University of Kent

# What Does Cyber Catastrophe Cost?

Tom Johansmeyer
23 January 2026

# Quick Note on Me

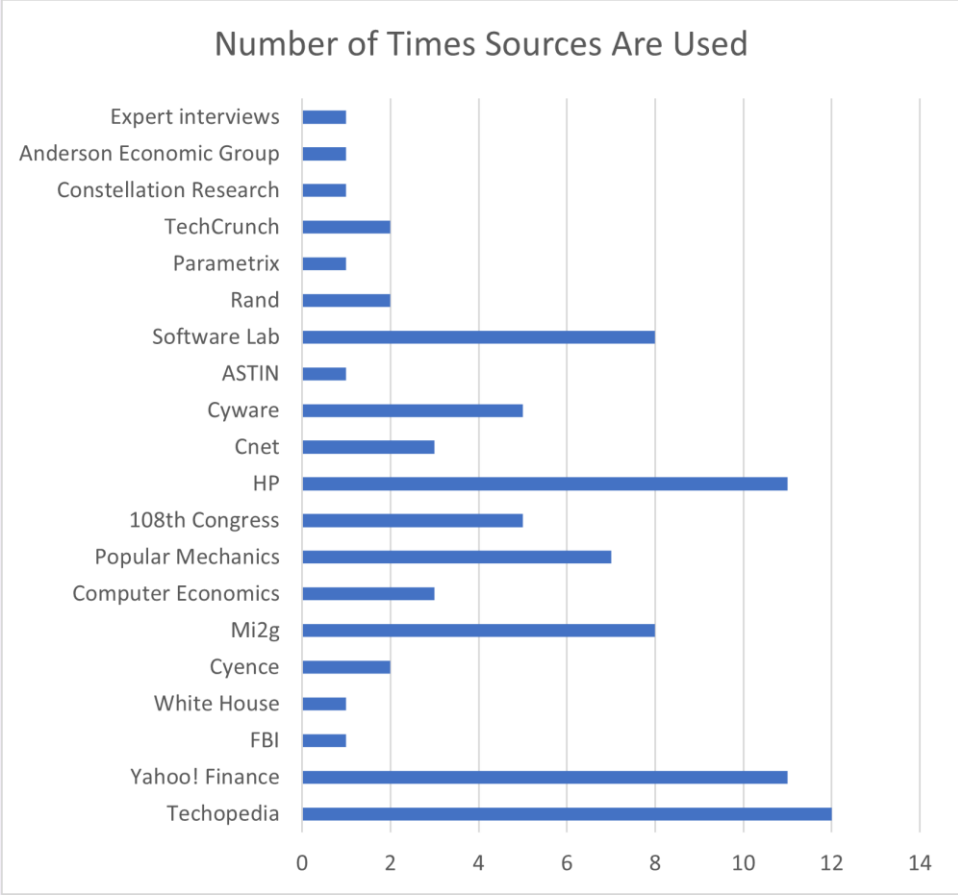
| By Day | By Night |
|---|---|
| Reinsurance broker – global head of alternative risk transfer, based in Bermuda | PhD candidate, University of Kent, Canterbury |
| Most of my work is natural disaster and weather – parametric natural catastrophe re/insurance risk transfer | Researching how the hyperbolization of cyber war risk creates an economic security problem by impeding the flow of capital to the cyber insurance sector |
| I do some cyber re/insurance broking, to include emerging markets (Türkiye) and sensitive risks (war) | Co-lead, economic and legal warfare project, Irregular Warfare Initiative; incoming EIC of the Journal of Strategic Competition |
| MA global diplomacy (SOAS), MBA accounting (Suffolk), BA philosophy and history (Ripon)<br>U.S. Army 1994-9 (Camp Casey/Stanley 1997-8) | |

***But what I really like to do is count stuff …***

# Research Methodology

University of Kent

- Objective: Identify the economic losses from major cyber catastrophe events from 1998 – present
- Resources: Publicly available reported estimates, insured loss estimates
- Methodology: Modeled on natural disaster economic loss databases like EM-DAT/CRED, Swiss Re *sigma*, Munich Re NatCatSERVICE (all of which are used extensively by academia, government, and commercial entities)
- Process:
  - Events with only 1 available estimate: Use it
  - Events with multiple estimates (tight range): Take the average except where there is a highly credible alternative
  - Events with multiple diverging estimates: Qualitative analysis of data sources to facilitate estimate election
  - Use contextual indicators where available/ possible



# The Process Itself

University of Kent

1. Gather list of historical cyber catastrophes
2. Identify all publicly available loss estimates for each
3. Compare the losses available to each other for a particular event, to include analysis of source credibility
4. Determine the best method for working with the data for each event (average the credible, average all, selection of only credible alternative)
5. Review catastrophe event case details to ensure consistence of loss estimate with the facts on the ground

# “Catastrophe” as a Label

University of Kent

- Catastrophe is not calamity; it’s just an easy way to categorize events of a certain type
- The label makes it easier and more accurate to study widespread/systemic events
- Big single losses (e.g., JLR in 2025 and Equifax in 2017) provide insight into narrow economic impact, but they don’t necessarily entail the broad range of secondary and tertiary effects associated with an event that has multiple direct victims
- Defining cyber catastrophe makes possible a conversation that has been difficult in the historical literature

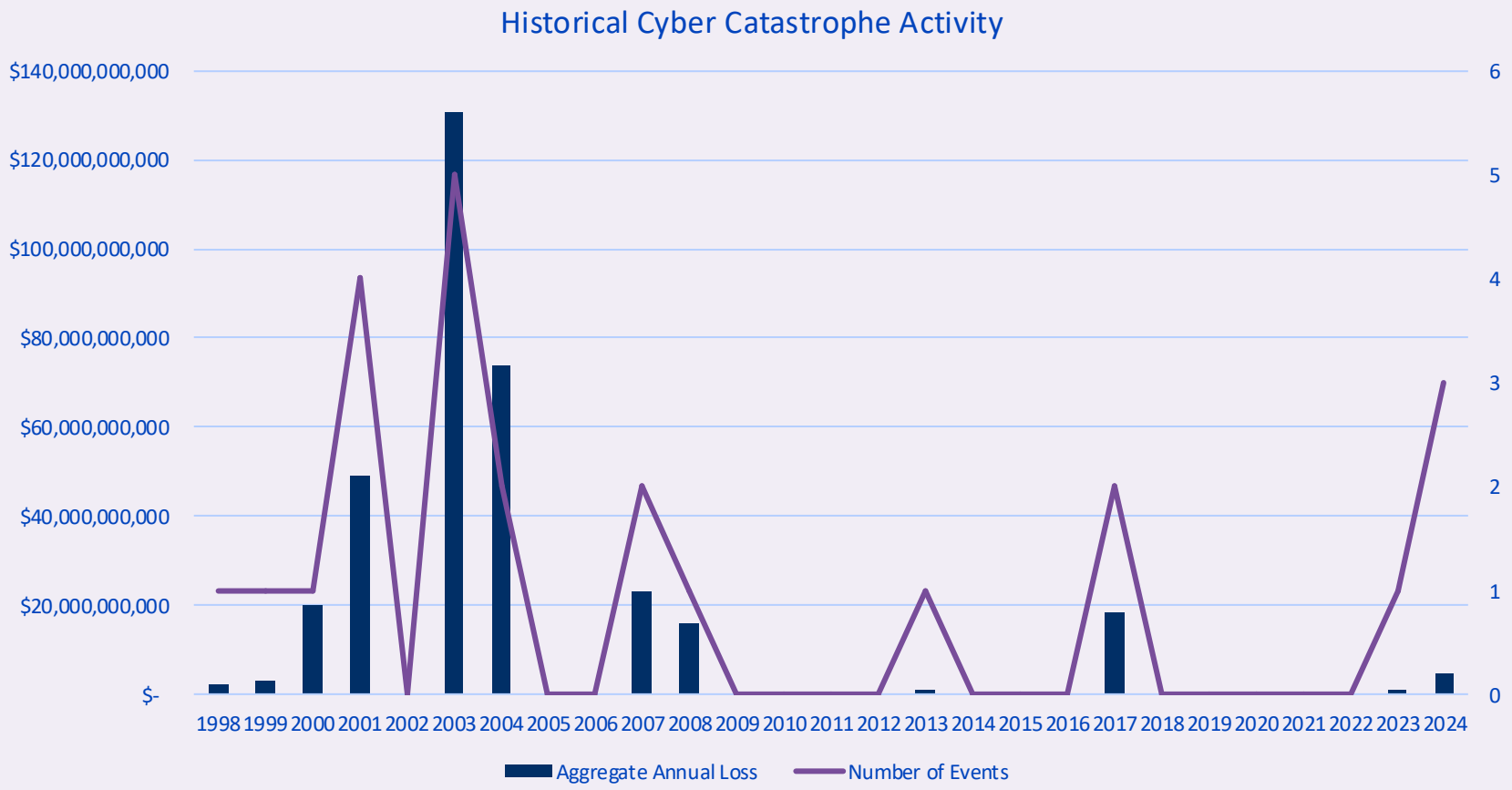
# What's a Catastrophe?

University of Kent

- The term is adapted from the insurance industry, where "catastrophe" refers to widespread events that have a significant impact on the market
- A catastrophe doesn't have to be cataclysmic, apocalyptic, or society-changing … most insurance catastrophes are pretty small
- In the United States alone, ~70 property-catastrophe events occur annually (and most tend not to be big deals)
- To study cyber catastrophes, the operating definition I've pulled together is:

| Element | Reason |
|---|---|
| Economic loss of > US$800 million in today's dollars | • Going < $1 billion yields two additional events since 1998, which adds to a small data set<br>• $800 million is indicative of meaningful impact, even if not broadly felt |
| Significant number of victims | • Draws from the insurance industry's "significant number of insurers and insureds"<br>• Presents large single-victim events from being included |

# Historical Cyber Catastrophe Activity

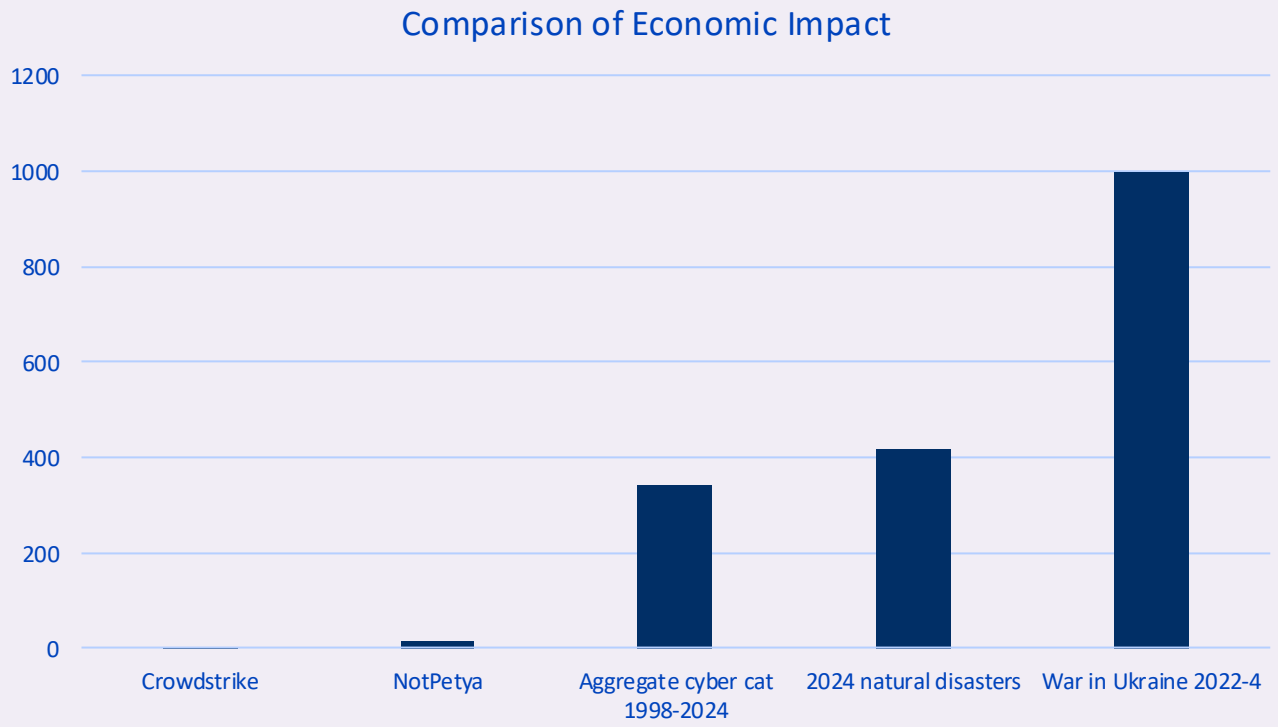



- Estimates for early years are debatable but still make a point
- 15+ years of cyber cat have had limited economic impact
- Smaller cats appear to be more likely going forward
- Cataclysmic events have not featured and are unlikely to

# How Big Is Big?

University of Kent

## Cyber catastrophes can be relatively costly, but their cost requires reference points – contextualization is crucial

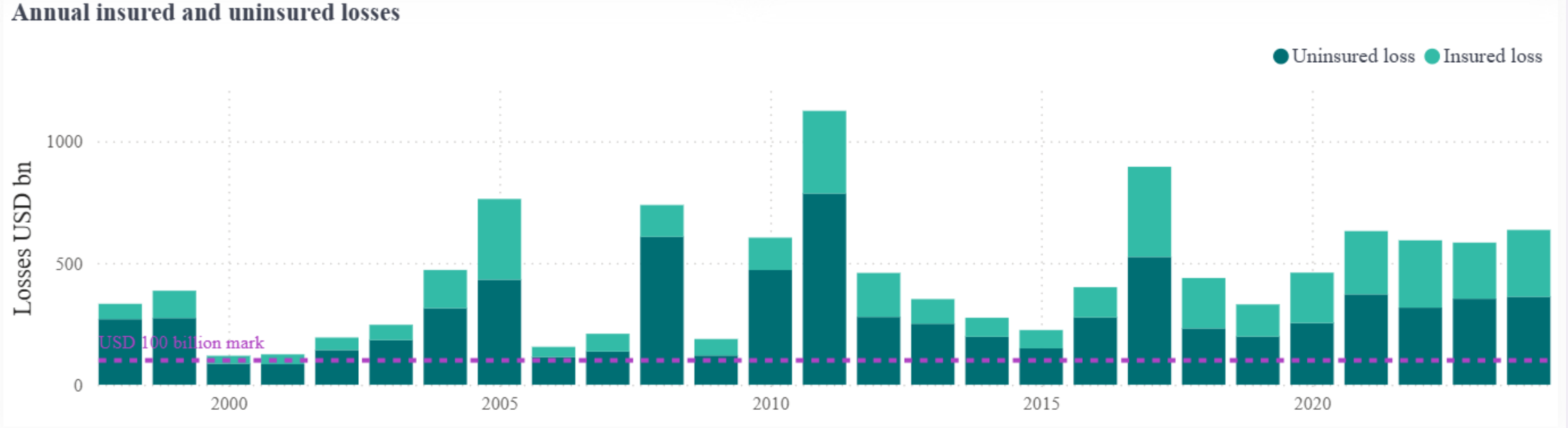



Physical damage events are by far more impactful than cyber events.

The KSE put Year-1 physical damage in Ukraine @ ~$100 billion … cyber cat only reached that level once, > 20 years ago

Annually, natural catastrophe far exceed aggregate cyber cat losses

# Nat Cats: Annually Severe




- Economic losses from nat cat in 2024: $635.8 billion
- Economic losses from cyber cat since 1998: ~$350 billion (adj. inflation)
- Only 2000 and 2001 were similar in scale to the cyber economic losses from 2003 (the most severe year)
- Annual nat cat economic losses are often greater than the aggregate of all cyber cat economic losses since 1998

# Areas for Future Research

- Why do cyber cat economic losses remain relatively low? *This could draw on the work of Smeets, as well as Rid, Gartzke, and others.*
- Why have cyber cat economic losses fallen precipitously since 2008 – and can this persist? *This would benefit from serious and rigorous research. It's easy to make guesses, but some heavy lifting would benefit the scholarship as a whole.*
- How does the historical scale of cyber cat economic impacts affect the decision to use (or increase the use of) offensive cyber operations? *Frankly, are there de-escalatory scenarios where offensive ops would make more sense? See Healey and Jervis provide a foundation for further work.*
- Does national security require a change in perception on the economic effects of cyber cats? *Or, has this already been baked into policy and operational decision-making that has not been expressed openly?*

# Questions?