PUBLISHED FEBRUARY 2022

War, Cyberterrorism, and Cyber Insurance

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

War, Cyberterrorism, and Cyber Insurance

Published February 2022

As cyber insurance coverage continues to evolve and grow in application, an increasing concern among policyholders is whether policies will cover them when cyber incidents impacting them are tied to cyber and technology disruptions stemming from attacks that may be supported by nation-states. In particular, malicious actors might be tied to a given political or ideological affiliation and are sometimes—either directly or indirectly—associated with nation-states and state-backed military units. While cyber insurance has paid claims from attacks attributed to nation-states, policy clauses and endorsements (i.e., riders) within cyber insurance such as the War Exclusion and Cyberterrorism endorsements create uncertainty over whether the policy will respond to certain attacks in the future.

The purpose of this section is to provide a general overview of the War Exclusion and Cyberterrorism endorsements within cyber insurance policies along with the nuances associated with attributing attacks to nation-states and malicious actors.

What Is the War Exclusion Within Cyber Insurance?

Most, if not all, cyber insurance policies include an explicit exclusion to losses arising out of or attributable to war and military actions, which are also present in most other types of property and casualty insurance policies. Various cyber insurance policies were reviewed and analyzed for this issue brief. The examples shown below from American International Group, Inc. (AIG) and AXIS Insurance were selected as illustrative from the policies reviewed. The policy forms referenced herein were obtained via the National Association of Insurance Commissioners' (NAIC) System for Electronic Rates & Forms Filing (SERFF) Access. Please note that the American Academy of Actuaries does not endorse these two insurance companies over other insurance companies but is using them as a representation of the inherent language utilized within cyber insurance policies.

The following is an example War Exclusion from an AIG cyber insurance policy, specifically its Specialty Risk Protector® CyberEdge℠ Security Failure/Privacy Event Management Insurance policy 101018 (12/13). For simplicity, the focus here is on the agreements within this specific coverage section, but there are other coverage sections with regard to Network Interruption and Cyber Extortion among others. The general exclusions are similar across the different coverage sections. Please note that this is a specific form and different insurance company cyber insurance policy forms vary from one another.

3. *Exclusions*

   The insurer shall not be liable to make any payment for Loss:

   (e) 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

As written, this War Exclusion is quite broad, and cyber-attacks stemming from military units within a nation-state have the potential to fall under this exclusion within the cyber insurance policy. In the following section, endorsements to the cyber policy that provide changes to the War Exclusion will be discussed as well as an introduction to additional terminology to better clarify the intent of the cyber policy. The policy endorsements provide some clarity, but ambiguity may still exist and may create uncertainty for policy issuers, policyholders, and regulators.

While the United States has been involved in recent military engagements and armed conflicts such as the "First Libyan Civil War,"[1] the Iraq War,[2] and the "War on Terror,"[3] it is important to note that there have only been five formally declared wars by Congress, the most recent being World War II.[4] Further, there has yet to be a certified act of terrorism for reimbursement under the Terrorism Risk Insurance Act (TRIA). The current TRIA law implements the Terrorism Risk Insurance Program, effective December 20, 2019, which reauthorized TRIA, originally passed in the aftermath of the terrorism attacks of Sept. 11, 2001.[5] While certain acts may be called "terrorism," only those that are deemed a "certified act of terrorism" by the secretary of the Treasury as defined by the law are eligible for coverage under TRIA.[6] Regarding war and TRIA, acts are not to be certified by the secretary if the acts are committed as part of the course of a war declared by the Congress.[7]

1 "Resolution 1973 (2011)"; UN Security Council; March 17, 2011.
2 "Authorization for Use of Military Force Against Iraq Resolution of 2002"; 107th Congress; Oct. 16, 2002.
3 "Authorization for Use of Military Force"; 107th Congress; Sept. 18, 2001.
4 "About Declarations of War by Congress"; U.S. Senate website.
5 "Terrorism Risk Insurance Program"; U.S. Department of the Treasury website.
6 "Certified Act of Terrorism"; IRMI Glossary; 2022.
7 *Title I of the Terrorism Risk Insurance Act of 2002—Terrorism Risk Insurance Program*; U.S. Department of the Treasury; 2005.

The Treasury Department provided guidance in 2016 that TRIA applies to stand-alone cyber insurance policies.[8] However, many organizations utilize their Technology Errors & Omissions and Professional Liability insurance policies to protect themselves from cyber incidents. That same guidance from the Treasury Department explicitly states that "Professional Errors and Omissions Liability Insurance" is excluded from the TRIA program. Hence, many organizations and their corresponding insurers are precluded from protection under the TRIA program to the extent that their insurance protection from cyber incidents is derived from a Professional Errors and Omissions Liability insurance policy. The American Academy of Actuaries Cyber Risk Task Force provided commentary to the U.S. Government Accountability Office[9] in June 2020 and the Department of the Treasury[10] in January 2021 in response to request for comments.

Endorsements to the War Exclusion and Defining Cyberterrorism

Given the War Exclusion above, how do policies respond to various cyber incidents when those incidents are tied to nation-states? The circumstances lie within an endorsement to the War Exclusion as well as an endorsement that introduces a new term—Cyberterrorism. In general, the War Exclusion and Cyberterrorism endorsement works as follows:

1. The definition of the War Exclusion is amended such that it does not apply to acts of Cyberterrorism.
2. The coverage sections are amended such that acts of Cyberterrorism are included within the coverage.
3. The term Cyberterrorism is defined accordingly.

Below are two examples regarding how policies are amended to provide coverage for Cyberterrorism.

Going back to the AIG cyber insurance illustration from its Specialty Risk Protector® CyberEdge℠ Security Failure/Privacy Event Management Insurance policy 132711 (05/19), two endorsements to the cyber policy are as follows:

8 "Guidance Concerning Stand-Alone Cyber Liability Insurance Policies Under the Terrorism Risk Insurance Program"; Federal Register; Dec. 27, 2016.
9 "Re: Cyberattack and the Terrorism Risk Insurance Program"; American Academy of Actuaries; June 1, 2020.
10 "Re: 2019 TRIA Reauthorization Proposed Rules Comments"; American Academy of Actuaries; Jan. 7, 2021.

AIG Endorsement Example #1

1. *The insurer shall not be liable to make any payment for Loss:*
   (2) war (whether war is declared or not), invasion, use of military force, civil war, popular or military uprising, rebellion, revolution, or any action taken to hinder or defend against any of these events

AIG Endorsement Example #2

2. *"Security Failure" also includes any failure or violation resulting from* ***Cyberterrorism****.*

AIG Endorsement #1 reads very similar to the original exclusion. While the War Exclusion remains, there is now have coverage from Cyberterrorism, but what does that term mean? A third endorsement to the cyber policy defines Cyberterrorism as follows:

AIG Endorsement Example #3

For the purposes of this endorsement, ***"Cyberterrorism"*** *means the premeditated use of disruptive activities against any computer system or network by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives. "****Cyberterrorism****" does not include any such activities which are part of or in support of any war or use of military force.*

In another example from AXIS, policy form AXIS PRO® TECHNET SOLUTIONS TM TECHNOLOGY PROFESSIONAL SERVICES LIABILITY AXIS 1010001 0117, the War Exclusion is stated as follows:

EXCLUSIONS

*This policy does not provide coverage for **Claims**, or coverage for any amounts:*

War

based upon or arising out of war, invasion, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power, or the confiscation, nationalization or destruction of, or damage to, property under the order of government or other public authority.

The following endorsements are then added to the AXIS policy via 1011688 0518 to provide coverage for acts of Cyber Terrorism as defined by AXIS.

AXIS Endorsement Example #1

Cyber Terrorism Coverage Endorsement Definition

It is agreed that:

1. The following new definition is added to the policy:
   ***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 entity committed for political, religious or ideological purposes and directed towards the destruction, disruption or subversion of communication and information systems, infrastructure, computers, the internet, telecommunications or electronic networks or the contents thereof or sabotage or threat there from. This shall include, but is not limited to, the intention to influence any government and/or to put the public in fear for such purposes.*

Axis Endorsement Example #2

2. The War exclusion, if any, is amended to add the following at the end thereof:
   *Notwithstanding the foregoing, this exclusion does not apply to acts of **Cyber Terrorism**.*

In both of these examples, coverage under the policy is provided for acts associated with cyberterrorism. However, acts associated with war or military force are not covered under the policy. The confusion and significant gray area associated with these endorsements and carve-back provisions come into play when analyzing attribution along with the intent and individuals behind the attack.

The last sentence of the AIG definition of Cyberterrorism says that it does not include *any such activities which are part of or in support of any war or use of military force.* Questions arise as to how the coverage would respond if a foreign government's military force was directly tied to an attack. Would an insurance carrier deny the claim, stating that the attack fell outside the scope of the Cyberterrorism clause? In other lines of business, for example property insurance, War Exclusions have been invoked with denial of coverage related to cyber incidents as experienced with the *Mondelez International, Inc. v, Zurich American Insurance Company 2018 WL 4941760 (Ill.Cir.Ct.)*, No. 2018L011008, property insurance case related to the NotPetya cyberattack. In contrast, there has yet to be a publicly known denial of a cyber incident corresponding to the War Exclusion under a cyber insurance policy. This is an important distinction as it means that cyber insurance policies might be continuing to pay claims even as private organizations are targeted by nation-state actors.

Next, some key examples of known cyberattacks and issues underlying attribution to different parties will be addressed.

Nation-state Attacks, Criminal Groups, and Attribution

When analyzing the endorsements and clauses above, the attribution (who was behind the attack) and the reasoning for the cyber-attack comes into play because a War Exclusion would require the identification of the party(s) who caused the incident. Under the War Exclusion, war does not have to be declared, and the Cyberterrorism definitions do not explicitly incorporate military action. To the extent that an attack is related to a nation-state's military unit—such as has been charged against the Russian military in the NotPetya attack[11] or the Russian General Staff Main Intelligence Directorate's (GRU) Main Center for Special Technologies (GTsST, also known as Unit 74455 and Sandworm) with the cyber-attacks against the Republic of Georgia[12]—there may be reasoning for the cyber insurance policy to deny coverage due to lack of coverage under the definition of cyberterrorism or the War Exclusion.

11 "Statement from the Press Secretary"; WhiteHouse.gov; Feb. 15, 2018.
12 "United States Condemnation of Russian Cyber-Attack on Georgia"; U.S. Mission to the OSCE; Feb. 27, 2020.

Further, when analyzing the groups behind an attack, nations and private threat intelligence teams may not always delineate between hacking groups and specific nation-states. While it is generally believed that the DarkSide and REvil hacking groups operate out of Russia, there has been no specific or direct connection between these hacking groups and the Russian government.[13,14] To the extent that a nation-state provides directives to these hacking groups to carry out certain attacks, there is a further gray area over whether the attribution of the attack is tied to the nation-state or the specific hacking group that may be simply carrying out orders from government leaders. As such, attribution of attacks is very difficult to achieve and is often not completed in a timely manner because it may take months or years to fully understand the scope of the attack.

Underwriters and actuaries are carefully analyzing the risks and footprints associated with the organizations that are being underwritten. The NotPetya incident in June 2017 is a prime example as many of the Western country-based entities impacted by the NotPetya attack were indirect targets of the attack. As the Russian military attacked organizations based in Ukraine, many Western-based organizations such as Merck, FedEx, Maersk, and Mondelez among others were impacted by the attack due to their operations in Ukraine.[15] Given that companies may be collateral damage to conflicts between nations, insurers need to determine whether the intent of the cyber insurance policy is to cover cyber incidents related to these conflicts as well as adjust pricing on cyber premiums to account for an organization's global footprint.

Table 1 shows a sampling of notable cyber incidents in which there has been public attribution surrounding the attacks. For the purpose of this issue brief, most of the examples in the sampling are related to incidents attributable to nation-states and their corresponding military units.

13 "DarkSide Ransomware Gang: An Overview"; Palo Alto Networks; May 12, 2021.
14 "Press Briefing by Press Secretary Jen Psaki, July 6, 2021"; WhiteHouse.gov; July 6, 2021.
15 "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs"; Wall Street Journal; June 27, 2018.

Table 2: Sampling of Cyber Incidents With Public Attribution

Incident	Approximate Attack Date / Disclosure	Approximate Attribution Date	Alleged Attacker	Attributed By
Sands Casino[16, 17]	02/11/2014	09/10/2015	Iran	United States
Sony Pictures Entertainment[18]	11/24/2014	12/19/2014	North Korea	United States
Office of Personnel Management Breach[19, 20]	06/05/2015	09/21/2018	China	United States
Wannacry[21]	05/12/2017	12/19/2017	North Korea	United States, United Kingdom, Australia, Canada, New Zealand, and Japan
Equifax Breach[22]	05/13/2017	02/10/2020	Chinese PLA	United States
NotPetya[23,24]	06/27/2017	02/14/2018	Russian military	United States,
United Kingdom, etc.				
Russian Cyber-Attack on Georgia[25,26]	10/28/2019	02/27/2020	Russian GRU	United States,
United Kingdom, etc.				
Solar Winds' Orion[27,28]	12/14/2020	01/05/2021	Russia SVR	United States
Microsoft Exchange Server Attack[29,30]	03/02/2021	07/19/2021	Chinese MSS	United States, United Kingdom, EU, NATO
Colonial Pipeline Attack[31,32]	05/07/2021	05/10/2021	DarkSide	United States
JBS Attack[33,34]	05/31/2021	06/02/2021	REvil (aka Sodinokibi)	United States
Kaseya Attack[35]	07/02/2021	07/04/2021	REvil	Self-acknowledged by REvil

16 "Worldwide Cyber Threats"; House Permanent Select Committee on Intelligence—Statement for the Record; Sept. 10, 2015.
17 "Las Vegas Sands—2014 10-K"; SEC.gov.
18 "Update on Sony Investigation"; Federal Bureau of Investigation; Dec. 19, 2014.
19 "Bolton Confirms China was Behind OPM Data Breaches"; *FedSmith*; Sept. 21, 2018.
20 "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say"; Wall Street Journal; June 5, 2015.
21 "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea"; WhiteHouse.gov; Dec. 19, 2017.
22 "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax"; U.S. Department of Justice; Feb. 10, 2020.
23 "Statement from the Press Secretary"; WhiteHouse.gov; Feb. 15, 2018.
24 "Foreign Office Minister condemns Russia for NotPetya attacks"; Gov.uk; Feb. 15, 2018.
25 "United States Condemnation of Russian Cyber-Attack on Georgia"; Op. cit.
26 "UK condemns Russia's GRU over Georgia cyber-attacks"; Gov.uk; Feb. 20, 2020.
27 "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)"; Cybersecurity and Infrastructure Security Agency; Jan. 5, 2021.
28 "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government"; WhiteHouse.gov; April 15, 2021.
29 "HAFNIUM targeting Exchange Servers with 0-day exploits"; Microsoft; Marc 2, 2021.
30 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China"; WhiteHouse.gov; July 19, 2021.
31 "FBI Statement on Compromise of Colonial Pipeline Networks"; Federal Bureau of Investigation; May 10, 2021.
32 "FBI Statement on Network Disruption at Colonial Pipeline"; Federal Bureau of Investigation; May 9, 2021.
33 "JBS USA Cyberattack Media Statement—May 31"; JBS Foods; May 31, 2021.
34 "FBI Statement on JBS Cyberattack"; Federal Bureau of Investigation; June 2, 2021.
35 "REvil gang asks for $70 million to decrypt systems locked in Kaseya attack"; *The Record*; July 4, 2021.

While the time to achieve public attribution associated with significant cyberattacks from governments has been decreasing—as seen with the Solar Winds' Orion, Colonial Pipeline, and JBS cyberattacks—Wannacry and NotPetya each took months of investigation before public attribution from the United States and United Kingdom. In that timeframe, cyber claims may have been paid out, but the insurer may have wanted to or still want to invoke exclusions or deny the claim as a result of the findings from the public attribution. Additionally, the choice to invoke such exclusions creates uncertainty in the courts when it comes to whose evidence and definitions will be the primary evidence around the attribution. The incidents in Table 2 are examples with press releases and quotes from government officials, but there is very little information provided as to how those conclusions were arrived at.

Actuaries and the War Exclusion / Cyberterrorism

These coverage clauses and endorsements will be increasingly important for all stakeholders and for actuaries practicing in the cyber insurance space as the impact of potential systemic, war-related, and military-related cyber incidents will influence both the pricing and reserving of losses falling under cyber policies. When these unique events cross the line from cyberterrorism to acts of war and invoke exclusions under the policies, they will likely be litigated in the courts, as is the case in the *Mondelez International, Inc. v. Zurich American Insurance Company* property insurance suit. The uncertainty around payouts associated with these litigated coverage cases will add complexity to the overall reserving process. Further, actuaries would do well to have a clear understanding of the types of cyber event scenarios to exclude from their pricing analyses if the cyber incidents are outside of the purview of the written cyber policy based on the policy wording.

Over time, greater clarity from the cyber insurance industry around the ambiguities noted above is essential. In the interim, it is important that actuaries working in the cyber insurance space be aware of the nuances and uncertainties created by these coverage conditions and the nature of cyber incidents.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**