

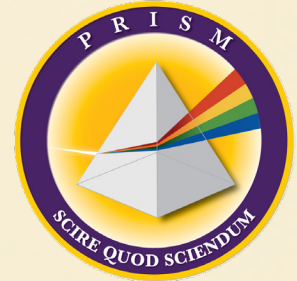
PRISM Perspectives

The Defender's Dilemma: Past Its Expiration Date

By Dr. Tom Johansmeyer

16 October 2026

Tom Johansmeyer, Ph.D., is co-head of Economic and Legal Warfare at the Irregular Warfare Initiative. His research focuses on the nexus of cyber and economic security and the intersection of extreme events and irregular warfare. He has a Ph.D. in international conflict analysis from the University of Kent, Canterbury. Based in Bermuda, where he also works in the reinsurance industry, Tom led the development of new industry-wide insured loss reporting tools for cyber and political violence catastrophe events.



The “[defender's dilemma](#)” is alive and well. The defender's dilemma is the [belief](#) that “attackers can fail repeatedly at no cost, while defense must hold “everywhere, always” is nothing if not controversial. Many have taken issue with this [maxim](#)—and developed [compelling cases](#) against the need for a 100 percent success rate in defense. Nonetheless, the dilemma [continues to be invoked](#). The oversimplification of offense and defense, over-crediting attackers with asymmetric advantage, and all-or-nothing tone pit the futility of defense against the fatalism of victimhood.

It's all a bit much.

The defender's dilemma has not been examined with regard to the economic effects of cyberattacks—to include the depth of harm caused. A review of the economic effects of cybercrime shows that the impacts of attack are manageable, which undermines the notion that a lone success by an attacker can be cataclysmic. Further, examining the attacker side of the equation—to include the cost of attack—reveals that there are constraints on their ability to act.

A decade ago, it was easier to see the defender's dilemma as a possibility. Today, it's much more difficult, making it time to retire the concept.

The Consequences Are Telling

The defender's dilemma's tone simultaneously

begs for vigilance while hinting at an impossible enormity. After all, it does credit attackers with the ability to conduct virtually endless operations at effectively no cost. While defense can be stressful and expensive, the ability of the global economy to absorb cyber activity has been demonstrated. While there are occasional attacks of noteworthy [economic effect](#), cyber catastrophe in the popular sense feared has [not materialized](#) and [isn't likely to](#).

To contextualize the threat, let's start with the annual economic harm attributable to cybercrime. Lofty figures reaching into the [tens of trillions of dollars](#) have been offered, but a more realistic tally is [\\$500 billion](#), developed recently using a rigorous and transparent methodology. This is not a menacing total, particularly in an economic environment where worldwide gross domestic product (GDP) exceeds [\\$118.35 trillion](#). The difference shows that the depth of impact from cybercrime is limited. This is not an impediment to post-attack recovery. Even when the economic effects of single attacks become large, they are not existential. The [2017 Equifax breach](#) wasn't much smaller than the effect of [NotPetya on Merck](#), with each well over \$1 billion. Neither caused long-term harm. The same is true of the 2025 Jaguar Land Rover attack, which had significant societal effects as well, when climbing to an economic effect of [\\$2.5 billion](#). While the effects were severe, the businesses affected did recover.

In fact, the notion that cyberattacks can be existential for businesses has largely been debunked. Although the 37 chronicled [since 2002](#) may miss a few, it's likely directionally correct relative to the "zombie stat" suggesting a 60% post-breach small business closure rate "that [refuses](#) to die."

Of course, there are still areas where the potential for severity remains a concern. Threats to critical infrastructure are often cited, although [no such case](#) has risen to significant economic or societal effect. The 2015 attack on the Ukrainian power grid (which also could be considered a "zombie stat" as well by this point) masks the reality that cyber-induced blackouts won't bring society to its knees.

The effects of cyberattacks are [generally reversible](#), which limits their ability to cause long-term harm. They don't [leave](#) "bomb craters and war ruins" and consequently have not been sufficient to justify a cataclysmic view of the threat. The limited impact calls into question a fundamental premise of the defender's dilemma – namely that attackers only need to be successful once.

Where The Defender's Dilemma Falls

Short

The assumption that attackers only need to be right once has to do some heavy lifting. There are two ways to look at this. One is from the victim's perspective. Yes, the goal is to repel all attacks while the attacker only needs to get through once. That's ostensibly the defensive burden, even though (as discussed above) a failure of defense tends to be manageable, if difficult. This is a myopic view of the problem, though, because it overlooks the broader challenges that attackers face.

As an attacker, it doesn't take long to realize that one success doesn't do much. Even to succeed just once requires either finding an unprepared victim or looking for gaps in prepared defenses. Successful attacks do occur, [but](#) "threat actors have to jump through multiple hoops to meet their objectives." It isn't easy. If doing this once is difficult, replicating that success becomes even more challenging.

Cost is an issue. Not only does this stand in contrast to the maxim itself, but it also relates to the need for threat actors to succeed regularly. The dated notion that cyber attacks are inexpensive [no longer holds](#). Even if you give the maxim some elbow room as hyperbolic but containing a kernel of truth, it bumps into the fact that successful cyber

attacks – particularly with scale and against financially resourced targets – are not free.

In addition to [compensating](#) employees, the larger and more advanced of these organizations have [expenses](#) for equipment, infrastructure, and even physical space. Thus, the notion that attacks are free to execute – or even come with *de minimis* expense – is questionable at best. As actors have grown in sophistication, they have even had to purchase raw materials, such as [zero-day vulnerabilities](#). The bills add up, which makes it harder to keep the lights.

That leads to the next challenge – revenues.

The defender's dilemma emphasizes that bad actors only need to overcome defenses once. If they want to continue to operate, however, they'll need to do it again and again. Conti generated [\\$180 million](#) in revenue across more than 400 attacks. Total [ransomware revenue](#) in 2024 approached \$900 million, which 2025 expected to be higher. That requires continued effort, suggesting further that attackers must succeed regularly to survive. The asymmetric view of a lone success relative to the need for foolproof protection simply doesn't stand up to scrutiny. Security is important and being successfully attacked is trying, but this falls far short of the fears stoked by the defender's dilemma.

Conclusion

The defender's dilemma may make for a handy slogan, feed some [fear-based marketing](#), and drive home the fact that there are threats requiring defense. Overstating the burden of security and implying a profound asymmetric advantage, though, isn't helpful. It's far more important to understand the threat in order to make security strategy more productive. There's a balance between security investment and potential for loss that must be understood, as with any cost-benefit analysis. The fatalism associated with the defender's dilemma, as best described by my [fellow Ripon College alum](#), belongs [in a museum](#).

Instead of over-crediting attackers and over-burdening defenders, let's focus on the facts. Cyberattacks can be costly and disruptive. However, they can be managed through prudent investments, disciplined practices, and ongoing learning. From time to time, attackers will get through, which makes response and recovery plans important, as well. These are problems to be solved – not hyped.