War and Cyber Operation Exclusion
(For use on commercial cyber insurance contracts)

1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover that part of any loss, damage, liability, cost or expense of any kind (together "loss") resulting:

   1.1. directly or indirectly from **war;**

   1.2. from a **cyber operation** that is carried out as part of a **war**; or

   1.3. from a **cyber operation** that causes a sovereign state to become an **impacted state**.

   Provided, however, paragraph 1.3 shall not apply to the direct or indirect effect of a **cyber operation** on 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**.

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

2. In determining attribution of a **cyber operation**, the insured and insurer shall have regard to whether the government of the **impacted state** formally or officially attributes the **cyber operation** to another sovereign state or those acting at its direction or under its control.

   In the absence of attribution by the **impacted state**, the insurer may rely upon a reasonable inference as to attribution of the **cyber operation** to another sovereign state or those acting at its direction or under its control having regard to such evidence as is available to the insurer.

   In the event that the government of the **impacted state** either takes an unreasonable length of time to, or does not, or is unable to attribute the **cyber operation** to another sovereign state or those acting at its direction or under its control, it shall be for the insurer to prove attribution by reference to such other evidence as is available.

Definitions

The following definitions apply for the purposes of this exclusion only:

3. **Computer system** means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, or 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 or as defined in the policy to which this endorsement is attached. If there is any inconsistency between definitions of **computer system** in this endorsement and the policy, the policy definition shall apply and shall override the inconsistent provisions in this endorsement.

4. **Cyber operation** means the use of a **computer system** by, at the direction, or under the control of a sovereign state to disrupt, deny, degrade, manipulate or destroy information in a **computer system** of or in another sovereign state.

5. **Essential service** means a service that is essential for the maintenance of vital functions of a sovereign state including but not limited to financial institutions and associated financial market infrastructure, health services or utility services.

6. **Impacted state** means a sovereign state where a **cyber operation** has had a major detrimental impact on:

    6.1. the functioning of that sovereign state due to disruption to the availability, integrity or delivery of an **essential service** in that sovereign state**;** and/or

    6.2. the security or defense of that sovereign state.

7. **War** means the use of physical force by a sovereign state against another sovereign state**,** or as part of a civil war, rebellion, revolution, insurrection, or military or usurped power, whether war be declared or not.