Why Insurers Need To Modernize Their War Exclusions

Vincent J. Vitkowsky
Gfeller Laurie LLP

Insurers need to modernize the War Exclusions in their policies. These Exclusions address many kinds of conflicts and actions in addition to war. They apply to attacks by nations and to those acting on a nation's behalf, whether or not war has been declared or exists. However, most War Exclusions are flawed because they fail to address the acute 21st Century risk of cyberattacks.

Two recent developments have added urgency. The first is a recent court decision holding that losses through a cyberattack were not excluded in numerous all-risk property policies. The second was the Russian invasion of Ukraine. But even before these developments, there were many uncertainties concerning how War Exclusions might be applied to cyberattacks. Also, the risk of possible widespread correlated losses, across business sectors or nations, already posed an unacceptable accumulation risk.

The clearest example of this risk is a Russian cyberattack in 2017 known as NotPetya, which was aimed at Ukraine but spread to other nations. It was a strain of "wiperware" encrypting the victims' data, permanently and inalterably, and spreading automatically, rapidly, and indiscriminately throughout the world. It is estimated to have resulted in approximately $10 billion in losses.

One impacted company was Merck &. Co., which alleged damages of $1.4 billion. Its all-risk property policies specifically provided coverage for the destruction or corruption of computer data and software. Its insurers invoked the Hostile/Warlike Action Exclusion in their policies. Merck brought suit, and last January, a court in New Jersey, noting that "no court has applied a war (or hostile acts) exclusion to anything remotely close to the facts herein," held that "the

exclusion only applied to traditional forms of warfare." *Merck & Co., Inc. v. ACE Am. Ins. Co., et al.,* No. UNN-L-2682-18 (N.J. Super. Ct. Law Div. Jan. 13, 2022).

The decision has been widely addressed and criticized in other publications. For present purposes, it is sufficient to note that no prior court had ever even been presented with the question, and that contemporary military doctrine recognizes cyberspace as a domain of warfare and conflict. The decision may not withstand appeal. Even if it does, other courts need not follow it.

Merck is the only decision construing a War Exclusion and a cyberattack under any type of policy. As a result, many questions remain open. For each new claim, it will be necessary to conduct a case-by-case analysis based on the specific facts and policy language.

This presents a problem, because the language of most current War Exclusions is entirely inadequate, addressing virtually none of the important issues in a cyberattack.

For example, the relevant language of the Hostile/Warlike Action Exclusion provides that there is no coverage for "Loss or damage caused by hostile or warlike action in time of peace or war … by any government or sovereign power … or by an agent of such government …."

Variations of another common form have been used in other policies, including standalone cyber insurance policies. These exclude "war, invasion, acts of foreign enemies, nations, hostile or warlike operations (whether war is declared or not) … civil war, rebellion, revolution, insurrection …," and related risks.

Most fundamentally, most current War Exclusions do not indicate whether a cyberattack could even fall within their scope.

Next, they do not indicate how they are triggered. What does "Hostile" or "Warlike" mean? What constitutes a military operation?

Initially, people trying to analyze the trigger focused on whether an attack had a "kinetic" effect, *i.e.,* the kind of effect resulting from bullets and bombs. In the sphere of public international law, this has been the approach of the US government since 2012, when it focused on the concept of the *use of force*. That term comes from Article 2(4) of the United Nations Charter, which does not define it, but does prohibit it against the territorial integrity or political independence of any nation. Art. 51 allows an aggrieved nation to respond, in self-defense, with its own use of force.

There are problems with this focus. First, international law is inherently vague. Parties can and do disagree about how much death and destruction is necessary to constitute the use of force. So it is an unreliable trigger.

Also, nations have tried to impose the traditional framework applied to kinetic war onto cyberattacks. This leads to another problem. In cyber conflict, nations take great pains to avoid doing anything that would clearly reach the threshold of the use of force. Instead, cyberattacks tend to merely disrupt systems and operations -- granted, sometimes significantly. They may not be acts of war, but they are not within the acceptable boundaries

of peacetime behavior, and often warrant a response. Thus, a use of force trigger is again unsatisfactory.

There are other open questions. How does the War Exclusion address a cyberattack that causes non-physical, economic loss only? At what level, if at all, is it triggered?

What about cyberattacks that impair critical infrastructure, or a government's ability to provide essential services? What are essential services?

There are questions beyond the effects of an attack. The operations of nonstate actors take place in a large gray area of potential coverage. For example, what if the attacker is not directed by a nation, but is an independent group voluntarily aligning with a nation in the course of a war or conflict? If it operates in a nation that is a non-belligerent, would losses from a retaliatory strike impacting that nation be excluded?

Then, there is the overriding question of Attribution – who launched the attack, and how is that proved? Most War Exclusions do not address this at all.

Finally, most War Exclusions do not address the key question of collateral damage. What happens when an exploit goes into the wild, intentionally or inadvertently? What victims fall into the War Exclusion? Among other things, this goes to the key concern of accumulation.

Late last year, progress was made when the Lloyd's Market Association released four "War, Cyber War and Cyber Operation Exclusions." They introduced several concepts that address some of the open questions. They define *cyber operations*, and address when they are excluded. One of the Exclusions provides an exception for a *bystanding cyber asset*, which is "a computer system … not physically located in an impacted state but is affected by a cyber operation." An *impacted state* is "any state where a cyber operation has had a major detrimental impact." Some of the Exclusions clarify the scope of *Essential Services*. And all four Exclusions have an identical provision on Attribution, setting forth factors and burdens of proof, and addressing payment obligations pending determination. Although the LMA Exclusions were directed to standalone cyber insurers, they could be adapted for use in other lines of business.

The LMA Exclusions are a worthy start. Other formulations are possible. Whatever the precise language, drafters should strive to reduce uncertainty and provide a fair balance of competing interests. They should give everyone, insureds and insurers, meaningful guidance as to the intended scope and operation of their policy's War Exclusion.

June 10, 2022

Vince Vitkowsky is a partner in Gfeller Laurie LLP.