Reforming the 'War Exclusion' in the context of rising Cyber Warfare

Service area / Coporate
Legal jurisdictions / Bermuda
Date / July 2022

The 2017 NotPetya cyber-attack highlighted the risk of cyber exposure arising from insurance policies not designed to cover cyber risk ("silent cyber") and brought into question whether traditional war exclusions in cyber-affirmative insurance policies are fit for purpose in relation to state-sponsored cyber incidents.

NotPetya Cyber-attack

In June 2017, data-destroying malware called NotPetya, which has since been attributed to Russia's military intelligence agency, infected hundreds of organizations in dozens of countries causing an estimated $10 billion in losses. Mondelez International, a multinational food company headquartered in Chicago, and Merck, a multinational science and technology company headquartered in Damstadt, suffered damage as a result of the attack and claimed under their respective 'all-risks' property insurance. Both companies had their claim rejected on the basis of a war exclusion clause and filed suit against their insurer. The Mondelez case is ongoing, but earlier this year the New Jersey Superior Court sided with Merck and its strict interpretation of the acts of war exclusion.

In the fallout from NotPetya, the insurance industry has sought explicit exclusions in non-cyber policies to minimise exposure to 'silent cyber'. In part, this effort is in response to regulatory initiatives, like that of the Bermuda Monetary Authority, which requires insurers to clarify whether or not they offer cyber coverage in non-cyber policies incepting 1 January 2024, either by including a clear exclusion language or by adding the necessary endorsement to the policies. Although the Mondelez and Merck cases involved claims under all-risks property insurance policies, these cases along with the rise in state-sponsored cyber incidents has caused insurers to review their war exclusions in cyber affirmative policies to ensure that they are fit for purpose.

Pitfalls of traditional war exclusions

War exclusions address traditional forms of kinetic acts of war conducted by a government (de jure or de facto) and as a result, in order to rely on the exclusion, the insurer must prove that a cyber-attack was a warlike action by a government or sovereign power rather than a criminal or terrorist act (which may be covered by the policy). The ability to attribute the act to a government is therefore incredibly important but is especially difficult in relation to cyber incidents where technology can be used in different ways to mask the identity of the actor or create a 'false flag'. Further, it is unclear what level of nation-statement involvement is necessary in order for the bad act to be attributed to it (i.e., safe harbour, tacit sponsorship, supervision or resourcing).

Issues surrounding coverage of state-sponsored cyber-attacks

Insurers who offer cyber insurance are reluctant to provide coverage for state-sponsored cyber-attacks for a number of reasons. Assessing the frequency and severity of cyber warfare, especially the potential for large accumulated losses,

remains a serious challenge for underwriters. There is also the moral hazard of providing coverage for state-sponsored cyber incidents – governments may be more likely to initiate state-sponsored cyber-attacks (or take other aggressive action which could result in a retaliative cyber-attack) if they know that resulting cyber losses will be mitigated by insurance pay-outs.

The way ahead

Various insurance associations and war exclusion reformers have put forward potential solutions to reform traditional war exclusions so that they are fit for purpose in light of state-sponsored cyber war, some of which are considered below.

Lloyd's Market Association

In December 2021, the Lloyd's Market Association issued four new cyber war and cyber operation exclusion clauses which allow for a scalable approach to coverage for cyber operations which are not excluded by the definition of war, cyber war or cyber operations and which have a major detrimental impact on a state.

All four precedent clauses contain the same provision concerning attribution, which determines that the "*primary but not exclusive factor in determining attribution of a cyber operation shall be whether the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located attributes the cyber operation to another state or those acting on its behalf". Pending such determination, the insurer may rely upon "inference which is objectively reasonable*". The burden of proof is on the insurer to prove that the war exclusion applies.

Requiring certification of attribution from a public body (e.g. government or an intelligence service) is problematic for several reasons. For one, governments do not make public attributions of most cyber incidents and may be reluctant to do so on a number of grounds, including a lack of conclusive evidence or to avoid jeopardizing intelligence sources. More fundamentally, the value a state puts on maintaining good political and economic ties with the alleged responsible state may outweigh the value of publicly attributing responsibility.

Geneva Association / International Forum of Terrorism Risk (Re)Insurance Pools

The Geneva Association ("**GA**"), a global association of insurance companies, and the International Forum of Terrorism Risk (Re)Insurance Pools ("**IFTRIP**") have proposed the introduction of a special category of hostile cyber activity ("**HCA**") to provide additional granularity to cover malicious incidents beyond cyber terrorism but not involving cyber warfare.

The GA/IFTRIP argue that policy language based around HCA will enable insurers to better delineate 'acts of war' and state-sponsored attacks from other malicious cyber incidents which would fall within coverage. For instance, clauses referencing HCA might stipulate that it is only necessary to prove that a state was involved rather than having to pinpoint which one.

John Bateman

John Bateman, a senior fellow in the Cyber Policy Initiative of the Technology and International Affairs Program at the Carnegie Endowment for International Peace, advocates for two complementary exclusions:

- A cyber catastrophe exclusion that would address uninsurable cyber catastrophes based on the scale of nature of losses, regardless of the perpetrator or any connection with war. This exclusion would act as the insurers' first line of defence against cyber losses during times of both peace and war; and
- A separate narrowly focused new war exclusion for cyber claims that would deal specifically with cyber losses arising from kinetic war.

As a way to sidestep the issue of attribution, Bateman offers a geographically based approach pursuant to which areas of kinetic warfare (or other territories at high risk of state-sponsored cyber operations) could be identified and losses suffered in these areas could then be excluded from coverage, regardless of the identity of the perpetrator.

In the context of hostile cyber acts, attribution remains one of the biggest hurdles when it comes to reforming traditional war exclusions. Bateman's geographic approach neatly sidesteps the issue of attribution however, the result may not be as the market intends. Applying Bateman's geographic approach to the NotPetya attack for example, only damages suffered within Ukraine would be excluded by the war risk exclusion and the collateral damage suffered outside of Ukraine (assuming the cyber catastrophe exclusion did not apply) would be covered.

Conclusion

Cyber warfare is increasingly regarded as part of a nation's arsenal alongside traditional military force and it is likely that acts of cyber war will increase in the future. The key to overcoming the challenge of reforming traditional war exclusions to make them fit for purpose in the context of cyber warfare will be through positive market dialogue between insurers, insureds and regulators so that common ground regarding what kinds of claims would be excluded from coverage can be reached.

References

Bateman, J. 5 October 2020. War, Terrorism and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions. War, Terrorism, and Catastrophe in Cyber Insurance:

Continued

Understanding and Reforming Exclusions - Carnegie Endowment for International Peace

"Cry Cyber and Let Slip the Dogs of War," Capsicum Re, July 23, 2019, https://www.capsicumre.com/wp-content/uploads/2019/07/Capsicum-Re-Cry-Cyber.pdf.

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

The Geneva Association. March 2021. Mapping a Path to Cyber Attribution Consensus – Research Report. Authors: Rachel Anne Carter and Julian Enoizi. Mapping a Path to Cyber Attribution Consensus | Research report | Geneva Association

The Geneva Association. January 2022. Insuring Hostile Cyber Activity: In search of sustainable solutions. Authors: Rachel Anne Carter, D. Pain and Julian Enoizi. Insuring Hostile Cyber Activity: In search of sustainable solutions | Research report | Geneva Association

Subscribe for more

Key contact

For further information or professional advice please contact our lawyer below:

Michelle Falcucci
Counsel

D +1 441 542 4522
E michelle.falcucci@careyolsen.com

Michelle Falcucci advises on all aspects of Bermuda corporate and commercia law, with a particular focus on M&A, corporate finance, joint ventures and debt and equity offerings.

FIND US

Carey Olsen Bermuda Limited
Rosebank Centre 5th Floor
11 Bermudiana Road
Pembroke HM 08
Bermuda

T +1 441 542 4500
E bermuda@careyolsen.com

FOLLOW US

Subscribe for more

Visit our corporate team at careyolsen.com

PLEASE NOTE