Research Center at Tel-Aviv University

for understanding the dynamics of cyber conflict and the decision-making process of states operating in this increasingly complex domain.

Keywords: *covert actions, cyber operations, national cyber strategies*

1. INTRODUCTION

In its 2019 Global Risks Report, the World Economic Forum ranked cyber attacks as one of the top ten risks, with respect to likelihood and impact (Myers and Whiting 2019). This concern is neither new nor surprising, given the anonymity that cyber attacks afford perpetrators and victims alike. By cyber attacks, which can be a part of an ongoing cyber operation, we mean both CNA (Computer Network Attack) and CNE (Computer Network Exploitation), as they cannot be fully separated (Siedler 2016).[1] Indeed, cyber technology enables countries to act covertly: the results of offensive actions in the cyber realm and their influence are not always exposed to the public eye. Furthermore, it is not always easy to identify who is behind a given attack. Even if the results of the attack are publicly observable—e.g., damage to a power grid leading to the severance of electricity supply—the victim can still dismiss these effects, arguing that they were the result of a technical fault. To date, our understanding of those strategic interactions between attacker and victim—and their decisions about whether or not to keep attacks covert—is theoretically and empirically limited.

Recent work regarding covert actions in the international arena offers three mechanisms that make the use of covert actions preferable for countries: sunk costs, counter-escalation risks and signaling resolve (Carson 2016; Carson and Yarhi-Milo 2017). These mechanisms, to be discussed in detail in Section 3, suggest that countries have strong incentives to engage in covert actions and keep those actions away from the public eye, domestically as well as internationally.

Yet an empirical investigation conducted on states' strategies in the wake of cyber attacks reveals a different picture. Notwithstanding the advantages of maintaining secrecy, it is not uncommon for victims to reveal the fact that they have been attacked. What causes victims of cyber attacks to "abandon" the covert space and move to the public arena in the aftermath of an attack? Existing literature does not offer satisfying answers (for exceptions see Edwards, Furnas, Forrest and Axelrod 2017; Poznansky and Perkoski 2018). To understand the puzzling strategic choice to abandon the advantages of ambiguity in favor of a public strategy, we need to understand the tradeoffs between the strategies. As not all countries choose to either publicly reveal

1 As Libicki concluded, "as long as the methods of cyber espionage look like the methods of cyberattack the discovery of one will raise fears about the imminence of the other." (Libicki 2018, 121)

the attack or to hide it, we recognized that the strategies of the victims vary between four possible approaches:

(1) "Pointing a finger" – publicly disclosing that an attack occurred (revealing vulnerability) and publicly putting the responsibility on a specific attacker;
(2) Admitting injury – publicly disclosing that an attack took place, while failing to identify an attacker;
(3) Revealing damage – disclosing damage but denying that it had been caused by a deliberate hostile attack (claiming technical malfunctions, system "glitches" etc.);
(4) Maintaining ambiguity – denying or downplaying any damage, thus reducing the chances that the attack would ever be divulged.

Table 1 summarizes those four strategies with illustrations from cyber attacks in recent years.

TABLE 1: VARIANCE IN VICTIM'S STRATEGIES DURING CYBER ATTACKS, WITH REAL-LIFE EXAMPLES

	Publicized		**Concealed**	
Victim's Strategy:	(1) Publicizing the attack and blaming the attacker (Public Strategy #1)	(2) Publicizing the attack and not blaming the attacker (Public Strategy #2)	(3) Partial concealment (claim of fault)	(4) Full concealment of the attack
Real-life Example:	DNC hack 2016	SingHealth hack 2018	USS John S McCain collision 2017	---

Our discussion focuses on the first two options, where the victim decided to make the attack public and sometimes also to reveal the attacker's identity. The third option (partial concealment) deals with cases where the alleged victim claims that a certain event was the result of a technical problem and not due to a cyber attack. To illustrate this option in a nutshell—since we do not delve into its details in the paper—let us look at the summer 2017 case of the *USS John S McCain*, which collided with a merchant ship in the Straits of Malacca, resulting in the death of 10 sailors (Werner 2018). The Chief of Naval Operations argued that there was no evidence suggesting the accident was the result of a cyber attack. However, according to experts, since the destroyer had a large navigational team as well as another team in charge of radar, it was impossible that human error had led to the accident. In addition, both the destroyers *USS McCain* and the *USS Fitzgerald*, which had been hit in a similar incident in June 2017, belong to the Seventh Fleet. Experts believed these attacks may have been related to Chinese or Russian intervention (Mass 2017).[2]

2 The Navy's investigation found no evidence of a cyber attack (Tritten 2017; Navy Releases Collision Report 2017).

After discussing the place of attribution and secrecy in cyber operations and their impact on states' strategic calculations, we develop our theoretical framework and examine two cases – hacking into the Democratic National Committee in 2016 and the SingHealth hack in 2018. It is particularly in the analysis of those two well-studied cases that our theoretical framework helps to shed new light on the national and international considerations leading countries to give up secrecy. We highlight the taxonomy of the different prototypes of these strategies and help to identify when countries might choose each strategy.

2. ATTRIBUTION AND SECRECY – AN INHERENT COMPONENT OF CYBER OPERATIONS?

The covertness of cyber attacks can be expressed in two ways. First, the attack itself is covert. Its technological characteristics enable an attacker to carry out the operation in a clandestine way, without revealing how it was carried out. The second aspect concerns the attackers themselves, who can maintain covertness.[3] It is often difficult to point out the source of an attack and to attribute it to a particular attacker. This problem is known as the Attribution Problem.

The Attribution Problem arises when the victim identified the attack, but has yet to identify the attacker. The immediate effect of this lack of certainty raises questions concerning the feasibility of retaliation, and the desire for it. Such a situation creates uncertainty as to the attacker's demands. It can be difficult to determine by technical means the motivation for an attack (Wheeler and Larsen 2003, 1). So, as Rid and Buchanan argue, "attribution is what states make of it" (Rid and Buchanan 2015, 7).

When an attribution process is conducted using intelligence sources and methods, it is difficult to expose it without endangering these sources. But if the domestic public—especially in a democratic polity—perceives the attribution as unreliable, the state may lose the legitimacy to retaliate (Lindsay 2015). An important part of the attribution process is its political implications. Indeed, "communicating attribution is part of attributing" (Rid and Buchanan 2015, 26). When an attack is executed, security researchers attempt to find out who is behind it. In order to do so, they examine the code, techniques and protocols that the attacker used. However, this is not considered legitimate proof in court and is seen, especially today, more as playing a "blame game" (Berghel 2017, 86).

Faith-based attribution happens when actors blame other actors for an attack if they believe the former carried it out. This also happens in modern politics, where politicians knowingly make incorrect statements, simply because no one checks their

3 On the distinction between clandestine and covert operations, see Poznansky and Perkoski, 2018, 403.

validity (Berghel 2017; Carr 2016). Healey (2013) also argues that scholarship should move forward from dealing with the attribution problem. Instead of asking "who is behind the attack?" the question should be "who is to blame for it?" (Healey 2013, 55) and what are the political consequences of blaming?

This study adopts Healey's approach in the sense that the technical attribution problem is not as crucial for our framework. In practice, countries routinely accuse each other even without disclosing the full technical process that led them to attribute the attack to a particular attacker. This was the case in the Sony hack (2014) and the "WannaCry" attack (2017) when the US blamed North Korea without fully disclosing technical evidence.

Despite the inherent overlap between cyber operations and covert actions, the scholarship has not fully explored this connection and has studied these fields separately for the most part. On the one hand, the cyberwarfare scholarship in International Relations and Security Studies hardly deals with the different aspects of secrecy in cyber operations, and mainly accepts the assumption that anonymity is an immutable feature of cyberspace rather than something actors select into and which they can therefore forfeit (for exceptions see Lupovici 2016; Poznansky and Perkoski 2018). On the other hand, scholars dealing with covert operations largely tend not to include cyber operations in their analyses (for exceptions see Brecher 2012). This study is an important step towards merging these bodies of literature.

Recent work regarding secrecy in cyberspace tends to study the considerations before the attack (Edwards, Furnas, Forrest and Axelrod 2017), the perpetrators' calculations (Poznansky and Perkoski 2018), and the effect of cyber attacks on democratic states' accountability to their citizens (Schulzk 2018). While these studies are an important step in combining the two literatures, more research is needed in order to understand cyber operations as covert actions and to investigate to what extent countries choose to use the advantages of this covertness or to give it up. In the following sections these considerations are examined from the victim's point of view. We focus on the victim, since in most circumstances the victim is the first to make a choice about whether to use covertness or forsake it.

3. GIVING UP SECRECY AS A NATIONAL STRATEGY

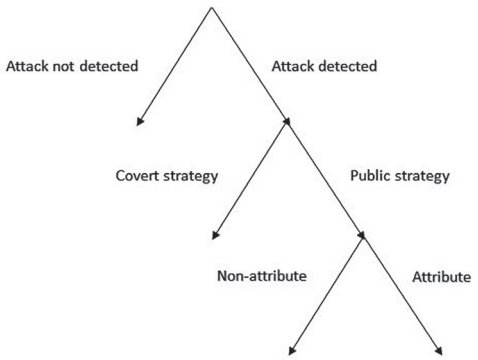
Three mechanisms are offered in the literature for making the use of covert actions preferable for countries. First are sunk costs, which refer to situations where states decide to take covert action because of non-recoverable resources: by choosing to use covert actions, leaders can employ a more "creative" way to address security threats

(Carson and Yarhi-Milo 2017, 135). Second are counter-escalation risks: using covert action can appear credible because of its impact on the risk of crisis escalation, since leaders using covert signaling tools can be free to engage in more aggressive behavior. This explanation is based mainly on the audience costs literature, which identifies a link between the type of action that the state takes and the costs the leader will have to bear as a result (see Fearon 1994; Tomz 2007). The last mechanism is signaling resolve: under certain conditions, the use of covert operations allows states to convey the desired message to their rivals, and therefore they do not have to act in the public arena (Carson 2016; Carson and Yarhi-Milo 2017, 134-135).

But it seems that during cyber attacks, that might be a part of an on-going operation or a one-time attack, the options available to the victim are different, and revealing the attack has its benefits. Generally, there are cases where the incentives to remain covert are not enough and decision-makers have other incentives—such as avoiding public humiliation, warning the attacker from taking future actions and more—that lead them to decide to publicly reveal the attack.

Once the victim has identified the attack and decides to use a public strategy, it has two major options as mentioned earlier: (1) reveal the attack and point a finger towards the attacker, or (2) reveal only the fact that the attack has occurred, without disclosing the identity of the alleged attacker. Figure 1 summarizes the strategies at earlier stages and as they lead up to the strategies at this stage.

FIGURE 1: VICTIM'S STRATEGIES DURING A CYBER ATTACK



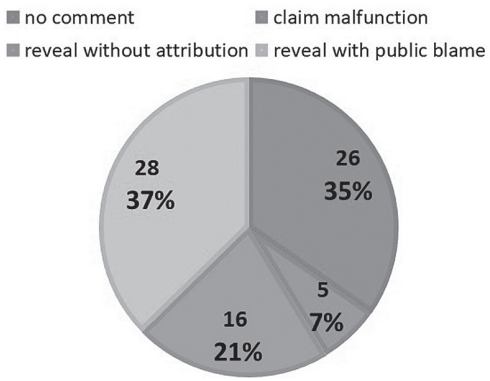
To assess the conditions under which countries that have suffered a cyber attack choose to reveal the attack and go public, we examined all known cyber attacks between rival states from 2015 to mid-2018. The framework of the Dyadic Cyber Incident Dataset (DCID) v1.1 (Maness, Valeriano and Jensen 2017) was the basis for the coding, and

new attacks from the Council on Foreign Relation Cyber Operations Tracker were added (Segal 2017). The unit of analysis in both datasets is state-sponsored cyber attacks.[4] We focus on state-sponsored actors because our purpose is to identify when states and their proxies conduct cyber operations in pursuit of their foreign policy interests. New variables originally collected by us were added in order to examine the victims' strategies. All data collected are open source.[5]

Our data indicate that there is wide variation in the victims' strategies: Between 2015 and mid-2018, 75 cyber attacks were conducted between rival states. In 44, the victims chose to address the attack publicly. Of those, in 16 the victim revealed the attack and did not attribute it. In the remaining 28, the victim revealed the attack and publicly attributed it to a specific attacker (Figure 2). Out of the 28 cases where victims chose to publicly reveal the attack and the attacker, only three states were not democratic.[6]

The data suggest that states frequently choose public strategies. Although at first glance, revealing the attack might be perceived as exposing a country's weakness, there are 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?

FIGURE 2: VARIANCE IN VICTIMS' STRATEGIES BETWEEN 2015 AND MID-2018



4 This paper focuses only on state-sponsored cyber attacks. Doing that allowed us to achieve in-depth insights regarding the ways countries operate during cyber conflict. Keeping out of the analysis other kinds of cyber attacks, such us multi-victim attacks and attacks against NGOs, might pose a methodological challenge. Due to the limited scope of this paper we do not treat these kinds of cyber attacks here, and will deal with them in future projects.

5 The "unknown-unknowns" cyber attacks are the ones that are not known to the public. This paper deals only with cyber attacks that have been publicly revealed and that had sufficient data on them in order to code it in our dataset.

6 According to Freedom House.

Reasons to publicly reveal the attack

In most cyber attacks the victim does not have full confidence regarding the identity of the attacker. Furthermore, there are questions around to what extent a victim that chooses to accuse the attacker is certain of the accuracy of its identification. If it possesses technical evidence that can be exposed, the attacker will have more difficulty denying the charges. However, more often than not this is not the case. It is common for a victim to point a finger at a particular attacker even without disclosing the full technical evidence that led to that attribution.

In the political and technical landscapes of our time, it is important to consider cyber attacks in the broader geostrategic context. In many cases there is an ongoing political tension that means it is in the victim's interests to reveal the aggressive actions of its adversary, a strategy known as Naming and Shaming. A Naming and Shaming strategy means publicly identifying perpetrators that are "doing wrong" and undermining international law and the rules-based order. This might look like the victim is admitting to its weakness. Yet, in a long-term cost-benefit analysis, sometimes it is better to "call out" the aggressor as violating international norms than to remain silent. This might help the victim and its allies to improve their cybersecurity readiness, while also reaffirming the victim's commitment to law and norms (on publicizing states activities see Carnegie and Carson 2018).

An additional consideration in revealing attacks is the need to avoid public humiliation. The victim can decide to disclose the attack due to the desire to avoid humiliation and degradation, which will most likely accompany the publication of the said attack by the attacker or by a third party. In a post-Snowden reality, remaining covert is hard. The general public is more aware of state activities and has the means to publicize them via social media as well as in various other ways. As a result, the political costs of transparency may be less than those associated with hiding an attack. This minimizes the victim's reputational damage and helps to improve overall cybersecurity of both victim and international allies alike.

Another goal may be showing strength in front of an international audience by warning the attacker against taking future actions. By disclosing the attack and accusing the attacker, the victim conveys a message that it has identified the attack and may intend to retaliate; plus, it has the technical know-how to identify the attack and point out the entity behind it. If the victim can say to the presumed attackers that it knows what they are up to, it implies that it also knows a lot more about the attackers' operations and capabilities. This may introduce uncertainty into the decision-making process and induce a strategic effect. Such was the case with the Obama-Xi agreement from 2015 that reduced Chinese industrial cyber espionage for a limited period of time (Spetalnick and Martina 2015). A country that exposes the attack and points a finger

at the attacker, while showing its methods of coping and the ways in which it operates to strengthen its defense capabilities, is portrayed as a leader in the international arena in dealing with cyber attacks.[7] Other countries will observe and learn from it, as was the case with the Democratic National Committee hack, which is discussed in detail later on.

Motivations not to reveal the attacker

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

(1) Safety of intelligence sources. The desire to avoid exposing intelligence and sources is an important reason not to make the identity of the attacker public. This is even more acute in cyberspace, because it is difficult to identify the attacker only 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 not to expose them.

(2) 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 might choose not to publicize the attack in order to avoid the chance that the exposure would lead to open confrontation. An aggressive public intervention by one country in another's affairs poses a political-strategic challenge to the victim in the eyes of the domestic public and the international community, who are watching and waiting to see how it responds (Carson 2016). Not revealing the identity of the attacker allows the victim to refrain from the obligation to respond, contain the attack and prevent undesirable escalation.

We expect victims to choose to reveal the attack publicly and attribute it when (a) they want to expose the aggressor and blame them for violating international norms; (b) avoid international and domestic humiliation; (c) warn the attacker. However, by revealing the attack and not attributing it, the victim can also avoid humiliation and there are covert ways to convey a deterrent message. Therefore, we hypothesize that in this case key reasons for not attributing the attack are (a) the safety of intelligence sources; and (b) preventing escalation. The two cases tested in the next section will help examine these expectations.

7 We are aware that there are other considerations for countries to reveal the attack, such as creating a false attribution for political reasons or faking non-existent capabilities by revealing; using the publicized attack for political reasons such as increase allied support; cases when there is a public leak and the victim is being forced to reveal the attack; internal political considerations and more. The scope of this paper will not allow us to deal with all these considerations but they will be taken into account in our larger research agenda.

4. GIVING UP SECRECY IN CYBER OPERATIONS – REAL-LIFE CASES

Two major cyber attacks that occurred in the past three years are examined. They allow us to illustrate the public strategies identified and described theoretically above.

Democratic National Committee Hack 2016

In April 2016, hackers gained access into the Democratic National Committee (DNC) network, stealing several gigabytes of data. From June-November 2016, WikiLeaks published 20,000 emails of DNC members, and in July 2016 the FBI began an investigation of the hack. The investigation revealed that in the months prior to the WikiLeaks releases, two groups of hackers operating under the auspices of the Russian government broke into the computers of the DNC and leaked the emails. This action was part of a broader Russian operation in the months before the presidential election in 2016, intended to influence the election results and to jeopardize the integrity of the democratic processes (Bump 2018).

On December 2016, President Obama publicly accused Russia of carrying out these attacks, warned that it must stop and said that the US had offensive cyber capabilities and it might respond. At the end of that month, President Obama ordered the expulsion of 35 Russian diplomats from the US, as well as the closure of sites which were used by the Russians to gather intelligence (Landler and Sanger 2016; Ryan, Nakashima and De Young 2016). The Department of Homeland Security (DHS) and the FBI published a joint statement describing the process of the Russian cyber attack, directly accusing military and civilian Russian intelligence agencies. According to the statement, "The US Intelligence Community is confident that the Russian Government directed the recent compromises of emails from US persons and institutions […] only Russia's senior-most officials could have authorized these activities." (Department of Homeland Security 2016). The operations of Russian intelligence agencies included "spear phishing" attacks of entities in government agencies, critical infrastructure, think tanks, universities, political organizations, and more, in order to steal information (Masters 2018).

The fact that the US chose to publicly accuse Russia of the attack helped strengthen its international standing by calling out Russia's undermining of the international order in trying to manipulate and sabotage democratic procedures. Such attempts to influence election results are perceived by Western democracies as damaging their political and institutional integrity. Other countries also saw and learned from the American experience. Following the exposure of the attack, the US became the focus of interest for other democratic countries—such as France and Germany—which were about to hold their own elections and feared Russian intervention. For example, the NSA

warned French officials that Russian hackers had compromised some elements of the election (Greenberg 2017).

The experience gained by the US in dealing with Russian activity enabled it to share information and assist other countries. The US became a role model for confronting Russian influence attempts and protecting election campaigns (Graham, 2017). This case demonstrates the value of our theoretical framework: by publicly revealing the attack, the US avoided public humiliation that could have happened if a third party or Russia itself had revealed the attack instead. Also, by conveying a deterrent message to the Russians, the US made a coercive threat and demonstrated resolve. It showed its will to spend valuable resources in order to make Russia pay a price for its offensive actions.

SingHealth Hack 2018

On 4 July 2018, data administrators detected unusual activity on one of SingHealth's IT databases. With more than two million patients, SingHealth is the largest health provider in Singapore. The security team immediately investigated the suspicious activity to determine its nature and whether it was malicious. On July 10th, after forensic investigations confirming it was a cyber attack, SingHealth, the Ministry of Health and the Cyber Security Agency (CSA) were informed (Tham 2018). The cyber attack resulted in the personal details of 1.5m SingHealth patients being accessed and copied; this included names, identification numbers, address, gender, race and date of birth, including the personal data of Singapore's Prime Minister. On July 20th, even while investigations were still under way, SingHealth and investigating authorities assessed that the situation had been stabilized and informed the public of the cyber attack, (Singapore Ministry of Health 2018).

Following the attack, a public Committee of Inquiry was established. A senior counsel in the Ministry of Justice summarized in front of the committee how advanced, determined and disciplined the attackers were: "The skill and sophistication used in the SingHealth attack highlights the challenges that cyber defenders face" (Tham and Baharudin, 2018). Speaking at a press conference on July 20th 2018, the Chief Executive of the CSA, David Koh, confirmed that: "We have determined that this is a deliberate, targeted and well-planned cyber attack, not the work of casual hackers […] we are not able to reveal more because of operational security reasons" (Koh 2018). From Koh's words it seems that for national security reasons the CSA wanted to keep its intelligence sources safe and did not reveal any information that could risk them.

Although the head of the CSA estimated that a nation state was behind the attack, and many security analysts even estimated it was China, Singapore was careful not to reveal the identity of the attacker in public. The decision to make the attack public

was based on two main considerations. The first derived from the theft of personal information that is critical for the daily life of citizens. As 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 personal details (Tham and Baharudin, 2018).

Another consideration for exposing the attack, but keeping the identity of the attacker undisclosed, was concern about 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. In such circumstances, the administration would appear to have failed to protect its citizens and to have made an attempt to conceal it.

While experts pointed fingers at China (Lee 2018), authorities remain tight-lipped. One explanation for that is the need to avoid escalation. China and Singapore have a close relationship, but differences have been experienced during numerous high-profile events, including Singapore's stance against China regarding the South China Sea dispute. The power differential between the two, and the will of Singapore not to take any steps that could risk this relationship and escalate the situation, seem to be among the main reasons why Singapore chose not to reveal the identity of the attacker. Further support for the decision not to reveal the identity of the attacker was given by the Minister-in-Charge of cybersecurity. In January 2019, the Minister stated that: "Revealing the identity of the perpetrator would not be in the Republic's national interest […] We've got nothing to hide here […] the only part that's been held back are those that pertain to sensitive national security matters and also patient confidentiality" (Nair 2019; Yufeng 2019).

5. CONCLUSIONS

Reasons ranging from attempts to Name and Shame or avoid public humiliation, to incomplete confidence about the identity of the attacker may lead victims of cyber attacks to reveal the fact they had been attacked. There is tension, however, between such reasons and the motivation to protect the safety of intelligence sources and the will to prevent escalation if an attack is revealed and even more so if the attacker is exposed. The preliminary results and analyses presented here demonstrate that despite a range of reasons to remain covert, countries that suffered cyber attacks have sufficiently strong incentives to reveal the fact they had been attacked. The three mechanisms presented in the literature as motivating decision-makers to keep the attack covert—sunk costs, counter-escalation risks and signaling resolve—do not always suffice in the cyber reality. Not only would victims make the attack public, but

under certain circumstances, they would even expose the attacker. This finding is both unintuitive and largely undocumented in the literature.

The will to avoid domestic and international humiliation if the attack will be exposed by a third party leads countries to give up the advantages of secrecy in cyberspace and reveal the fact that they had been attacked. Furthermore, attributing the attack to a specific attacker helps the victim to warn the attacker from taking future actions and be model for other countries who deal with similar attacks. Such was the case in the DNC hack where the US not only set the standard for other countries in the West but also aided them in preventing potential threats to the integrity of their democratic process.

National security considerations such as keeping intelligence sources safe and avoiding escalation play an important part in the decision to reveal the attack without attributing it to a specific attacker. Such was the case in the SingHealth hack. To protect citizens' online identity and e-government business, the attack was made public by the government in Singapore. Yet, its source remained undisclosed, possibly to avoid causing a geostrategic threat of escalation.

Future research is essential. In particular, in this paper we limited the theoretical discussion and empirical work to public strategies exclusively. We did not deal with the other two options from Table 1 – partial concealment and full concealment of the attack and did not analyze the attackers' strategies and the utility of the interaction between both sides.

Acknowledgments
We thank Dana Litman, Adi Lotan and Eden Poch for excellent research assistance.

REFERENCES

Berghel, Hal. "On the Problem of (Cyber) Attribution." *Computer* 3, no. 50 (2017): 84-89. https://www.computer.org/csdl/mags/co/2017/03/mco2017030084.pdf

Brecher, Aaron. "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations." *Michigan Law Review* (2012): 423-452. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/mlr111&id=452&men_tab=srchresults

Bump, Philip. 2018. "Timeline: How Russian agents allegedly hacked the DNC and Clinton's campaign." *Washington Post*, July 13, 2018. https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons-campaign/?utm_term=.f7d3b8b7fe50

Carnegie, Allison and Austin Carson. "The Spotlight's Harsh Glare: Rethinking Publicity and International Order." *International Organization* 72, no. 3 (2018): 627-657. https://doi.org/10.1017/S0020818318000176

Carr, Jeffrey. 2016. “Faith-based Attribution?” *Medium*, July 10, 2016. https://medium.com/@jeffreyscarr/faith-based-attribution-30f4a658eabc

Carson, Austin. “Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War.” *International Organization* 70, no. 1 (2016): 103-131. https://doi.org/10.1017/S0020818315000284

Carson, Austin and Keren Yarhi-Milo. “Covert Communication: The Intelligibility and Credibility of Signaling in Secret.” *Security Studies* 26, no. 1 (2017): 124-156. https://doi.org/10.1080/09636412.2017.1243921

Edwards, Benjamin, Alexander Furnas, Stephanie Forrest and Robert Axelrod. “Strategic Aspects of Cyberattack and Blame,” *Proceedings of the National Academy of Sciences* 114, no. 11 (March, 2017): 2825-2850. https://doi.org/10.1073/pnas.1700442114

Fearon, James. “Domestic Political Audiences and the Escalation of International Disputes.” *American Political Science Review* 88, no. 3 (1994): 577-592. https://doi.org/10.2307/2944796

Graham, Chris. 2017. “French Election: Are Russian Hackers to Blame for Emmanuel Macron’s Leaked Emails - and Could They Target UK Election?” *The Telegraph*, May 6, 2017. https://www.telegraph.co.uk/news/2017/05/06/russian-hackers-blame-emmanuel-macrons-leaked-emails-could/

Greenberg. Andy. 2017. “The NSA Confirms it: Russia Hacked French Election ‘Infrastructure’”, *Wired*, September 5, 2017. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

Healey, Jason. “The Spectrum of National Responsibility for Cyberattacks.” *Brown Journal of World Affairs* 18, no. 1 (2013): 57-70. https://www.jstor.org/stable/24590776

Koh, David. 2018. “*CSA on Investigations regarding the Deliberate Cyber Attack*,” YouTube video, 0:31, July 20, 2018. https://www.youtube.com/watch?v=toM_WXImOBc&index=3&list=PLH2CR4s1lqyiZZ1n6wVvW_uMMR4fFXrW4

Landler, Mark and David Sanger. 2016. “Obama Says He Told Putin: ‘Cut it Out’ on Hacking.” *New York Times*, December 16, 2016. https://www.nytimes.com/2016/12/16/us/politics/obama-putin-hacking-news-conference.html

Lee, Justina. 2018. “Suspected China cyberhack on Singapore is a wake-up call for Asia,” *Nikkei Asian Review*, August 21, 2018. https://asia.nikkei.com/Spotlight/Asia-Insight/Suspected-China-cyberhack-on-Singapore-is-a-wake-up-call-for-Asia

Libicki, Martin. 2018. “Drawing Inferences from Cyber Espionage,” *2018 10th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8405013

Lindsay, Jon. “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack.” *Journal of Cyber Security* 1, no 1 (2015): 53-67. https://doi.org/10.1093/cybsec/tyv003

Lupovici, Amir. “The ‘Attribution Problem’ and the Social Construction of ‘Violence’: Taking Cyber Deterrence Literature a Step Forward.” *International Studies Perspectives* 17, no. 3 (2016): 322-342. https://doi.org/10.1111/insp.12082

Maness, Rayn, Brandon Valeriano, and Benjamin Jensen. “Codebook for the Dyadic Cyber Incident and Dispute Dataset Version 1.1.” (2017). https://drryanmaness.wixsite.com/cyberconflcit/cyber-conflict-dataset

Mass, Warren. 2017. “Cyber Experts Believe Hacking may have Caused Collision of USS John S. McCain.” *The New American*, August 22, 2017. https://www.thenewamerican.com/tech/computers/item/26753-cyber-experts-believe-hacking-may-have-caused-collision-of-uss-john-s-mccain

Masters, Jonathan. 2018. “Russia, Trump, and the 2016 U.S. Election.” *Council on Foreign Relations*. February 26, 2018.https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

Myers Joe and Kate Whiting. 2019. “These are the biggest risks facing our world in 2019.” *World Economic Forum*, January 16, 2019. https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/

Nair, Suresh. 2019. “Singapore Healthcare cyberattack: Not revealing hacker still a ‘puzzler’.” *The Independent*, January 16, 2019. http://theindependent.sg/singapore-healthcare-cyberattack-not-revealing-hacker-still-a-puzzler/

Navy Office of Information. *Navy Releases Collision Report for USS Fitzgerald and USS John S McCain Collisions*, 2017. https://www.navy.mil/submit/display.asp?story_id=103130

Poznansky, Michael and Evan Perkoski. “Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution.” *Journal of Global Security Studies* 3, no. 4 (2018): 402-416. https://doi.org/10.1093/jogss/ogy022

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37. https://doi.org/10.1080/01402390.2014.977382

Ryan, Missy, Ellen Nakashima and Karen De Young. 2016. “Obama administration announces measures to punish Russia for 2016 election interference.” *The Washington Post*, December 29, 2016. https://www.washingtonpost.com/world/national-security/obama-administration-announces-measures-to-punish-russia-for-2016-election-interference/2016/12/29/311db9d6-cdde-11e6-a87f-b917067331bb_story.html?utm_term=.e4a51ff3e57d

Schulzke, Marcus. “The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty.” *Perspectives on Politics* 16, no. 4 (2018): 954-968. https://doi.org/10.1017/S153759271800110X

Segal, Adam. 2017. *Tracking State-Sponsored Cyber Operations*, Council on Foreign Relations, November 6, 2017. https://www.cfr.org/blog/tracking-state-sponsored-cyber-operations

Siedler, Endresen. “Hard power in cyberspace: CNA as a political means.” *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, (2016). https://ieeexplore.ieee.org/abstract/document/7529424

Singapore. Ministry of Health. *Cyberattack on SingHealth’s IT System*. August 6, 2018. Accessed December 31, 2018. https://www.moh.gov.sg/news-highlights/details/cyberattack-on-singhealth’s-it-system.

Spetalnick, Matt and Michael Martina. 2015. “Obama announces ‘understanding’ with China’s Xi on cyber theft but remains wary.” *Reuters*, September 26, 2015. https://www.reuters.com/article/us-usa-china/obama-announces-understanding-with-chinas-xi-on-cyber-theft-but-remains-wary-idUSKCN0RO2HQ20150926

Tham, Irene. 2018. “Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore’s worst cyberattack.” *The Straits Times*, July 20, 2018. https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

Tham, Irene and and Hariz Baharudin. 2018. “Attempt on July 19 was detected and cut off on same day, thanks to heightened monitoring.” *The Straits Times*, October 6, 2018. https://www.straitstimes.com/tech/hackers-made-another-intrusion-attempt-as-probe-was-under-way

Tomz, Michael. “Domestic Audience Costs in International Relations: An Experimental Approach.” *International Organization* 61, no. 4 (2007): 821-840. https://doi.org/10.1017/S0020818307070282

Tritten, Travis. 2017. “Navy Chief: There’s no evidence recent collisions were caused by hacking.” *Business Insider*, August 30, 2017. https://www.businessinsider.com/navy-chief-no-evidence-recent-collisions-were-caused-by-hacking-2017-8

United States. Department of Homeland Security. *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*: DHS Press Office, October 7, 2016. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

Werner, Ben. 2018. “USS John S. McCain Collision, A Year Later.” *USNI News*, August 21, 2018. https://news.usni.org/2018/08/21/35947.

Wheeler, David and Gregory Larsen. *Techniques for Cyber Attack Attribution*. Alexandria, VA, 2003. https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf

Yufeng, Kok. 2019. “SingHealth attacker known: Iswaran.” *The New Paper Singapore*, January 16, 2019. https://www.tnp.sg/news/singapore/singhealth-attacker-known-iswaran