Technological Threat Attribution, Trust and Confidence, and the Contestability of National Security Policy

Dr William Hoverd

Centre for Defence and Security Studies,

Massey University

A Talk Presented to the Waikato Dialogue onThe Implications of Emerging Disruptive Technologies for International Security and New Zealand

Slide One

The world has been asked to believe that China and North Korea are sources of cyber threat and that Russia has been conducting offensive cyber activities in the Ukraine and the 2016 U.S election. Western populations are being asked to trust the words of intelligence agencies and their political leaders that these technological threats are real. The often-classified nature of the threat results in governments not being able to provide the public with an evidence base for any threat attribution that it might make against another nation state.

In this talk, I will review recent 2018 New Zealand Government national security discourse around cybersecurity. I demonstrate that this discourse is engaging in technological threat attribution. By technological threat attribution, I mean language which directly places responsibility for the source of a cyber-threat onto a specific nation state. After the NZ document review, I will briefly discuss the threat attribution literature, the problem of cyberthreat metaphor, and securitization theory to problematize this cyber threat attribution discourse. My point will be to show how this threat attribution language constructs a discourse of cyber threat that does not always have a publicly available evidence basis. I argue that an evidence gap challenge emerges where the public is asked to trust and have confidence in a particular technological threat attribution claim without any further assurance. Consequently, there is potential for trust and confidence issues to arise because it is sensible for the public to ask, in the light of this evidence gap, whose security claim should be believed and why? It seems a critical social responsibility for cyber security discourse makers and academia to first acknowledge this conundrum and then strive to develop frameworks to better understand the trust and confidence challenges around technological threat attribution. Today, my concluding goal will be to point to some potential solutions that might be available to cyber discourse makers to mitigate this challenge.

In 2018, the New Zealand Labour Coalition Government has labelled cybersecurity as a particular focus of the national security threatscape that it manages.[1] The 2018 Department of Prime Minister and Cabinet Cyber Security Strategy Refresh, has stated that New Zealand recognizes that the relevance of cyber security concerns now extends across multiple branches of government.[2] And now when we look closely at the 2018 Government cyber discourse, it becomes clear that across the New Zealand national security sector a discourse is emerging where cyber technological threat is being attributed to Russia and North Korea. And this threat attribution discourse is usually accompanied by an argument that New Zealand is not immune from this threat and additional cyber infrastructure development is required. For example:

Slide Two

In February 2018, Mr Andrew Hampton, the Director General of the Government Communications Security Bureau stated that:

> **"The GCSB's international partners have today attributed the NotPetya cyber-attack to the Russian Government.**
> "While NotPetya masqueraded as a criminal ransomware campaign, its real purpose was to damage and disrupt systems," Mr Hampton said.
> "Its primary targets were Ukrainian financial, energy and government sectors. However, NotPetya's indiscriminate design caused it to spread around the world affecting these sectors world-wide.
> "While there were no reports of NotPetya having a direct impact in New Zealand, it caused disruption to some organisations while they updated systems to protect themselves from it."[3]

Slide Three

Similiary, in the 2018 winter issue of *Line of Defence* the Right Honorable Mr Andrew Little, Minister Responsible for the GCSB and NZSIS stated that:

> "In terms of cyber threats, the GCSB noted a 15 per cent increase in serious incidents affecting New Zealand in the year to June 2017.
>
> Incredibly nearly a third of these had indicators of connection to foreign intelligence agencies."
>
> New Zealand organisations were subject to both direct and indirect threats, and New Zealand infrastructure is being used as staging points by threat actors to target systems in other countries.
>
> Motivation varies from espionage to revenue generation and seeking to secure political outcomes.

---

[1] Andrew Little "Andrew Little addresses the National Security Conference." *Line of Defence Magazine*, Winter 2018 Volume 1 Issue 8. Pp. 33-35.
[2] Department of the Prime Minister and Cabinet. *Refresh of New Zealand's Cyber Security Strategy and Action Plan*. (Wellington: NZ 2018), 6
[3] https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/

> **In February, the Government added New Zealand's voice to the international condemnation of the NotPetya cyber-attack which international partners have now attributed to the Russian Government. It targeted Ukraine, but had a global impact – including affecting supply chains in New Zealand.**
>
> **In December, New Zealand also expressed concern about international reports which link North Korea to the major Wannacry ransomware campaign"[4]**

Slide Four

A similar type of attribution claim can be also found in the July 2018, the Ministry of Defence's Strategic Defence Policy Statement which states that:

> "Physical distance is no protection in cyberspace, and New Zealand is subject to a growing cyber threat from state sponsored and other malicious actors…. Cyber blurs boundaries between conflict and peace, and public and private. (Page 18)
>
> **Russian 'active measures' in the 2016 United States Presidential election brought to light 'cyber enabled information warfare 'as a disrupter in liberal democracies. (Page 19)**
>
> **North Korea has a substantial store of chemical and biological weapons, a significant cyber capability (which it has shown a willingness to use)…. (Page 21)"[5]**

Across these three examples, we see a clear demonstration that the New Zealand Government is attributing cyber threats to Russia and North Korea. However, other than the discourse claim itself, there is no publicly available evidence supporting these specific attributions. We also see in these three examples that the threat attribution for a cyber-attacks occurring across nation states is linked explicitly to a governmental claim that there is a growing cyber threat environment impacting adversely on New Zealand and by implication that there is an increased need for investment in the nation's cyber infrastructure.

In the academic literature it is the political construction of cyber threat attribution in national security that is useful here. In 2013, Myriam Dunn Calvety[6] argued that "The link between cyberspace and national security is often presented as an unquestionable and uncontested "truth." However, there is nothing natural or given about this link: It had to be forged, argued, and accepted in the (security) political process." She argues that cyber security discourse is in actual fact constituted by a variety of authority figures in Governments. For Dunn Calvety, the political nature of cyber discourse is further complicated by the fact that the very building blocks of cyber security language employ analogies or metaphors to describe and explain the effect of unsolicited changes in code

---

[4] Andrew Little "Andrew Little addresses the National Security Conference." *Line of Defence Magazine*, Winter 2018 Volume 1 Issue 8. Pp. 33-35.

[5] New Zealand Government. Strategic Defence Policy Statement 2018.

[6] Myriam Dunn Cavelty; From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, *International Studies Review*, Volume 15, Issue 1, 1 March 2013, Pages 105–122, https://doi.org/10.1111/misr.12023

across networks. This metaphorical language is potentially distorting and results in a tendency to describe the cyber landscape at hand as unruly, dangerous or threatening when in actual fact much of the cyber environment is benign and intended to be enabling.

Once consequence of the political construction of cyber discourse is that there are real risks when it comes to generating accurate attribution claims. In 2014, Thomas Rid and Ben Buchanan argued that "Doing attribution well is at the core of virtually all forms of coercion and deterrence, international and domestic. Doing it poorly undermines a state's credibility, its effectiveness, and ultimately its liberty and its security." They also noted that in cyber security, the attribution debate is evolving surprisingly slowly.[7] Ultimately, for Rid and Buchanan, who provide a detailed technical account of the attribution process, they find that developing the evidence for cyber-attack attribution is a difficult and costly process which inevitably only indicates the likely source of an attack. And this evidence cannot easily determine motive or the political gain that may have initially generated any attack. They conclude with the finding that *attribution is what states make of it*. That attribution is effectively a political act used by states for advantage and positioning.

Slide Five

Locally, the technical challenge and political nature of attribution claims is evident when we look closely at the GCSB's National Cyber Security Centre Annual report when it states:

> **"Publicly reporting attribution is a significant [Political] decision and is not made by the NCSC alone. Public attribution is one way to reduce the efficacy of malicious cyber actors by revealing their tools or increasing the reputational costs of illegitimate activity. However, it also carries risk for New Zealand and is considered alongside our other national objectives including the need to maintain our ability to protect the networks that are of importance..."[8]**

So given that there is academic and local technical agreement that cyber threat attribution is ultimately a political act; why might the Labour Coalition government be making these threat attribution claims, why now and what might be the risks inherent in this attribution?

I think there are three explanations. Firstly, there is a clear discussion in other sections of these documents that NZ is part of the Five Eyes network and is speaking in solidarity with our partners. The challenge here is that there is no unclassified evidence to support our partner's claims, the public have to trust the veracity and motives of these partners, and they have to trust that NZ's politicians are maintaining an independent viewpoint and are not simply repeating some other nation's claim.

A second explanation can be sourced from DPMC's National Cyber Policy Office Release of April 2018 which takes the form of a letter written by the Right Honorable Claire Curran, then Minister of Broadcasting, Communication and Digital Media. The topic of the letter is

---

[7] Thomas Rid & Ben Buchanan (2015) Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37, DOI: 10.1080/01402390.2014.977382

[8] https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-2016-17-Unclassified-Cyber-Threat-Report.pdf

the REFRESH OF NEW ZEALAND'S CYBER SECURITY STRATEGY AND ACTION PLAN which is currently underway now in 2018.

Slide Six

Claire Curran stated:

> **"We will need to consider the mechanisms available to us to dissuade or deter malicious cyber activities, particularly where it is state-sponsored or state condoned. This includes the option of publicly attributing malicious cyber activity as a way of holding states to account.**
>
> The clear trend is an upward trajectory of cyber security threats. Cyber threat actors are increasingly bold, brazen and disruptive. New Zealand's geographical location does not exempt us from this threat."[9]

Clearly, the Labour coalition has made a political decision to publicly attribute what it describes as malicious cyber activity to particular nation states as part of being a good international citizen who upholds a rules based order. The challenge is that the evidence for the threat and the rationale behind this recent shift to public attribution are not made transparent and the NZ public is being represented by this claim. In this case, the New Zealand public is asked to trust that the correct decisions and attributions are being made and that the government is not being selective in who it calls to account.

A third explanation comes from the the Copenhagen school which developed the securitization theory that focuses on "speech acts" and the significance these acts can have upon political agenda settings and political relations.[10] Securitization theory suggests that when a threat is identified and a "speech act" identifying it is utilised, this discourse prioritises the threat on the political agenda in such a way that it necessitates the development of urgent mitigation measures that could potentially extend even to the encroachment of privacy, the need for secrecy and the utilisation of force.[11] For the Copenhagen school, securitisation speech acts emphasize the dangers of the cyber threat environment and legitimate additional government funding for the construction of various infrastructures designed to protect the public from the threat. The challenge here again it is the speech acts that have the power for change, not any evidential basis that may sit behind the act. The public has no choice but to trust that those who are making the speech act are fully informed by subject matter experts and are making the best national security decisions possible.

Taken together these explanations suggest that the various 2018 New Zealand Cyber security attribution speech acts indicate that a political shift is occurring which is attempting to:

1. Align NZ closer to its Five Eyes partners,

---

[9] https://www.dpmc.govt.nz/sites/default/files/2018-04/ers-18-paper-refresh-of-new-zealands-cyber-security-strategy-and-action-plan_1.pdf

[10] McDonald, "Securitization and the Construction of Security", 565-568

[11] Kassab, "In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare", 65

2. Call out certain acts of cyber aggression where NZ can then position itself as good cyber citizen, and

3. Justify and legitimate the development of additional domestic cyber security infrastructure.

The international and domestic consequences that might result from this attribution language are yet to be seen or understood. One could facetiously ask is NZ increasing its cyber threat environment through this discourse or is the nation just so inconsequential that its government can safely make these claims insulated in the knowledge that we are unlikely ever to be the direct target of any such attack?

More seriously, my purpose today has been to highlight that the threat attribution language being used by the NZ government has a weakness in it. A trust and confidence challenge could emerge from the evidence gap that underlies the politically constructed nature of this cyber security discourse. In a civil society environment where the evidence for attribution is unavailable and the integrity of state institutions such as the GSCB or the Minister for Broadcasting's judgement have recently been called into doubt, it is possible that future trust and confidence issues may arise around the efficacy of this language and the effectiveness of current Government cyber initiatives. In 2015 and 2016, similar trust and confidence issues occurred in the justification of counter terrorism funding where evidence of a domestic radicalisation threat has never eventuated and the claim of the Jihadi bride risk was found by the media to have little evidentiary basis and to have been exaggerated.

In a contemporary environment where the New Zealand Government's national security discourse can become contested it seems a critical social responsibility for security policy makers and academia to first acknowledge this conundrum and then strive to develop frameworks to better understand the trust and confidence challenges around threat attribution and apply it to this emerging cyber discourse.

Slide Seven

A civic challenge exists for both Government and academia to consider how to best address the weakness of national security threat claims. When it comes to those engaged in generating the Government's cyber security discourse, I think there are at least nine or so possible ways that they may wish to mitigate this potential trust and confidence issue. They are that:

1. Cyber discourse makers must accept that national security discourse justifications that arise from classified sources cannot provide a persuasive public evidence basis for their assertions.
2. Therefore, cyber discourse makers could publicly note that, at times, there is a gap here between evidence, cyber policy and threat attribution claims.
3. Cyber discourse should acknowledge that its claims are inherently political and therefore potentially contestable which will allow the discourse to be more reflexive and self-regulate its claims in a more nuanced manner.

4. Nuanced cyber threat discourse lessens the possibility that a Government institution or representative will be subsequently called to account for making an incorrect or exaggerated claim.
5. The 2018 cyber security strategy refresh offers a real opportunity to engage with the public. In addition to its current almost exclusive focus on engaging private companies, it could offer the NZ public an education capacity and offer more government transparency around the nature of cyber threat.
6. Cyber threat discourse needs to clearly differentiate between the prevalence of cybercrime events and state sponsored cyber-attacks to ensure that the actual prevalence and nature of cyber security threats are properly represented to the public.
7. One place where a degree of transparency and limited evidence exists for the actual nature and prevalence of cyber threats to New Zealand is found in the annual reports of the National Cyber Security Centre. Its carefully constructed and communicated data could and should be more widely distributed and utilised as an evidence basis.
8. It must be acknowledged that in a post-wiki leaks, post Kim Dotcom world where New Zealand is firmly part of the Five Eyes network there will be limits to public trust for any aspect of national security discourse and that this is normal.
9. And lastly, one way to address the confidence challenge and limited trust around secrecy in national security discourse is to regularly craft language that clearly notes that a fine balance exists between secrecy and transparency. This balance relies heavily on building a trusting and transparent relationship and repairing past breaches of confidence.