FAQ: Cyber Risk War Exclusions

Cybersecurity is an ongoing challenge, but organizations are not alone when it comes to safeguarding their organization's network/computer system and digital assets. HUB International's team of cybersecurity and technology experts address some common questions below:

What is a war exclusion?

A war exclusion is a typical provision clause in All-Risks policies that excludes coverage for losses caused by war or hostile warlike acts. The clause is broad (see examples detailed below) and attribution is a key component. Insurers must provide factual attribution that a cyberattack was deployed as a weapon by a government and/or entity working for or linked to the government.

As a result of the ongoing conflict, exclusionary language and potential coverage limitations in cyber insurance policies are a primary focus. There are questions as to what implications there could be and if coverage could be denied based on the war exclusion if a cyberattack purported to be related to the ongoing conflict resulted in a loss.

Coverage limitations are material because, in the case of Russia, it has been launching DDoS and wiperware attacks against Ukraine prior to its invasion — and continues to do so well after it. If the malware makes it to North American shores, as NotPetya did, losses could be denied based on the war exclusion clause.

If my organization has a cyber policy in place, will it be covered in the event of a cyberattack?

Sanctions — or the penalties imposed by one country on another for aggressive activity or breaking international law — are among the most detrimental actions nations can take, short of going to war.

A sanction exclusion covers any sanction imposed by the United Nations, as well as those levied by the United States, United Kingdom and the European Union.

To date, more than 5,500 sanctions have been imposed on Russia, including businesses and individuals, such as the wealthy oligarchs who are close to the Kremlin.

In certain circumstances, the sanction exclusion can prohibit the payment of extortion or ransomware demands.

For the past two years, insurers began refusing to pay (or reimburse insureds for payment of) extortion demands to cybercriminals/ransomware gangs who are on the OFAC list – which continues to grow – or because of the February 2022 OFAC directive. For example, while Conti (a Russia-friendly ransomware gang) is not on the OFAC "no pay" list, payment to Conti is barred because of the OFAC directive.

Threat actors are constantly evolving, changing their attack methods and names to evade the law.

As of now, DDoS and wiperware have been the primary attack methods. However, this exclusion could arise if there were a ransomware-related event that occurred, and it was determined to be initiated by sanctioned groups and/or individuals. (Therefore, ransom payment would be barred to these groups and/or individuals.)

What types of attacks are possible?

Russia is deploying military-grade cyber weapons of war and using network-destroying wiperware. Although the attacks so far have been targeted, some of these weapons are worms that are designed to propagate within and outside of target networks, including:

- WhisperGate
- HermeticWiper
- IsaacWiper
- Ransomware gangs siding with Russia
    - Conti
    - Lockbit

Again, this scenario is not new.

In 2016, Russia attacked Ukraine with DDoS and wiperware. One weapon, NotPetya, was aimed at terrorizing Ukrainians. Implanted on a tax software site used by 85% of the country's citizens, the malware wiped users' computer systems and propagated to others. NotPetya then spread to the rest of the world, creating a cyber pandemic that led to massive business-interruption issues, as well as property losses in the U.S.

NotPetya and North Korea's WannaCry malware were built on a lost National Security Agency (NSA) cyber weapon called Eternal Blue. These wiperwares are extremely difficult to clear by design. Some firms spent over a year fighting it, while many others had to permanently dispose infected computers, peripherals and network equipment. Subsequently, some firms faced D&O lawsuits over disclosures and insider trading issues.

What is the difference between terrorism and an act of war as it relates to a cyber policy exclusion?

While the policy language used in war exclusions varies by carrier, the intent is to exclude loss resulting from acts of war. Similarly, there is no uniformity of language for negotiated cyber terrorism carve-backs; however, the intent is to give coverage back for loss related to cyber terrorism. As such, the definition between terrorism and an act of war will be different depending on the policy.

Cyber terrorism is often defined as attacks or intimidation against a computer system or network motivated by politics, religion or ideology.

In many cases, NotPetya was deemed a triggering event because of the cyber terrorism carve-back language, and therefore payable under certain cyber insurance policies. For other types of policies, litigation was necessary to make the determination. Some insureds sought to recover business-interruption losses under K&R policies, which are designed for paying ransoms, not interruption. Another insurer sought to invoke a war exclusion, because it had offered cyber interruption on its property form.

Conversely, most cyber policies exclude war, whether declared or not.

Ukraine has declared Russia's invasion and ongoing attacks a war, as has NATO and the United States. Most cyber policies also exclude warlike actions, such as the release of a cyber weapon because of war would likely qualify.

Remember, the war exclusion is extremely broad, barring coverage for direct and indirect causes of loss or liability. It also has an all-encompassing definition of conflict.

The following war exclusion samples may help illustrate this:

SAMPLE WAR EXCLUSIONS	
Beazley	***War and civil war:*** For resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority.
AIG	***Arising out of, based upon or attributable to any:*** ... war, invasion, military action (whether war is declared or not), civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events.
AXA XL	Strikes or similar labor action, war, whether declared or not, invasion, act of foreign enemy, civil war, mutiny, coup d'état, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions.

SAMPLE WAR EXCLUSIONS	
London	Strikes or similar labor actions, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions. The language in war exclusions as well as cyber terrorism carve backs are subject to change going forward. At this time, HUB has not seen any affirmative stances on changing the war exclusion language or cyber terrorism carve-back language, however there is heightened scrutiny surrounding this language as it relates to future policy terms and conditions.

SHIELDS UP: Resilience through review resources and response

Cybersecurity and Infrastructure Security Agency (CISA) has released guidance for all organizations under its Shields Up campaign. It includes recommendations for corporate leaders and CEOs, ransomware response recommendations and additional resources on cyber preparedness.

Business leaders should work with their IT teams to ensure they are taking the necessary steps to enhance their cybersecurity posture and prepare to respond to the current threat landscape as it continues to evolve. Now may also be the right time to leverage any pre-breach resources or services available from one's insurance carrier.

HUB's cyber and technology specialists can help in a variety of ways, including:

- Business-continuity plans
- Cyber incident response planning
- Vendor recommendations for information security audits
- Thorough review of existing policies
- Dedicated tech and cyber breach response and claims advocates

HUB has the tools, expertise, and experience to help clients prepare for the unexpected and manage through a crisis, should it arise.

Contact your HUB Cyber Risk expert for more information about instituting best practices across your business, and insuring your cyber risk.

hubinternational.com

HUB