FS Club
News Events Partnerships

WAR, TERRORISM AND HOSTILE CYBER ACTIVITY: CONSENSUS AND CLARITY WITHIN THE CYBER FRONTIER

Dr Rachel Anne Carter, Director Cyber, The Geneva Association

Webinar

Wednesday, 14 April 2021, 15:00 BST

A Word From Today's Chairman

FS Club

Professor Michael Mainelli

Executive Chairman

Z/Yen Group

FS Club

Platinum Sponsors

Invest Northern Ireland

CDI 综合开发研究院 China Development Institute

FINANCE MONTRÉAL

G T Global Times Consulting

Seoul Together we stand

Busan Finance Center

HK FINANCIAL SERVICES DEVELOPMENT COUNCIL 香港金融發展局

LuxembourgforFinance Agency for the Development of the Financial Centre

AIFC

ABU DHABI GLOBAL MARKET

Dubai International Financial Centre

Gold Sponsors

Aptitude SOFTWARE

BRIDGEWORKS

FEATURE SPACE OUTSMART RISK

ARBORETUM

Crown Agents Bank

CERIDIAN

ENTRUST

Silver Sponsors

Bottomline

GPS global processing services

BCS CONSULTING Expect Excellence

P2 CONSULTING

The Technium Global SERVICE WITH INTEGRITY

expert.ai

CLOUDSOFT

PRAXITY™ Empowering Business Globally

Bronze Sponsors

Profile Software

(expleo)

CONTACT PARTNERS

alyne

ESTATES AND INFRASTRUCTURE EXCHANGE®

Personal Sponsors

Challenge Curve

Currencycloud

worldpay

mastercard

RADIX

ZB

LEI GLOBAL LEGAL ENTITY IDENTIFIER FOUNDATION

cuffassociates PART OF THEBES GROUP

Volanté

THE TRANSPARENCY TASK FORCE

CYGNETISE

Catalina Consulting

AMSOM

GIBRALTAR STOCK EXCHANGE

Today’s Agenda

FS Club

- 15:00 – 15:05 Chairman’s Introduction
- 15:05 – 15:25 Keynote Presentation – Dr Rachel Anne Carter
- 15:25 – 15:45 Questions & Answers

Today's Speaker

Dr Rachel Anne Carter

Director, Cyber

The Geneva Association

Dr. Rachel Anne Carter

THE
GENEVA
ASSOCIATION

INSURANCE FOR A BETTER WORLD

War, Terrorism And Hostile Cyber Activity: Consensus And Clarity Within The Cyber Frontier

April 2021, FS Club Webinar

Insuring cyber terrorism, hostile cyber activity and cyber war: Opportunities and challenges for the industry

The challenge of insuring cyber terrorism and hostile cyber activity (HCA) thus depends upon the ability of the industry to

1. Accurately and clearly articulate the risks and any parameters or limits on coverage to stakeholders.
2. Identify the responsible actor or type of actor (terrorist, state actor, criminal etc.).
3. Discern the type of attack, whether it be cyber terrorism, HCA or cyber war.

In addition to clarity around coverage, the outcome of the attribution process is an important factor in determining whether insurance will ultimately cover a loss or who should ultimately pay. This also relates to issues associated with how malicious actors can be held accountable.

Geneva Association & IFTRIP Cyber Terrorism and Cyber Warfare Task Force: Uniting insurers, reinsurers and pools to better understand risks

THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

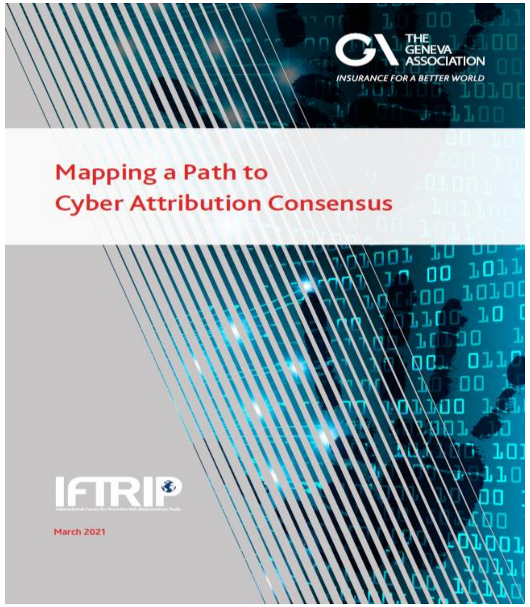
Cyber War and Terrorism:
Towards a common language to promote insurability

IFTRIP

July 2020

Report 1:

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



THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

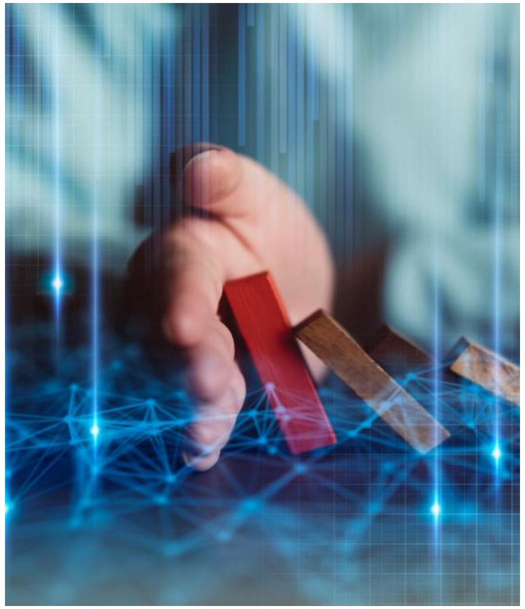
Mapping a Path to
Cyber Attribution Consensus

IFTRIP

March 2021

Report 2:

Rachel Anne Carter and Julian Enoizi, *Mapping a Path to Cyber Attribution Consensus*, March 2021



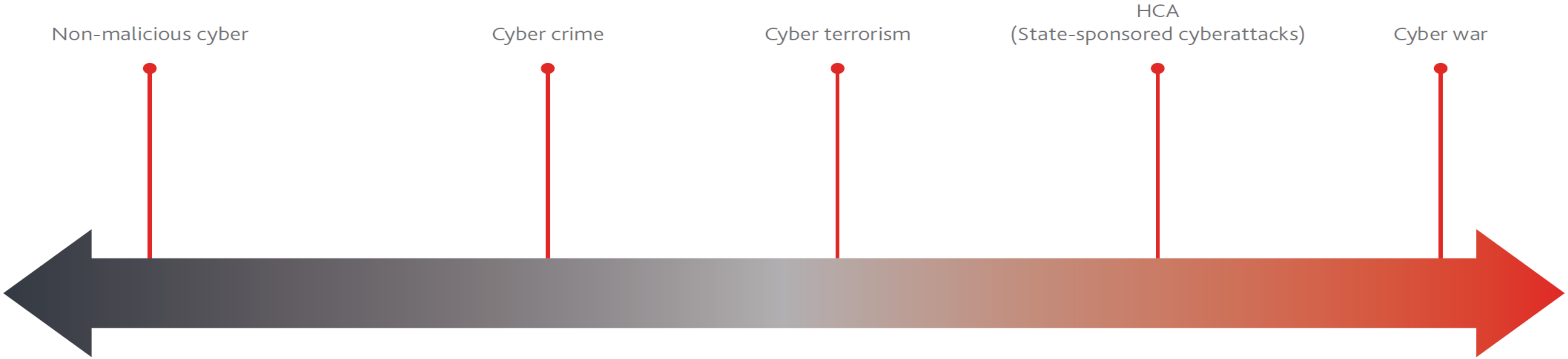
Report 3:

Rachel Anne Carter, Darren Pain, Rory Egan and Peter Zimmerli, *Impact, Quantification and Solutions* (illustrative title- expected June 2021)

All reports can be downloaded at: https://www.genevaassociation.org/cyber-war-and-terrorism

Accurately articulating the risks and any limits on coverage

Current spectrum of cyber activity



Source: Christian Wells, Pool Re

Research report: Cyber War and Terrorism: Towards a common language to promote insurability
by Rachel Anne Carter and Julian Enoizi

Poll 1

Do you feel existing insurance coverage uses terminology to explain cyber risks that are easily read and understood by those purchasing policies?

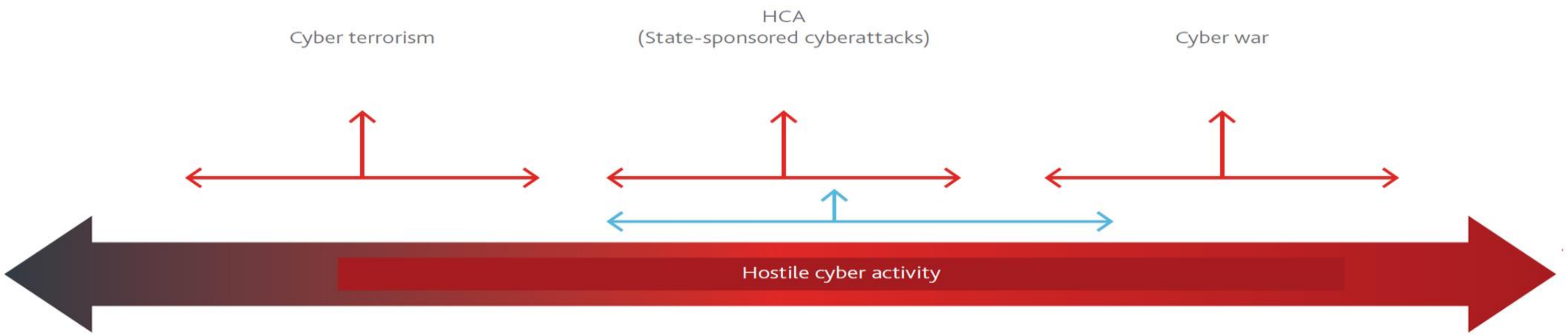
1. Yes, the insurance industry is doing a great job and most language used is clear and concise and easily understood
2. The language used to describe cyber events is mostly understood with minor clarification needed in some instances
3. The language is opaque and it is not at all clear what is covered and what is not covered

Accurately articulating the risks and any limits on coverage

INSURANCE FOR A BETTER WORLD

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)

Spectrum of cyber activity after introducing the term 'hostile cyber activity' (HCA)



Source: Christian Wells, Pool Re

INSURANCE FOR A BETTER WORLD

Research report: Cyber War and Terrorism: Towards a common language to promote insurability
by Rachel Anne Carter and Julian Enoizi

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

The COVID-19 pandemic draws attention to the importance of clear insurance policy wording.

A proposed new term, 'hostile cyber activity', strives for greater clarity in the language describing cyber perils.

Poll 2

Does the term Hostile Cyber Activity (HCA) effectively narrow the gap between cyber terrorism and cyber war?

1. Yes, it clearly articulates and categorises the behavior
2. No, it does little to promote terminological clarity
3. Yes, it helps to reduce the grey area between different types of malicious cyber activity but much work must be done in the future to continue to optimize the wording concerning how to describe such behavior

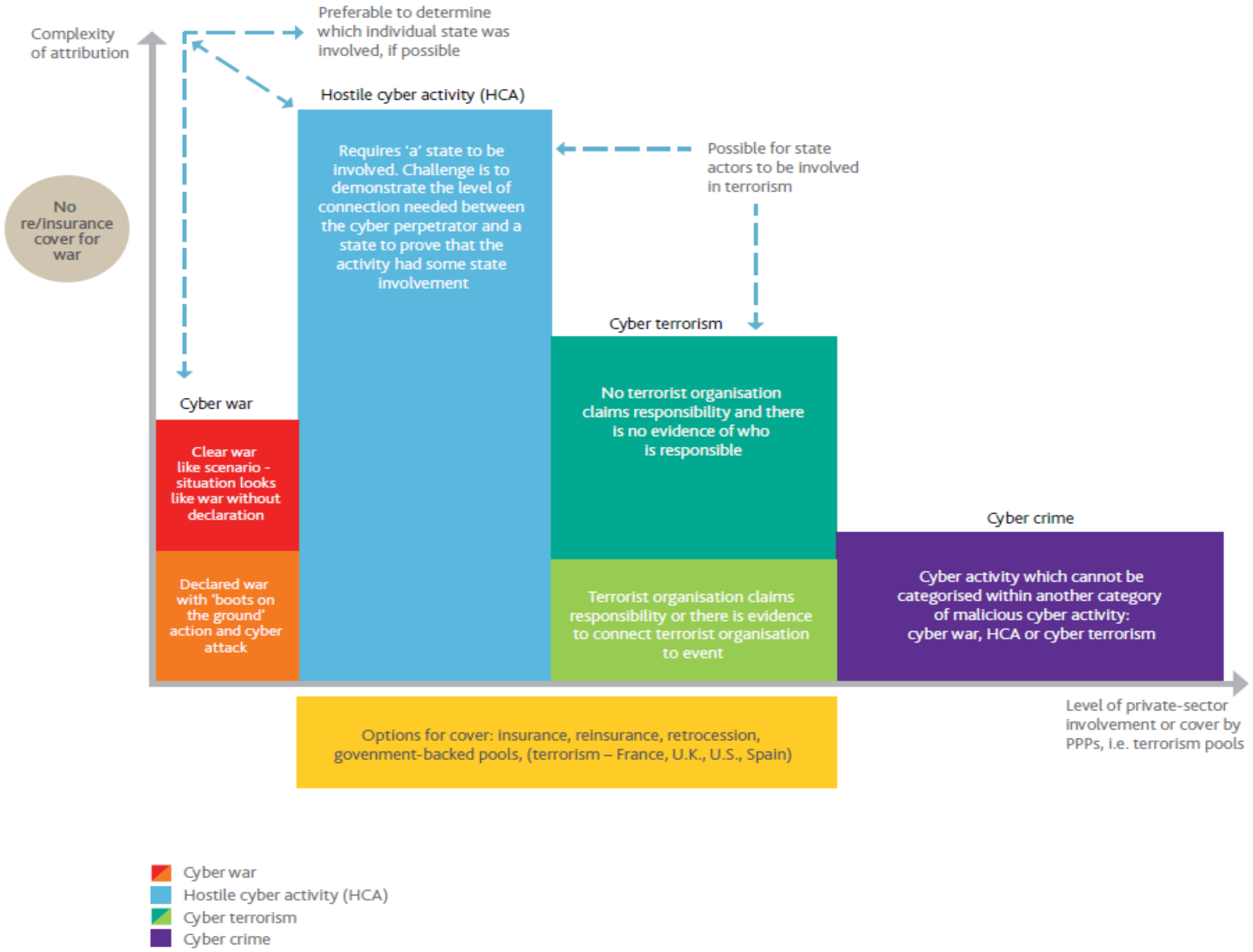
Accurately articulating the risks and any limits on coverage

- Hostile cyber activity seeks to improve consistency and transparency a it related to the spectrum of risk underwritten.
- HCA can result in destructive or disruptive outcomes for the insured.
- HCA can also occur where individuals or a corporation suffers collateral damage during a cyber attack that was perpetrated against a different target.
- A precondition to HCA is that prima facie the act is war like.
- Recognition must be made that there is still challenges particularly within the property insurance markets in covering hostile cyber activity. However, it was the lack of a common definition or common understanding which goes to the core of the insurability challenges.
- At present we have a situation where there is increasing threat with the increased transformation to online activity and an expansion of cyber terrorism

Mapping a path to cyber attribution consensus

- Attribution – The process of allocating responsibility for a cyber attack to an actor and in many cases the assigning of ultimate responsibility to a state.
- Attribution plays a large part in characterizing an event (war, cyber terrorism, HCA, crime). The process 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.
- 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.
- It is very complex process to attribute and characterise an event

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

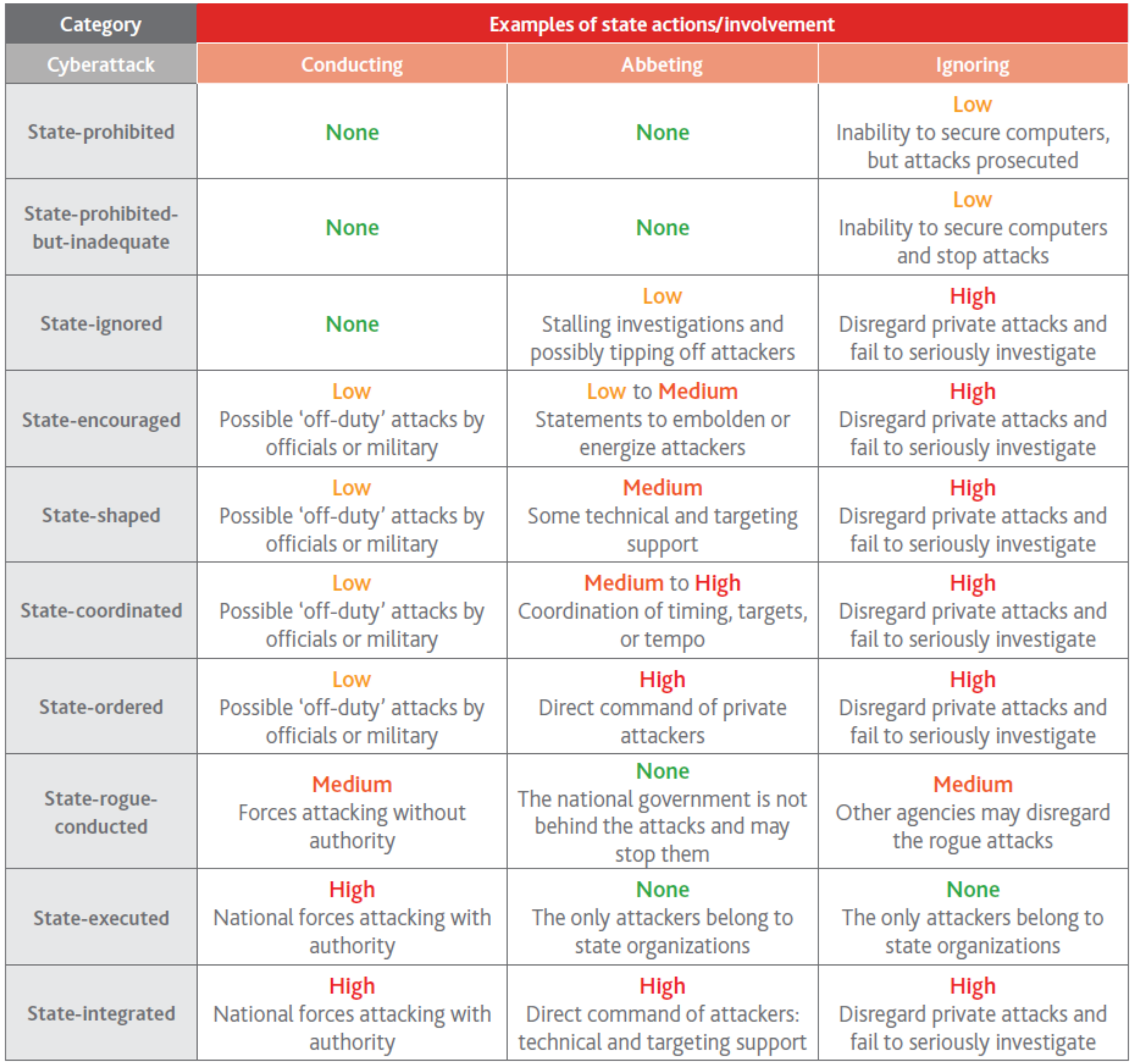

Complexity of attribution
Preferable to determine which individual state was involved, if possible
Hostile cyber activity (HCA)
No re/insurance cover for war
Requires 'a' state to be involved. Challenge is to demonstrate the level of connection needed between the cyber perpetrator and a state to prove that the activity had some state involvement
Possible for state actors to be involved in terrorism
Cyber terrorism
Cyber war
No terrorist organisation claims responsibility and there is no evidence of who is responsible
Clear war like scenario – situation looks like war without declaration
Cyber crime
Declared war with 'boots on the ground' action and cyber attack
Terrorist organisation claims responsibility or there is evidence to connect terrorist organisation to event
Cyber activity which cannot be categorised within another category of malicious cyber activity: cyber war, HCA or cyber terrorism
Level of private-sector involvement or cover by PPPs, i.e. terrorism pools
Options for cover: insurance, reinsurance, retrocession, government-backed pools, (terrorism – France, U.K., U.S., Spain)
🟥 Cyber war
🟦 Hostile cyber activity (HCA)
🟩 Cyber terrorism
🟪 Cyber crime

Mapping a path to cyber attribution consensus

- A useful advancement in the way in which we insure cyber terrorism and hostile cyber activity (if covered under a specific policy) and exclude war is to push for an industry wide consensus or convergence regarding the process of attribution and identifying the responsible actor and the type of act undertaken.
- Identification of the actor and any corresponding responsibility and accountability is essential for safeguarding the community from malicious risks. It also helps insurers to track certain events
- The challenges associated with attribution and characterisation is not just about who is responsible and accountable but who is undertaking the attribution and characterisation process as for example, some governments may not want to attribute as it is questionable regarding whether it is in their interest to do so.

Mapping a path to cyber attribution consensus- state involvement

- Some state actors may engage in plausible deniability and in doing so may use techniques such as planting “false flags” to suggest that the actor was someone else.
- Benefit of HCA for attribution is that it may not be necessary to require attribution to a specific named state, rather, it is most likely going to be sufficient to show (through overt activity) that a state was involved.
- There are a variety of different ways in which “a” state may be deemed to have been involved (see table)



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

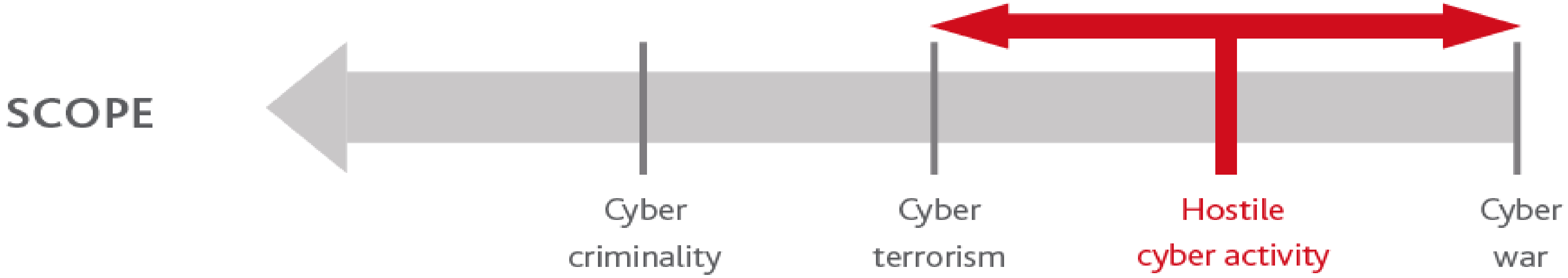
Source: Healey 2011

Mapping a path to cyber attribution consensus- Process

THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

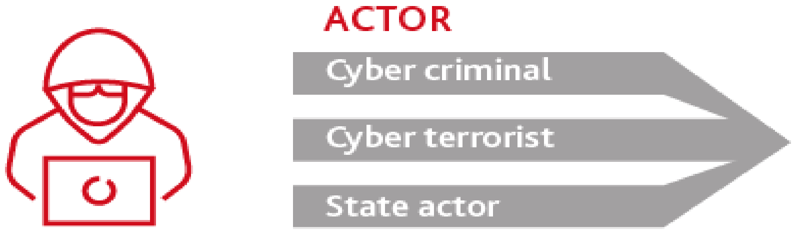
Illustration of the attribution process

1. **Initial characterisation of action**
   Was there a suspicion that the act was one of cyber terrorism, HCA or cyber war?



1a. **Technical analysis including private companies, police and intelligence services investigations**
Often done secretly and information often cannot be found in the public domain

1b. **Attribution to actor (carried out 'in house' at present)**



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

Mapping a path to cyber attribution consensus- Developing International Norms

- Potential future end goal to ensure there is greater transparency, accountability and efficiency in the attribution process is to develop a series of international norms.

- Developing international norms is not (*realistically*) going to be achievable in the short term but it is a reasonable to seek to have international norms implemented in the medium to longer term.

- In order to seek to implement an international norm, it might be advisable to seek to have groups of states who are following the same norms and adapting the international norm into their own domestic context.

- Challenge- the practicality of the challenge is not just getting consensus but it is also getting agreement from the states who are adopting the norm to give up some of their freedoms.

- Development of any international norms should be something which is done amongst various sectors working together: re/insurance companies, large corporates, academics, technology and cyber experts.

Poll 3 & 4

Should the insurance industry help lead the development of an international norm or harmonized process for the attribution and characterisation of an event?

1. Yes, it is important to get full consistency with the way events are categorized
2. No, this should be a matter which the insurer undertaking the process should have the autonomy to determine (and clearly state) how such categorization occurs

If the insurance industry was to be involved in leading the development of an international norm, who else needs to be at the metaphorical table discerning this?

1. All insurance companies and the corporate customers
2. Insurance companies, security firms, technology providers, corporates
3. Insurance companies, security firms, technology providers, corporates, government representatives

Geneva Association & IFTRIP Cyber Terrorism and Cyber Warfare Task Force: Uniting insurers, reinsurers and pools to better understand risks

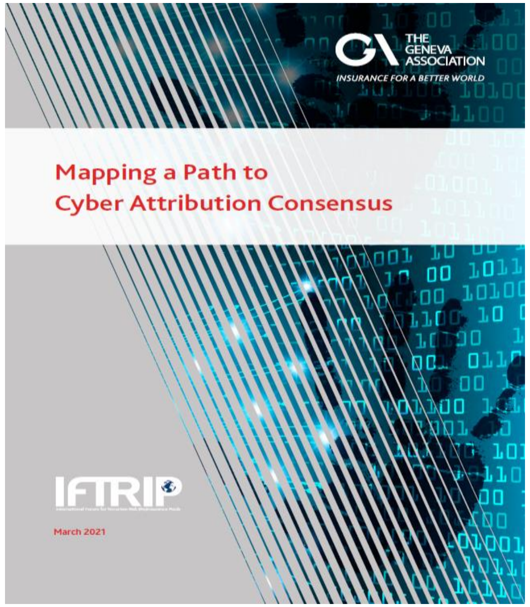
THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

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

IFTRIP
July 2020

Report 1:

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

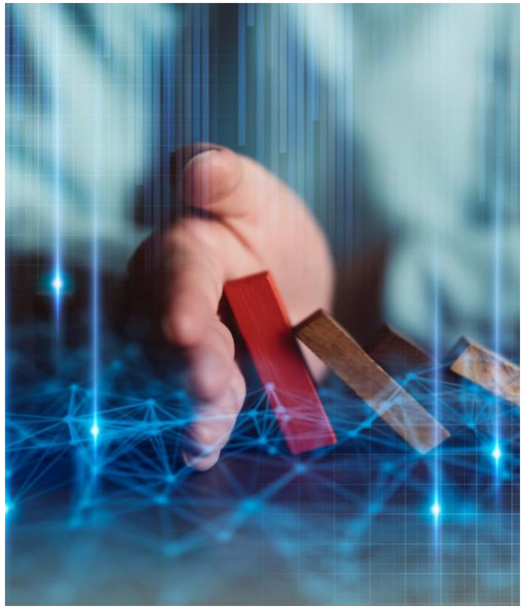

THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

Mapping a Path to
Cyber Attribution Consensus

IFTRIP
March 2021

Report 2:

Rachel Anne Carter and Julian Enoizi, *Mapping a Path to Cyber Attribution Consensus*, March 2021



Report 3:

Rachel Anne Carter, Darren Pain, Rory Egan and Peter Zimmerli, *Impact, Quantification and Solutions* (illustrative title- expected June 2021)

All reports can be downloaded at: https://www.genevaassociation.org/cyber-war-and-terrorism

Comments, Questions & Answers

FS Club

FS Club

Platinum Sponsors

Invest Northern Ireland

CDI 综合开发研究院 China Development Institute

FINANCE MONTRÉAL

G T Global Times Consulting

Seoul Together we stand

Busan Finance Center

HK FINANCIAL SERVICES DEVELOPMENT COUNCIL 香港金融發展局

LuxembourgforFinance Agency for the Development of the Financial Centre

AIFC

ABU DHABI GLOBAL MARKET

Dubai International Financial Centre

Gold Sponsors

Aptitude SOFTWARE

BRIDGEWORKS

FEATURE SPACE OUTSMART RISK

ARBORETUM

Crown Agents Bank

CERIDIAN

ENTRUST

Silver Sponsors

Bottomline

CLOUDSOFT

GPS global processing services

PRAXITY™ Empowering Business Globally

BCS CONSULTING Expect Excellence

P2 CONSULTING

The Technium Global SERVICE WITH INTEGRITY

expert.ai

Bronze Sponsors

Profile Software

(expleo)

CONTACT PARTNERS

alyne

ESTATES AND INFRASTRUCTURE EXCHANGE®

Personal Sponsors

Challenge Curve

Currencycloud

worldpay

mastercard

RADIX

ZB

LEI GLOBAL LEGAL ENTITY IDENTIFIER FOUNDATION

cuffassociates PART OF THEBES GROUP

Volanté

THE TRANSPARENCY TASK FORCE

CYGNETISE

Catalina Consulting

AMSOM

GIBRALTAR STOCK EXCHANGE

Thank You For Listening

FS Club

Forthcoming Events

- Mon, 19 Apr (10:00-10:45) Financial Centres Of The World 2021: Focus On Frankfurt
- Tue, 20 Apr (11:00-11:45) Esop Sofa: Hot Topics In Employee Share Ownership - Newspad Review
- Wed, 21 Apr (14:00-14:45) Why 2021 Will Be A Record Year For M&A In The Knowledge Economy - Consulting, Software & Technology Services
- Fri, 23 Apr (12:00-12:45) If We Have Financial Services Bills, What Should Be In A Digital Services Bill?

Visit **https://fsclub.zyen.com/events/forthcoming-events/**