Browne Jacobson

Is a state-sponsored cyber attack an act of war?

30 May 2023

Previous
Insurance tech – the Sky's the limit

The recent Lloyd's Cyber War requirements have led to an increased focus on the interplay between cyber and war covers and exclusions, and the consequences for insurers. The recent decision of the Appellate Division in New Jersey in Merck & Co. Inc. v. Ace American Insurance Company provides some interesting guidance on whether a state-sponsored cyber attack amounts to warlike action.

The case and first instance decision

Merck suffered property damage as a result of the NotPetya cyber attack in 2017. NotPetya was so named as it resembled the Petya ransomware attack but, unlike Petya, NotPetya did not include a recovery feature (essentially it amounted to 'wiper' malware). It was widely suspected that NotPetya was attributable to the Russian state, although this had not been established

The defendant insurer argued that the losses were not covered due to a policy exclusion in respect of '*hostile or warlike action in time of peace or war*'.

The first instance judge determined that the exclusion did not apply. In reaching that conclusion, the court considered the fact that the exclusion did not make any reference to cyber (or similar) and that the language had not been changed notwithstanding the increased frequency of cyber attacks. The failure of insurers to change their wordings made it reasonable for the policyholder to consider the exclusion only applied to more traditional forms of warfare.

The insurers appealed the judgment.

The appeal

The appeal was rejected. In reaching her decision, the Judge stated:

"*The exclusion of damage caused by hostile or warlike action by a government or sovereign power in times of war or peace requires the involvement of military action. The exclusion does not state the policy precluded coverage for damages arising out of a government action motivated by ill will…terms similar to "hostile or warlike action" by a sovereign power are intended to relate to actions clearly connected to war or, at least, to a military action or objective*".

In light of the above, even if NotPetya had been proven to be attributable to the Russian state, the damage would still not have been excluded owing to the lack of a war or military objective.

Considerations for insurers

This decision further underlines the importance for insurers to carefully consider the language used in their policy wordings, particularly in relation to policy exclusions. If they intend to exclude coverage for cyber attacks, it would be prudent to expressly say so and not rely on more general exclusions, such as those for war, terrorism or similar perils.

Contents

Key contact

Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

You may be interested in...

Coverage disputes and policy interpretation

Policy drafting and distribution