RT ProExec

Attribution:
Who Decides if it's an Act of War?

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

INTRODUCTION

A war exclusion only matters if someone decides the attack was an act of war. That decision — the attribution of a cyberattack to a sovereign state — has historically been the single most contentious element in any cyber war exclusion dispute. It was the central issue in the $1.4 billion Merck/NotPetya litigation. It is now the central issue in the current wave of Iran-linked cyberattacks.

The March 2026 attack on a Fortune 500 medical device manufacturer illustrates the problem. The threat actor publicly claimed responsibility. Multiple cybersecurity research firms linked the group to Iran's Ministry of Intelligence and Security (MOIS). The U.S. Department of Justice seized the group's domains and confirmed in court filings that the attack was conducted by MOIS. Yet as of this writing, the targeted company itself has not publicly attributed the attack to a specific state actor, and Cybersecurity and Infrastructure Security Agency (CISA) has not issued a formal attribution statement.

If a claim is filed under a cyber policy with a war exclusion, the outcome may depend on a question that most policies do not clearly answer: who has the authority to determine whether the attack was state-sponsored? This article is a companion to RT ProExec's recent publication, "Iran, Cyber War, and Your Policy," which analyzed war exclusion frameworks broadly. This piece examines the attribution mechanism specifically — how different carriers define it, why it matters, and what the current precedent tells us.

1. The Precedent: NotPetya and Merck

In June 2017, the NotPetya malware spread across the world, ultimately causing an estimated $10 billion in global damage. The attack originated in Ukraine but affected thousands of companies internationally, including pharmaceutical giant Merck, which saw over 40,000 of its computers destroyed.

Merck filed a claim under its $1.75 billion "all risks" property insurance policy. Its insurers denied the claim, arguing that the NotPetya attack was an act of war attributable to Russia and therefore excluded under the policy's "hostile / warlike action" exclusion. The U.S. and U.K. governments had formally attributed NotPetya to Russia's military intelligence agency, the GRU, and the U.S. Department of Justice indicted six Russian military officers in connection with the attack in 2020.

Despite this attribution, the New Jersey trial court ruled in Merck's favor in January 2022, finding that the traditional war exclusion language in the policy was not intended to apply to cyberattacks. The New Jersey appellate court upheld that ruling, concluding that the insurers had not demonstrated the attack constituted "hostile" or "warlike" action as those terms had been understood in the insurance industry. The case settled for a confidential amount in January 2024, just days before the New Jersey Supreme Court was scheduled to hear oral arguments.

The Merck case established a critical precedent: even when a government formally attributes a cyberattack to a nation-state's military or intelligence apparatus, traditional war exclusion language may not be sufficient to deny the claim. This precedent is precisely what drove the cyber insurance market to develop modern war exclusion frameworks with explicit cyber definitions, Impacted State concepts, and in some cases detailed attribution mechanisms.

Why Merck Still Matters

The Merck litigation was decided under traditional property policy war exclusion language — not under a modern standalone cyber war exclusion. The modern frameworks used by leading cyber carriers today were developed in direct response to the Merck outcome. These newer frameworks attempt to define with greater specificity what constitutes state-sponsored cyber activity and how attribution is determined. But the fundamental question remains: who decides?

2. How Carriers Handle Attribution

The modern cyber war exclusion frameworks adopted since 2022 take varying approaches to the attribution question. The differences are material, and they may determine how a claim is resolved when the facts on the ground are ambiguous.

Detailed Attribution Frameworks

Some carriers include explicit attribution mechanisms in their war exclusion endorsements. These frameworks typically refer to determinations by specific categories of governmental authorities such as the intelligence agencies of G7 nations, the FBI, the Department of Homeland Security, or equivalent bodies in other countries. Under these frameworks, the war exclusion is triggered only when a recognized authority has formally attributed the attack to a state actor. This approach provides the most predictability for policyholders, because the triggering standard is defined in advance. A policyholder can evaluate at the time of policy placement what level of government action would be required to invoke the exclusion.

Carrier Discretion

Other carriers reserve the right to make their own attribution determination, either explicitly through policy language that allows the insurer to assess whether the attack was state-directed, or implicitly through vague language that does not specify who makes the determination. Under this approach, the insurer may rely on a combination of government statements, cybersecurity research, media reporting, and its own internal assessment to decide whether the war exclusion applies. This creates less predictability for the policyholder, because the attribution standard is not defined until a claim is filed.

Silent on Attribution

Several carriers include modern war exclusion frameworks that define "Cyber Operation" or "Hostile Cyber Activity" as acts "by, at the direction, or under the control of a sovereign state" but are entirely silent on who determines whether that standard has been met. The policy defines what must be true, but not how or by whom that determination is made. In a claim scenario, this silence leaves the attribution question to the claims adjustment process or, ultimately, to litigation.

Approach	How It Works	Advantage	Risk
Detailed Government Framework	War exclusion triggered only when a specified governmental authority (G7 intelligence, FBI, DHS, etc.) formally attributes the attack to a state actor.	Provides the most predictability. Policyholder can evaluate the standard at time of placement.	Attribution may be delayed, politically influenced, or never issued. CISA staffing challenges in 2026 have delayed government response.
Carrier Discretion	Insurer retains the right to assess attribution based on available evidence, including government statements, cybersecurity research, and its own analysis.	Allows the carrier to act on available evidence without waiting for formal government attribution.	May create disputes if the policyholder disagrees with the carrier's assessment. The standard is not transparent to the policyholder at time of placement.
Silent	Policy defines state-sponsored activity as excluded but does not specify who determines whether the standard is met.	No inherent advantage. Ambiguity may favor either party depending on the circumstances.	Most likely to result in litigation. Neither party has a defined framework to point to.

3. The Current Test Case: Iran and the March 2026 Attacks

The March 2026 Iran-linked cyberattacks present the first major real-world test of these modern attribution frameworks. Consider the current state of evidence:

The threat actor (Handala) publicly claimed responsibility for the attack and stated it was retaliation for U.S. military strikes on Iran. Multiple cybersecurity research firms, including Palo Alto Networks' Unit 42, have linked Handala to Void Manticore, a state-sponsored actor operating under MOIS. The U.S. Department of Justice seized Handala's domains on March 20, 2026, and stated in court filings that the attack was conducted by MOIS. The Federal Bureau of Investigation (FBI) director stated publicly that "Iran thought they could hide behind fake websites and keyboard threats."

Yet formal government attribution through the traditional channels that some policy frameworks reference has not occurred. CISA has launched an investigation but has not issued a formal attribution statement. No G7 joint attribution statement has been released. The targeted company itself has not publicly attributed the attack to a state actor.

This creates a split depending on which carrier's war exclusion the policyholder is on. A policy with a detailed government attribution framework may not trigger the war exclusion, because no formal government attribution meeting the policy's specified standard has been issued. A carrier using discretionary assessment may conclude that the Department of Justice (DOJ) court filings, FBI statements, and cybersecurity research collectively establish state attribution. A carrier with silent language faces the same ambiguity that characterized the early stages of the Merck litigation.

It is also worth noting that CISA, the agency most commonly referenced in attribution frameworks, has been operating at significantly reduced capacity in early 2026 due to federal staffing challenges. The agency's ability to issue formal attribution statements may be affected by these operational constraints, which could delay or prevent the type of government determination that some policy frameworks require.

4. The Attribution Paradox

For policyholders, the attribution question presents a paradox. If the attack is formally attributed to a state actor, the war exclusion may apply potentially denying the claim entirely (unless a geographic carve-back restores coverage). If the attack is not formally attributed, the war exclusion may not apply but the policyholder still suffered the same loss from the same attack. In other words, the policyholder's coverage outcome may depend not on what actually happened, but on whether a government agency issues a public statement about what happened. The same attack, with the same impact, could be covered under one carrier's form and excluded under another's — not because of differences in the coverage grant, but because of differences in how attribution is defined.

This paradox is compounded by the political dimension of attribution. Government attribution decisions are influenced by diplomatic, intelligence, and national security considerations that have nothing to do with insurance. A government may delay or withhold attribution to preserve diplomatic flexibility. A government may issue attribution through one channel (such as DOJ court filings) but not another (such as a formal intelligence community statement). The insurance outcome should not depend on these considerations, but under current frameworks, it often does.

Carriers that use detailed government attribution frameworks may argue this approach provides certainty. But certainty only exists when the government acts. When it does not — or when it acts ambiguously — the policyholder is left in a gray zone that the policy was supposed to resolve.

5. Broker Considerations

The attribution mechanism in a war exclusion is one of the most technically important and least discussed elements of a standalone cyber policy. The following points may warrant review in connection with current and upcoming placements:

1. Identify the Attribution Framework
Determine whether the carrier's war exclusion includes a detailed attribution mechanism, relies on carrier discretion, or is silent. This is a threshold question that determines how much predictability the policyholder has before a claim arises.

2. Evaluate the Government Standard
For policies with government attribution frameworks, identify which authorities qualify. Does the policy reference G7 intelligence agencies specifically? Does it include law enforcement agencies such as the FBI or DOJ? Does it require a formal public statement, or would a court filing or testimony suffice? The March 2026 DOJ seizure and FBI statements may meet some policy standards but not others.

3. Consider the CISA Factor
CISA is the agency most commonly associated with U.S. government cyber attribution. If CISA is operating at reduced capacity or is unable to issue timely attribution statements, policies that require CISA-specific determinations may create delays or ambiguities that have nothing to do with whether the attack was actually state-sponsored.

4. Assess Ambiguity Risk
For policies with silent or vague attribution language, discuss with clients that the attribution question may not be resolved until the claims process or litigation. Ambiguity in attribution language has historically not favored policyholders in large-loss scenarios.

5. Compare Across Carriers
Attribution mechanisms vary significantly across the market. When quoting multiple carriers on the same account, the attribution framework should be evaluated alongside the geographic carve-back, triggering event definitions, and other coverage components. Two policies with identical coverage grants can produce very different outcomes if their attribution mechanisms differ.

CONCLUSION

The Merck litigation taught the insurance market that traditional war exclusion language could lead to unintended coverage outcomes. The market responded by developing modern frameworks with explicit definitions, geographic carve-backs, and in some cases detailed attribution mechanisms. Those frameworks are now being tested for the first time by a live, large-scale, state-linked cyberattack.

The March 2026 Iran-linked attacks have demonstrated that attribution is not a binary question. Evidence can accumulate from multiple sources — the threat actor's own claims, cybersecurity research firms, law enforcement court filings, and executive branch statements — without producing the single, definitive government determination that some policy frameworks require. The question of who decides remains open, and the answer depends on which carrier's form the policyholder is on.

Retail brokers who can evaluate attribution frameworks alongside coverage grants and exclusion structures are providing the level of analytical depth that the current environment demands. The war exclusion framework is the first question. Attribution is the question inside the question. Taking both into account can support a more thorough placement and help mitigate the risk of coverage disputes.

For further analysis of the broader insurance implications of the Iran-linked cyberattacks, see RT ProExec's companion articles: "Iran, Cyber War, and Your Policy," "When the Management Tool Becomes the Weapon," and "Wiper vs. Ransomware: Same Policy, Completely Different Claim."

SOURCES AND CITATIONS

The factual assertions in this article are based on the following publicly available sources and the author's analysis of cyber insurance coverage structures.

"Merck-Settlement of $1.4 Billion Coverage Dispute Over NotPetya Cyberattack Places Renewed Spotlight on War Exclusions in 2024." Pro Policyholder. January 2024. https://www.propolicyholder.com/2024/01/merck-settlement-1-4-billion-coverage-dispute-notpetya-cyberattack-places-renewed-spotlight-war-exclusions-2024/

"How Will the Merck Settlement Affect the Insurance Industry?" IBM Think. 2024. https://www.ibm.com/think/insights/merck-settlement-affect-insurance-industry

"Merck Reaches Settlement in Closely Watched NotPetya Insurance Case." Cybersecurity Dive. January 8, 2024. https://www.cybersecuritydive.com/news/merck-settlement-notpetya-insurance/703922/

"Merck's Win in NotPetya Insurance Dispute: What It Means." Bank Info Security / ISMG. May 2023. https://www.bankinfosecurity.com/merck-ruling-a-21983

"Merck Awarded $1.4 Billion for NotPetya After 5 Years of Legal Battle." Risk & Insurance. May 2022. https://riskandinsurance.com/merck-awarded-1-4-billion-for-notpetya-after-5-years-of-legal-battle/

U.S. Department of Justice. "Justice Department Disrupts Iranian Cyber Enabled Psychological Operations." March 20, 2026. https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations

"DOJ Confirms Seizure of Domains Linked to Iran-Backed Threat Actor." Cybersecurity Dive. March 2026. https://www.cybersecuritydive.com/news/doj-seizure-domains-iran-threat-actor/815306/

"FBI Seizes Handala Leak Sites After Stryker Cyberattack." Cybernews. March 2026. https://cybernews.com/news/fbi-seizes-handala-leak-sites-after-stryker-cyberattack/

"U.S. Accuses Iran's Government of Operating Hacktivist Group That Hacked Stryker." TechCrunch. March 20, 2026. https://techcrunch.com/2026/03/20/u-s-accuses-irans-government-of-operating-hacktivist-group-that-hacked-stryker/

Palo Alto Networks, Unit 42. "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran." March 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

Mula, James. "Iran, Cyber War, and Your Policy: War Exclusions, Coverage Implications, and What Policyholders Need to Know Now." RT ProExec. March 2026. https://blog.ryanspecialty.com/iran-cyber-war-and-your-policy

All sources were accessed between March 11 and April 2, 2026. This article does not reproduce copyrighted material; all factual claims are paraphrased from the cited sources.