Cyber Attribution: Challenges and Opportunities for Multi-Disciplinary Analysis
Amy Ertan

Abstract

This article explores how cyber attribution is performed in the UK and addresses current barriers to identifying deceptive actors. Through interviews with UK-based experts in cyber attribution, this article explores how false flag operations can be identified, in an arena where the technical evidence may be deliberately falsified to implicate third parties. Four methods of implementing non-technical evidence were identified through the interviews: interdisciplinary teams; training technical colleagues on political context; information-sharing platforms; and outsourcing. Interdisciplinary conversations are required to combine the visions of professionals within cyber intelligence and attribution, and to work towards a best-practice approach to false flag attribution.

Keywords: cyber attribution, cyber warfare, cyber-attacks, advanced persistent threats, deception, false flag attacks, national security.

Introduction

It is often a notoriously difficult endeavour to track down and attribute the responsible actor(s) for a cyber-attack. As efforts to identify a culprit, cyber attribution represents ‘the ability to describe who did what to whom with the degree of certainty required by the needs of law, policy, or doctrine’. Particularly given where attackers engage in deceptive methods to avoid identification, confident attribution may not always be possible where the evidence is not available or analysable. Worse, more often than not, the process lacks repeatability. Attacks involving nation-states involve unique challenges that further complicate attribution attempts, enabled by the greater resources at their disposal. Amongst other factors, the use of ‘false flags’, where an attacker pretends to be someone other than themselves, is a tactic to frame other threat actors. A false flag operation could be as simple as malicious marketing, perhaps inserting imagery appearing to show another threat actor claiming responsibility. It could also

1 Acknowledgement: This work was supported by the Engineering and Physical Sciences Research Council under Grant EP/P009301/1.
be as straightforward and simple as inserting other languages into malware. As well as enabling attackers to avoid detection, false flags may be used as a form of manipulation, and where investigators of an event fail to realise that the false flags are not genuine hints, may lead to incorrect attribution and misattribute an attack.

Particularly in critical national security cases, the need for confident attribution is considered extremely valuable. Without the ability to tie a cyber-attack to a responsible agent, there can be no political or legal enforcement of regulation, or counteraction. At the same time, incorrect attribution may have severe consequences, including misdirected sanctions or potential counterattacks. The consequences to misattribution may be severe, further achieving a threat actor’s goals if a target state is misled by technical indicators. Misinformation has previously shown itself to have catastrophic consequences beyond individual attacks. A review of intelligence used to justify the 2003 Iraq War, for example, highlighted how key decision-makers were misled by incomplete and misinterpreted intelligence to the extent that the outbreak of war was based on false allegations that Iraq had developed weapons of mass destruction. The proliferation of technology over the approximate past half-century has further enabled a new attack vector for false flag operations, with overlapping and unique features. The question of cyber attribution therefore shows itself to be much more than a technical problem, and rather represents a political problem in the context of global diplomacy and conflict.

False flag operations are most likely detected as deceptive exercises due to mistakes or shortcomings made by the threat actor, from examples of poorly translated text that uncovers true linguistic origins, to actors forgetting to set up Virtual Private Network (VPN), Internet Protocol (IP)


5 Robert Draper, To Start a War: How the Bush Administration Took America into Iraq (New York: Penguin Press, 2020). While the intelligence surrounding Iraq’s WMD program was a mix of fraudulent, misinterpreted, and cherry-picked, it must also be acknowledged that full awareness of the program was intended to be as opaque as possible by the Iraqi Government to ensure the survival of Saddam Hussein’s regime. See John Nixon, Debriefing the President: The Interrogation of Saddam Hussein (New York: Penguin Random House, 2016).

proxies, or further obfuscation correctly. Deceptive techniques are frequently uncovered within a technical analysis of the attack, with a range of technical mechanisms present through intrusion-based analysis models such as the ‘Cyber Kill Chain’.

However, while recognising the efforts of often excellent investigative work, it appears unsatisfactory to rely on attacker incompetence to determine the true narrative and build a conclusive case towards a confident attribution. If an attacker is sophisticated enough to avoid making simple errors—a conceivable scenario, particularly considering nation-state actors with advanced capabilities—, then technical evidence may not offer an accurate snapshot of events.

This article argues for an interdisciplinary approach to attribution; including strategic and wider political awareness of the context surrounding an attack, complementing a traditional technical investigation. It focuses on the context in which nation-state attribution is highly desirable. This applies, for example, to events threatening national security, or where nation-state attribution would have an impact on a wider geopolitical and diplomatic scale. This allows the report to put aside ‘the value of attribution’, as a worthwhile but separate debate, and focus on instances where it is generally considered necessary to aim towards cyber attribution. Through fifteen interviews with UK-based experts across industry, academia, think-tanks, and government, this article analyses the current challenges in identifying and attributing false-flag operations, and goes on to discuss perspectives on how wider context and political intelligence may assist attributive efforts. Interviewees included experts across the technical and non-technical spectrum, with participants holding role titles including analyst and managerial roles in ‘Geopolitical Intelligence’ and ‘Strategic Intelligence’ and ‘Cyber Defence Detection and Response Analysts’ on the contextual side, to ‘Cyber Operations Intelligence’, ‘Malware Analysis’, and Security Operations Center team leads having a greater technical focus. With the pressure to attribute prevalent in current political affairs, this article explores

---

9 All interviews were conducted anonymously and will be cited accordingly. No attribution is attached to any quote from an interviewee within this article.
10 A Security Operations Center (SOC) is a term that generally refers to the centralised security function that is responsible for managing information security for an organisation. For more information on a SOC’s scope and structure, see “What is a SOC,” Crowdstrike, 21 May 2020, www.crowdstrike.com/epp-101/security-operations-center-soc/.
potentially effective approaches to attributive challenges. The challenge of false flag scenarios, in which threat actors actively encourage misattribution through the planting of counterfeit clues, will remain a consistent theme through each section.

Practitioner Perception Bias

It is worth noting that across the UK experts interviewed, their insights were shaped by their professional experiences relating to cyber defence. While overall experts did not seem to differ in the conclusions that contextual intelligence could be beneficial through broadening and strengthening an evidence base, there were certain topics on which attitudes tended to cluster into opposed perspectives. There are a number of possible influences forming attitude divisions, with the most consistent opinion splits aligning with role-type. The views, priorities, and suggestions from experts appear to be influenced foremost by whether their role tended to focus on contextual or technical analysis. That said, it is likely that additional influences stem from organisation type and size, as well as management structure and colleague background.

There were a number of topics in which these role biases appeared to present themselves. First, there is observable variance on exactly how far contextual analysis could resolve challenges in attribution. Colleagues working in political research were unanimously supportive of process changes to supplement existing methodologies with non-technical evidence. This argument that ‘more is better’ when building out the most likely narrative was not seen to the same extent in technical cyber defence of malware-focused colleagues, who were more likely to see contextual intelligence as a ‘nice to have’ benefit.

Considering how false flag operations necessitate additional concerns and a change in approach, technical analysts tended to show more confidence that false flags are not a usual challenge at this time. Instead, they argued that false flag operations go beyond the minimum requirements for an actor merely wishing to avoid attribution and maintain a claim to ‘plausible deniability’. The argument states that the difficulties in maintaining false flag operations over time are vast, and tradecraft mistakes are therefore likely. While attackers will almost always use an anonymisation service, such as Tor, mistakes will occur more often or not, revealing a genuine technical attribute such as an IP address or their ‘true’ location. Mistakes were highlighted as the main method through which false flags were detected, and technical experts did not view this as a shortcoming. In comparison, experts with expertise in politics and policy showed more concern, highlighting the wider diplomatic consequences of errors, in a complicated and nuanced exercise. Technical and political (context-driven) colleagues were also split on the frequency of attacks. Technical colleagues reported false flag operations as being relatively rare in the wild, while political colleague’s response noted that as undetected operations remain
unquantifiable, the amount of false flag attacks is likely significantly underreported. Political colleagues also tended to focus on potential futures, with experts expressing ‘wariness’ that as false flag operations become more feasible, they would be more commonly observed in the wild.

An interesting insight came from two intelligence experts who felt they ‘wore both hats’, having engaged in technical and contextual analysis. Both experts felt the frustrations of colleagues with opposing views and felt unable to describe how these might be practically addressed. This raises an interesting challenge where the overall goals of experts are united, yet favoured objectives and methods differ widely depending on each party’s standpoint and priorities.

**The Analysis Gap**

Research on the topic of cyber attribution generally stems from two distinct fields: Technical and Contextual. The first portion focuses on the technical detail and scientific foundations of tracing an attack to a point of origin. The technical-focused literature appears designed for a scientific audience, exploring tactical methods of reviewing immediate methods and defence experiments. The second focuses on the contextual challenges to attribution, and the strategic questions of the after-effects of attribution. This literature tends to be more journalistic or policy-focused in nature, commenting on observed threats and wider themes such as the difficulty in securing transnational cooperation, rather than procedure-level guidance for practitioners. For example, a Tallinn Paper, *Responsible Attribution*, concentrates on broader concepts across ‘cyberspace’ and laments the ‘overreliance upon signals intelligence (SIGINT) without physical corroboration from human intelligence (HUMINT)’\(^{11}\). Egloff highlights the importance of public attribution as a policy tool contributing to a nation’s deterrence strategy\(^{12}\), and further highlights the need for greater institutional transparency and greater cross-sector engagement when publicly attributing attacks\(^{13}\). In a similar approach, Carr reflects on the challenges of attribution beyond pure technical barriers, such as the oversight and verification of the intelligence industry, and how false flags may ‘take advantage of geopolitical tensions’\(^{14}\). Articles of this type often suggest that the very structures and approaches to attribution must change\(^{15}\), though, they do not propose particular incremental solutions or actions that could be taken by an

---


\(^{14}\) Carr, *Responsible Attribution: A Prerequisite for Accountability*, 4.

individual organisation or by a state acting unilaterally. A review of cyber conflict political science literature argues that the field has ‘perhaps focused on theoretical work at the expense of empirical work, acknowledging how the limited available data relating to cyber attribution makes it difficult to engage with quantitative research at a sub-national level’. Likewise, Boebart highlights the distinction in cyberattacks that prompt two stages of analysis: the technical determination of which machine is responsible for an attack, and the non-technical challenge of linking an actor to the machine. The divide in the literature between the technical and contextual challenges accurately reflects the existing divide that often presents in modern attribution practices. Overall, while the best-resourced organisations may have dedicated colleagues to add contextual analysis, in practice many SOCs (or, in smaller organisations without a dedicated SOC, personnel with cybersecurity-related responsibilities) do not have the luxury of engaging services that are not universally deemed essential for cyber defence.

To overcome this divide, the existing consensus is to require intelligence analysts to use ‘generalist broad-thinking capabilities’ in an investigation. In practice, intelligence analysts conduct a technical review of the attacker’s tools, techniques, and procedures for an attack and rely on actor error to detect false flag operations. Experts were divided on how far the reliance on technical mistakes represent a vulnerability on the defender’s part. Many of the interviewees on the contextual side raised concerns that sophisticated actors may not make mistakes so easily, while the technical practitioners tended to show more confidence in current attributive practises.

While attribution is complicated by both technical factors and by contextual issues, complications are further compounded by a lack of

18 This project’s interview findings revealed that the majority of interviewees did not have in-house contextual analysis taking place, with the exception of colleagues employed at a financial institution, a large consultancy practice, and the UK Government. Additionally, pure technical colleagues did not see the necessity of the contextual analysis within the process, while the more context-driven colleagues felt like context was not always given the attention they thought appropriate. On multiple occasions interviewees highlighted that where colleagues in leadership had a primarily technical skillset and focus, attributive efforts were less likely to engage with contextual analysis, including strategic and political analysis.
consensus on a unified approach. There does not appear to have been significant analysis undertaken in the space between the two sides in terms of how to practically and effectively address some of the operational challenges around cyber attribution and false flag attempts.

Technical and Contextual Challenges in Attribution

This section outlines a variety of challenges relating to attribution, highlighting how complicated and multifaceted attributive efforts may be. These outlined technical problems of attribution compound in ways that are well-documented.

In general, the very structure of the Internet and computing architecture raise opportunities for diverting blame because it is a network that prioritises innovation and collaboration over security. For example, while current internet infrastructure is based on IP addresses as a marker of identity, this attribute, along with physical location and activity sources, can be easily falsified, or ‘spoofed’ through the use of Virtual Private Networks or proxy servers, and may facilitate a false flag exercise by masking an actor’s physical location. Current architectures are not required to keep any information on the previous states, preventing analysis on previous actions.

---


This feature of short-lived, or ephemeral, knowledge means information such as protocol details may not be available between local and other cyberspace components and may not be retained after execution. This structures contributes directly to the obscurity and complexity that investigative intelligence analysts face today, including challenges around system log or incident data overload when examining the nuances of advanced, complex, or multi-faceted attacks, sifting through technical indicators, or deciphering how malicious activity may deviate from benign cyber behaviour in order to highlight suspicious activity\textsuperscript{23}.

As these challenges highlight, there are a number opportunities to use the feature of the net to deliberately complicate attribute efforts. Technical attribution of false flag attacks may not always be possible due to obfuscation, advanced attack methods preventing investigation of key attack attributes, or the sheer number of technical limitations due to the Internet’s inherent features\textsuperscript{24}. Where technical evidence is insufficient for confident attribution, contextual analysis has the potential to corroborate or discount hypotheses based on wider political or attacker motive-based considerations.

\textit{The Advantages of Contextual Analysis}

The divide between technical and contextual analysis in attribution highlights a practice gap: SOCs across the world analysts examine technical information to attribute, while not necessarily considering individual, societal, political and/or general contextual factors. Contextual analysis has strong potential to contribute to the exercise. Geopolitical analysis, focusing on politics, international relations, and geographical landscapes, offer a lens to see incidents within a wider context. Strategic analysis, or more specifically, the analysis of the intentions and motives of threat actors, provide another perspective through which one can analyse the why and through what methods a threat actor is likely to attack as part of an operation. These considerations illustrate the context around what might appear to be a standalone attack; highlighting that particularly large-scale, sophisticated operations are not orchestrated in a vacuum.

While existing research currently does not focus on potential solutions for the analysis gap in attribution, the experts interviewed highlighted several benefits of incorporating contextual forms of evidence into existing intelligence protests. For example, several larger organisations referred to internal project attempts to map geopolitical events against cyber events to understand potential drivers for incidents. The importance and challenge seemed to lie in the format of the intelligence, with actionable and


\textsuperscript{24} Boebert, “A Survey of Challenges in Attribution.”
confident content allowing teams to pre-empt increased cyber-activity from a certain actor, or to a certain target. Geopolitical analysis was considered to be valuable in contributing to a broader evidence base, where additional sources of information would only complement confidence in a leading hypothesis. The saying, ‘never put your eggs in one basket’, was referred to by one security researcher, using additional levels of analysis to supplement rather than replace technical understanding.

Practitioner attitudes reflect academic literature. Guerrera and Bartholomew outlined how ‘even the most advanced threat actors may rely on publicly available tools’, again highlighting how technical analysis may not allow for identification of a particular actor. Where malware or tools could be downloaded from online platform, such as VirusTotal, the attacker has the opportunity to minimise time, cost, and resource of developing custom attack methods, and is able to hide behind a ubiquitous tool rather than a specific instrument linking them to their previous crimes. Similar to false flag operations, deception of this form represents a hindrance to any attempt to connect a cyber-attack with the correct responsible agent.

Technical obfuscation is just one significant set of problems within ‘the challenge of attribution’, according to one interviewee. The issues relating to cyber-attribution specifically have been highlighted by prominent scholars in recent years, building on the trail of non-cyber intelligence research on attribution and geopolitical affairs. Many of the themes and complications attributing in traditional intelligence may also be applied to cyber attribution. For example, there may be difficulties securing transnational cooperation, particularly where the nation-states involved are suspected actors. Simultaneously, the lack of transparency of intelligence bodies, necessary and unnecessary, raises further national security complications. In not revealing their processes or evidence, an intelligence agency’s findings may be subject to question, and may be perceived as illegitimate or biased by third-party countries. Simultaneously, in revealing ‘sources and methods’, a state may inadvertently offer adversaries valuable information on how to circumvent certain techniques in future. In addressing practical challenges and limitations in cyber intelligence, the

26 Jajodia, et. al., Cyber Warfare.
geopolitical and strategic considerations should not be ignored, and wider challenges remain on the horizon.

At present, the methodologies in which attribution is attempted has the potential to reflect, exacerbate, minimise, and divert challenges. Focusing on how attribution takes place in practice, Carr’s Tallinn Paper, \textit{Responsible Attribution}, criticises the ‘overreliance upon signals intelligence (SIGINT) without physical corroboration from human intelligence (HUMINT)’. In a similar critique, the diamond attribution model often used by intelligence analysts—analysing ‘Adversary’, ‘Infrastructure’, ‘Victims’, and ‘Capabilities’—allows for technical analysis but ‘fails to consider the larger geopolitical context in which an attack occurs’. As Bartholomew and Guerrera state, ‘deficient hiring practices…overemphasize specialist technical knowledge and eschew broader-thinking capabilities’. Correspondingly, several of the experts interviewed lamented on the lack of a strategic process or ‘best practice’ methodology or training principles, as well as the challenge of finding appropriately-skilled personnel. This reflects a challenge outlined by Bartholomew and Guerrero-Saade, who highlighted the current skillsets and lack of relevant contextual-based training as an obstacle to successful attribution.

Combining evolving threat actor behaviours, developing political contexts, shifting threat vectors, and the practical difficulties in running a SOC (or wider information security function) practitioners are left with a long list of interrelated challenges. This is not addressed in practice, however, as intelligence relating to analysis of the motives and intentions of threat actors is not necessarily considered in a cyber intelligence setting. False flag operations reveal additional weaknesses, and Bartholomew and Guerrero highlight that efforts rely ‘on a combination of fungible technical indicators, mistakes, overlaps, and luck’, highlighting a number of operations in which false flags were used to mislead investigators. A useful example describes how the suspected-Russian-affiliated Sofacy group created an extremist Islamic persona ‘CyberCaliphate’ in 2014, during the TV5Monde hack. Bartholomew and Guerrera highlight the specific ‘blame-shifting’ behaviours of false-flag operations, and report how a lack of awareness in the wider threat landscape may well have resulted in misattribution. Examining the challenges of attribution for sophisticated advanced persistent threat (APT) level threats such as typical nation-state attacks, the issue of false flag operations becomes extremely relevant in terms of

\begin{thebibliography}{9}
\bibitem{31} Carr, \textit{Responsible Attribution}, 1.
\bibitem{32} Sergio Caltagirone and Andrew Pendergast, \textit{The Diamond Model of Intrusion Analysis} (Hanover, MD: Center for Cyber Intelligence Analysis and Threat Research, 2013).
\bibitem{33} Edwards, et. al., “Strategic Aspects of Cyberattack, Attribution, and Blame,” 2826.
\bibitem{34} Bartholomew and Guerrero-Saade, “Wave your false flags!,” 9.
\bibitem{35} \textit{Ibid.}, 10.
\bibitem{36} \textit{Ibid.}, 9.
\end{thebibliography}
potentially severe consequences in cases of incorrect attribution. If an intelligence team relies on technical attributes such as the technical Indicators of Compromise (IoCs), time-stamps, IP addresses, and so on, false flag operations have the potential to falsify much if not all of the technical evidence. With counterfeit data as a primary source, even sophisticated forensic analysis may be misled as a result.

Given the potential for false flag operations to mislead attribution efforts, the range of interviewee perspectives on the usefulness and necessity of contextual approaches may be considered concerning, particularly given the diverging approaches to attribution practiced even between the relatively small sample size of UK-based experts. The lack of consensus and agreed best practices to attribution in contextual terms raise a number of opportunities to include multidisciplinary approaches beyond pure technical analysis. The following sections reflect the views of practitioners on how examining the challenges of attributing false flag attacks, four proposals are highlighted to implement additional layers of analysis: interdisciplinary teams; training technical colleagues on geopolitical content; information-sharing platforms; and outsourcing. A discussion on the practitioners’ experience in attribution reflects on the perspective gap currently existing between technical and non-technical analysis and reaffirms the need for multi-disciplinary approaches to attribution.

Advancing Attribution: Opportunities

When considering the most effective ways to incorporate strategic analysis into an intelligence process, observations are categorised into the following four proposals: interdisciplinary teams; effective training; strategic information sharing platforms; and outsourcing. This section recognises that some or all of these recommendations are incorporated among international actors with the most resources, with national cyber security centres or financial institutions perhaps being two examples. The opportunities highlighted below are derived from the interviewees’ recommendations on improving attribution practices primarily across private industry.

Creating Interdisciplinary Teams

Several organisations report intelligence teams comprising of political and technical colleagues, reflecting the view of intelligence through collaboration rather than a ‘silo-ed’ role. An ideal communication structure between contextual and technical cyber defence colleagues would involve ‘at least a two-way information flow’. Examples were highlighted whereby a political intelligence expert developed relationships with technical colleagues and could raise and receive information on an ad-hoc, responsive basis. Joint reports were provided where the political team would send a draft for technical colleagues to review and include technical input. This was

37 Edwards, et. al., “Strategic Aspects of Cyberattack, Attribution, and Blame.”
described as an informal relationship where colleagues ‘could just call and flag “What do you think about this?”’.

There are two main limiting factors surrounding interdisciplinary teams: the dependence on organisational management to support and create such a structure, and the resources available to the team. Organisational culture has an undeniably strong effect on resulting team structures. The inclusion of political and technical analysts within the same team was in every case a decision made strategically by senior management or team leads, operating within certain limits, including budget, resources, and time constraints given their objectives. Organisations with very little resource tended to have little to no qualitative input beyond recognising the technical behavioural set of Techniques, Tools, and Procedures for threat actors, while those at larger organisations either had strategic colleagues within a team or worked closely with another team to secure strategic and geopolitical context. The phrase ‘nice to have’ or ‘luxury’ was used across interviews when referring to less technical and/or contextual research. This raises a challenge to the political analyst to present their analysis as a valuable asset in an environment typically characterised through quantitative measures and data.

Effective Context Training

With many organisations do not have the financial ability to hire in-house political analysts, the options remain either to try and incorporate contextual analysis into a technical analyst’s role. This would encourage critical analysis of events by looking at the intentions and motives of state actors and state policy to infer potential threat actors. While experts report a precedent in ‘on-the job’ training to ‘less-technical’ colleagues to enable technical skill development, it is possible that critical thinking and contextual awareness could be taught within a wider colleague training package. This training would need to be refreshed and carefully thought out but may assist in enabling technical colleagues to build out a narrative using interdisciplinary skills and bringing in political considerations. There are a few precedents for this, with cybersecurity training institution, SANS, having retired a course on ‘Active Defence, Offensive Countermeasures, and Cyber Deception’. This course offered hands-on proactive defence strategies walkthroughs and emphasised the need to understand an adversary’s intentions38. The SANS course that comes closest to considering actor behaviour in the threat landscape is ‘Cyber Threat Intelligence’, which does not mention deception within the syllabus39. Covering the threat landscape and attacker motivations alongside technical training and may provide the

basis for a syllabus or training structure when designing additional or internal training opportunities.

While experts consider this may be a sufficient workaround depending on how often the team will attribute, this method relies on employees to have a set of skills beyond what is generally required on a technical cyber analyst’s job description. To place responsibility for all aspects of attribution on employees specialising in particular skills—for example, malware analysis and reverse engineering—involves a risk that they may not be well-equipped to deal with different aspects.

**Information-sharing platforms**

Faced with knowledge-gaps in the team, one option for organisations would be to source the required contextual information from an intelligence sharing platform that could host geopolitical updates and expectations. Platforms such as the Cyber Security Information Sharing Partnership (CiSP), a joint industry and government initiative, enables cyber threat information-sharing. The interviewees suggested, however, that CiSP was more network-defence focused, rather than an information sharing platform. Simultaneously, while other networks such as ThreatMatrix also provide a predominantly technical view, it is possible a ‘political-cyber’ feed would likely benefit analysts and represent a ‘value-add’ information system that is not yet widely available.

The difficulties associated with information-sharing are not unique to geopolitical intelligence. In an industry where information-sharing is a profitable enterprise, there is often a lack of motivation for threat intelligence organisations to share their most exclusive content. In a pessimistic sense, this may translate to the majority of members benefiting from the contributions of a few proactive actors. This ‘free-rider’ effect was also a limitation mentioned by one interviewee, who cited it as a barrier to engagement with certain information-sharing platforms.

**Outsourcing**

Many interviewees expressed a preference for delegating or deflecting attribution attempts away from their own team, reporting incidents either to the National Cyber Security Centre or to specific threat intelligence bodies. Smaller companies may make better investments than those focusing on attribution in-house, through, for example, hiring a skilled threat-hunting team who are specifically dedicated to identifying and tracking advanced relevant threats. They may also choose to secure political intelligence through an established vendor rather than hire full-time political analysts.

Limitations discussed relate largely to reputability and affordability. First, the intelligence sources should be picked wisely. If the intelligence sources are reputable and established brands, irresponsible reporting and

---

the ‘race to attribute’, referring to rushed and potentially mistaken analysis, should not be of major concern. Public blogging and reporting are considered of greater concern, with the threshold for publication requiring significantly less rigour than established vendors, with increased chances of misattribution and incorrect assertions. Second, a major drawback for outsourcing attribution resource and intelligence can be the cost-prohibitive nature of threat intelligence products. Few organisations, except for governments and global corporations, will be able to justify more than one intelligence product.

**Proposal Evaluation**

Having classified four possible proposals, it is noted there is no objectively superior path to implement well-rounded analysis. In general, some proposals require a lot more effort and organisational commitment than others. Hiring and managing an interdisciplinary team represents a greater expenditure—and in many cases, a departure from a precedent—compared with relying on vendor intelligence. In general, experts were open-minded as to how political analysis may be incorporated into intelligence, though were unsure how this might be practically implemented at their organisation. The proposals represent hypothetical solutions. This highlights the managerial and practical difficulties in proposing new approaches in the attribution space, where there is no objective best-practice model.

**Addressing Perspective Gaps**

Given false flag operations have the potential to mislead attribution including efforts to attribute potential APT-type cyber-attacks, the current gap is concerning. Engagement with experts from various sectors, disciplines, and role-types highlighted a breakdown in overall consensus in specific areas that will translate into different proposed solutions. Bringing the technical and political fields of conversation together offers the chance to connect the researcher and the technical analyst, exploring how the more qualitative, theoretical- and local knowledge-led political approach might practically assist in the day-to-day challenges faced by practitioners. It also highlights the challenge in balancing the diverse needs between intelligence analysts, researchers, and policymakers.

**Conclusion**

Investigating the intentions and motives of threat actors, as well as understanding cyber events within a wider geopolitical context, was considered an advantage particularly concerning the issue of false flag operations. Four proposals were highlighted to implement additional layers of analysis: interdisciplinary teams; training technical colleagues on political
issues; information-sharing platforms; and outsourcing. A range of proposals offers flexibility to approach the current gap as the efficacy of each proposal depends on the size and nature organisation in question. The inclusion of additional layers of analysis, including strategic and political evaluations, go some way to addressing the existing gap between purely technical and context-driven approaches, reaffirming the need for multi-disciplinary approaches to attribution. Answers should be understood as a product of experts’ perspectives that appears to align to their role type, as well as other attributes of their work environment and perceived objectives. There therefore exists further opportunity to determine productive cooperation between different groups of stakeholders.