



FARELLA
BRAUN + MARTEL LLP



OCTOBER 18, 2022

Caught in the Crossfire: How will the War Exclusion affect commercial policyholders?

Tyler Gerking, and Patrick Loi

Insurance Recovery Practice Group, Farella Braun + Martel LLP

This presentation is provided for informational purposes and does not constitute legal advice.

Overview

- Historical case law on War Exclusions in property policies
- The scope of existing War Exclusions in cyber policies
- Efforts by insurers to limit coverage for state-backed cyber-attacks
 - Lloyd's model clauses
 - Lloyd's requirements for exclusions drafted by insurers
- Special Territory Exclusions

War Exclusions in Property Policies

i. Hostile/Warlike Action Exclusion Language

- A. 1) Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack:
- a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces;
 - b) or by military, naval, or air forces;
 - c) or by an agent of such government, power, authority or forces;

This policy does not insure against loss or damage caused by or resulting from Exclusions A., B., or C., regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

- Historical case law on property policy War Exclusions.
- *Merck* and *Mondelez* cases arising out of the NotPetya ransomware attack have caused insurers to reevaluate their exclusions.

The Existing War Exclusion in Cyber Policies

14. Based upon or arising out of **any act of war (whether war is declared or not)**, invasion, or the confiscation, nationalization or destruction of, or damage to, property under the order of government or other public authority, provided, however, this exclusion does not apply to **Cyber Terrorism**.

Cyber Terrorism means an act or series of acts of any person or group of persons, whether acting alone or on behalf of or in connection with any organization, **committed for social, political, economic, religious or ideological purposes**. This shall include, **but is not limited to**, the intention to influence any government or to put the public in fear for such purposes by using activities perpetrated electronically or otherwise which result in a **Security Event** involving **You**, or that are directed towards the destruction, disruption or subversion of communication and information systems, infrastructure, computers, the internet, telecommunications or electronic networks, or the contents thereof

Lloyd's Model Exclusion No. 1

War, Cyber War and Cyber Operation Exclusion No. 1

(For use on commercial cyber insurance contracts)

1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of war or a cyber operation.
2. The insurer shall have the burden of proving that this exclusion applies.

Lloyd's Model Exclusion No. 1

Definitions

6. **Computer system** means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.
7. **Cyber operation** means the use of a **computer system** by or on behalf of a **state** to disrupt, deny, degrade, manipulate or destroy information in a **computer system** of or in another **state**.
8. **State** means sovereign state.
9. **War** means:
 - 9.1. the use of physical force by a **state** against another **state** or as part of a civil war, rebellion, revolution, insurrection, and/or
 - 9.2. military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order of any government or public or local authority,whether war be declared or not.

Lloyd's Model Attribution Language

Attribution of a **cyber operation** to a **state**

3. 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.
4. Pending attribution by the government of the **state** (including its intelligence and security services) in which the **computer system** affected by the **cyber operation** is physically located, the insurer may rely upon an inference which is objectively reasonable as to attribution of the **cyber operation** to another **state** or those acting on its behalf. It is agreed that during this period no loss shall be paid.
5. In the event that the government of the **state** (including its intelligence and security services) in which the **computer system** affected by the **cyber operation** is physically located either:
 - 5.1. takes an unreasonable length of time to, or
 - 5.2. does not, or
 - 5.3. declares it is unable toattribute the **cyber operation** to another **state** or those acting on its behalf, it shall be for the insurer to prove attribution by reference to such other evidence as is available.

Lloyd's Model Exclusion No. 2

War, Cyber War and Cyber Operation Exclusion No. 2

(For use on commercial cyber insurance contracts)

1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of:
 - 1.1. **war** or a **cyber operation** that is carried out in the course of **war**; and/or
 - 1.2. retaliatory **cyber operations** between any **specified states**; and/or
 - 1.3. a **cyber operation** that has a major detrimental impact on:
 - 1.3.1. the functioning of a **state** due to the direct or indirect effect of the **cyber operation** on the availability, integrity or delivery of an **essential service** in that **state**; and/or
 - 1.3.2. the security or defence of a **state**.
2. The insurer shall have the burden of proving that this exclusion applies.
3. Subject to the exclusions above and the other terms, conditions and exclusions contained in this insurance, **the following limits shall apply to any other cyber operation(s):**
 - 3.1. *{response}* for any cover in relation to all loss arising out of one **cyber operation**;
 - 3.2. *{response}* in the aggregate for the period of insurance.

These limits shall apply within the full policy limit and not in addition thereto.

Unless an amount is specified in 3.1 and 3.2, there shall be no coverage for any cyber operation(s).

Lloyd's Model Exclusion No. 2

9. **Essential service**, for the purposes of this exclusion, means a service that is essential for the maintenance of vital functions of a **state** including without limitation: financial institutions and associated financial market infrastructure, health services or utility services.
10. **Specified states** means China, France, Germany, Japan, Russia, UK or USA.

Lloyd's Model Exclusion No. 3

War, Cyber War and Cyber Operation Exclusion No. 3

(For use on commercial cyber insurance contracts)

1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of:
 - 1.1. **war** or a **cyber operation** that is carried out in the course of **war**; and/or
 - 1.2. retaliatory **cyber operations** between any **specified states**; and/or
 - 1.3. a **cyber operation** that has a major detrimental impact on:
 - 1.3.1. the functioning of a **state** due to the direct or indirect effect of the **cyber operation** on the availability, integrity or delivery of an **essential service** in that **state**; and/or
 - 1.3.2. the security or defence of a **state**.
2. The insurer shall have the burden of proving that this exclusion applies.

Lloyd's Model Exclusion No. 4

War, Cyber War and Cyber Operation Exclusion No. 4

(For use on commercial cyber insurance contracts)

1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind (together "loss") directly or indirectly occasioned by, happening through or in consequence of:
 - 1.1. **war** or a **cyber operation** that is carried out in the course of **war**; and/or
 - 1.2. retaliatory **cyber operations** between any **specified states** leading to two or more **specified states** becoming **impacted states**; and/or
 - 1.3. a **cyber operation** that has a major detrimental impact on:
 - 1.3.1. the functioning of a **state** due to the direct or indirect effect of the **cyber operation** on the availability, integrity or delivery of an **essential service** in that **state**; and/or
 - 1.3.2. the security or defence of a **state**.
2. Paragraph 1.3 shall not apply to the direct or indirect effect of a **cyber operation** on a **bystanding cyber asset**.
3. The insurer shall have the burden of proving that this exclusion applies.

Lloyd's Model Exclusion No. 4

- 7. **Bystanding cyber asset** means a **computer system** used by the insured or its third party service providers that is not physically located in an **impacted state** but is affected by a **cyber operation**.

- 11. **Impacted state** means any **state** where a **cyber operation** has had a major detrimental impact on:
 - 11.1. the functioning of that **state** due to the direct or indirect effect of the **cyber operation** on the availability, integrity or delivery of an **essential service** in that **state**; and/or
 - 11.2. the security or defence of that **state**.

Lloyd's Requirements for State-Backed Cyber-attack Exclusions

Requirement for exclusions in standalone cyber-attack policies

It is important that Lloyd's can have confidence that syndicates are managing their exposures to liabilities arising from war and state backed cyber-attacks. Robust wordings also provide the parties with clarity of cover, means that risks can be properly priced and reduces the risk of disputes.

We are therefore requiring that all standalone cyber-attack policies falling within risk codes CY and CZ must include, unless agreed by Lloyd's, a suitable clause excluding liability for losses arising from any state backed cyber-attack in accordance with the requirements set out below. This clause must be in addition to any war exclusion (which can form part of the same clause or be separate to it). At a minimum, the state backed cyber-attack exclusion must:

1. exclude losses arising from a war (whether declared or not), where the policy does not have a separate war exclusion.
2. (subject to 3) exclude losses arising from state backed cyber-attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state.
3. be clear as to whether cover excludes computer systems that are located outside any state which is affected in the manner outlined in 2(a) & (b) above, by the state backed cyber-attack.
4. set out a robust basis by which the parties agree on how any state backed cyber-attack will be attributed to one or more states.
5. ensure all key terms are clearly defined.

Special Territory Exclusion

1. There shall be no coverage afforded or benefit provided by this Policy for any:
 - (i) entity organized, headquartered, incorporated, registered or established in an **Excluded Territory**;
 - (ii) natural person that is resident or located in an **Excluded Territory**;
 - (iii) claim, action, suit or proceeding brought or maintained in an **Excluded Territory**; or
 - (iv) loss of, theft of, damage to, loss of use of, encryption of, interruption to the operations or availability of, or destruction of any property (tangible or intangible) located in an **Excluded Territory**, including, but not limited to, any computer system, data, money or securities located in an **Excluded Territory**.
2. For purposes of this endorsement, “**Excluded Territory**” means:
 - (i) The Republic of Belarus;
 - (ii) The Russian Federation; and/or
 - (iii) Ukraine.

Questions?



Patrick Loi
415.954.4996
ploi@fbm.com



Tyler Gerking
415.954.4968
tgerking@fbm.com