RESEARCH BRIEF

Mapping a Path to Cyber Attribution Consensus

THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

Rachel Anne Carter, Director Cyber, The Geneva Association

Insuring cyber risk

The rapid pace of digital transformation, accelerated by COVID-19, is driving increased demand for cyber risk protection. There are a number of ways in which this can be achieved. Insurance is one mechanism, which focuses on the economic protection of a business if it experiences a cyberattack.

Cyberattacks can have a truly global impact, wreaking havoc across systems, companies and societies. In the context of cyber terrorism and war, large accumulations of loss arise not only from the intended targets but also from collateral damage.

Attribution is key to identifying the responsible actor in such events, and in many cases ultimate responsibility is assigned to a state. It is also an essential component in discerning the type of attack, whether cyber terrorism, hostile cyber activity (HCA) or cyber war. Consequently, the outcome of the attribution process plays an important role in determining whether insurance will ultimately cover a loss or who should ultimately pay.

Insurance policies covering cyberattacks typically exclude war risk. Minimally, war has been defined as a state of conflict between states or nations, so a key question when applying a war exclusion is whether a state actor is ultimately responsible. At present, it is debatable whether it is sufficient to establish if the hostile actor is a state, rather than having to also establish which particular state or state actor is responsible. With cyberattacks it can be difficult to determine whether the accountable party is a nation-state and, therefore, whether a war exclusion might apply to an insurance policy.

Another challenge is the inconsistency associated with attribution as carried out by governments, their agencies and private organisations. If a government engages in public attribution it could be motivated by political factors as much as technology- and intelligence-based evidence. More commonly, governments participate in accurate and precise attribution but do not make their determinations public or disclose them in a timely manner. To resolve such inconsistency, there are efforts to develop a widely-accepted framework for cyber attribution, focusing on a common approach, both in terms of the actor and the behaviour.

In 2020, The Geneva Association and The International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP) introduced the term HCA in the first report in a three-part series on cyber terrorism and cyber war (CTCW) to help clarify behaviour where there was previously a degree of ambiguity. In terms of responsibility, HCA seeks to distinguish between what is potentially insurable and what is not (war). The second report in the series was published in March 2021 and provides insurers with a framework for attributing and characterising cyber incidents, seeking to promote international collaboration, validating international norms or conventions that could help streamline the attribution process.

Table 1: Actors and their capabilities

	Cyber crime	Cyber terror	HCA	Cyber war
Cybercriminal	✓	✗	✗	✗
Cyber terrorist	✓	✓	✗	✗
State actor	✓	✓	✓	✓

Source: The Geneva Association

The attribution process

The key aspects of attribution include:

- **Technical attribution:** decoding the digital footprint of an event
- **Political attribution:** understanding and addressing various factors, which may cause a state to attribute or to claim involvement of another state
- **Legal attribution:** satisfying the burden of proof

Technical evidence and know-how

The first challenge is to effectively use what is known about the technology and the vector of the attack to hypothesise about the identity of a possibly responsible individual, group, organisation or state. Depending upon the cyber perpetrator and the objectives of an attack, additional effort may be made by the cyber actor to disguise their true identity. A cyber adversary may adopt techniques used by well-known cyber groups to mimic their online behaviour and make it more difficult to determine the true perpetrator of the attack.

Attributing a cyber event to a state is increasingly difficult. That a state was merely aware of an activity is unlikely to be sufficient. Although HCA may not require attribution to a specific state, proof of state involvement will be needed; most likely active or overt involvement.

Political and legal considerations

Even if the technological problems are overcome and a particular person, entity or organisation is identified as having launched a cyberattack, there remains the question of whether or not a state can be held responsible for that individual's or organisation's actions.

There is no international standard at present for attribution; there are no laws, regulations or treaties that promote consistency. International politics can also lead to attribution determinations that are not correct.

Understanding the connections between a state and the perpetrator(s) carrying out the attack will be important in determining if the attack can be attributed to the state. This will require analysing the state's control over the perpetrator through a holistic assessment of the circumstances, rather than by analysing the act itself, and benefits the state may have received from the cyberattack. If the actor was a government agency, part of the national military or otherwise a body of the state, there will likely be sufficient connection between the actor carrying out the attack and the state accused of being responsible for an attack. In many other cases, the connection will not be as strong. Table 2 illustrates different layers of potential interconnectivity between states and actors.

State-integrated, state-executed, state-ordered, state-coordinated, state-shaped actions will likely be used to help prove attribution and characterisation (state involvement and thus war or warlike activity or HCA). Imposing responsibility on a state becomes more circumstantial for state-encouraged, state-ignored, state-prohibited actions.

The challenge is not only achieving certainty but the implications of having to retract an attribution if subsequent evidence suggests that a state was not as involved in the coordination or execution of an attack as once thought.

Another pivotal aspect is the role of contract law. Insurance centres on a contractual relationship between the insurer and the insured. Resultantly, contract law will shape the ultimate determination of whether insurance coverage exists under a policy. Therefore, the ultimate authority on attribution for insurance purposes will be legal institutions and instruments: courts, tribunals and judges, statutes, regulations and legal precedent (where it exists). As discussed, attributing an event to a state or entity could significantly affect the coverage and payment or the legitimate denial of a claim.

Figure 1 shows an illustrative framework of the attribution process in practice, including key steps and components.

Table 2: The spectrum of state responsibility explained

Category	Examples of state actions/involvement		
Cyberattack	Conducting	Abbeting	Ignoring
State-prohibited	None	None	Low Inability to secure computers, but attacks prosecuted
State-prohibited-but-inadequate	None	None	Low Inability to secure computers and stop attacks
State-ignored	None	Low Stalling investigations and possibly tipping off attackers	High Disregard private attacks and fail to seriously investigate
State-encouraged	Low Possible 'off-duty' attacks by officials or military	Low to Medium Statements to embolden or energize attackers	High Disregard private attacks and fail to seriously investigate
State-shaped	Low Possible 'off-duty' attacks by officials or military	Medium Some technical and targeting support	High Disregard private attacks and fail to seriously investigate
State-coordinated	Low Possible 'off-duty' attacks by officials or military	Medium to High Coordination of timing, targets, or tempo	High Disregard private attacks and fail to seriously investigate
State-ordered	Low Possible 'off-duty' attacks by officials or military	High Direct command of private attackers	High Disregard private attacks and fail to seriously investigate
State-rogue-conducted	Medium Forces attacking without authority	None The national government is not behind the attacks and may stop them	Medium Other agencies may disregard the rogue attacks
State-executed	High National forces attacking with authority	None The only attackers belong to state organizations	None The only attackers belong to state organizations
State-integrated	High National forces attacking with authority	High Direct command of attackers: technical and targeting support	High Disregard private attacks and fail to seriously investigate

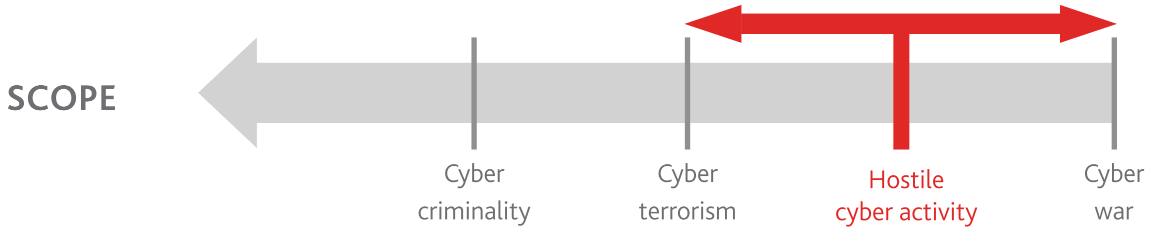
Source: Healey 2011

Figure 1: Illustration of the attribution process

Attribution

1. Initial characterisation of action

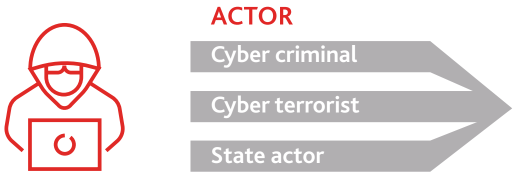
Was there a suspicion that the act was one of cyber terrorism, HCA or cyber war?



a. Technical analysis including private companies, police and intelligence services investigations

Often done secretly and information often cannot be found in the public domain

b. Attribution to actor (carried out 'in house' at present)



Thoughts about attribution to action only for own purposes i.e. not publicly known

2. Second characterisation of action

Process takes into account the actor

3. Communication of the attribution

Type of attribution	Enough for insurance?
Private (only to actor) • Often private for security/intelligence purposes	No
Semi-private • To actors such as other government intelligence services	No
Public without evidence • Credible country is attributing	May not be enough for insurance to use in court
Dubious country is attributing	Unlikely that attribution will be used by court; insurer has to prove with evidence
Public with evidence • Re/insurers can use the same evidence • Public evidence based attribution • Traditionally, country is attributing • Indictment of those responsible (legal path) • Recent trend: country is inditing responsible individuals and/or state	Yes

Source: The Geneva Association

This framework can be used to simplify the process of attribution and characterisation and dispel uncertainty by reducing complexities to a series of steps and checklists which may be used by insurers. As products are currently designed, the re/insurance community would benefit from a recognised system for attributing cyber events, enabling the holistic assessment of potential industry exposures – and promoting insurability.