

Cyber War and Terrorism:

*Towards a common language
to promote insurability*

Cyber War and Terrorism:

*Towards a common language
to promote insurability*

Rachel Anne Carter, Director Cyber, The Geneva Association

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

The Geneva Association

The Geneva Association was created 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 in the future, 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—Aleksandr Pobedimskiy / Shutterstock.com

July 2020

Cyber War and Terrorism: Towards a common language to promote insurability

© The Geneva Association

Published by The Geneva Association—International Association for the Study of Insurance Economics, Zurich.

Contents

1. Executive summary	6
2. Introduction	8
3. Current terminology and concepts	12
3.1. War	12
3.2. Terrorism	13
4. Hostile cyber activity	14
5. Principal types of loss	17
6. Limitations	19
7. Conclusions	20

Acknowledgements

The authors (Rachel Anne Carter and Julian Enoizi) first wish to thank Christian Wells, General Counsel of Pool Re, for leading the expert group on common language. The authors also extend their gratitude to the members of the cyber terrorism and cyber war (CTCW) task force and those who contributed to this project.

Leadership team: Chuck Jainchill (AIG); Daniel Mesfin (Allianz); Christian Wells and Chris Yeates (Pool Re and IFTRIP); Matthew Harrison (Hiscox); Tony Ellwood (Lloyd's Market Association); Cyrus Delarami and Rory Egan (Munich Re); Szymon Mitoraj (PZU); and Eric Durand (Swiss Re).

CTCW experts: Jannice Koch (Allianz); Anna Fenech, John Park and Christopher Wallace (ARPC and President of IFTRIP); Neil Arklie (Aviva); Alexandra Maunie and Mathieu Cousin (AXA); Peter Zimmerli (Axis Capital); Francois Vilnet (GAREAT and IFTRIP); Dennis Sno (Hannover Re); Philip Lienau (HDI Global); Matthew Webb (Hiscox); Ed Butler (Pool Re and IFTRIP); Daniel Largacha Lamela (MAPFRE); Franz Gromotka (Munich Re); Chris McEvoy (Partner Re); Masashi Yamashita (Sompo Holdings, Inc); Sie Liang and Alexander Bosch (SCOR); Kei Kato (Tokio Marine); and Sandro Senaldi (Vittoria Assicurazioni).

Foreword

Until recently, cyber risk was perhaps the most pertinent and certainly one of the most contentious threats in re/insurance. It would be a mistake to assume that the grave challenges posed by the coronavirus pandemic in any way relegate those posed by cyber risk. If anything, the spread of COVID-19 is an acute reminder that our globalised world has become interconnected to the point where an obscure biological virus from a single source can rapidly trigger economic and cultural disruption not witnessed since the Second World War. With our reliance on technology and intangible networks only set to increase, the next virus to so aggressively threaten our global economy and way of life may well be digital.

The current crisis has underscored the importance of linguistic clarity in the re/insurance industry. Litigation and reputational damage are potential consequences of ambiguity. Ambiguity has been exposed in policy wordings and, more fundamentally, in policyholders' understanding of the practical limits of what commercial insurance can offer against systemic, correlated losses.

The purpose of this research report is twofold. First, it aims to contribute to the debate on definitions of cyber war and cyber terrorism by proposing a new term, hostile cyber activity (HCA). Not intended to be binding or definitive, the term reduces the ambiguity surrounding an increasingly prevalent type of activity that falls somewhere between cyber terrorism and cyber war. Greater clarity should also improve the consistency and transparency with which the associated spectrum of risks are underwritten. Second, the report lays the groundwork for two forthcoming papers on cyber terrorism and cyber warfare. A common language with which to discuss and more accurately insure cyber activity will help to better define the limits of what can be privately re/insured. The two papers will examine attribution, international coordination and impact and quantification and shed light on potential public-private solutions designed to facilitate the development of a robust and sustainable commercial re/insurance market for cyber risk.

The Geneva Association and the International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP) are uniquely placed to offer the perspectives presented in this paper. Both have diverse, international memberships and networks of expertise which, combined, were able to offer the necessary range of practitioners' insights into the different aspects of this multifaceted peril.



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 is catalysing an increasing need for cyber risk protection. However, insuring cyber exposure is challenging due to the risk of accumulation and terminological ambiguity surrounding cyber policy wording, especially in the context of war and terrorism.

Against this backdrop, this report introduces the term 'hostile cyber activity' (HCA) as a potential tool for the insurance industry to mitigate this ambiguity. HCA sits somewhere between the existing notions of cyber terrorism and cyber war as understood within an insurance context. The intent is to cause serious damage in or to another state regardless of publicity or the causing of terror. As such, it is different from cyber terrorism. Even though it tends to be perpetrated by, on behalf of, or with the financial (or moral) support or encouragement of nation states, HCA cannot be classed as an act of war as it is currently defined. On that basis, the term might help to distinguish between what is clearly insurable and what is not (war) (Biener et al. 2015).

A lack of commonality is also a problem in other areas of insurance, such as traditional property insurance. In cyber space, the need for precise terminology is particularly acute in the case of malicious cyberattacks, which open up governments, businesses, individuals and communities to new exposures and uncertainties.



Potential effects of cyber events

According to Lloyd's (2017), a malicious cyber event that takes down a major cloud service provider could lead to economic losses of more than USD 50 billion, equivalent to a major earthquake or hurricane. In a specific U.K.-based scenario in which a cyber blackout affects the U.K. power grid, 'The knock-on effects of the outage include disruption to transportation, digital communications, and water services for a further 8 to 13 million people'. Cyber events have the potential to affect all aspects of the lives and livelihoods of individuals as well as create significant disruption to the functioning of societies on a global scale.

Towards a common language

A lack of common definitions lies at the core of the challenge of promoting the insurability of cyber risk. Common terminology will lead to a sustainable cyber market where re/insurers can make informed choices about the levels of coverage and insureds can be certain of their insurance coverage. Progress towards commonality would also help those who insure physical and non-physical cyber risks to assess accumulation risks, which are too large for individual companies or even the global re/insurance sector to bear.

Cyber incidents are not bound by geography and can simultaneously generate destruction or disruption in multiple jurisdictions and across various lines of business. To promote global sustainability of the cyber insurance market, re/insurers should be able to determine accumulation risk holistically (across jurisdictions, industry segments and various lines of business). Comparability is necessary for such an industry-wide assessment of accumulation risk.

A clearer view of aggregate accumulation would also put the industry in a stronger position in negotiations with governments on solutions for uninsurable risks or risks which jeopardise the solvency of the industry.

The first in a series of three, this report focuses on terminology and introduces HCA as a potential tool for the industry to continue to bridge the gap between terrorism and war. It seeks to distinguish between what is clearly insurable and what is not, with the aim of reducing uncertainty. The second report will look at the importance and difficulty of attribution in the current cyber insurance framework and proposed remedies. The final report will seek to quantify the impact of potential losses. It will also propose potential solutions from insurers, capital markets and public entities.



2. Introduction

As the digital revolution continues and more companies, individuals and societies move business and personal transactions online, awareness of the associated risks is paramount. The insurance industry must respond to a rapidly evolving world in which dangerous cyber activities and evolving attack vectors make it necessary to continuously assess and optimise insurance products and adapt coverage. Agile and radical thinking and action will be required to mitigate cyber risk and promote societal preparedness and prevention measures against malicious cyber activity.

The main risks – cyber criminality, terrorism and war – move beyond the mere physical domain. The cyber domain is instead used as a platform from which loss is generated. The loss itself may be physical, non-physical or a hybrid and can range from disruptive to destructive. The impact and group(s) affected will vary with the type of loss. Against this backdrop, this report will focus on cyber terrorism and war and seek to attain a common language for describing certain cyber events to promote insurability.

Cyber terms in insurance

In the insurance context, terms such as cyber terrorism and cyber warfare have been developed to categorise complex cyber activities and demarcate insurance cover. The definitions and understanding of these terms may differ depending on the way they are applied in different settings, e.g. military or political. To date, the use of these insurance terms has varied between jurisdictions, companies and even lines of business. A global consensus on the exact behaviour or a set of criteria that define a cyber event as either terrorism or warfare is currently lacking.¹

In analysing the potential gap between terrorism and war in the cyber context, the report introduces 'hostile cyber activity' (HCA) as a new term which aims to reduce uncertainty in the language used to describe potential malicious behaviour classed somewhere between terrorism and warfare. Narrowing this gap offers the opportunity for increased insurability as individual companies can assess such risks, make informed decisions about coverage and provide clarity and set parameters of coverage for an insured. If the term succeeds

¹ An individual policy may also use the insurance terminology 'cyber terrorism' or 'cyber war'. The exact definition is found within the contract, and thus the specificities of coverage are likely to vary between re/insurers.

in reducing uncertainty, the outcomes and issues associated with coverage in future disputes could be anticipated without lengthy legal battles and potential reputational damage.

HCA is becoming the preferred method of states (or others) to inflict damage on other states, whether economically or in terms of social cohesion. It is also likely to apply where one state tolerates the execution of attacks. In state-led or state-tolerated attacks, HCA acts as a buffer between behaviour that is not declared cyber terrorism and falls short of the threshold for cyber war. The main types of loss captured by HCA are

- Property loss and damage and potentially bodily injury
- Economic or financial loss and damage, including to essential or critical infrastructure
- Operational interruption.

The cyber insurance market views cyber terrorism as a category of disruptive malicious cyberattack motivated by political, ideological or religious goals; the traditional property and casualty (P&C) lines of insurance view it as the natural extension to cyber of the existing terrorist threat, which generates physical or non-physical damage. As such, it qualifies as cyber-triggered terrorism.

The type of loss envisioned varies depending on the school of thought, cyber (standalone market) or non-cyber (traditional property and casualty lines). Two examples are

- Cyber terrorism coverage from the non-cyber school of thought covers physical damage;
- Coverage from the cyber school of thought focuses on the economic disruption, response costs and financial loss caused by a cyber event with frequent exclusions for physical damage.

The language complexities are exacerbated by the fact that every line of business and every company has different sets of definitions. The definitions employed may even vary within global re/insurance companies depending upon jurisdiction. Coverage can thus deviate significantly, further complicated by the lack of universal law, processes or procedures to guide understanding and interpretation of the various definitions.

The diversity of coverage and lack of a clear framework upon which cyber terrorism and cyber war are understood make them nebulous insurance concepts. The variation in criteria for the behaviour (or exact act) that amounts to an act of cyber terrorism

or cyber war can make it difficult for insureds to understand their coverage. In contrast, despite similar variation in the definition of a hurricane, the type of natural phenomenon this term encompasses is well understood.

Although the development of a common language for terrorism and war in the cyber context will pose a continual challenge for the industry, this report proposes the term HCA as an intermediate option. However, it also recognises the different viewpoints of re/insurers regarding the magnitude of the grey area between cyber terrorism and cyber war. This lack of consensus is due to the complexity of the risks, different commercial perspectives, legal systems and risk appetites involved. The objective is to move towards clarity and initiate discussions on potential solutions.

With this in mind, this report sets out to

- Identify and explore an increasingly prevalent type of activity that falls into the gap between the definitions of cyber terrorism and cyber war
- Provide a starting point for advancing terminological commonality
- Facilitate industry discussions with governments and regulators on insurability and sustainability
- Set the stage for forthcoming Geneva Association reports (deep dive into attribution, impact, quantification and solutions).

Narrowing the gap between 'cyber terrorism' and 'cyber war'

Recent discussions on the terms cyber terrorism and cyber war have tended to focus on a type of activity that lies in the substantial gap between them (see Figure 1a and Figure 1b). Figure 1a shows the current situation and Figure 1b illustrates a potential narrowing of the gap through the use of the term HCA. In the case of cyber war, cyber activity is perpetrated by or on behalf of one state with the hostile aim of damaging another state directly or indirectly. Furthermore, cyber war generally requires a declaration of war, a context with a recognised act of (traditional) war or, alternatively, the impact or magnitude of an event which is such that internationally it is likely to be linked to warfare. In the case of cyber-triggered terrorism, an activity is carried out using a cyber-domain but is motivated by political, religious or other ideological reasons and designed to exert influence or generate fear. In the cyber school of thought, this could result in physical or non-physical damage; in the non-cyber school of thought, it tends to be limited

to an act resulting in physical damage. To date, this delineation has not materialised, as there has yet to be a serious incident of terrorism involving a cyber trigger.

The purpose of analysing insurance or other types of coverage or indemnification for cyber terrorism, cyber war or HCA is not to protect the state on the receiving end of the incident, but rather the individuals and corporations hit in the attack. HCA can result in collateral damage to individuals or corporations by action aimed at the state in which they are based or to individuals and corporations situated in non-involved states. In general, this type of hostile behaviour is not expressly dealt with under existing insurance cover. However, there are examples of carriers openly

providing coverage, particularly in traditional lines of business such as property insurance.

Adoption of the term HCA as an intermediate solution illustrates that the industry is seeking to enhance clarity and work together to promote insurability and address the massive potential gap between insured and economic losses.² Further and in any event, there is an inherent logical or philosophical difficulty with the insurance industry paying the bill for a form of activity conducted or encouraged by a nation state against private interests.

Cyber terrorism and cyber war are considered self-evident phenomena in their own right but of a different and, when correctly defined, relatively limited nature.

Figure 1a: Current spectrum of cyber activity



Source: Wells 2020

² At present, war is excluded from insurance policies, whether occurring from physical 'boots on the ground' or in the cyber context. Alternative options for uninsurable risks will be explored in the third report in this series.

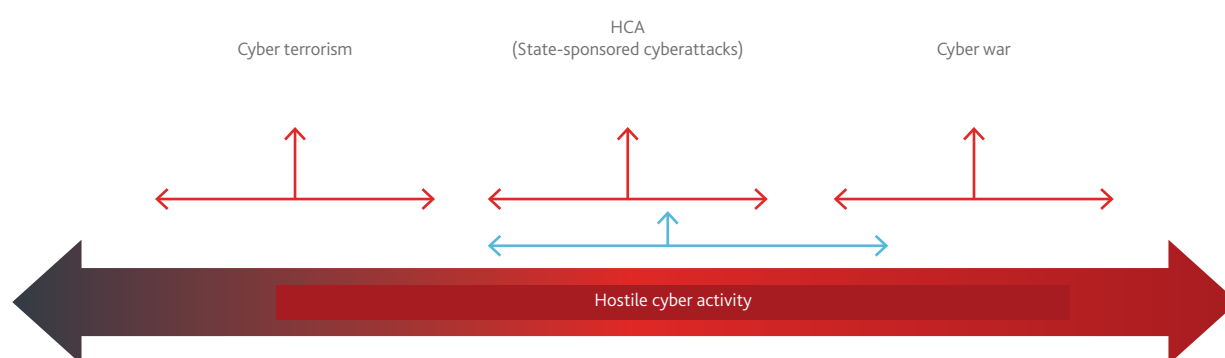
Moreover, as illustrated by Figure 1a and Figure 1b, there is a substantial gap between them.³ Rather than trying to stretch the meanings of cyber terrorism and cyber war⁴ to narrow the gap from each end, we need to examine the increasingly prevalent and real phenomenon which lies somewhere between cyber terrorism and cyber war and categorise the risk/exposure (as illustrated in Figure 1b). This will encompass destructive (physical losses) and disruptive (non-physical losses) cyberattacks and seek to resolve differences between the way the cyber and non-cyber schools of thought determine the problem and its possible solutions. The term HCA can already be substituted for warfare⁵ that is frequently deployed and causes major loss and damage.

Inadequate and imprecise wording may conflate coverage issues. The cyber school of thought increasingly uses exclusions and carve backs, which may exacerbate the issue further (Banham 2019).

Misunderstandings can result in a potential coverage gap, which may only be realised in the aftermath of a cyber event. The challenge for the industry is to work toward a common understanding of behaviour and elucidate this in coverage to prevent litigation and reputational damage. This process is likely to take time, with a lack of consensus remaining in the interim. Educating insureds and society about the risks and coverage available is also key, especially where there is variation between carriers.

Introduction of the term HCA offers a more robust approach to avoid inadvertently covering war or excluding risks that could be handled by commercial policies. A deeper understanding of the aggregate risk posed by cyber terrorism (disruptive and destructive) and cyber-induced war and the state of the industry's appetite and capacity is imperative to determine global solutions for increasing the private deployment of capital.

Figure 1b: Spectrum of cyber activity after introducing the term 'hostile cyber activity' (HCA)



Eliminating the gap between cyber terror and cyber war by introducing the term 'hostile cyber activity': the potential gaps between cyber terrorism and HCA and between HCA and cyber war are smaller than the original gap between cyber terrorism and cyber war (red). Introducing HCA may even result in an overlap between HCA and cyber war (blue).

Source: Wells 2020

- 3 Although much of the coverage globally available for cyber terrorism and cyber warfare creates a potential gap, opinions on the magnitude of the gap differs. This is symbolic of the global lack of consensus and variance in coverage. An example of a relatively narrow gap exists in the U.S. under the Terrorism Risk Program; although cyber war is outside the scope of being a certified act of terrorism (as defined by the Terrorism Risk Insurance Act), other behaviour that doesn't qualify or fit within the definition of an act of terrorism or HCA may be covered (depending on the underlying contract).
- 4 War and, by definition, cyber war, is excluded because the aggregate risk is simply too large to insure. Exclusions for warfare have been included in most insurance policies since 1938. More recently, war exclusions have been adapted to include the cyber environment. At present, some market players are reluctant to cover damage which was caused by nation states who were acting in a warlike manner regardless of the mechanism in which the damage was caused.
- 5 In general, warfare as a concept extends to behaviour which is warlike but short of a declared war. Insurance clauses often cover an act of war but may not extend to the broader concept of warfare. For this reason, the action of a nation state that was hostile and reflective of warlike behaviour but not declared or actual war would thus be deemed 'warfare' and potentially considered as HCA.



3. Current terminology and concepts

3.1. War

In an insurance context, 'war is considered to be a state of armed conflict between two or more parties. It is generally characterised by extreme violence, aggression, destruction and mortality using regular or irregular military force' (Capsicum Re 2019). However, 'denial (of cover) is only tenable when a loss event occurs after a declaration of war is made by one party or another or a state of war has been recognized. Prior to this point, hostile acts are simply that' (Ibid, p. 7). The problem with this definition is that the way in which it applies in different states is likely to vary depending upon understanding, cultural norms and attitudes towards conflict (van der Dennen 2005).

Under international law, Article 2 of the Geneva Convention refers to war and armed conflict as 'declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them'.⁶ It further specifies that declared war or armed conflict includes 'partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance'. Although the Geneva Convention refers to declared war within an international legal setting, this definition is not universally applied; there may be variations of the definition proposed in Article 2. Some states also have their own definitions that are influenced by historical experience, cultural norms and legal practices, and thus may deviate considerably from that of the Geneva Convention. Even under international law there is ambiguity in the terminology. Any reference to war is categorised using the traditional notions of declared war or armed conflict.

From an insurance viewpoint, it would be highly beneficial for internationally recognised bodies and/or nation states to agree on a common definition of war. There are typically clear lines of demarcation and objective criteria as to what constitutes 'declared war'. The lines become blurred when attempting to interpret 'undeclared war' or acts thereof. To date, there is no example of a declared war that has occurred purely within cyber space or been recognisably accompanied by acts in the cyber space. This report therefore proposes that any act by a nation state short of 'declared war' should fall under the broader definition of HCA.

⁶ 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/365-570005>

3.2. Terrorism

Current notions of terrorism are little better, if generally more recent, than those of war. Views on the specific criteria to classify behaviour as terrorism are similarly divergent between sovereign states.⁷ As stated by the Council of Europe (2017), 'This lack of agreement has very practical consequences'.

Historically, terrorism has been perpetrated by governments against individuals (albeit en masse) to influence them. As a phenomenon, it has existed for over 2000 years. More recently, terrorism has been perpetrated almost exclusively by individuals, groups or organisations against states, such as the Irish Republican Army against the U.K., ETA (Euskadi Ta Askatasuna) against Spain and Al Qaeda and ISIS/Daesh. The nature of terrorism has changed over a (relatively short) period of about 50 years, leading to transformed and ultimately complex definitions of terrorism.

Modern terrorism, although still evolving, tends to

- Involve violent or significantly disruptive acts and impacts (such as loss of life or physical damage or disturbance to critical infrastructure)
- Be perpetrated by individuals or small groups (to avoid detection during preparation)
- Be aimed at generating immediate publicity and provide the terrorist organisation or individuals with actual or perceived power
- Be designed to generate fear among the general public with the purpose of achieving political, religious or ideological change, almost regardless of any wider aim.

Although a terrorist incident of the nature just described using a cyber trigger has yet to occur, many consider it likely to happen in the near future.

⁷ See 'IFTRIP comparative of global terrorism pools (including those covering cyber risks)', May 2010. This compares different definitions and coverage of terrorism and terrorism triggered by cyber events as applied to various states in which a government-backed terrorism insurance pool exists.



4. Hostile cyber activity

HCA refers to generally, but not invariably, covert attacks aimed at economic targets or at undermining or destabilising public life (including democratic processes) or public trust, using cyber means or triggers perpetrated generally by, on behalf of or with the practical support and/or moral encouragement of nation states with the aim or consequence of causing one of more of the following

1. Disruption to any level of government⁸
2. Death or injury (physical or mental)
3. Property damage and losses
4. Direct and indirect business interruption (BI)/disruption
5. Economic/financial loss and damage
6. Environmental damage (e.g. pollution)
7. Undermined or diminished public trust
8. Civil unrest
9. Political strife
10. Loss/damage to relationships or reputation (or plain embarrassment)⁹

⁸ For example, this might include ransomware attacks on cities. This occurred in Baltimore in May 2019 when a ransomware attack prevented the city from taking or receiving online payments to any city department, and government employees were blocked from accessing their email and computer systems. The disruption had wider societal implications for those who rely on the functionality of the Baltimore city and government departments. A similar situation occurred in Atlanta in March 2018. See: 'Baltimore Government held hostage by hackers' ransomware', BBC News (23 May 2019) accessed at <https://www.bbc.com/news/world-us-canada-48371476>

⁹ Please refer to the Appendix for a draft of common language.

At present, the main aims of perpetrators from the non-cyber and cyber schools of thought appear to be 3–5 and 5–7 above, respectively, subject to exclusions.

HCA is proposed as a new term for acts that are not classified as terrorism or war as currently defined. The terms cyber and activity have some degree of market commonality, but hostile needs to be justified. The Oxford English Dictionary defines 'hostility' as 'the state or fact of being hostile'; 'hostile action' as 'that which is exercised by one community, state or power against another'; and 'hostile' as 'of, pertaining to or characteristic of an enemy' and 'of the nature or disposition of an enemy; unfriendly'. The definition of 'hostility' used in the U.S., as per the Webster's Dictionary, focuses on the behaviour being 'deep-seated usually mutual ill will, hostile action, overt acts of warfare'.

These definitions confirm that the word 'hostility' is closely related to, but has a wider concept than, 'war' and is substantially different from notions of 'terrorism'.¹⁰ The introduction of HCA is intended as an interim solution while the industry is engaged in the intellectual debate on consensus for mutually and cross-jurisdictionally accepted common language for nation state-backed cyber activity. Further, HCA can be distinguished from 'hybrid warfare', the type of conduct perpetrated, for example, by Russia in Ukraine. Also, the term 'hostile' offers a clear distinction from simple error, systems failure and criminal hacking, which is not in itself hostile. An activity becomes hostile when it is perpetrated by or on behalf of a state and is aimed at one or more of the 10 outcomes listed above.





HCA sits somewhere between cyber terrorism and cyber war (see Figure 2).

- Its intent is to cause serious damage in or to another state regardless of publicity or the causing of terror;
- It tends to be perpetrated by, on behalf of or with the financial (or moral) support or encouragement of nation states; and/but
- It can be distinguished from terrorism and falls short of war as currently defined. It is reasonable to presume that the activity is currently regarded by the state involved as a satisfactory proxy for war – hence the label 'hostile'.

To give a physical yet fictional example of HCA, consider the following scenario: the seizure of foreign-owned vessels by the Iranian Revolutionary Guard in the Straits of Hormuz, perpetrated by cyber means. If this ever occurred, it would fall short of war but would likely be classed as hostile activity by one state towards others, causing economic loss.

Whether the objective of HCA can be limited to causing damage to people or corporations, or if it must have at least some intention of causing damage (of any kind) at a regional or even national level, is a difficult question. In 2009, Google's servers were attacked to obtain classified information held there by the U.S. government. It is widely accepted that

Figure 2: Overview of cyber activity

	 Cyber crimes	 Cyber terror	 Hostile cyber activity (HCA)	 Cyber war
Motivation	Money	Chaos/'money'	Disruption/ destruction/influence/ chaos	Dominance/influence
Expectation	Value	Fear/destroy	Fear/destruction/ disruption/power	Takeover/destroy
Publicity/ prominence	As low as possible	As high as possible	Varies but generally mid range	Low/high

Source: Mitoraj 2020

¹⁰ Terrorism refers to actions conducted by a terrorist, terrorist group or organisation. The motivations of terrorism are largely linked to causing chaos and obtaining money to support a cause, traditionally for religious, political or ideological gain. In contrast, war is an activity between nation states with the motivation to influence, politically or geopolitically, or to gain control over land, assets or governance.

this attack was carried out on behalf of or by another sovereign state. After this event, Google was 'the first U.S. firm to voluntarily disclose an intrusion that originated [potentially by a sovereign state]' (Nakashima 2013). This event does not fall within the definition of cyber war (as a war had not been declared between the U.S. and accused sovereign state,¹¹ and the act did not accompany a de facto war, i.e. a recognised state of war between several states without an actual declaration). As the cyber perpetrators were purportedly connected to the sovereign state, the act would likely not satisfy existing definitions of cyber terrorism.

As emphasised throughout this report, there is divergence across the market regarding the wording used by individual carriers. Thus, some standalone markets may cover this type of risk within existing product offerings. However, for those companies that are not explicit regarding the parameters of their coverage, there may be uncertainty. If behaviour cannot be clearly categorised under the policy and does not fall within existing definitions, it would be captured by the term HCA. In this way, coverage issues can be resolved without the need for a lengthy and expensive legal battle. Introducing the term HCA brings greater clarity to grey areas, and in doing so, promotes insurability.¹²

11 Based upon the definition of war or armed conflict as defined under Article 2 of the Geneva Convention. It is important to note that this is one international perspective which is largely, but not universally, accepted. Consequently, others may argue that the reality of a modern war may not require a formal declaration of war but rather the actual behaviour.

12 However, in order to fit within the proposed terminology of HCA, it is likely that such an incident would only be deemed as HCA if it affected multiple companies or if it occurred on multiple occasions.



5. Principal types of loss

HCA is likely to cause destructive and/or disruptive impact. 'Destructive impact' refers to any or all of the following: physical damage to the IT hardware or components of a computer system; property damage; death or personal injury. Examples include shutting down the cooling systems of gas turbines, opening the sluice gates of dykes and closing the safety valves on pressurised water tubes.

'Disruptive impact' refers to the unavailability of systems, services and infrastructure. Examples include ATM blocking, the hacking of bank accounts, causing computer outages or data corruption in hospitals and the emergency services and attacking the power grid, resulting in blackouts and the interruption of food and fuel distribution chains. An act which is purely disruptive but significant is envisioned to be covered by the term HCA. Certain damage falls under both categories ('hybrid damage'). HCA may also involve physical activity. However, the term is not intended to encompass the intrinsic value of intellectual property, the theft of which is a separate, long-established area of exposure for which few insurance products exist.

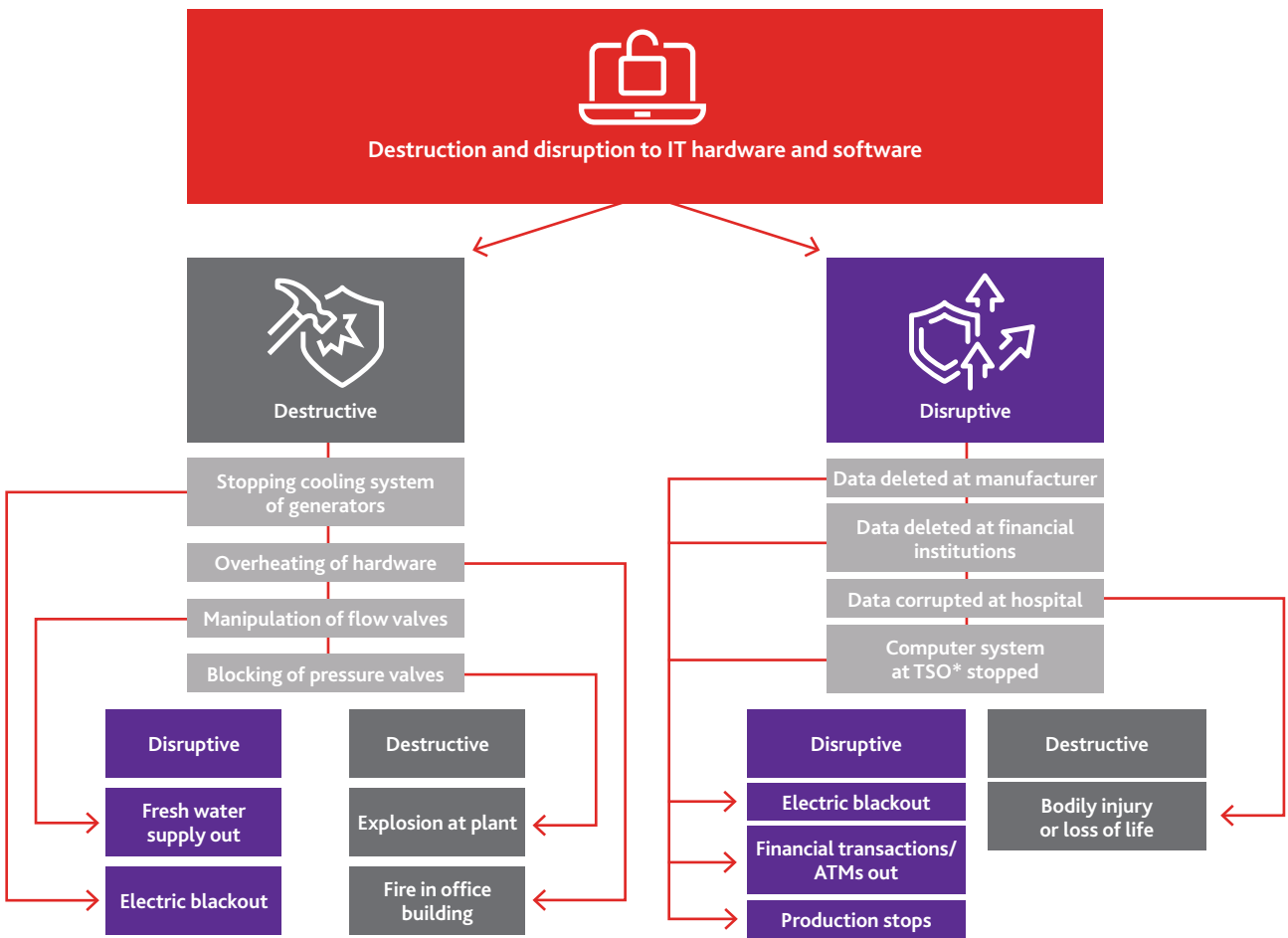
The impact of HCA will likely occur in two stages, referred to as 'primary' and 'secondary' impact in this report.



The impact at either stage may be destructive (e.g. primary: property damage caused by IT software functioning under the control of the perpetrator; secondary: loss of life due to the interrupted supply of medicines) or disruptive (e.g. primary: suspension of production until control has been restored and further HCA prevented; secondary: lack of essential services due to property damage). The type of impact at either stage is independent of that of the other, as shown in Figure 3.

It is to be expected that incidents of HCA will generate large individual and aggregate losses. From a re/insurance viewpoint, the issue of insurability will ultimately hinge upon the aggregate effect.¹³

Figure 3: Disruptive and destructive impacts of cyber events



*Transmission system operator (TSO), also known as regional transmission organization (RTO) in the U.S., is high-voltage electricity transmission between generation and distribution.

Source: Durand 2020b

13 Biener et al. 2015 offer a comprehensive analysis of insurability criteria in the context of cyber insurance, e.g. randomness of loss occurrence and maximum possible loss.



6. Limitations

Despite its utility, introduction of the term HCA comes with some limitations.

Grey areas: Gaps between the definitions of cyber terrorism and cyber war may continue to exist.

Attribution: Attribution will inevitably be difficult with predominantly covert activity, unless a particular group or nation state credibly claims responsibility. A level of certainty needs to be achieved to link the cyber act to a specific nation state and the needed certainty threshold will be different between the political attribution and the legal attribution. Attribution should also be timely, so that both damaged entities and the insurers can swiftly come to a conclusion about coverage. For the legal certainty, it often will be enough to say that the cyber act was conducted by 'a' nation state (as opposed to a terrorist organisation or a criminal group) without having to name it.

Delay in identification: It may be that HCA can only be identified after a series of events has been perpetrated. A single event may not suffice, even if it is subsequently identified as HCA, for example through the imposition of sanctions or retaliatory action.

Collateral damage: Although it is considered to extend to collateral damage in common language, the insurability and treatment of HCA is obviously a matter for the market.

The concept of HCA is still developing and other limitations will emerge. Additional words and phrases may need to be defined. As with existing lines of business, there will be trade-offs between operability and insurability. Even considering these factors, introducing the term HCA is a favourable development.



7. Conclusions

As identified in this report, there are inconsistencies in the definitions of cyber terrorism and cyber war in the insurance industry. Resulting grey areas create confusion and misunderstanding, and in some instances have resulted in litigation and reputational damage. As a means of preventing coverage gaps and having courts determine the scope of cover for acts that lie between cyber terrorism and cyber war, the report introduces the term HCA as an intermediate solution based on a proposed common language.

HCA is an increasingly prevalent form of interstate aggression that represents a growing threat to individuals and corporations, against whom it is often deployed. The resilience of individuals and corporations to HCA would be greatly improved by specific coverage. The availability of viable coverage, perhaps supported in the first instance by state-backed pools, would

- Mitigate the likelihood of sovereign governments having to compensate total or partial losses suffered by businesses as a result of HCA
- Mitigate the moral hazard inherently faced by any government acting as a last-resort insurer
- Help to develop optimal risk sharing between the public and private sectors over time.

The term HCA is predominantly introduced to resolve issues associated with terminological ambiguity and uncertainty, and thus to provide greater clarity around existing coverage within the market. With greater clarity across the global re/insurance market it will be possible to properly assess specific coverage and potential protection gaps and to look at possible solutions to enhance insurance coverage.

The term HCA is not intended to bind the companies who contributed to the research for this report. The term is envisioned as a stepping stone for the industry, to be optimised and adapted as the risk evolves and industry knowledge, understanding and practices converge. This will likely require deconstruction of the historical narrative which divided the positioning and justification for coverage of property and non-property damage by the cyber and non-cyber schools of thought. The two schools of thought will likely become interconnected in the future.

There are broad benefits to continuing to develop a common language for cyber war and cyber terrorism. First, it aims to improve the ability of the insurance industry to discuss the phenomenon which it describes without impairing competitive and contractual freedom.

Another significant industry-wide advancement that is likely to be achieved through commonality and comparability will be the ability to holistically analyse the potential accumulation risk from cyber terrorism or cyber war. This will enable the industry to marry capacity and appetite with product demand and exposure. Comparability and a common language will also put the industry in a stronger position in discussions with governments on backstops or pooling solutions – a particularly valuable benefit as state involvement and the potential scale of claims make government support desirable.

Appendix

Hostile cyber activity

Example of common language

The approach to definitions and use of common language varies greatly between what might be called the Anglo-Saxon school, which is extremely detailed, and the continental approach of mainland Europe, which is more open or broad. For a rapidly changing phenomenon such as HCA, the latter may prove more durable. However, the former is better suited to the purposes of this report, i.e. to provide an interim solution for the industry to optimise and calibrate in working towards something longer-lasting. A discussion draft of common language is offered purely as an illustrative starting point. Current forms of HCA, defined by Pool Re's definition of cyber and the U.K. Counter-Terrorism and Security Act 2019, might be categorised by the descriptions given below.

1. The commission, preparation or instigation of a hostile act that is or may be
 - a. Carried out by, on behalf of or with the financial, moral or practical support of a state other than the home state; or
 - a. In the interest of a state other than the home state.via the means set out in paragraph 2 to cause the adverse consequences set out in paragraph 3.
2. A hostile act is an act committed, prepared or instigated, or caused, occasioned or contributed to by means of damage to or the destruction or disruption of any computer system. This may occur via any alteration, modification, distortion, erasure/corruption of data or disruption of processes where loss is directly or indirectly contributed to, caused/occasioned by or arises/results from a virus or similar mechanism, hacking, phishing or a denial of service attack. The following terms bear the meanings ascribed to them:
 - a. **Computer system** refers to a computer or other equipment, component, system or item which processes, stores, transmits or receives data;

- b. **Data** refers to data of any sort, including (without limitation) tangible or intangible data, programmes, software, bandwidth, cryptographic keys, databases, documents, domain names, network addresses (or anything similar), files, interfaces, metadata, platforms, processing capability, storage media (electronic, optical or holographic), fiber networks, transaction gateways, user credentials, passwords and websites;
- c. **A denial of service attack** is any action or instructions constructed or generated with the ability to damage, interfere with or otherwise affect the availability or performance of networks, network services, network connectivity or computer systems. Denial of service attacks include, but are not limited to, the generation of excess traffic into network addresses, the exploitation of system or network weaknesses, the generation of excess or non-genuine traffic between and amongst networks and the procurement of such actions or instructions by other computer systems;
- d. **Hacking** refers to unauthorised access to or usage of any computer system;
- e. **Phishing** refers to access or attempted access to data by means of misrepresentation or deception;
- f. **A virus** or similar mechanism refers to programme code, programming instructions or any set of instructions constructed with the purpose and ability (or purposely used) to damage, interfere with, adversely affect, infiltrate or monitor computer programmes, computer systems, data or operations. This can involve self-replication or not. Examples include, but are not limited to, Trojan horses, worms, logic bombs, malware and the exploitation of bugs or vulnerabilities in a computer programme to damage, interfere with, adversely affect, infiltrate or monitor as above.

3. A **hostile act** is an act resulting in one or more of the following in the home state, regardless of whether that state is the target:

- a. Disruption of any level of government or branch thereof
- b. Death, injury (physical or mental), damage or disruption to the public, the armed forces, the diplomatic service, the police or the secret services
- c. Property damage and loss (e.g. fire or explosion from a cyberattack) of impacted entities (aka Property Damage (PD))
- d. Business interruption/disruption or operational interruption/disruption (i.e. operation does not have to be 100% down) at impacted entities from property damage (aka business interruption (BI))
- e. Business interruption/disruption or operational interruption/disruption from disruptive cyberattacks at impacted entities (aka cyber-induced non-damage business interruption (NDBI) or cyber BI)
- f. Indirect business interruption/disruption or operational interruption/disruption (at indirectly impacted entities) from disruptive or destructive cyberattacks to other entities (contingent business interruption (CBI) or supply chain) or to critical infrastructure (supply chain, service provider, off-premise power, utilities)
- g. Economic/financial loss and damage from any of the above or general social impact
- h. Environmental damage (e.g. pollution)
- i. Undermined or diminished public trust in the rule of law, institutions of government or democratic processes
- j. Civil unrest
- k. Political strife
- l. Loss of reputation or embarrassment

PROVIDED that loss or damage falling under (c), (d) and (e) suffered by a single company or corporate group (as defined in applicable law) is deemed not to result from HCA.

4. It is immaterial

- a. Whether a person is aware that the activity in which they are or have been engaged is classed as HCA
- b. Whether a state for/on behalf of/in the interests of which HCA is carried out has instigated, sanctioned or is otherwise aware of the carrying out of the activity
- c. Whether any state is a state de jure or de facto.

References

- Banham, R. Cyber coverage confusion. *Risk Management*. 1 October 2019. <http://www.rmmagazine.com/2019/10/01/cyber-coverage-confusion/>
- Biener, C., M. Eling, and J.H. Wirfs. 2015. Insurability of cyber risk – An empirical analysis. *University of St. Gallen Working Paper on Risk Management and Insurance No. 151*.
- Baltimore Government held hostage by hackers' ransomware. 23 May 2019. BBC News. <https://www.bbc.com/news/world-us-canada-48371476>
- Cambridge Centre for Risk Studies. 2016. *Cyber terrorism: assessment of the threat to insurance*.
- Cambridge Centre for Risk Studies. 2017. *Cyber terrorism: Assessment of the threat to insurance*.
- Capsicum Re. 2019. *Cry cyber and let slip the dogs of war: Exploring the issues of attribution in the context of war and cyber*.
- Club des Juristes. 2018. *Insuring Cyber Risk*.
- 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. <https://ihl-databases.icrc.org/ihl/WebART/365-570005>
- Cornish, P., D. Livingstone, D. Clemente, and C. Yorke. 2010. *On cyber warfare*. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf (accessed 13 March 2020).
- Council of Europe. 2017. War and terrorism. <https://www.coe.int/en/web/compass/war-and-terrorism>
- CRO Forum. 2016. Concept paper on a proposed methodology for cyber risk.
- Durand, E. 2020a. Impact matrix. *Presented at the Geneva Association and IFTRIP Cyber Terrorism and Cyber War Task Force Scenario Analysis Event (Munich, January 2020)*.
- Durand, E. 2020b. Destructive and disruptive impacts of a cyber event. *Presented at the Geneva Association and IFTRIP Cyber Terrorism and Cyber War Task Force Scenario Analysis Event (London, February 2020)*.
- Geers, K., D. Kindlund, N. Moran, and R. Rachwald. *World War C: Understanding nation-state motives behind today's advanced cyber attacks* (FireEye Report: Security Reimagined).
- Healey, J. 2011. The spectrum of national responsibility for cyberattacks. *The Brown Journal of World Affairs* 18 (1). 57–70.
- ICT Cyber Desk. 2016. *Cyber-terrorism activities. Report No. 19*.
- IFTRIP. 2018a. *Cyber terrorism and pools*.
- IFTRIP. 2018b. *Cyber terrorism and cyber warfare definitions*.
- IFTRIP. 2019a. *Cyber terrorism and warfare definition*.
- IFTRIP. 2019b. *Cyber terrorism and pools*.
- Kim, A. In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks. *CNN News*. 8 October 2019. <https://edition.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html>
- Kiyuna, A, L. Conyers. 2015. *Cyberwarfare sourcebook*.
- Law, R.D. 2015. *The Routledge history of terrorism*. Oxon and New York: Routledge.
- Lloyd's. 2017. *Counting the cost: Cyber exposure decoded. Emerging risks report 2017 – technology*.
- McGuinness, D. How a cyber attack transformed Estonia. *BBC News*. 27 April 2017. <https://www.bbc.com/news/39655415>

Mitoraj, S. Cyber crimes, cyber terror and cyber war. *Presented at the Geneva Association and IFTRIP Cyber Terrorism and Cyber Warfare Task Force Workshop (London, 24 February 2020).*

Nakashima, E. Chinese hackers who breached Google gained access to sensitive data, U.S. officials say. *Washington Post*. 20 May 2013. https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html

Ottis, R. 2018. Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Peterson, A. The Sony Pictures hack, explained. *Washington Post*. 18 December 2014. <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>

Rigletti, G. 2017. Defining the threat: what cyber terrorism means today and what it could mean tomorrow *International Journal of Business and Cyber Security* 1 (2).

Van der Dennen, J.M.G. 2005. On war: Concepts, definitions, research data – A short literature review and bibliography. <https://core.ac.uk/download/pdf/12857871.pdf>

Wells, C. Towards common terminology. *Presented at the Geneva Association and IFTRIP Cyber Terrorism and Cyber War Task Force Scenario Analysis Meeting (Munich, January 2020).*

With the COVID-19 pandemic we are seeing more than ever the manifestations of our profoundly interconnected world. The crisis is a stark reminder of other looming threats, physical and digital, with the potential to cause extreme disruption. In an insurance context, the pandemic underscores the importance of clear policy wording. This report proposes a new term, 'hostile cyber activity' (HCA), to describe a cyber act that falls between cyber war and cyber terrorism, and in doing so, aims to bring clarity to the language used to describe cyber risks, thereby promoting enhanced insurability and cyber resilience for society.

The Geneva Association

International Association for the Study of Insurance Economics

Talstrasse 70, CH-8001 Zurich

Tel: +41 44 200 49 00 | Fax: +41 44 200 49 99

secretariat@genevaassociation.org