ATTRIBUTION IN CYBERSPACE: BEYOND THE "WHODUNNIT"

May 2018

Anushka Kaushik

I. Introduction

"The UK government judges that the Russian government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack. We call upon Russia to be the responsible member of the international community it claims to be rather then secretly trying to undermine it", stated Lord Tariq Ahmad of Wimbledon, the Foreign Office Minister of State, in early 2018.[1] NotPetya was easily one of the most devastating cyber-attacks in recent times, affecting Europe, Asia, and the Americas. The attack was estimated to have cost businesses almost $1.2 billion.[2] The NotPetya virus encrypted the hard drive of infected computers and was primarily seen as a Russian state-sponsored cyberattack masquerading as ransomware. The United Kingdom was joined by the United States and Australia in publicly attributing NotPetya to the Russian military.[3]

Attribution refers to the action of regarding something as being caused by a thing or person. In cyberspace, attribution goes beyond the simple action of finding out who's responsible behind aggressive behaviour online. The goal of this paper is to outline the process of attribution in cyber-attacks, especially in the current context of states indirectly sponsoring cyber-attacks against other entities by outsourcing hacking to non-state hackers. The paper also aims to highlight the challenges to the process of attribution in this context.

II. The process of attribution

Attribution in cyber-attacks typically involves analysis at three levels; the technical (how), the operational (what), and the strategic (who and why).[4]

At the technical level, there are various tools available for investigators that indicate the techniques used for a specific cyber-attack. Targeting analysis is one such example where the attention is focused on the target and can reveal the type of intruder or even the organisational structure of the attacker. Whether the attacker is working with a larger organisation or if there are numerous players can also be found by locating an individual and then zooming out at the institutional level or vice versa. The infrastructure used for malicious activities as well as mistakes made during the cyber-attack all contribute to the attribution process.

[1] UK National Cyber Security Centre, (15 February 2018) Retrieved from https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack
[2] "UK and US blame Russia for 'malicious' NotPetya cyber-attack" (15 February 2018) Retrieved from http://www.bbc.com/news/uk-politics-43062113
[3] Australia-: "Australian Government attribution of the 'NotPetya' cyber incident to Russia" (16 February 2018) Retrieved from http://minister.homeaffairs.gov.au/angustaylor/Pages/notpetya-russia.aspx
US, UK- : "US joins UK in blaming Russia for NotPetya cyber-attack" (15 February 2018) Retrieved from https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine
[4] Rid, T & Buchanan, B (2015) Attributing cyber-attacks, Journal of Strategic Studies, 38 (1-2), pp4-37. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382

It's difficult to clearly delineate between the operational and strategic levels since they overlap to a great degree. Moreover, analysis at these three levels is almost never a step-by-step process that follows a defined chronology or sequence. In some cases, the geopolitical context and other non-forensic sources of intelligence become the first clues in attribution, before the technical indicators can flag or identify malicious activity. Analysis at the strategic level, therefore, can begin before examining the technical aspects. Strategic analysis to examine an adversary's motivation is guided by an understanding of the priorities of other states, be it commercial, military, or economic. The geopolitical context can also be a tipoff for future cyber-attacks. To some extent, this helps in understanding the rationale of an intrusion.

III. Attribution in practice: the case of Chinese economic espionage online

One of the most significant and public cases of attribution in cyber-attacks was the 2014 indictment of five Chinese military hackers by the United States.. This indictment was on the counts of economic espionage, maintaining unauthorised access to the computers of and stealing information from six American companies including United States Steel Corp and Westinghouse Electric Co.[5] Chinese state-owned companies are believed to have hired a unit of the Chinese People's Liberation Army (PLA)[6] to assemble a database of corporate intelligence and all five accused were found to be working with the unit, argued the indictment.

The US had been harbouring suspicions that economic espionage was being carried out by hacker groups operating out of China for almost a decade. The Chinese state was quick to vehemently deny any involvement and called the charges 'preposterous' and accused the US of having double standards and betraying the commitment to build reliable military-to-military relations.[7] Perhaps owing to the strong statement by China's foreign ministry, mainstream media organisations picked up the story and reported on it extensively. Phrases classifying cyber space as the "new battlefield" for economic warfare and strategy filled viewers' television screens. Some political commentators argued that this would not significantly alter China's behaviour. The significance lies in the fact, however, that this was a huge step on the part of the US in publicly denouncing a state it had strong economic ties with.

On the prosecution, United States Attorney General Eric Holder stated that "the range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response".[8]

Following the public denouncement of China and the indictment of Chinese citizens, then US President Barack Obama and Chinese premier Xi Jinping reached an agreement on increased communication and cooperation between the two countries to investigate and prevent cyber-crimes emanating from their territory. Both countries also confirmed that they wouldn't knowingly conduct or support cyber-enabled theft of intellectual property.[9] Furthermore, data analysis carried out in 2016 revealed an overall decline in China-based intrusion activity against private and public-sector organisations since mid-2014.[10] Publicly naming and shaming aggressor states, therefore, could be an effective deterrent in preventing malicious behaviour in cyber space.

[5] United States Department of Justice (May 19, 2014). Retrieved from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[6] Unit 61398 belonged to the Second Bureau of PLA's General Staff Department (GSD) and is believed to consist of military cyber members and specialize in computer network operations

[7] Kaiman, J (May 20, 2014) "China reacts furiously to US cyber-espionage charges", The Guardian. Retrieved from https://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges

[8] Finkle, J., Menn, J., & Vishwanatha, A (November 20, 2014) "U.S. accuses China of cyber spying on American companies" Retrieved from http://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120

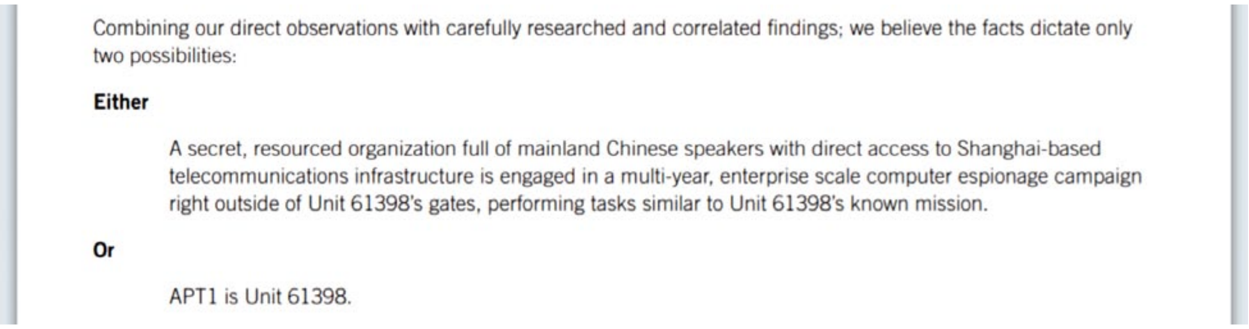
[9] Brown, G. & Yung, C (January 19, 2017) "Evaluating the US-China Cybersecurity Agreement", The Diplomat Retrieved from https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/

[10] Redline Drawn: China recalculates its use of cyber espionage", FireEye, 2016. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

The attribution process has been extensively documented by private cybersecurity firms in reports that are free and accessible to the public. The first report proves that the Chinese hacker group referred to as ‘APT1’,[11] suspected of economic espionage since 2006, and a unit within the Chinese military, were the same. The second was released after the indictment in 2014 and the cooperation agreement between the two countries, as a review of Chinese-based cyber espionage operations.

▸ **“APT1: Exposing one of China’s Espionage Units”**
Mandiant, 2013[12]

▸ **“Redline Drawn: China recalculates its use of cyber espionage”**
FireEye, 2016[13]



Combining our direct observations with carefully researched and correlated findings; we believe the facts dictate only two possibilities:

Either

A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398’s gates, performing tasks similar to Unit 61398’s known mission.

Or

APT1 is Unit 61398.

Image: This image is taken from the last section of the Mandiant report which traces APT1’s activities through an analysis of the individual hackers involved, attack lifecycle, and infrastructure. Their conclusion reads: “Either a secret, resourced organszation full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398’s gates, performing tasks similar to Unit 61389’s known mission, or APT1 is Unit 61389.”

[11] APT stands for Advanced Persistent Threats which refers to a continuous network attack carried out by groups for purposes like stealing data or planting destructive code. APT1 is a single group of operators, originating from China, and believed to be conducting online espionage since 2006.

[12] APT1: Exposing one of China’s Espionage Units”, Mandiant, 2013. Retrieved from https://www.firereye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[13] Ibid

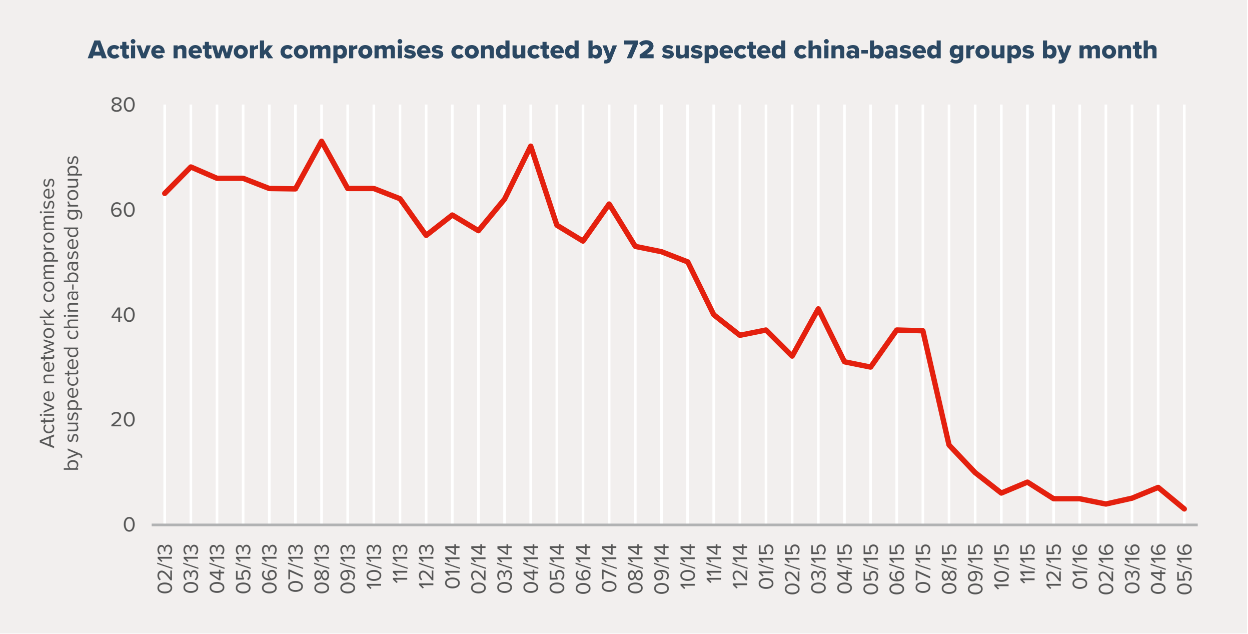


Image: A graph in the report outlining the decline in active network compromises[14] from 2013 to 2016 by China-based groups

In addition to technical analysis, the three reports highlight operational and strategic aspects:

- **Establishing links between individual hackers and the Chinese government** by highlighting individuals behind the keyboard, accompanied by an analysis and summary of their online activities that point to their involvement. For example, one of the actors, “UglyGorilla” had been active since 2004 and previously expressed interest in China’s cyber troops.

- **Motivations behind the hacking** as indicated by the organisation or people targeted. One of the reports identifies the primary hacker behind the operation and the location of the unit in Shanghai. This unit is believed to hack into companies in order to steal corporate trade secrets, primarily relating to the satellite, aerospace and communication industries.

- **Importance of the political environment**, for instance Chinese domestic reforms, in playing a part in the overall reduction of active network compromises from China-based hacker groups.

This extensive documentation and communication of the attribution process is important for establishing credibility. The credibility of attribution depends on factors like strong evidence, a track record of accuracy and precision, and objective and unbiased analysis. When one state publicly attributes malicious behaviour to another, it is as essential for that accusation to appear credible and legitimate as the actual attribution process. Recognising this, the RAND Corporation published a report in 2017 that called for a Global Cyber Attribution Consortium that would provide an independent investigation of major cyber incidents for the purpose of attribution.[15] In order to avoid accusations of bias, the authors argued that any credible and transparent attribution would ideally not include the formal representation of nation-states Membership would include representatives from two sectors: (1) technical experts from cybersecurity and information technology

[14] Network compromise has been defined as successful remote entry into a victim’s network, in the report.
[15] Davis, J., Boudreaux, B., Welburn, J., Aguirre, J., Ogletree, C., McGovern, G., Chase, M (2017) Stateless Attribution: Toward International Accountability in Cyberspace. RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR2081.html.

companies, as well as academia, and (2) cyberspace policy experts, legal scholars, and international policy experts from a diversity of academia and research organisations.

While transparency and credibility in cyber attribution are enormously vital, the feasibility of such a consortium, devoid of any state role, is highly doubtful.

This credibility, however, is further challenged as some states outsource cyber-attacks to hackers with the aim of obfuscating their involvement.

IV. Challenges to attribution: The state and outsourcing hacking

> *"Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures. Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack."*[16] - US DoD Cyber Strategy published in April 2015

The idea that states can obfuscate their involvement in malicious behaviour online through hiring or outsourcing non-state hackers poses a particularly significant challenge in the realm of cyber security.

It's important to explore the conditions that would incentivise states to hire non-state hackers. While plausible deniability is obvious, there are several factors that can influence such a decision.

The extent of state support for non-state hackers can depend on the alignment between the goals of the state and the hacker, the degree of support needed relative to the difficulty of achieving a given operational objective, and the value of the state's objective relative to the expected consequences of actually getting caught as presented in the following matrix.[17]

Attractiveness of state support for non-state hackers

Prospective Agent Qualities	Unskilled	Skilled
Opposed	▶ **Delegation least attractive:** Requires side payments and large investment (least deniability)	▶ **Delegation less attractive:** Requires side payments but low investment (legal deniability)
Supportive	▶ **Delegation somewhat attractive:** Requires litte convincing but large investment (material deniability)	▶ **Delegation very attractive:** Can be achieved with permissive policy (full deniability)

Borrowed from "Honing cyber attribution: A framework for assessing foreign state complicity", Justin K. Canfil

[16] United States Department of Defense Cyber Strategy, 2015. Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[17] Canfil, J (2016) Honing cyber attribution: A framework for assessing foreign state complicity, Journal of International Affairs, 70 (1), pp 217-226. Retrieved from https://www.questia.com/library/journal/1G1-476843518/honing-cyber-attribution-a-framework-for-assessing

The matrix, as developed by Justin Key Canfil, posits two prospective agent qualities as opposed or supportive to state goals, juxtaposed with whether they are skilled or unskilled. For example, states would have strong incentive to delegate when the agent is in support of state goals leading to a common objective and the high possibility of deniability for the state. This would make the state less vulnerable to international consequences.

Outlining conditions that influence a state's decision to outsource helps the attribution process by narrowing down possible suspects as it provides clues towards which states would have the motivation, means, and opportunities to do so.

V. Conclusion

Attribution in cyber-attacks is a complex process which requires numerous pieces of information, from technical, operational, and strategic levels, to come together. The political environment within which a cyber-attack occurs and the actors it involves greatly shapes the process and outcome of attribution in cyberspace.

A significant change today is that, in general, security companies are publishing their attribution processes which are accessible to the public and in ways that can, to a large extent, be consumed by the average user. Given that cyber-attacks, especially in public discourse, tend to be mired in hype and crises, making such information public, easily accessible, and most importantly readable for a layman is critical. This will also reinforce the credibility given the increasing number of cases of states publicly accusing each other of indirectly sponsoring cyber-attacks.

Communication of these technical processes is becoming commonplace especially when it comes to highly sophisticated attacks which affect several countries. Proponents of clearer communication of attribution processes argue that it bolsters credibility of the message and messenger, facilitates stronger collective defences, and can improve the process of attribution itself by allowing knowledge-sharing within the growing network of IT experts and cybersecurity firms.

While technical attribution may be getting better, the increasingly prevalent use of hackers or 'proxies' hired directly or indirectly by state actors to carry out cyber-attacks on their behalf only stands to make the attribution problem worse. Non-state hackers who are politically motivated or private intermediary actors functioning on the behalf of states are monumentally muddying the waters of attribution. In this regard, publicly attributing a cyber-attack to a state can act as a deterrent. However, these instances are greatly informed by geopolitical and strategic contexts which implies that it heavily depends on the particular state/non-state actor, victim state, and process of attribution.

Public and private sector collaboration is needed to develop a common framework for the communication of attribution processes. Collaboration of this nature potentially offers many benefits. For instance, publishing details about the process and making them public is likely to enhance the quality of attribution and even increase market competition. In the case of the Chinese hackers involved in economic espionage and indicted by the US, competition among security companies partly drove the publishing of details and reports. Moreover, in today's context, gaining credibility while publicly attributing a cyber-attack to a state is imperative since it also legitimises measures taken against them.