THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

Mapping a Path to Cyber Attribution Consensus

IFTRIP

International Forum for Terrorism Risk (Re)Insurance Pools

March 2021

Mapping a Path to Cyber Attribution Consensus

Rachel Anne Carter, Director Cyber, The Geneva Association

Julian Enoizi, Pool Reinsurance Company Limited, and Secretariat, International Forum of Terrorism Risk (Re)Insurance Pools

The Geneva Association

The Geneva Association was founded in 1973 and is the only global association of insurance companies; our members are insurance and reinsurance Chief Executive Officers (CEOs). Based on rigorous research conducted in collaboration with our members, academic institutions and multilateral organisations, our mission is to identify and investigate key trends that are likely to shape or impact the insurance industry, highlighting what is at stake for the industry; develop recommendations for the industry and for policymakers; provide a platform to our members, policymakers, academics, multilateral and non-governmental organisations to discuss these trends and recommendations; reach out to global opinion leaders and influential organisations to highlight the positive contributions of insurance to better understanding risks and to building resilient and prosperous economies and societies, and thus a more sustainable world.

International Forum of Terrorism Risk (Re)Insurance Pools

The International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP) is a collaboration between global terrorism (re) insurance pools. It was formally ratified at the National Terrorism Reinsurance Pools Congress organised by the Australian Reinsurance Pool Corporation (ARPC) in Canberra in October 2016. The organisation was founded with the goal of promoting initiatives for closer international collaboration and sharing expertise and experience to combat the threat of potential major economic loss resulting from terrorism. The activities of IFTRIP include facilitating a range of international cross-organisational working groups, collective impact initiatives and international events, including an annual conference where a community of experts from the industry alongside business decision-makers ensure delegates stay up to date with the latest thinking and discussions around the risks posed by extreme events. IFTRIP is governed by the IFTRIP charter and is bound by local and international regulations.

Photo credits:
Cover page – Titima Ongkantong / Shutterstock -

Geneva Association publications:
Pamela Corn, Director Communications
Hannah Dean, Editor and Content Manager
Petr Neugebauer, Digital Media Manager

Suggested citation:
The Geneva Association. 2021. *Mapping a Path to Cyber Attribution Consensus*. Authors: Rachel Anne Carter and Julian Enoizi. March.

www.genevaassociation.org

Contents

Acknowledgements

The authors (Rachel Anne Carter and Julian Enoizi) first wish to thank Chuck Jainchill, Cyber Product Development Leader, AIG for leading the expert group on attribution. The authors also extend their gratitude to the members of the cyber terrorism and cyber war (CTCW) task force and the external contributors to this project, especially Kaja Ciglic (Microsoft) and Yuval Porat (KAZUAR), who provided technical guidance, and to external reviewers, including Kai-Uwe Schanz, Matt Harrison, Lawrence Winter, Richard Ifft, Francisco Espejo Gil and others who provided guidance on the report.

Leadership team: Chuck Jainchill, AIG; Daniel Mesfin, Allianz; Dennis Sno, Hannover Re; Philipp Lienau, HDI Global; Christopher Wallace, ARPC and President of IFTRIP; Francois Vilnet, GAREAT and IFTRIP; Christian Wells, Pool Re and IFTRIP; Tony Ellwood, Lloyd's Market Association; Cyrus Delarami, Munich Re; Franz Gromotka, Munich Re.

CTCW experts: Jannice Koch, Allianz; Neil Arklie, Aviva; Alexandra Maunie, AXA; Mathieu Cousin, AXA; Peter Zimmerli, Axis Capital; Matthew Webb, Hiscox; Anna Fenech, ARPC and IFTRIP; Daniel Largacha Lamela, MAPFRE; Rory Egan, Munich Re; Chris McEvoy, Partner Re; Chris Yeates, Pool Re and IFTRIP; Szymon Mitoraj, PZU; Sie Liang Lau, SCOR; Alexander Bosch, SCOR; Kei Kato, Tokio Marine; Masashi Yamashita, Sompo Japan Insurance Incorporated.

Foreword

Cybercriminals are known to exploit society's vulnerabilities during times of crisis. That is why authorities were quick to sound the alarm on cyber threats in early 2020, when the pandemic emerged.

The warning was justified. In mid-2020, the United States Federal Bureau of Investigation (FBI) reported a 400% increase in the number of cybercrime incidents. In a July 2020 survey of 1,000 global IT leaders, 90% of them indicated an increase in cyberattacks due to the pandemic. We are seeing one invisible virus compound another.

In this context, businesses need to be proactive on two fronts: 1) safeguard themselves against the spectrum of cyber risks by exercising rigorous 'cyber hygiene', and 2) plan their event response. There is a role for insurance in both respects. Our cyber terror and cyber war initiative focuses on the second; namely, promoting the insurability of cyber risks.

In the first report of our cyber terror and cyber war series, published in July 2020, we tackled the 'what?', aiming to bring clarity to the language used to define types of hostile cyberattacks in insurance policies.

This second report addresses the 'who?' by pushing for a recognised, industry-wide approach to attribution, or identifying the responsible actor. We propose a series of steps and checklists, in order to structure the process of attribution and characterisation for insurers. The report further stresses the importance of building collaboration across sectors – insurance, technology, government and others. This would set the stage for developing an international norm to promote a consistent and streamlined approach for attribution.

The third and final report in the series, on public-private solutions, will suggest ways for insurers and government actors to collaborate in protecting society from cyberattacks – an increasingly urgent matter, especially in light of the pandemic.

Jad Ariss
Managing Director

The Geneva Association

Christopher Wallace
President, IFTRIP

CEO, Australian Reinsurance Pool Corporation, ARPC

1. Executive summary

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 cyber risk protection can be achieved which include a high level of cyber hygiene, implementing and investing in standards for cyber security, not merely in terms of initial security measures but also a strategy for maintaining and upgrading security. Insurance is one mechanism, which focuses on the economic protection of a business if it experiences a cyberattack. Even though insuring cyber risk is challenging, not least due to the potential for large accumulations of loss, insurance as part of a broader security strategy can reduce overall losses. It can encourage behaviour that promotes the robustness of online systems and incentivises good cyber hygiene.

Cyberattacks can have a truly global impact, wreaking havoc across systems, companies and societies. In this report's context of cyber terrorism and war, large accumulations of loss arise not only from the intended targets but also from collateral damage. Such collateral damage affects corporations (or other entities, such as not-for-profit organisations, healthcare providers, etc.), government entities and individuals located in the target state or connected to the target state.

In such events, to identify the responsible actor, attribution is a key factor. It is 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 is an important factor to determine whether insurance will ultimately cover a loss or who should ultimately pay. This also relates to issues associated with how to hold malicious actors accountable. Responsibility and accountability are critical in safeguarding society from malicious cyber acts. Specifically for cyber insurers and insureds, attribution and accountability can be critical, given the widespread use of war exclusion clauses within policies and the values at stake.

> Attribution is an essential component in discerning the type of cyberattack, whether cyber terrorism, hostile cyber activity or cyber war.

The process of attribution is the allocation of responsibility for a cyberattack to an actor, and in many cases the assigning of ultimate responsibility to a state. Attribution plays a large part in characterising an event (war, cyber terrorism, HCA, crime). The processes of attribution and characterisation are often used to assess the applicability of any sub-limits for cyber terrorism and where losses can be ceded to terrorism pools. Further, effective attribution can help insurers avoid breaches of sanctions that may prohibit the making of payments for cyber extortion to certain organisations, individuals or states.

Insurance policies covering cyberattacks – both dedicated cyber policies and more traditional policies that extend to cyber events – typically exclude war risk. War is not an insurable risk under traditional insurance policies, but the scope of 'war exclusions' has been subject to debate and differences in application and language used by insurers. 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. In traditional military conflict it is often (but not always) obvious to discern from where a hostile act emanated. However, with a cyberattack it can be more difficult to determine whether the accountable party is a nation-state and, therefore, whether a war exclusion might apply to an insurance policy.

With a cyberattack 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.

In 2020 The Geneva Association and IFTRIP introduced the term *hostile cyber activity* (HCA) 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). Since the introduction of the term, divergent opinions regarding its insurability have emerged. It is likely that any products available to cover hostile cyber activity will be determined by individual carriers and specific markets based upon commercial considerations.

Another current 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. However, more commonly governments participate in accurate and precise attribution but they do not make their determinations public or disclose them in a timely manner. Public attribution is a careful consideration of the benefits and costs which are associated with pointing the fingers publicly at an attacker, and potentially even framing the attacker as an 'enemy' or as a threat to national security. In many cases, governments may refuse to engage another state because it would not benefit their interests. In such cases the government may leave attribution to private entities or limit disclosure.

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.

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. Although there would be advantages to such a framework that extends beyond cataloguing technical factors, it is unlikely to get the required support in the foreseeable future due to differences in commercial priorities, legal systems, and other factors.

These barriers notwithstanding, this report seeks to promote international collaboration, validating international norms or conventions that could help streamline the attribution process. Comparability of attribution and characterisation approaches across jurisdictions will be critical for industry-wide assessment of accumulation risk and, ultimately, for the insurability of cyber risk. This is all the more important as the dependence of businesses, governments and societies on interconnected online systems has the potential to facilitate large-scale disruption and destruction upon the occurrence of a viral cyber event. Unsurprisingly, there are questions around the ability of the private insurance industry to absorb the losses from a catastrophic cyber event that is not bound by geography or industry. More fundamentally, one can also ask why the private insurance industry should pick up the bill for nation-state induced attacks at all.

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.

The re/insurance community would benefit from a recognised system for attributing cyber events, enabling the holistic assessment of potential industry exposure – and promoting insurability.

2. Introduction

Within the context of insurance, attribution is an important factor when analysing a cyber loss event and determining the parameters of coverage. Attribution is 'the process of finding out the chain of actors involved in cyber attacks' and in many cases assigning ultimate responsibility to a state or other defined group.[1] Attribution is a large part of determining the characterisation of an event (war, cyber terrorism, HCA, crime or something else). This report looks in detail at how various pieces of technical evidence are influenced by political factors and existing legal systems and the processes employed to determine responsibility.

Approaches to cyber terrorism and war

The term 'cyber terrorism' (as introduced into insurance market parlance approximately ten years ago) was designed to clarify coverage where actors with malicious political, religious, social or ideological motives might use the same methods as disgruntled insiders, criminals or hacktivists. In most circumstances, this term was used to clarify that coverage was available for malicious cyber events, regardless of motive, as long as the actor was not carrying out an act as a component of a broader military conflict. The categorisation of events as cyber terrorism or hostile cyber activity (HCA) or cyber warfare goes further than just labelling. It may assist insurers to track the types of events that have occurred, establish coverage, determine their probability and allocate capital accordingly.

Categorising events as cyber terrorism or hostile cyber activity or cyber warfare may assist insurers to track the types of events that have occurred, establish coverage, determine their probability and allocate capital accordingly.

The precise way that cyber terrorism has been incorporated into underwriting is a commercial matter that differs from firm to firm and market to market. However, generally in standalone, non-physical cyber damage products, cyber terrorism has been commonly included within the head of coverage, whereas in the more traditional, non-cyber-specific (and often physical damage oriented) products, terrorism (including cyber terrorism) is either excluded or may be purchased as an add-on to a traditional insurance policy that covers terrorism.

Although there is capacity available to cover cyber terrorism, policies vary in the amount covered and terms, such as requirements for physical damage or

1 Guitton 2015.

presence of sub limits. Notwithstanding the difference in definitions used by individual carriers, ideally the process of attribution would be neutral and apply regardless of the re/insurer providing coverage. This consistency would be even more beneficial if it were also applied globally. It would help promote higher limits and boost capital available for these risks within the broader cyber insurance markets.

Activating the cyber war exclusion

Attributing an event to a state or state actor, and possibly characterising it as cyber war, opens the possibility of activating war or similar exclusions. The question of the war exclusion or parts of it in the context of a nation-state attack is currently being tested in coverage disputes between property insurance carriers and their insureds relating to the NotPetya malware.[2]

Initially, the insured must illustrate an attack has occurred in which it suffered loss. The burden is then on the insurer to prove the exclusion clause. By illustrating that an excluded act has occurred, the insurer is then able to assert that the relevant exclusion applies, and the loss suffered by the insured is outside of cover.[3]

Hostile cyber activity: A tool to simplify attribution

In 2020, The Geneva Association and IFTRIP introduced the term hostile cyber activity (HCA) as a mechanism to promote terminological clarity.[4] The term HCA can minimise the opportunity for a mismatch of respective understandings between the insurer and the insured and promotes greater contract certainty. In terms of the attribution process itself, HCA can be used to attribute activity where there is proof of state involvement that has not necessarily occurred within a war or warlike environment.[5] Essentially malicious conduct by a nation-state that falls short of war and therefore may not be excluded under a conservative interpretation of most war exclusion clauses would be HCA.

There are different levels of commercial appetite to cover HCA. However, there is agreement that for behaviour to be characterised as HCA, a state must be responsible.

In looking at physical examples of hostile activity, the International Court of Justice (ICJ) was asked to assess which factors indicated state involvement. The ICJ determined that factors such as the training, arming or equipping of a group by a state or a government, or official department or body connected to an alleged state, indicates state involvement. The ICJ also considered the level of control and the knowledge or probable knowledge of the state thought to be responsible and how this might implicate responsibility.[6] Thus, even if it is challenging to narrow down responsibility and pinpoint an exact state from a list of potential state actors, these factors assist insurers to determine if it is objectively reasonable to attribute to a state actor.

Table 1 offers an overview of the relevant actors and their respective capabilities to carry out different acts of cyber terrorism, hostile cyber activity or cyber war, potentially resulting in a different attribution. Factors which determine how the ultimate event is characterised may require not just an attribution of the actor but also additional considerations such as the motivation of the actor. If the actor is deemed to be 'a' state, it may also be necessary to discern if the actor was a state actor or a state-sponsored actor as this too may assist in the characterisation of the event as cyber terror, HCA, cyber war or cyber crime.

Table 1: Actors and their capabilities

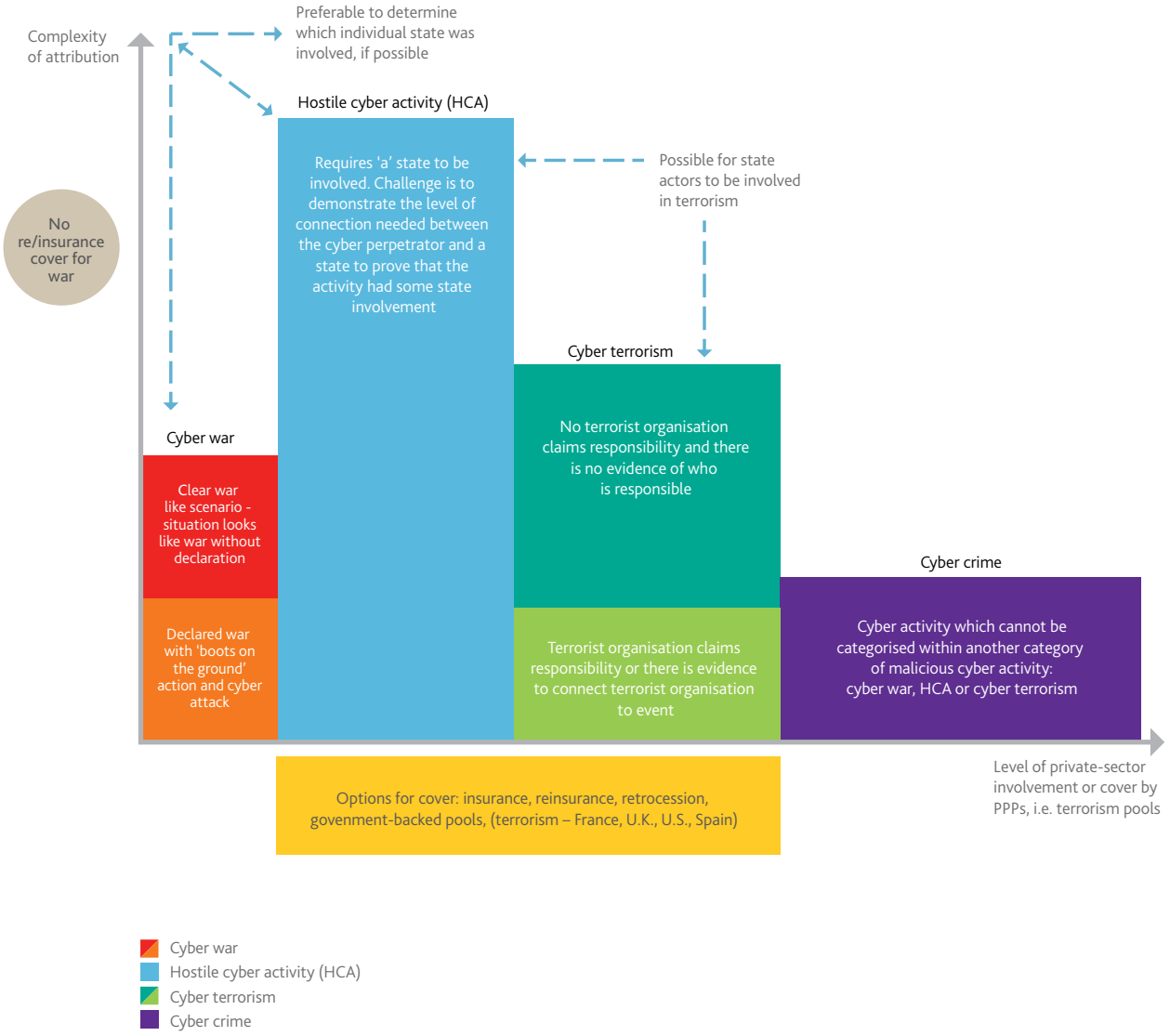
	Cyber crime	Cyber terror	HCA	Cyber war
Cybercriminal	✔	✘	✘	✘
Cyber terrorist	✔	✔	✘	✘
State actor	✔	✔	✔	✔

Source: The Geneva Association

2 See: Dyson 17 January 2019; Corcoran 8 March 2019; Menapace 2019.
3 See: Dyson 17 January 2019; Corcoran 8 March 2019.
4 The Geneva Association 2020. Authors: Rachel Anne Carter and Julian Enoizi.
5 Holland and Chiacu 22 December 2014.
6 Nicaragua v. United States of America 1984, 1986.

Figure 1 illustrates and summarises the levels of complexity associated with attributing cyber war, HCA or cyber terrorism and the implications for private-sector involvement.

Figure 1: The relationship between the complexity of attribution and level of private-sector involvement



Source: The Geneva Association

3. Attribution: More than just semantics

Once a cyberattack has taken place and damage ensues, the processes of attribution and characterisation kick in if it is suspected that the event is cyber terrorism, HCA or cyber war.[7] Based upon the Geneva Convention,[8] 'war' or a 'warlike' situation requires two or more states acting in a hostile manner towards each other.[9] Attribution of the responsible actor as a state is thus an important precondition to the operation of an exclusion clause.[10]

Within the insurance-specific gaze, there is likely to be a differentiation between coverage in the standalone cyber market and the non-affirmative insurance market, where potential cyber exposures are contained within traditional property and liability insurance policies which may not implicitly include or exclude cyber risk. If the event was unequivocally within the cyber cover provided, it is likely the process will be more seamless than if there is a challenge over the categorisation of the event.

During the Sony Attack,[11] and although private individuals and many intelligence services were working on the process of attribution, the results of this attribution remained outside of the public domain for a period of time, despite public pressure. Although a number of political leaders – most prominently, the U.S. President attributing a cyberattack for the first time ever – publicly blamed a specific state, there was no reliance on the cyber war exclusion by insurers.[12] The facts giving rise to the Sony Attack were within the probable loss scenarios which standalone cyber insurers had envisioned a loss arising from. It also underlines that not all cyberattacks from states will fall under 'war'; a much more severe attack is needed for such a characterisation.

Drawing parallels between terrorist organisations that operate in the physical world and those that operate in the cyber world, to date there is no evidence to suggest that terrorist organisations in the online environment would not seek to claim responsibility for physical terror attacks. Terrorist organisations are often driven by notoriety; they seek publicity and fear of significant disruption and

7 Attribution is a large part of determining the characterisation of an event (war, cyber terrorism, HCA, crime or something else). However, to simplify the process, many consider attribution and characterisation as two separate but interlinked processes.

8 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949, Article 2 as accessed at https://ihl-databases.icrc.org/ihl/WebART/365570005

9 The Geneva Association 2020. Authors: Rachel Anne Carter and Julian Enoizi.

10 War exclusions and war risk exclusions are not only confined to international warfare but typically include terms like rebellion, revolution and civil war. When there is rebellion, revolution or civil war it is possible that the actor is not a nation-state. This report however will not go into the contested divide between revolution and terrorism.

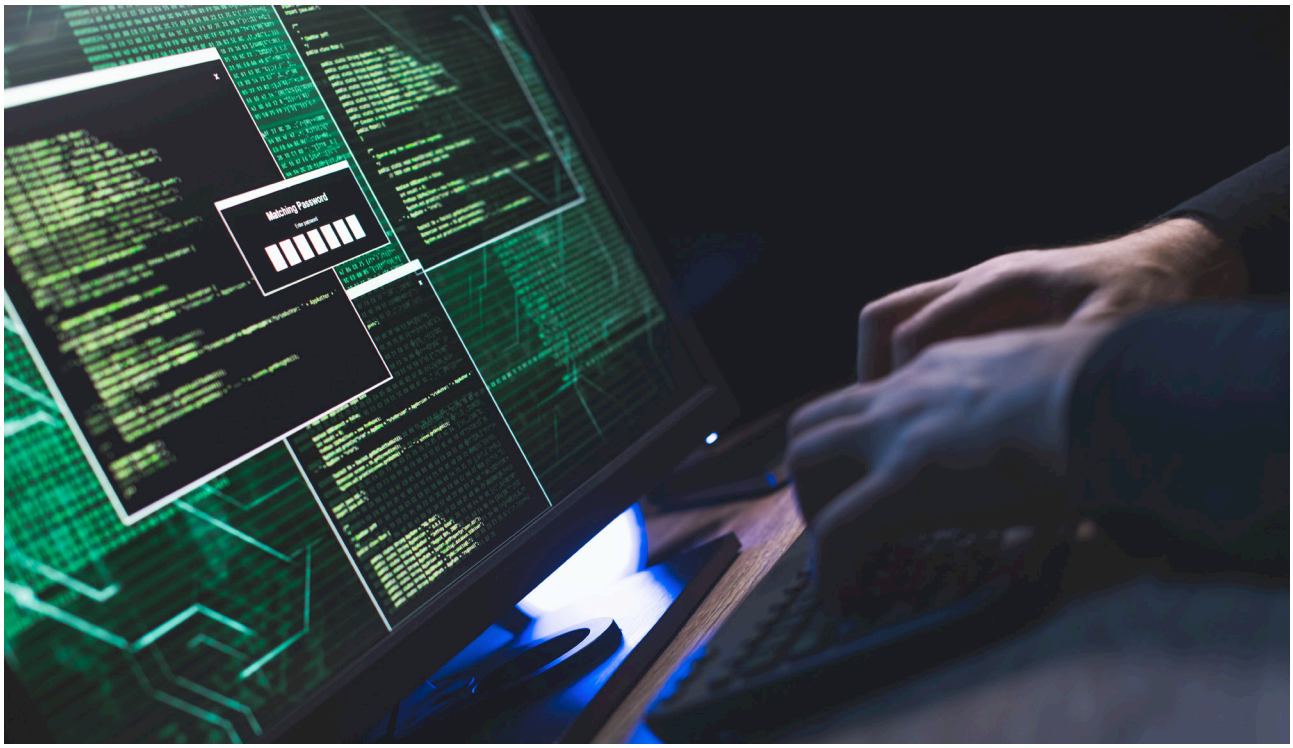
11 Tsagourias and Farrell 2018.

12 For example, the U.S. attributed North Korea as having been involved in WannaCry. see: U.S. Government, 19 December 2017.

destruction connected to them.[13] If an organisation claims responsibility and there is reasonably believable evidence, the process of attribution may be simpler. However, instances where groups claim attacks (both physical and cyberattacks) for notoriety but are not the real perpetrator present a greater challenge.

In contrast, a state or state actor is more likely to conduct a cyber event in a stealthy manner to hide its identity; for example, where an attack is driven by espionage. It could be in the perpetrator's interest to promote a narrative of plausible deniability. However, there is duality associated with the state actor, whereby aside from stealthy attacks, in other instances the perpetrator may also seek to plant a 'false flag' to give the impression that the attack was carried out by another group or another state. However, if the strategy of the attacking state was to signal their strength, they are more likely to hint at their involvement in a covert rather than overt manner.

For other types of attacks – for example, where the perpetrator is seeking to leverage power or achieve a certain objective – they may see advantages in highlighting their involvement in an overt but subtle way. In these types of attacks, which are designed to be destructive or sufficiently disruptive, a state may hint that they are involved or that they are the perpetrators.[14]



13 Although many terrorist organisations are driven by notoriety, an organisation may still wish to instill fear, chaos, disruption and destruction without necessarily taking the credit in order to avoid being targeted.

14 Greenberg 27 February 2019.

4. Technical, political and legal factors affecting attribution

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

This section explore these factors and their potential interdependency.

Attribution: Technical evidence and technical know-how

The first challenge with attribution is to effectively use what we know about the technology and the vector of the attack to hypothesise about the identity of a possibly responsible individual, group, organisation or state (note that any technical hints will not constitute irrefutable evidence on its own but will, at best, only provide circumstantial evidence).[15] 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.[16] There are a number of disguises which a cyber actor may use in order to create the illusion that the act was carried out by someone other than themselves.[17]

Technology can be used in different ways to mask the identity of the attacker or to create a 'false flag' (see Box 1). 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.[18]

Attributing a cyber event to a state is increasingly difficult (see Box 1). 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. Even if it were possible to technically

15 If other evidence (such as human intelligence) exists to prove the origin of the attack, this can be used in preference to technical factors. For example, if there is a written authorisation to carry out or launch a cyberattack this would be key.

16 The need to disguise activity is more probable where the policy objective of an attack is likely to be espionage, and less likely where the objective is to exert power from the attack and thus send more clear signals to highlight who may have the capacity and capability of conducting such an attack.

17 Skopik and Pahi 2020.

18 Kara and Aydos 2019; Egloff, and Wenger 2019; Voelz, and Soliman 2016.

determine a degree of involvement of a state or state actor in a cyber event, 'the difficulties of attribution allow a degree of plausible deniability. Perpetrators can cover their own tracks and implicate others, particularly when third-party servers and botnets in unrelated countries can be used to originate attacks and provide cover for the actual attacker'.[19]

Box 1: The practitioner's view – understanding and responding to a changing cyber security landscape

In recent years, the global community has been confronting two emerging phenomena that are simultaneously affecting the nature of threats, attacks and damage, and the capability to effectively conduct technical and political attribution. The first is the increasing involvement of state actors in attacks on businesses and infrastructure, as well as military and security targets. The second is the proliferation of offensive cyber technologies from state actors to non-state actors, such as cyber terrorists and criminal organisations.

These two phenomena have exposed leading industries and businesses to new kinds of targeted and sophisticated attacks that cannot be prevented by the products currently available in the cybersecurity market or other broader risk management tools. As a result, these two phenomena are continually increasing both the overall global damage and the number of mega cyber events, with damage measured in billions of dollars and occasionally exposing organisations to existential threats. Another result of these phenomena are limited capabilities to determine attribution.

The most basic kind of technical attribution would be to identify the use of infrastructure, such as computers or servers. However, this kind of attribution has not been very effective, as it can be manipulated with relatively simple techniques, allowing the attacker to either hide the source of the attack or to obtain control of servers and computers for the purpose of carrying out attacks.

A sophisticated technical attribution method is to identify the technologies, code indicators or attack tools being used to conduct the attack. However, sophisticated attackers, usually leading state actors, know enough about the characteristics of attacks conducted by other players to be able to imitate them and maliciously implant 'false flags'. It is becoming increasingly difficult to attribute a cyberattack to a state actor, due to the proliferation of cyber offensive technologies and operational capabilities and the leakage of certain attack tools developed by state and non-state actors alike. Certain state actors even tend to initiate a leakage of attack tools, in order to hide their responsibility for using the tools themselves. In other cases, state actors use publicly available tools, technologies and methods, in order to hide their identity and to avoid exposing their methods of operation and capabilities.

Another option is collecting intelligence about operational activities necessary for conducting cyberattacks. However, this intelligence is often classified due to the importance of protecting assets or methods of operation.

Attribution is also becoming more complicated because certain state actors are demonstrating systematic synergy with non-state actors, either cyber terrorists, criminal organisations or hacktivists. There are at least three major levels of collaboration:

1. Governmental outsourcing of cyberattacks to non-state actors
2. Symbiotic relationships – non-state actors are serving the interests of state actors and in return, receiving governmental permission or even support in order to conduct profitable attacks
3. A synergy in which non-state actors, usually organised crime groups, are acting in alignment with the interests of a state actor, practically working like 'two arms on the same body'

19 Chatham House Report November 2010.

In these situations, even given perfect data on the operational and technological aspects of the attacks, it would be difficult to determine who actually initiated the attack and if there was active governmental involvement. This type of collaboration often involves a passive relationship between the actor and the government; for example, where the government is aware of cyber actions within their jurisdiction but there is a failure to prevent future events and a failure to punish those involved.

It should be noted that sophisticated attackers are also capable of successfully misleading researchers regarding the motivation related to the attacks by creating secondary benefit to hide the original motivation, conducting secondary attacks or leaking attack tools used for additional attacks. In addition, the symbiosis between state and non- state actors is creating a growing uncertainty in countries where major corporations are seen as an arm of the government and an additional tool for achieving superiority in certain global fields. Moreover, in many cases, political and security considerations influence intelligence agencies and decision makers when determining attribution, preventing them from officially connecting it to a specific state actor.

Evidently, the ability to determine attribution is deteriorating and uncertainty is increasing. This requires adopting two measures simultaneously: 1) Deploying efforts to improve the collaboration on effective attribution, including sharing intelligence, improving research and defining clearer attribution guidelines; and 2) Considering technological and insurance solutions that are more non-attributional, e.g. developing new technologies capable of protecting high profile organisations that might be targeted by sophisticated attacks. This also means better classification of very sensitive assets, such as critical infrastructure and sensitive IP, and protecting them by implementing technologies that offer segregation and compartmentalisation. These solutions can allow insurers to provide proper coverage without overrelying on attribution and minimising the effects of accumulation.

Source: Yuval Porat, KAZUAR Advanced Technologies

Attribution – Political and legal considerations

Even if all the technological problems are overcome and a particular person, entity, 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. Against this backdrop, this section will now look at the effect of political considerations on the attribution and characterisation processes.

There is no international standard at present for attribution; there are no laws, regulations or treaties that promote consistency.[20] To optimise the attribution process in the future, it is important to begin discussions between various re/insurers and other stakeholders globally to promote greater convergence on approaches, where possible.

International politics can also lead to attribution determinations that are not correct. The value a state puts on maintaining good political and economic ties with the alleged responsible state may trump the value of publicly attributing responsibility accurately. The leader or official responsible for making the attribution statement (for example, the head of state, foreign minister, state agency, etc.) may also affect the outcome.

The value a state puts on maintaining good political and economic ties with the alleged responsible state may trump the value of publicly attributing responsibility accurately.

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,

20 Although there have been some international discussions regarding the need for international convergence, there are no legal instruments in place at present. See: UNIDIR Resources 2017.

there will likely be sufficient connection between the actor carrying out the attack and the state who is 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. The International Court of Justice, in Nicaragua v United States of America, suggested that factors linked to state connectivity might include equipping, training, facilitating and encouraging the perpetrator(s).[21] Applying the ICJ's views to Figure 3, it is likely that state-integrated, state-executed, state-ordered, state-coordinated, state-shaped actions will 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, i.e. when the state's measures to prevent attacks or attempts to punish those engaged are inadequate.

Table 2: The spectrum of state responsibility explained[22]

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

21 Nicaragua v. United States of America 1984, 1986.
22 Healey 2011.

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.

In some instances there may be political distaste or other sensitivity which may prevent calling out the behaviour of a particular state. The state which does engage in public attribution may experience retaliation from the incriminated state. Political considerations are subjective and provide additional challenges when overlaid with broader factual, technical and legal matters.

A different aspect bridging political and legal considerations concerning attribution relates to sanctions or other restrictions at a company which has been affected or for the insurer paying money to a cyber adversary. For example, if a company suffers from ransomware it may want to pay the ransom to contain losses and speed-up recovery from the attack. Before making a decision on the payment or non-payment of a ransom, a company needs to weigh up a number of factors: commercial, political, legal considerations. It would also need to minimise violating any sanctions regulations, including international sanctions as defined by the UN or imposed at the national level.[23]

Box 2: U.S. case study: Evil Corp and the ransomware 'WastedLocker'

Attribution plays a critical role in an organisation's effecting compliance with United States sanctions laws and regulations. On 1 October 2020, the Office of Foreign Assets Control (OFAC) in the United States Department of the Treasury – the U.S. agency responsible for administering and enforcing economic sanctions – issued an advisory on the potential risks associated with facilitating ransomware payments to actors who may be sanctioned or have a sanctions nexus.[24] Ransomware is malicious code used to encrypt electronic data, interrupt operations or otherwise block access to a computer system or/and data in order to extort payments from victims in return for the restoration of their computer system and/or data. Like other cyber malicious actors, ransomware perpetrators rarely want to be identified.

In its advisory, OFAC made clear that more than just the victim of ransomware is responsible for determining that their payment to a bad actor does not violate sanctions obligations. Companies that facilitate ransomware payments on behalf of victims – including insurance companies offering cyber extortion insurance coverage – also risk violating OFAC requirements. Not only are U.S. citizens prohibited from engaging in transactions with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), but non-U.S. persons assisting U.S. persons and U.S. persons assisting non-U.S. persons may violate sanction restrictions.

OFAC has the authority to impose both criminal and civil penalties on persons and entities, subject to U.S. jurisdiction – and civil penalties for sanctions violations are based on strict liability. As a result, a company may be held civilly liable even if it did not know that it was engaging in a transaction with a sanctioned party. In order to mitigate that risk, OFAC advises that it has discretion in determining its response to an apparent violation. Implementing a sanctions compliance program which includes attribution due diligence is an important factor when OFAC determines how to respond to an event. A core part of such a compliance program will be doing whatever can be done in attributing the ransomware to the correct actor. While it is often impossible to make a timely determination of the bad actor when confronting a ransomware attack, doing all that is possible is important for the both the victim, their advisors, their financial institutions and their cyber insurer. And when attribution leads to sanctioning a person or entity, payment or reimbursement by an insurer is prohibited.

A recent example is illustrative. In the summer of 2020, a strain of ransomware known as 'WastedLocker' was linked by several cybersecurity sources to a cyber actor calling itself 'Evil Corp'. Evil Corp is a Russian-based cybercriminal organisation that had been using malware in 2015 to infect computers and harvest login credentials from financial institutions around the world, causing hundreds of millions of dollars of damage to these financial institutions and their customers. As a result, in December 2019, OFAC designated Evil Corp and its leader as sanctioned persons and prohibited U.S. persons from engaging in transactions with them. U.S. insurance companies (and non-U.S. insurance companies insuring U.S.-based risks) must now consider the evidence attributing WastedLocker to Evil Corp when confronted with a ransomware claim involving the use of WastedLocker.

23 Department of US Treasury 1 October 2020.
24 Department of US Treasury 1 October 2020.

Box 3: European Union case study: Sanctions imposed by the Council of the European Union

The insurance industry needs to place a high priority on compliance with and adherence to sanctions in all their dealings (including under cyber insurance policies). In an environment where there is reliance on external providers who negotiate on behalf of insurers, due diligence procedures should factor these additional risks, specific to the cyber market, into account. Many re/insurers will thus only engage in relationships with established and trusted partners who have a track record in meeting such obligations. Companies who feel that they must meet a ransom demand are faced with serious corporate damage and even existential threats and thus these factors often weigh into any decisions regarding ransom payment. There will always be a sensitivity in insurers reimbursing ransoms paid to attackers who may be state-sponsored. The insurance industry can support this aim by internal and external processes to ensure compliance.

In practical terms, on 30 July 2020, the Council of the European Union for the first time ever imposed sanctions against several Russian and Chinese individuals, a unit of the Russian military intelligence agency (GRU) and two companies from North Korea and China, based on their alleged participation in major cyberattacks in recent years (for example WannaCry and NotPetya). The restrictive measures imposed by the Council of the EU prohibit financially supporting any listed persons, entities or organisation. If an insurance company paid a ransom sum to a cyber perpetrator on this list of individuals, entities or organisations, even as a means of minimising losses, then the payment would likely be illegal due to specific sanctions or regulations. The consequences could be very serious.

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.

The legal challenge in determining attribution is that a court may be presented with highly technical material which may not be verifiable. This can create a challenge when the plaintiff is seeking to establish the burden of proof.

Understanding the technical nature of a factual matrix, such that a state can be deemed responsible, requires a thorough knowledge of the cyber landscape,[25] a working knowledge of information technology or operational technology, operability of electronic and computer systems, intricacies of software and other matters. In presenting their cases, attorneys would often have to rely on the aid of an expert witness.[26] This is not, however, different from the cybercriminal cases that have gone to trial over the past twenty years, where expert witnesses are often called to the stand, and judges have had to learn about important technical intricacies.

An additional legal challenge is traceability of the evidence and issues associated with collecting digital evidence. There may be uncertainty regarding who has the rights to obtain, store and produce digital evidence and issues of admissibility.

25 If there continues to be more litigation surrounding cyberattacks, over time the courts may be able to better contextualise technological changes.

26 There are a number of guidelines regarding the use of digital evidence which are available to law enforcement, and prosecutors. See International Association of Chiefs of Police (Law Enforcement Cyber Center). Litigation Guides-Digital Evidence and Witnesses. https://www.iacpcybercenter.org/prosecutors/litigation-resources/; U.S. Department of Justice (Office of Justice Programs, National Institute of Justice). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. **https://www.ncjrs.gov/pdffiles1/nij/199408.pdf**; U.S. Department of Justice (Office of Justice Programs, National Institute of Justice). Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. https://www.ncjrs.gov/pdffiles1/nij/211314.pdf

5. An illustrative framework for attribution

The following is an illustrative framework of the attribution process in practice, including key steps and components.

1. Initial characterisation of action

Was there a suspicion that the act was one of cyber terrorism, HCA or cyber war? Although it is theoretically possible to make this determination without knowing the actual state or group, the identity should be definitively determined whenever possible.

a. Technical analysis (including private companies, police, and intelligence services investigations): often done secretly and information cannot be found in the public domain

b. Attribution to actor (carried out 'in-house' at present[27])

i. Identification of precise actor: cybercriminal, cyber terrorist or state actor.

ii. Question: Could it be a state actor?

NO
Therefore, the act cannot be categorised as 'war', which currently requires state-versus-state dynamics in the form of a declared war or warlike environment.[28]

YES
Was it clearly a state actor who was involved?[29]

a. YES
Focus may shift instead to a closer examination of the action (as per the next step)

27 'In-house' attribution means a company, such as an insurer or reinsurer, undertakes the attribution process itself, e.g. to determine if an exclusion clause operates. Companies will often hire specialist private companies or those with intelligence capabilities to help them determine who was responsible and how the act is likely to be categorised should it be litigated at a later stage.

28 A 'war' exclusion in an insurance policy is rarely limited to just war. Although the exact scope and wording will vary between carriers, in many instances this exclusion will encompass other uses of military force and rebellions or civil wars that would not be deemed to be a warlike act within the Geneva Convention.

29 Factors which may be taken into account to assess whether the actor is a state actor include circumstantial evidence, motivation, degree of involvement or control, magnitude of the attack, impact as well as probable involvement of certain military or intelligence personnel.

b. NO

Was it a state-sponsored actor? Did an actor connected to the state carry out the act? Unfortunately there is no universally-accepted global practices upon which a determination can be made that the perpetrator might be a state actor.[30]

2. Second characterisation of action

a. Characterisation process, taking into account the actor: Was the event cyber terrorism, HCA or cyber war?[31]

3. Communication of the attribution

a. Private (only for the use of the party attributing, i.e. there should be no external communication)[32]

b. Semi-private (the party attributing and, for instance, another government)[33]

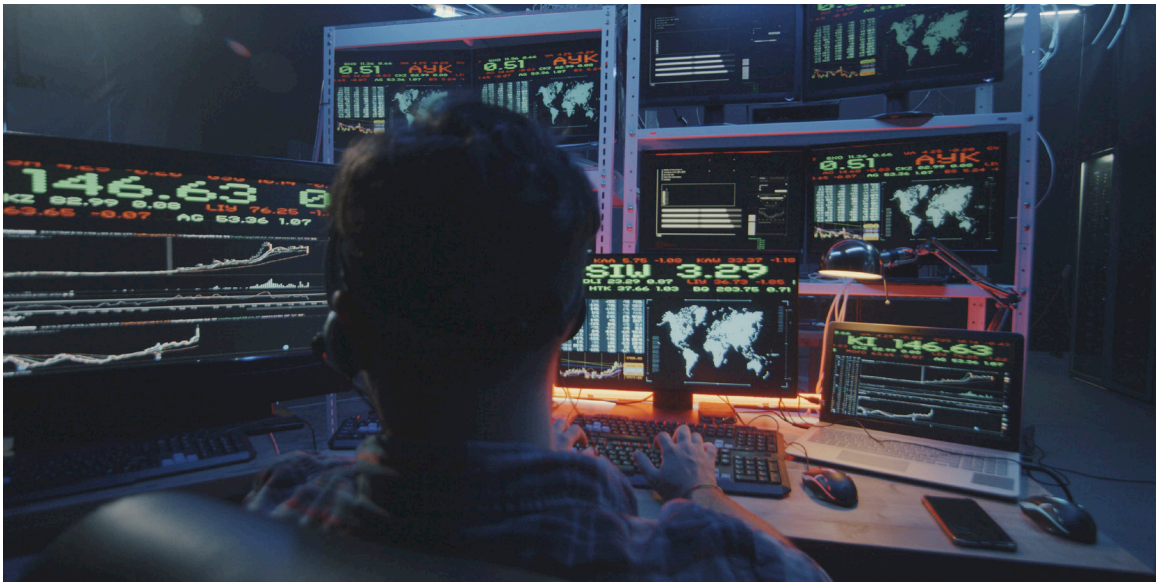
c. Public attribution with evidence (best-case scenario, but rare)

d. Public attribution without evidence

i. Has an attribution been made by a competent authority or state?

NO (dubious country)[34]
Re/insurer will need to prove attribution through other evidentiary means. This other evidentiary material will be assessed by a court.

YES (credible country)
Depending upon the legal system and the state making the attribution without evidence, in some cases a court may accept the attribution without the re/insurer having to provide additional evidence.



30 A number of companies and technical providers support the MITRE Att&CK Framework which is essentially a technical catalogue of various events with some categorisation. See The MITRE Att&ck Framework: What you need to know. 17 June 2020. https://www.tripwire.com/state- of-security/mitre-framework/mitre-attack-framework-what-know/

31 Divergent views exist regarding the level of violence necessary for an event to be an act of war as there is no threshold level of damage or destruction necessary for such categorisation. For example, North Korea firing rockets into South Korea on its own is not enough to be war, but the collective set of actions might be enough to characterise the attack as part of war.

32 Often private attribution is carried out by private security firms that have evidence and are able to use this evidence to reach a position regarding attribution. These firms may charge a fee and their attribution could potentially be used in litigation.

33 This will also include attribution by non-state actors such as private companies, researchers, universities and others who may have technical capabilities that enable them to look at responsibility for an attack (at least from a technical evidentiary viewpoint).

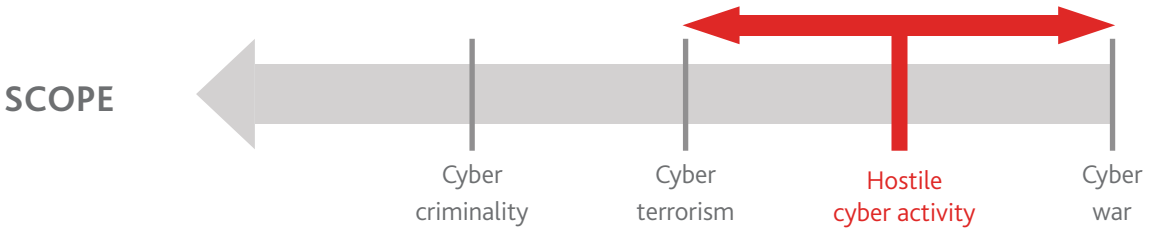
34 The question of who is a dubious country and who is a credible country will be determined by the state who relies upon the attribution. If that state does not require further evidence, then legally, the fact that the state made an attribution that another state was responsible for the cyberattack may be sufficient to uphold the attribution if tested in a court of law.

Figure 2: Illustration of the attribution process

Attribution

1. Initial characterisation of action

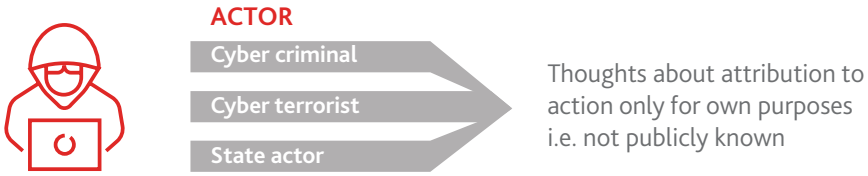
Was there a suspicion that the act was one of cyber terrorism, HCA or cyber war?



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)



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

6. The way forward: Towards an international consensus

So far, this report has worked through the process of attribution. It has also identified the many challenges of the process and looked at questions which must be considered to discern how attribution and characterisation processes may be changed or optimised in the future. In addition, there is a view that having greater international consensus around attribution and characterisation may benefit the insurability of cyber risk.

The report will now look at the ability to seek consensus between insurers (and insureds), states and other stakeholders from different geographies. In doing so, it will examine the potential to begin discussions through a multilateral forum – for example, the G7 or G20 – about how to optimise the attribution process, towards developing an international norm.[35] The norm may focus on the procedure and establishing a common framework for how to attribute and characterise or develop a series of questions. The aim would be to promote greater consistency and a streamlined process. Further it would be ideal for insurers and insureds alike to have a broad agreed framework regarding the allocation of responsibility.

If the framework is sufficiently broad, it can capture a variety of ways in which the attribution process can be applied to promote consistency. The framework could showcase similarities and differences between jurisdictions. This can thus serve the dual purpose of expanding the knowledge base of the authorities responsible for attribution within a state and enabling them to see how idiosyncrasies applied within their jurisdiction compare with similar, competent bodies in other jurisdictions. It may also enable discussions between different authorities concerning similar cyber events, with the aim of harmonising procedural best practices and the questions in the attribution process.

A global discussion on an international norm would be worthwhile and help build momentum, even if some states choose not to adopt it.

Realistically, despite the potential value, some states would choose not to participate by incorporating frameworks and international norms. States that do not support the norm may go further and disregard a norm or act. However, having a global discussion of the norm through a multilateral platform such as the G20 or G7 may help build momentum.

35 Bateman October 2020.

In reality it is preferable to start with a number of states with similar processes of attribution. These states can then replicate and build off each other and create hubs where illustrative or good practices for attribution can be observed. In this way there will be sustained momentum to optimise the existing processes by replacing them with an international norm in due course. One of these hubs could be Europe, where for example there may be a drive to seek consistency between EU member states. If a number of states support a norm or a 'best' practice for attribution and it is adopted across European countries, it might then be possible to look at a cross-continental application in due course.

Even in the best-case scenario, implementing an international norm may take a considerable amount of time. Furthermore, without an international body in existence, who would have the legitimacy to authorise such a norm?[36]

Also, in developing an international norm, attribution should be looked at holistically and analysed within its broader objective of providing economic protection against cyber terrorism, cyber warfare and HCA. The purpose of such international collaboration or consensus seeks to minimise the economic impact to individuals, businesses and society. When considering the impact, it will be important to think about the effect of an individual event, as well as the effect generated by a series of cyber terror events, HCA or cyber war.

Unfortunately if certain states are unable or unwilling to take part in discussions on international norms, other states may deem such practices of little use; following an international norm will require the compliant state to give up some of their own rights and freedoms regarding attribution. However, there are many examples of international legal concepts originating with a small proportion of adoption by the international community. Over time, as the international norm grew, more states adhered to the principles.

Practically, however, it is recognised that from the perspective of both insurance and international diplomacy, global norms are a longer-term proposition rather than something likely to be rolled out in the short to medium term. Instead, what can be concretely achieved in the short term is to begin formal collaboration between selected insurers, technology providers, large corporates, governments and intelligence providers. This collaboration and ability to discuss across various sectors will hopefully result in more international consistency of the procedures used and thus the probability of a more consistent method for attributing and characterising. Initiating the development of an international norm requires understanding, commitment and a consistent vision regarding any changes. Once there is agreement on exactly what to change, it is possible to discuss and research the various options. This is likely to be more effective if the various stakeholders who may be affected by cyber events are engaged.

> It is achievable in the short term for selected insurers, technology providers, large corporates, governments and intelligence providers to begin formally collaborating.

Part of the challenge stems from terminological ambiguity in the definitions of terrorism and cyber warfare at the state level and how this is influenced by politics, legal systems, culture and diplomatic reality. Consequently, part of the first step might be to develop a lexicon or agreement regarding consistent terminology, so that at least in the process of discussing solutions, there is a common understanding of key notions. There are already some cyber lexicons within industry-specific bodies or regulators.[37] However, there is no cross-jurisdictional lexicon agreed between the various sectors (insurers, pools, governments, intelligence agencies, technology providers and other global corporates). Speaking the same language (technical terms used consistently by stakeholders) would enable a level discussion and provide a foundation for devising international norm.

The insurance industry is thus beginning discussions in this direction. As the collective understanding and agreement between different carriers occurs, this will create more scope for future discussions with governments, technology providers and large corporates to see how the different stakeholders can start to work together over time and develop cross-sectoral solutions.

36 There are a number of bodies in existence who could be useful in further promoting convergence such as the UN (and specifically the UNGGE processes) as well as international instruments including The Global Commission on the Stability of Cyberspace, the Paris Call etc. which may be used as part of the overall solution. These bodies and the international instruments are however focusing on different cyber objectives and not allocating responsibility for actors of a malicious cyber act. This may be due to the fact that at present, no body and no instrumentality has the legitimacy to authoritatively publicly attribute the actor and the event.

37 For example: Financial Stability Board November 2018. https://www.fsb.org/2018/11/cyber- lexicon/

Box 4: The benefits of shared terminology and understanding of international cybersecurity and the consequences of nation-state activity

Digital transformation and global supply chains have enabled new capabilities and efficiencies for many organisations, while also increasing interconnectivity across sectors and regions. Interconnectivity can enhance cybersecurity by extending the impacts of an organisation's or sector's risk management efforts. However, it also can result in cybersecurity risks, if there are shared dependencies on organisations or sectors with poor cybersecurity hygiene.

Moreover, in today's fast-paced environment, rapidly evolving cyber threats are difficult to adapt and respond to without the appropriate information, tools and expertise. Cross-sectoral collaboration can drive understanding and awareness of cybersecurity risk exposure and translate directly into effective cybersecurity policy that reduces overall risk levels and supports the functioning of global digital resources. Now is a more critical time than ever for organisations to form new partnerships to facilitate cybersecurity resilience, as well as promote peace and stability in cyberspace.

Every sector has a stake in a safe and secure cyberspace, and each can benefit from dialogue with organisations that hold a high concentration of knowledge in reducing cybersecurity risk. In the near term, the private sector can leverage its collective knowledge and expertise to advance shared terminology and understanding of international cybersecurity and the consequences of nation-state activity. Increased collective understanding can also lay the groundwork to establish shared positions on government accountability. This could include working on shared definitions of what constitutes state or state-sponsored cyberattacks, shared knowledge of the most prolific actors in this space, and shared understanding of which elements are required for robust attribution of particular attacks.

Source: Kaja Ciglic, Microsoft

Conclusion

Attribution is a major challenge for the provision of cyber insurance, in particular in the context of cyber terrorism, HCA and cyber war. It is often an inherently difficult process. To begin with, it requires differentiating between three types of actors: the cybercriminal, the cyber terrorist and the state actor. The way a cyber event is categorised often depends upon the actor involved in carrying out an attack and whether this actor is 'a' state or 'a' terrorist organisation. For a state actor in particular, there is often little or no incentive to leave any trace of identity in the context of attribution. This presents special challenges in the areas of HCA and cyber warfare.

State actors have little-to-no incentive to reveal their identity in the context of attribution, presenting special challenges in the areas of HCA and cyber warfare.

Against this backdrop, this report has provided a framework for simplifying the process of attribution and characterisation. It has sought to dispel uncertainty by reducing complexities to a series of steps and checklists which may be used by insurers.

In order to continue to simplify and optimise the existing process of attribution and characterisation, multilateral dialogue could pave the way for international consensus as a long-term objective. Multilateral forums focused on improving attribution can serve the dual purpose of expanding the knowledge base of the authorities responsible for attribution and other stakeholders and enabling formal or informal discussions between them concerning similar cyber events. On that basis it might be possible to look at a potential harmonisation between best practices in the procedure and questions asked during the attribution process. Although any international norms, if developed, would not realistically be universally accepted, they may be adopted by groups of states.

Improved comparability across jurisdictions would boost industry-wide assessment of accumulation risk and, ultimately, facilitate the insurability of cyber risk. However, at a global level, such an ambition is further down the road.

Finally, beyond the topic of attribution, the market, regulators and governments may recognise that a certain level of accumulation risk – whether part of war, cyber terrorism, cyber crime or something else – is not insurable. Like a pandemic, a catastrophic cyber event – regardless of who caused it or why – might require government intervention (backstops, pools, etc.); this will be further explored in a forthcoming Geneva Association report.

Annex
Certification under cyber terrorism pools – Lessons for commercial insurers engaged in cyber attribution

In order to pay out for a cyber terrorism event, the process of certification for government-backed terrorism pools may be applied in a similar way to attribution. The relevant terrorism pools or competent authority will have to certify that an event was an act of cyber terrorism and thus that the pool provides insurance cover for any of the resultant damages. All the IFTRIP pools accepting cyber risks have government certification processes, the more formal ones seeming to be those of the U.K. and the U.S. To date, certification as regards acts of terrorism has only been performed for physical acts.

In some cases, the indirect way to label a cyberattack as a terrorist event is to consistently apply the same term used for any police investigation, court cases or other related government matters. The way an event is labelled may be for reasons not made public or due to evidence which is suppressed from the public during an investigation or court hearing.

To date, none of the international government-backed terrorism pools have needed to certify an event as an act of cyber terrorism. However, it is likely the process and considerations would be similar to those employed for a physical act of terrorism.

The following pools belong to IFTRIP:

- Australia (ARPC)
- Austria (GRAWE)
- Belgium (TRIP)
- Denmark (FINANSTILSYNET)
- France (CCR & GAREAT)
- Germany (EXTREMUS)
- India (GIC)
- Israel (INCD)
- Nepal (NEPAL RE)
- Netherlands (NHT)
- Russia (RATIP)
- South Africa (SASRIA)
- Spain (CCS)
- Sri Lanka (NITF)
- U.S. (TRIP)
- U.K. (Pool Re)

If there is no certification, however, it is still possible for the private market to engage in attribution for an event. If there is no government certification there is likely to be the requirement, at minimum, for a court judgment or arbitration process to consider the available evidence and make a determination on the balance of probabilities. If this is dealt with under the commercial market rather than via a government certification process, the burden and degrees of proof and other components of the court judgment or arbitration process can be prescribed and modified by the contractual wording upon which the cover is given.

There can, however, be a link between the reaction of the commercial market after an event and potential government certification. Three events in the U.K. in 2017 – Westminster Bridge, London Bridge and Borough Market – resulted in the withdrawal of terrorism cover in commercial insurance for hired vehicles. The commercial market only reinstated such cover once pooling became available as well as the interposition of the Motor Insurers Bureau, an industry-funded body previously used only for uninsured motorists. In the light of the potential scale of the resulting exposures, there was a need for an independent and authoritative certification process of some kind. However, unlike with the Pool Re scheme, government funds were not at risk.[38]

There is a legislatively-entrenched process for certification, which may differ between the pools covering cyber terrorism. However, in most cases, it is only the relevant stakeholders who must make a decision about certification in a prescribed manner. Where certification is performed by a government, it takes place behind closed doors, for obvious and generally good reasons. It is a sporting certainty that there will be inter-departmental discussions, but there will be no insight into that process. In the U.K., there is a dispute process available if certification is declined, but this would take place in the absence of Pool Re or its legal representatives.

Governments may have all kinds of justifiable motives in play when certifying an act of terrorism. In many cases, their diplomatic, military, and political or security interests take precedence over the technical correctness of the certification. Other reasons why a decision on certification might be contrived include sending a certain message – to citizens, national governments and others – or avoiding revealing information indirectly. This factor is of major concern in the field of attribution and may ultimately have to be accepted.

As an example, in April 2017, the Westminster car/knife attack was perpetrated by an individual with no evident links to a group or state. For this reason, it appeared not to trigger the Pool Re definition of acts of terrorism (physical act of terrorism), but the U.K. Prime Minister described the act as one of terror within 30 minutes of it happening. The comments of the U.K. Prime Minister are likely to have contributed to the certification of this event.

Certification may also be more likely if the incident is sufficiently small that, despite the government backing the scheme as a whole, no government money will be needed to top up the funds available under the pool scheme. Alternatively, if the event is truly catastrophic and of a magnitude that requires government assistance, the certification has a larger probability of occurring. Events in the grey area, where there is a chance the government may be required to top up, are less likely to result in certification.

In the U.S., there has been no certification of the attack in the 2013 Boston Marathon, which appeared to be terrorism as defined in TRIA. The insured loss for the Boston Marathon did not exceed USD 5 million, which is the minimum threshold before an event can be certified in the U.S. It was publicly noted that the insured losses falling below the threshold were the reason for the lack of certification.

38 Not all pools operate the same way. For example, in Spain the CCS insures both terrorism as well as damage caused by uninsured, stolen or unknown vehicles and thus there are likely to be different considerations. A further difference with the Spanish system is that the CCS' funds are not government funds and these are only at risk if an event is so large that it overwhelms the resources of the CCS, requiring the use of a state guarantee (this has not happened since the CCS was established in Spain).

References

13 July 2020. Yemeni Houthis say they hit Saudi oil facility in drone, missile attack. *Reuters*. https://www.reuters.com/article/us-saudi-security- yemen/yemeni-houthis-say-they-hit-saudi-oil-facility-in-drone-missile-attack-idUSKCN24D0U6

13 July 2020. Munich Re the latest carrier to settle Merck NotPetya Dispute. *The Insurer.*

Banks, W.C. 2019. Symposium on Cyber Attribution: The Bumpy Road to a Meaningful International Law of Cyber Attribution. *American Journal of International Law* 113: 191.

Bateman, J. 2020. Alternative Exclusions for Cyber Claims. Carnegie Endowment for International Peace.

Bateman, J. October 2020. War, Terrorism and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions. Carnegie Endowment for International Peace.

Bergman, R. and Lee Myers, S. 7 May 2020. China's Military is tied to Debilitating New Cyber Attack Tool. *The New York Times*.

Boutin, B. 2019. Symposium on Cyber Attribution: Shared Responsibility for Cyber Operations. American *Journal of International Law* 113, 197.

Brussels Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018, Press Release (2018) 074 https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20

Broeders, D. et al. April 2020. 2020 Policy Brief: *Three Tales of Attribution in Cyber Space: Criminal Law, International Law and Policy Debates*, The Hague Program for Cyber Norms Policy Brief.

Butler, E. Overview of the Cyber Threat Landscape. Unpublished: presented at the Geneva Association and IFTRIP Cyber Terrorism and Cyber Warfare Task Force, London Workshop. PowerPoint Presentation. Last modified 11 December 2019.

Centre for European Policy Studies. 2 April 2020. Operation *Irini in Libya: Part of the Solution or Part of the Problem*. https://www.ceps.eu/operation-irini-in-libya/

Centre for Risk Studies, May 2016. Cambridge University: Cyber Terrorism: Assessment of the Threat to Insurance.

Chatham House Report. September 2015. Cyber Security at Civil Nuclear Facilities – Understanding the Risks.

Chatham House Report. November 2010. On Cyber Warfare. Author: Paul Cornish. https://www.chathamhouse.org/sites/default/files/public/Research/International% 20Security/r1110_cyberwarfare.pdf.

Clearsky Cyber Security, February 2020. Fox Kitten Campaign: Widespread Iranian Espionage-Offensive Campaign.

Club des Juristes: Insuring Cyber Risk. January 2018.

CRO Forum. June 2016. Concept Paper on a proposed methodology for cyber-risk.

Coburn, A. et al. 2019. Solving Cyber Risk: Protecting Your Company and Society. Wiley.

Corcoran, B. 8 March 2019. What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict, *Lawfare* 1.

Crowdstrike. *Who is Fancy Bear?* 12 February 2019. https://www.crowdstrike.com/blog/who-is-fancy-bear/

Davis II, J. S. et al. 2017. Stateless Attribution: Toward International Accountability in Cyberspace. Rand Corporation. ISBN 978-0-8330-9840-5.

Department of US Treasury. 1 October 2020. Advisory of Potential Sanctions Risks for Facilitating Ransomware Payments. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_1001202 0_1.pdf

Dyson, B. 17 January 2019. Zurich's $100 million cyber claim battle could trigger a policy overhaul. *Standard and Poor Global Market Intelligence.* https://www.spglobal.com/marketintelligence/en/news/insights/trending/oTtjvLuR6 VnNRR4pi42NQ2

Egan, B. J. Remarks on International Law and Stability in Cyberspace. Presentation given to the Berkeley Law School, California on 10 November 2016. https://2009-2017.state.gov/s/l/releases/remarks/264303.htm

Egloff, F.J 2020. Public attribution of cyber intrusions *Journal of Cybersecurity* 1–12.

Egloff, F.J. and Wenger, A. 2019. Public Attribution of Cyber Incidents *CSS Analyses in Security Policy, ETH Zurich*, May (No. 244).

Eichensehr, K. E. 2019. Symposium on Cyber Attribution: Decentralized Cyber Attack Attribution. *American Journal of International Law*. 113, 213.

European Parliament. 19 February 2018. Attribution of the NotPetya attack. https://www.europarl.europa.eu/doceo/document/E-8-2018-001005_EN.html

Finlay, L. and Payne, C. 2019. Symposium on Cyber Attribution: The Attribution Problem and Cyber Armed Attacks. *American Journal of International Law* 113, 202.

Geers, K. et al. World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks. FireEye Report: Security Reimagined.

Greenberg, A. 22 August 2018. The untold story of NotPetya: the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack- ukraine-russia-code-crashed-the-world/

Greenberg, A. 27 February 2019. US Hackers Strike on Russian Trolls Sends a Message- But What Kind? *Wired*. https://www.wired.com/story/cyber-command- ira-strike-sends-signal/

Guitton, C. 2014. Achieving Attribution. PhD thesis.

Guitton, C. 2015. Attribution. In Jean-Loup Richet (Ed.), *Cybersecurity Policies and Strategies for Cyberwarfare* Prevention. 37-60. Hershey PA: IGI Global.

Guitton, C. 2016. *Inside the Enemy's Computer: Identifying Cyber Attackers*. Hurst & Company.

Guitton, C. and Korzak, E. 2013. The Sophistication Criterion for Attribution. *The RUSI Journal* 158(4) 62-68.

Hare, F. 2012. The Significance of Attribution to Cyberspace Coercion: A Political Perspective. 2012 *4th International Conference on Cyber Conflict*, NATO CCD COE Publications.

Healey, J. 2011. The Spectrum of National Responsibility for Cyberattacks. *The Brown Journal of World Affairs* 18(1): 55–70.

Holland, S. and Chiacu, D.. 22 December 2014. Obama says Sony hack not an act of war. *Reuters*. https://www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141222

ICT Cyber Desk: Cyber Terror Activities, Report No 19 (Q4 2016).

IFTRIP. March 2019. Cyber Terrorism and Cyber Warfare Definitions.

IFTRIP, October 2018. Cyber Terrorism and Cyber Warfare Definitions.

Institutionalising Cyber Attribution. https://www.iicom.org/wp- content/uploads/InstitutionalisingCyberAttribution.pdf

International Association of Chiefs of Police (Law Enforcement Cyber Center). Litigation Guides – Digital Evidence and Witnesses. https://www.iacpcybercenter.org/prosecutors/litigation-resources/

Jardine, E. and Porter, N. 2020. Pick Your Poison: The Attribution Paradox in Cyberwar.

Ilker, K. and Aydos, M. 2019. The Ghost in the System: Technical Analysis of Remote Access Trojan. *International Journal of Information Technologies and Security* 11 (1): 73–84.

Maglaras, L. et al, "Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures" (2019) *ICST Transactions (Preprint)* 1.

Mazarr, M. J et al. 2019. The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment. Rand Corporation. ISBN 978-1-9774-0272-1.

Menapace, M. 2019. As Cybersecurity Risks Evolve, So Must Our Preparedness.

Microsoft, 2020. Protecting People in Cyberspace: The Vital Role of the United Nations in 2020.

Microsoft Policy Papers, 2020. An Attribution Organisation to Strengthen Trust Online: Establishing an International Cyberattack Attribution Organisation to Strengthen Trust Online.

Mitre Att&ck Framework. 2020. https://attack.mitre.org/

Mitre Att&ck Framework: What you need to know. 17 June 2020. https://www.tripwire.com/state-of-security/mitre-framework/mitre-attack- framework-what-know/

Mondelez International Incorporated v Zurich American Insurance Company (05/27/16 CCL 050) – Civil Action Cover Sheet- Case Initiation.

Mueller, M. et al. 2019. Cyber Attribution: Can a New Institution Achieve Transnational Credibility? *The Cyber Defence Review*. Spring. 107.

Nakashidze, G. 28 February 2020. Cyberattack against Georgia and International Response: Emerging Normative Paradigm of Responsible State Behavior in Cyberspace? *EJIL Talk: Blog of the European Journal of International Law* https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response- emerging-normative-paradigm-of-responsible-state-behavior-in-cyberspace/

National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) for Japan, 27 July 2018. Cybersecurity Strategy Paper. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

National Cyber Security Centre. 29 May 2020. *Weekly Threat Report* www.nscs.gov.uk/report/weekly-threat-report-29th-may-2020

National Cyber Security Centre (U.K.). 14 February 2018. Russian military 'almost certainly' responsible for destructive 2017 cyber-attack. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

NetDiligence. 30 June 2020. Cyber Risk Summit: Summer 2020, Cyber War and Terrorism Panel.

Nicaragua v. United States of America. 1986. ICJ 14.

Nicaragua v. United States of America. 1984. ICJ 392 [Jurisdiction and Admissibility], 215 [Declaration of Intervention], 26 [Provisional Measures].

North Atlantic Treaty Organisation, Article 5. https://www.nato.int/cps/en/natohq/topics_110496.htm

Office of the Director of National Intelligence (United States of America). 14 September 2018. *A Guide to Cyber Attribution*.

Paris Call for Trust and Security in Cyber Space, 11 December 2018.

Perlroth, N. et al. 27 June 2017. Cyberattack Hits Ukraine Then Spreads Internationally. *The New York Times*. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Romanosky, S. and Boudreaux, B. February 2019. Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government. RAND (National Security Research Division). 1–36.

Satariano, A. and Perlroth, N. 15 April 2019. Big companies thought insurance covered a cyberattack. They might be wrong. *The New York Times*. https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya- attack.html

Schmitt, M. N. 2013.Classification of Cyber Conflict. *International Law Studies* 89, 233–251.

Schmitt, M. N. 2017. Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum. *Harvard National Security Journal* 8, 239 – 282.

Schmitt, M. N. 2014. Rewired Warfare: Rethinking the Law of Cyber Attack. *International Review of the Red Cross* 96(893): 189–206.

Schmitt, M. N. 2014. The Law of Cyber Warfare: Quo Vadis? *Stanford Law and Policy Review* 25: 269–300.

Skopik, F. and Pahi, T. 2020.Under False Flag: Using Technical Artefacts for Cyber Attack Attribution. *SpringerOpen* Journal 3(8): 1–20.

Smith, B. 14 February 2017. Transcript of Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention.

Statement from the U.S. Foreign Policy Press Secretary. 15 February 2018. NotPetya. https://www.whitehouse.gov/briefings-statements/statement-press- secretary-25/

Stoltenberg, J. 28 May 2019. Remarks at the Cyber Defence Pledge Conference, London. https://www.nato.int/cps/en/natohq/opinions_166039.htm

The Geneva Association. 2018. *Advancing Accumulation Risk Management in Cyber Insurance.* Authors: Daniel Hofmann, Steve Wilson and Rachel Anne Carter. August.

The Geneva Association. 2020. *Cyber War and Terrorism: Towards a common language to promote insurability.* Authors: Rachel Anne Carter and Julian Enoizi. July.

The MITRE Att&ck Framework: What you need to know. 17 June 2020. Tripwire Researcher. https://www.tripwire.com/state-of-security/mitre-framework/mitre- attack-framework-what-know/

Tran, D. 2018. The Law of Attribution: Rules for Attributing the Source of a Cyber Attack. *Yale Journal of Law and Technology*, 20: 376.

Tsagourias, N. and Farrell, M.D. 2018. Cyber Attribution: Technical and Legal Approaches and Challenges. The Fletcher School, Tufts University (Centre for International Law and Governance). https://sites.tufts.edu/cilg/2018/10/07/cyber- attribution-technical-and-legal-approaches-and-challenges/

U.K. Government. 15 February 2018. Foreign Office Minister condemns Russia for NotPetya attacks. https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

UK Government. 30 July 2020. Foreign Secretary Welcomes first EU Sanctions Against Malicious Cyber Actors. Press Release. https://www.gov.uk/government/news/uk-enforces-new-sanctions-against-russia- for-cyber-attack-on-german-parliament

UNIDIR Resources. 2017. *The United Nations, Cyber Space and the International Peace and Security: Responding to Complexity in the 21st Century.*

United States Cyberspace Solarium Commission, March 2020.

U.S. Department of Justice (Office of Justice Programs, National Institute of Justice). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

U.S. Department of Justice (Office of Justice Programs, National Institute of Justice). *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors.* https://www.ncjrs.gov/pdffiles1/nij/211314.pdf

U.S. Government, 19 December 2017. Press Briefing on the Attribution of WannaCry Malware Attack to North Korea. https://www.whitehouse.gov/briefings- statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to- north-korea-121917/

U.S. Department of Treasury. 15 March 2018. Treasury Sanctions Russian Cyber Actors for Interference with 2016 Elections and Malicious Cyber Attacks. Press Release. https://home.treasury.gov/news/press-releases/sm0312

Vavra, S. 9 September 2019. Microsoft, Hewlett Foundation preparing to launch non-profit that calls out cyber-attacks–CyberScoop. www.cyberscoop.com/microsoft-cyber-peace-institute-hewlitt

Voelz, G. and Soliman, S. 2016. Identity, Attribution and the Challenge of Targeting in the Cyber Domain. *Marine Corps University Journal* 7(1): 9.

Voreacos, D. et al. 3 December 2019. Merck Cyberattack's $1.3 Billion Question: Was It an Act of War? *Bloomberg.* https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3- billion-question-was-it-an-act-of-war

Walker, K. Blog: An Update on State-Sponsored Activity. https://blog.google/technology/safety-security/update-state-sponsored-activity

Willis Towers Watson. 2019. *The Terrorism Pool Index: Review of Terrorism Insurance Programs in Selected Countries 2019/ 2020.*

Wright, J. 23 May 2018. Cyber and International Law in the 21st Century. Attorney General's Office, United Kingdom.

Businesses, governments and societies increasingly depend on interconnected online systems, making them vulnerable to viral cyber events and large-scale disruption and destruction. Key factors in determining whether insurance will ultimately cover related losses include characterising such events and the outcome of the attribution process, or identifying the responsible actor. This second report in our series on cyber terrorism and cyber war provides insurers with a framework for attributing and characterising cyber incidents, emphasising the need for international collaboration to promote consistency and a streamlined process.

The Geneva Association

International Association for the Study of Insurance Economics
Talstrasse 70, Zurich, Switzerland
Tel: +41 44 200 49 00

www.genevaassociation.org