Journal of Strategic Competition — Vol. 2, No. 1, 2026

Rewriting History: Understanding Historical Catastrophic Cyber Economic Losses

Tom Johansmeyer[1]

Abstract

Cyber security strategy suffers from a gaping hole in the historical literature: Estimated economic impact. The ongoing debate over the potential severity of different forms of cyber attack, including cyber war, rages on without any quantitative reference points. While a lack of historical data is usually accepted as a reason for this, the path of least resistance overlooks a rich history of twenty-four major cyber events since 1998. This article offers the first such analysis of the estimated economic losses from historical catastrophic cyber attacks. The reliance on publicly available estimates results in a complicated and nuanced process for developing the dataset, but accepting the significant limitations in the data and thus the study on which it is based yields a starting point not just for improved cyber security scholarship but also deeper analysis and ongoing refinement of the underlying data. Without data, study of the nexus of cyber security and economic security is an exercise in guesswork. Guesswork is not necessary, and this article provides the foundation for a new line of scholarship, not to mention improvements areas of ongoing study.

Keywords: economic security, cyber security, security strategy, cyber war

1 Co-director, Economic and Legal Warfare Project, Irregular Warfare Initiative; Early Career Researcher, Institute of Cyber Security for Society (iCSS), University of Kent; PhD Candidate; University of Kent, Canterbury.

Introduction

Nobody seems to know how much major catastrophic cyber attacks could cost, and nobody seems to want to find out. For what is largely believed to be an economic security problem, the absence of an exercise focused on the potential economic consequences of catastrophic cyber attacks is noteworthy. A few efforts have been made, but they are isolated and of questionable effect. Further, the few attempts available – generally for the commercial community – appear to have come in isolation relative to historical data on catastrophic losses. In fact, the historical scholarship has generally ignored a rather robust potential dataset when contemplating the problem of estimated economic loss quantum with regard to catastrophic cyber attacks. This article seeks to remedy that problem.

The role of cyber operations in strategic competition has led to extensive research (and speculation) as to the potential effects of such activity, including the scale of economic impact that can be expected. In fact, concerns about the potential economic effect of cyber operations has led to questions ranging from whether cyber operations can have anything other than short-term impact to whether they could be too impactful and dangerous to wield responsibly. The historical scholarship has sought to address these concerns, but the absence of reliable historical data on the economic losses from cyber attacks has made analysis more difficult. To fill the gap in the historical literature, improve the study of the economic effects of cyber operation, and to further support research into strategic competition, this article develops and presents the first aggregated dataset of economic losses from catastrophic cyber attacks from 1998 to today. The newly formed dataset can serve not just as a foundation for future research regarding the cost of catastrophic cyber events but also provide an important input for any economic security analysis involving the cyber domain. Further, the dataset that this article yields should also serve as a starting point for future refinement of both the list of events itself and the estimated economic impacts associated with each event. To see this article concluding with a robust set of opportunities for future research is to have read it properly.

The process of turning unrelated, often contextless historical data on the cost of catastrophic cyber events into a cohesive historical dataset is both messy and important. Publicly available estimates can be notoriously unreliable, particularly when they are published through popular media without methodology or sourcing (when someone else's estimates are presumably republished). Sometimes, one is forced to choose the best of the worst available alternatives, with no clear criteria for how to decide what the best of the worst is. In many cases, only one estimate is available, and we are left to the mercy of what the internet has not yet forgotten, ignorant to where that estimate may have come from. It is worth enduring the pains brought by the data available because of the purpose involved. Developing an understanding of the economic consequences of past catastrophic cyber events is crucial to improving cyber security and economic security research.

This article's primary contribution to the literature is to produce a data set of economic losses associated with historical catastrophic cyber events and the reasons those numbers were selected from the wide range of past calculation efforts. Secondarily, this article provides the broad set of data, sources, and analysis necessary for other scholars to build their

own views of the "best" data set using the available underlying data provided throughout this article. Finally, the role the data set produced could play in cyber and economic security strategy is explored, to include potential use cases for the data. However, such efforts are not intended to be exhaustive. The collection of estimated economic losses from historical cyber catastrophes in this article should be taken as the first step in an iterative research process open to interested scholars across disciplines.

Literature Review

The debate over the potential economic effects of catastrophic cyber attacks largely occurs without context. First comes the question of major events and their overall impacts, with cyber war a typical focal point. The discussion of the risk itself, without regard to economic consequence, comes down to a case of dueling experts, who offer differing interpretations of past events and a healthy dose of speculation with regard to how they could have been worse. Those in opposition, of course, cite the past as evidence of a lack of catastrophic activity in the cyber domain, whether from war or other causes. The truth is somewhere in the middle – as it always is – with the economic discussion still largely absent, at least with any supporting evidence.

Douzet and Gery claim that cyber war, for example, is a distinct possibility, even calling the cyber domain "a field of confrontations,"[2], although they do concede that cyber war has not yet "reache[d] its cruising speed."[3] Stone says that although cyber war may not have arisen yet, it could,[4] and Eilstrup-Sangiovanni echoes the sentiment, opening her article with the claim that the "capacity of states to use modern information and communication technology (ICT) to inflict grave economic, political, and material harm on enemies has been amply demonstrated," citing the likes of preemptive U.S. cyber attacks against Iraq in 2003 and Syria and Iran in 2007.[5]

Despite the claims and examples above, critics of the concept of cyber war bring strong arguments to support their view. Rid, Gartzke, and Brooking and Lonergan offer what have become the classic arguments against cyber war. Rid famously asserts that cyber war will not and cannot happen, largely because it is inconsistent with the Clausewitzian tradition. Gartzke contends that cyber war could only be possible if a foreign power "has decided it can stand toe-to-toe with conventional U.S. military power,"[6] which is consistent with Brooking's and Lonergan's belief that the page has been turned on "Cyber Pearl Harbor."[7]

2 Federick Douzet and Aude Gery, 2021, "Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace," *Journal of Cyber Policy*, vol. 6, no. 1, p. 110, https://doi.org/10.1080/23738871.2021.1937253.

3 Douzet and Gery, 2021, p. 99

4 John Stone, 2013, "Cyber War Will Take Place!" *Journal of Strategic Studies*, vol. 36, no. 1, p. 103, https://doi.org/10.1080/01402390.2012.730485.

5 Mette Eilstrup-Sangiovanni, 2018, "Why the World Needs an International Cyber Convention," Philosophy and Technology, vol. 31, pp. 379-380, https://doi.org/10.1007/s13347-017-0271-5.

6 Thomas Rid, 2012, "Cyber War Will Not Take Place," Journal of Strategic Studies, vol. 35, no. 1, ,p. 10, https://doi.org/10.1080/01402390.2011.608939.

7 Emerson T. Brooking and Erica Lonergan, 2023, "Welcome to Cyber Realism: Pars-

Further, there are more detailed considerations. Smeets distinctly refers to cyber weapons as "short-lived" and "temporary," contrasting them with "Kalashnikovs mass-produced in the early 1950s [that] could still kill people."[8] Their usefulness fades fairly quickly, according to Smeets, because of the speed with which their ability to cause harm declines.[9] Even with these compelling arguments against cyber war, fear persists.

Cyber war is largely believed to be among the most catastrophic manifestations of risk and impact in the cyber domain, but there is still plenty of concern about cyber attacks below the threshold of war, whether from state actors, those acting on behalf of states, or non-state actors with incentive to affect major attacks via the cyber domain. While some of the events cited as instances of cyber war – such as NotPetya – are also applicable for consideration outside the cyber war context, two studies commissioned by insurance marketplace Lloyd's of London are more insightful.[10] The first came in 2023, a $3.5 trillion estimated economic impact from a broad attack on the global financial system, with the economic impact spanning five years and stretching around the world.[11] It follows a 2015 report featuring an estimated economic loss of $243 billion to possibly more than $1 trillion from a cyber attack that causes a widespread blackout in the northeastern United States.[12]

Although the methodologies associated with these efforts may have some merit, the fact that data is limited, and the historical record is seen as thin (an issue this article seeks to remedy). As a result, the heavy lifting expected of extrapolation is magnified, making it difficult to ascribe much credibility to the prediction of such extreme events. The lack of input data, which this article seeks to address below, generally limits understanding the potential economic impacts from future events has largely been a speculative exercise.

Research Methodology

The process of developing the historical event set began with conventional internet searches to build upon the previous work in this space,[13] starting with sixteen historical events. Many estimates were found in articles with lists of catastrophic cyber events and attendant

ing the 2023 Department of Defense Cyber Strategy," *War on the Rocks*, 25 September, https://warontherocks.com/2023/09/welcome-to-cyber-realism-parsing-the-2023-department-of-defense-cyber-strategy/.

8 Max Smeets, 2018, "A matter of time: On the transitory nature of cyberweapons," *Journal of Strategic Studies*, vol. 41, nos. 1-2, p. 6, www.tandfonline.com/doi/full/10.1080/01402390.2017.1288107.

9 Smeets, 2018.

10 Josephine Wolff, 2021, "How the NotPetya attack is reshaping cyber insurance," *Brookings*, 1 Decembrer, https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/.

11 Lloyd's of London, 2023, "Lloyd's systemic risk scenario reveals global economy exposed to $3.5trn from major cyber attack," *Lloyd's of London*, 18 October, https://www.lloyds.com/about-lloyds/media-centre/press-releases/lloyds-systemic-risk-scenario-reveals-global-economy-exposed-to-3.5trn-from-major-cyber-attack.

12 Lloyd's of London, 2015, *Business Blackout: The insurance implications of a cyber attack on the US power grid*, n.d., https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf.

13 Tom Johansmeyer, 2023, "How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector," International Journal of Security, Privacy and Trust Management, vol. 12, no. 1, p. 6, https://aircconline.com/ijsptm/V12N1/12123ijsptm01.pdf.

quanta, and then the events in those lists became the fodder for further searches. As the addition of sources became dilutive, new sources were ultimately added only when they added a new event or differentiating estimate. For the twenty-four catastrophic cyber events found through the process above, evaluation of estimate data consists of contemplating the credibility of the sources from which that data is pulled and using basic statistical methods to describe the data and determine its usefulness.

It can be difficult to determine a threshold that both indicates significance and also captures a significant number of historical cases. This is particularly difficult in the study of cyber catastrophe activity, given how few there have been (as this article and the prior research discussed above contend) and how manageable their economic impacts ultimately were. If one were to choose NotPetya as the cutoff, for example, fourteen of the cases discussed in this article would be excluded. Using WannaCry would still eliminate twelve. As a result, the determination of an economic loss reporting threshold becomes seemingly arbitrary. The choice of a round and intuitively meaningful number becomes tempting, and using $1 billion would indeed meet that standard and result in twenty-two of the twenty-four cases isolated in this study's data set to be considered.

Instead, this article uses a threshold of $800 million in economic losses from a major cyber attack affecting a significant number of victims. By setting the threshold at $800 million in 2025 dollars, the dataset gains two more records than if the threshold were set at $1 billion. Given the size of the data set, every additional relevant and meaningful event becomes useful, even if lowering the threshold only adds two relatively small events (even by the standards of the historical data captured). Using a lower threshold becomes more difficult, as smaller events tend not to receive public attention, resulting in a dearth of available data and perspective. Large losses from single-victim attacks are excluded.

With source material identified, the data collected is then evaluated for credibility – to include the credibility of the sources used – to facilitate the selection of final estimates for use in the dataset of historical catastrophic cyber event economic losses. This is an imperfect, qualitative, and subjective process, as this methodology explains and as the analysis below shows. Estimates are selected from the data gathered based on a range of methods and the context of the estimate. Outliers are excluded on a common-sense basis, relying on the author's judgment, a statement both necessary and likely to make methodological purists cringe. They are welcome to vent their frustration and exact their revenge in future studies, hopefully in a manner that will advance the underlying purpose of this article. Source credibility matters throughout the selection process, and it is informed at times by descriptive statistics. Sometimes, however, statistical analysis is not helpful. If there is one credible source and four that are not, then it is easy to dismiss the four if it seems there is one underlying source that was republished and amplified.

Throughout this study, only publicly available data is used, although there have been limited cases of conversations with experts (cited as such) in an effort to validate publicly available information or otherwise add context important to the exercise of determining the estimated economic effects of historical cyber catastrophe events. In using only publicly available information, it becomes easier for the research community to generate their own views of historical cyber catastrophe events – to include perspectives competing with those

offered in this article. Additionally, it obviates the concerns associated with proprietary and classified data sets, particularly with regard to reconstructing the conclusions drawn in this article or in challenging them. Researchers with access to relevant protected data (either proprietary or classified), should it exist, could come to much different conclusions than those advanced here.

Analysis of Source Material

The source material examined for this study spans twenty sources and offers a total of ninety-three estimates across twenty-four past catastrophic cyber events from 1998 to 2025, with the most recent in 2024. While the average event has data from 3.5 underlying sources, there is little commonality. Ten have either one estimate or several identical estimates (with no alternatives). Thirteen more have multiple estimates that are not identical. One event, 1998's Chernobyl, has only a range with an inexact upper end – "Several Billions." [14] Further, the sources themselves vary in quality and reliability. Eight sources provide estimates for at least five events, which is because they are articles designed to have popular appeal rather than demonstrate academic rigor. This is evidenced by their "listicle" format, a content marketing technique that is used to make articles eye-catching, easy to read, and more likely to be shared.[15] Seven sources provide estimates for one event. Five of the sources used in this study are traditional news outlets, although this does not count the cases where a credible source's estimate is communicated via a traditional news outlet (e.g., Cyence for WannaCry or the White House for NotPetya).

The seven sources used once require specific attention. The FBI's estimate for the 1999 Melissa event, $80 million, was considered an outlier after careful consideration. On the other hand, the White House estimate for NotPetya has been repeatedly cited and deemed the most credible. Its $10 billion estimate has become the standard, in part because of its use in popular media.[16] However, at the 7th ASTIN Cyber Workshop, an insurance industry event at which research on cyber catastrophes was presented, a speaker (this author) made an off-the-cuff remark that pegged the economic impact of NotPetya at $8 billion.[17] For MOVEit, which had two conflicting estimates in one source,[18] the author reviewed the underlying records and found that they are in consistent with publicly available estimates. Based on this effort, an expert source in the insurance industry was consulted (see Appendix B for a detailed discussion of MOVEit). Finally, it may be

14 Andrew Beattie, 2012, "The Most Devastating Computer Viruses," *Techopedia*, 11 March, https://www.techopedia.com/2/26178/security/the-most-devastating-computer-viruses.

15 Armando Roggio, 2016, "Content Marketing: The Hard Working Listicle," *PracticalEcommerce*, 17 March, https://www.practicalecommerce.com/Content-Marketing-The-Hard-Working-Listicle.

16 Andy Greenberg, 2018, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

17 Tom Johansmeyer, 2023a, "How Bad Can Systemic Cyber Get?" *ASTIN, 7th ASTIN Cyber Workshop – A market set for growth*, https://doi.org/10.13140/rg.2.2.23767.48801.

18 Carly Page, 2023, "MOVEit, the biggest hack of the year, by the numbers," *TechCrunch*, 25 August, https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/.

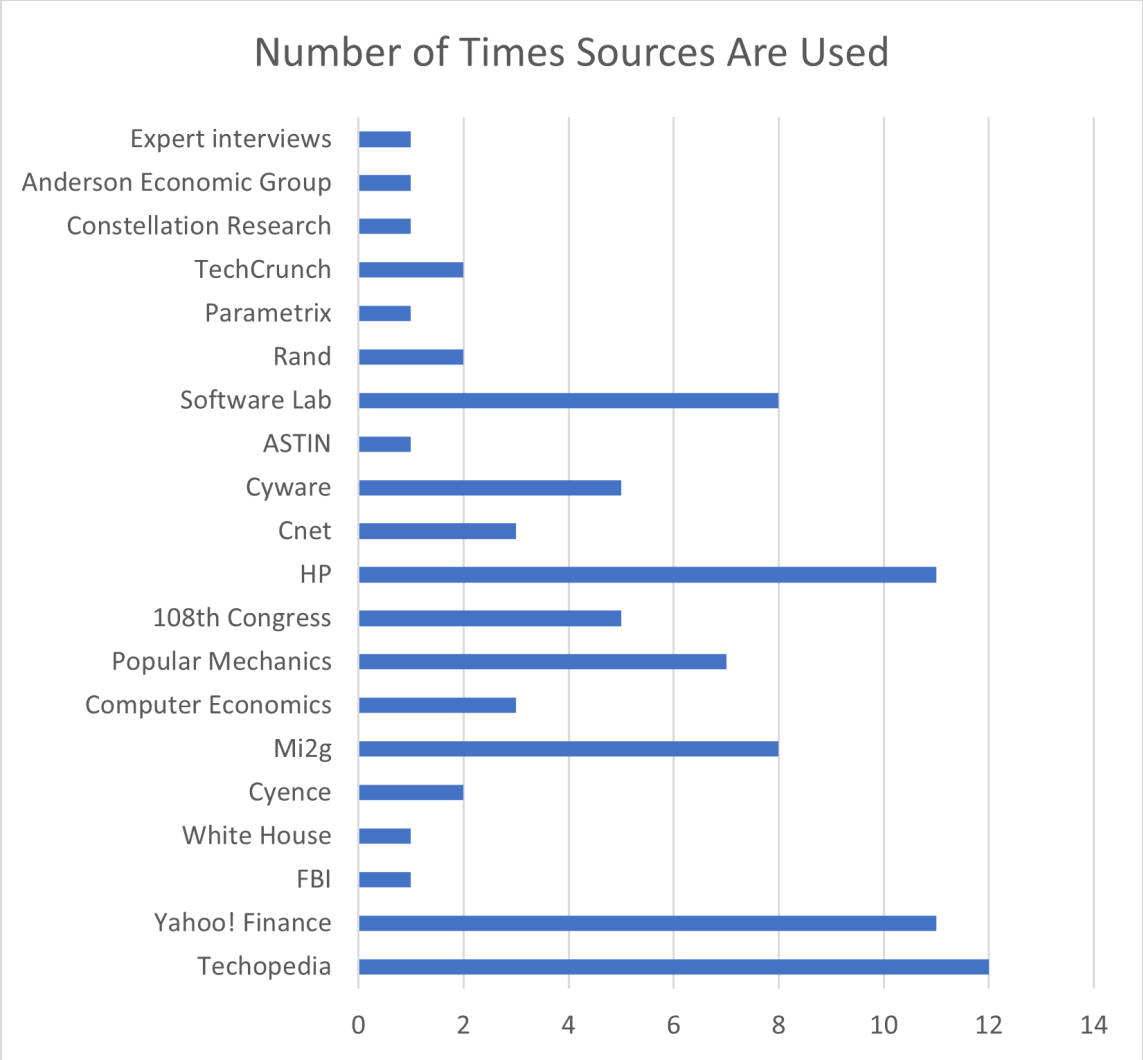

Figure 1: Number of Times Sources Are Used

tempting to see the 108th Congress as a government source, but it is testimony in which previously published estimates are referenced. The testimony has more in common with listicles than genuine government sources.

As for the credibility of the seven expert sources (e.g., cyber security and analytics firms) found (excluding the interview mentioned above), there is a range. Mi2g provides several credible estimates, having undertaken the effort to produce them approximately twenty years ago. Although there is no underlying methodology offered, the context in which the estimates are found suggests that some such methodology exists. Further, Mi2g offers insight into events that have largely remained overlooked, adding eight this study's findings where it is the sole source. Perhaps the greatest indicator of Mi2g's credibility is the criticism to which it has been subjected by other experts. Mi2g has been accused of "spreading fear, uncertainty and doubt about cyberterrorism risks," for example.[19] That said, by contemporary views of estimated loss quantum, the Mi2g estimates could be considered mundane, and there are cases where Mi2g itself took to de-escalating language.[20]

Four more expert sources are relatively straightforward. Anderson Economic Group[21] and Constellation Research[22] appear to offer industry-specific expertise and can generally be accepted as credible. Cyence and Parametrix are respected cyber analytics and modeling firms. The Cyence estimate for WannaCry appears to have become the standard and has been used and republished regularly. Cyence and Parametrix conflict widely on Crowdstrike, but both can be seen as expert sources, given that experts can disagree. The two remaining expert sources used in this study are more difficult to accept. Computer Economics, a technology research firm with three estimates in this study, has two of them come from a range in an article on Cnet, and a third forming the low end of the range for SQL Slammer.[23] Without access to how the estimates were formed, further critique is not possible, but the fact that its estimates are outliers impairs the source's credibility. For Rand, it only supplied the high and low ranges of NotPetya, both of which are extreme outliers at $3 billion and $57 billion.[24]

Included among the listicles mentioned above are corporate sources (Cyware, Software Lab, and HP Tech Takes). The Cyware and Software lab listicles represent conventional content marketing efforts meant to draw attention to their websites, offering no original research. Although the estimates they provide are dubious on their own and likely pull from sources no longer available, they are useful for finding events requiring further research. HP Tech Takes is more complicated, because it claims to offer its own methodology: "Most

19 John Leyden, 2002, "Why is mi2g so unpopular?" *The Register*, 21 November, https://www.theregister.com/2002/11/21/why_is_mi2g_so_unpopular/.

20 Robert Lemos, 2003, "Counting the cost of Slammer," *Cnet*, https://www.cnet.com/tech/tech-industry/counting-the-cost-of-slammer/.

21 Christopher Smit, 2024, "Dealers Are Set to Lose Nearly $1 Billion Over CDK Cyberattack [UPDATE]," *Motor1*, 1 July, https://www.motor1.com/news/725118/dealers-lose-1-billion-cdk-cyberattack/.

22 Larry Dignan, 2024, "UnitedHealth sees $1.35 billion to $1.6 billion hit in 2024 due to Change Healthcare cyberattack," *Constellation Research*, 16 April, https://www.constellationr.com/blog-news/insights/unitedhealth-sees-135-billion-16-billion-hit-2024-due-change-healthcare.

23 Lemos, 2003

24 Jonathan Welburn and Aaron Strong, 2022, "Systemic Cyber Risk and Aggregate Impacts," *Risk Analysis*, vol. 42, no. 8, p. 1617, https://doi.org/10.1111/risa.13715.

of the computer virus cost estimates you'll find in other articles online come from a single source."[25] Yet the likelihood that the article uses bespoke calculations is quite low. Aside from the delta between this article and Mi2g for one estimate, Swen,[26] most of the estimates are utterly familiar. Those for MyDoom, SoBig, ILOVEYOU, WannaCry, Zeus, and Sasser have all appeared in other publications evaluated for this study and predate the HP Tech Takes publication. Swen, Klez, and CodeRed appear to be different from prior estimates and represent a unique contribution, although there may be preexisting estimates for them that are no longer available via conventional internet searches.

The fact that the estimates used come from publications (and other sources) with vastly different purposes does introduce concerns about bias. While it would be appropriate to raise questions about whether some regions would attract more attention than others, the size of economic impact necessary to qualify for inclusion in this study naturally attracts larger events that would span regions. This is as true of an event like Yaha, which arose from a conflict between India and Pakistan in 2002 and 2003.[27] Moreover, for larger events, multi-regional scale is clear, with NotPetya affecting at least sixty-five countries.[28]

The possibility of under-reported events due to region is less a concern than the prospect of over-estimating them. The concern was raised above with regard to Mi2g, which had publicly sustained such criticism, and the hyperbolic language used to describe NotPetya in a 2018 government announcement speaks to the same issue.[29] For the commercial entities – either cyber security experts and vendors offering relevant services or publishers seeking to attract readers – the benefit of advancing an alarmist perspective is to create interest in the problem and potentially demand for something commercial, from more information (publishers) to security capabilities (vendors). Risks associated with this bias do permeate the data set developed in the study below. However, the estiamted economic losses from the events studied are still relatively small compared to other forms of widespread economic harm (such as natural disasters[30]), which suggests that even if the estimates developed from public sources with a clear bias are indeed exaggerated, they are still small enough not to change materially the view that the economic harm from widespread cyber attacks may be far lower than previously believed.

25 Tom Gerencer, 2020, "The Top 10 Worst Computer Viruses in History," *HP Tech Takes*, 4 November, https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history.

26 Mi2g, 2003, "Minmail to become 4th worst malware over weekend," *Mi2g*, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/211103.php.

27 BBC, 2003, "Indian hackers target Pakistan," *BBC*, 13 March, http://news.bbc.co.uk/2/hi/technology/2847455.stm.

28 Bill Chappell, 2017, "'Petya' Ransomware Hits At Least 65 Countries; Microsoft Traces It To Tax Software," *NPR*, 28 June, https://www.npr.org/sections/thetwo-way/2017/06/28/534679950/petya-ransomware-hits-at-least-65-countries-microsoft-traces-it-to-tax-software.

29 Tom Johansmeyer, 2024b, "Cyber Attacks in Perspective: Cutting Through the Hyperbole," *Irregular Warfare Initiative*, 25 June, https://irregularwarfare.org/articles/cyber-attacks-in-perspective-cutting-through-the-hyperbole/.

30 Tom Johansmeyer, 2024c, "Why Natural Catastrophes Will Always Be Worse than Cyber Catastrophes," *War on the Rocks*, 5 April, https://warontherocks.com/2024/04/why-natural-catastrophes-will-always-be-worse-than-cyber-catastrophes/.

Analysis of Historical Catastrophic Cyber Economic Loss Estimates

The evaluation of the sources above provides crucial context for the data that to follow below. Using those sources, it has been possible to construct a data set of estimated economic losses from catastrophic cyber events since 1998. The twenty-four catastrophic cyber events occurring during that period are broken into four categories in Table 1, below: (1) events where there is either one source of data or a small number of identical or nearly identical sources, (2) events that have multiple sources of estimated economic impact that tend to be reasonably consistent, (3) events with multiple sources that are divergent, and (4) one event that requires special, separate consideration.

Table 1: Summary of Results by Category

Category	No. Events	Agg. Econ. Loss
Events with one or several identical estimate sources	10	$93.0 bn
Events with multiple estimate sources that are reasonably consistent	6	$45.4 bn
Events with multiple divergent estimate sources	7	$237.2 bn
Events requiring special consideration	1	$2.3 bn

Category 1: One Estimate or Duplicate Estimates

For estimates with either one source or multiple consistent sources (likely duplicate estimates), it is easy to decide on a defining economic loss estimate. After all, a choice of one is not really a choice. Table 2 below shows that ten events have only one estimate, and four more have two identical estimates

Table 2: Estimates with Either One Source or Several Consistent Sources

Event	Year	No. Sources	Selected Econ. Loss	Adj. Econ. Loss (2025)
Sasser	2004	2	$500 mn	$960 mn
StormWorm	2007	1	$10 bn	$17.5 bn
Zeus	2007	2	$3 bn	$5.2 bn
CryptoLocker	2013	1	$665 mn	$980 mn
Minmail	2003	1	$8.9 bn	$17.5 bn
Conficker	2008	4	$9.1 bn	$15.9 bn
Yaha	2003	1	$11.1 bn	$21.7 bn
WannaCry	2017	3	$4 bn	$5.2 bn
CDK	2024	1	$1 bn	$1 bn
Change Healthcare	2024	1	$1.6 bn	$1.6 bn

Category 2: Multiple Different – but Reasonably Consistent – Estimates per Event

The six events in this category have underlying estimates from multiple sources, but the various publicly available estimates for each event are relatively close to each other. Their ranges from lowest to highest estimates are less than 40% of the highest estimate. CodeRed has nine estimates ranging from $2 billion to $2.75 billion. SQL Slammer is similarly robust, with seven estimates. The five for NotPetya are more varied, but stripping out the severe outliers that come from one source that has a fluid methodology and questionably wide range ($3 billion and $57 billion) leaves three estimates in a tight range with a clear choice based on data credibility.[31] The same is true of Melissa when the one outlier event (at $80 million) is removed. The results are in Table 3.

Table 3: Estimates with Multiple Sources in a Tight Range

Event	Year	No. Sources	Original Avg. Est.	Original Est. Range	Selected Econ. Loss*	Adj. Econ. Loss (2025)
CodeRed	2001	9	$2.25 bn	$750 mn	$2.25 bn	$4.7 bn
SirCam	2001	4	$1 bn	$250 mn	$1 bn	$2.1 bn
SQL Slammer	2003	7	$1.1 bn	$450 mn	$1 bn	$2 bn
NotPetya	2017	5	$9.3 bn	$2 bn	$10 bn	$13 bn
Swen	2003	2	$9.8 bn	$1.25 bn	$9.2 bn	$18.1 bn
Melissa	1999	4	$1.1 bn	$400 mn	$1.3 bn	$2.9 bn

Note: *These calculations exclude outlier estimates.

31 Welburn and Strong, 2022, pp. 1617-8.

Given the tight ranges, it comes as little surprise that the average would be at least indicative of the final estimate selected. The average and selected estimate are the same for CodeRed, SQL Slammer, and SirCam, and the selected estimate is within 20% of the average for the remaining three cases. As a result, it is reasonably easy to have confidence in the six selected estimates in Table 3, if for no other reason than that any estimate selected in such a tight range – including the two ends – would be reasonable.

Table 4: Understanding Estimate Ranges (Excluding Outliers)

Event	Low End	High End	Average	Midpoint	Selected
CodeRed	$2 bn	$2.75 bn	$2.25 bn	$2.38 bn	$2.25 bn
SirCam	$1 bn	$1.25 bn	$1 bn	$1.11 bn	$1 bn
SQL Slammer	$750 mn	$1.2 bn	$1 bn	$975 mn	$1 bn
NotPetya	$8 bn	$10 bn	$9 bn	$9 bn	$10 bn
Swen	$9.2 bn	$10.4 bn	$9.78 bn	$9.78 bn	$9.2 bn
Melissa	$1.1 bn	$1.5 bn	$1.3 bn	$1.3 bn	$2.3 bn

The high and low ends of CodeRed are only 22% from the average, as shown in Table 4. The fact that the midpoint is higher than the average suggests that the clustering of estimates below it supports using the average, although this does overlook the risk that the concentration of estimates represents republishing from the same underlying source – a risk identified in this study that one must accept, as there is no way to mitigate it. The same approach applies to the estimates for Melissa, with the FBI outlier estimate excluded. Finally, Swen and NotPetya are different cases, where source quality proved more important than statistical analysis. Both use expert sources with high levels of credibility relative to the others available – Mi2g for Swen[32] and the U.S. government for NotPetya.[33]

Category 3: Estimates with Multiple, Divergent Sources

Determining the final selection for the five events in this category was much more difficult than doing so for the two categories above. The ranges are wide, and although there is some clustering of estimates, that may not be indicative of a best selection, particularly when an estimate has two clusters with a significant range between them. The distances from the midpoint in Table 5 generally exceed 40% of the midpoint value. The estimates selected, relative to the average and the range, indicated that there is a much greater role for judgment in the evaluation of this set of estimates.

32 Mi2g, 2003.
33 Greenberg, 2018.

Table 5: Estimates with Multiple Sources that Diverge

Event	Year	No. Sources	Original Avg. Est.	Original Est. Range	Selected Econ. Loss[31]	Adj. Econ. Loss (2025)
ILOVEYOU	2000	9	$10.6 bn	$7.3 bn	$15 bn	$32.3 bn
Klez	2001	4	$14.3 bn	$10.8 bn	$18.9 bn	$39.6 bn
Nimda	2001	2	$1.1 bn	$865 mn	$1.5 mn	$3.1 bn
SoBig	2003	5	$34 bn	$7 bn	$37 bn	$73 bn
MyDoom	2004	8	$31 bn	$34.5 bn	$38 bn	$72.8 bn
MOVEit	2023	3	$8.9 bn	$15.8 bn	$1 bn	$1 bn
Crowdstrike	2024	2	$3.2 bn	$4.4 bn	$1.7 bn	$1.7 bn

To arrive at realistic estimates for the five events above – four of which are among the five largest in history – it is necessary to dismiss the outliers. The level of effort (and risk) associated with this varies. Of the eight estimates available for MyDoom, five are $38 billion, with one more at $38.5 billion. The other two are outliers and come from the same source (Techopedia), which uses them to form a range of $4-22 billion, with both ends below the cluster at $38 billion.[34] The remaining results still have a credibility problem given the nature of their sources (HP and Cyware blogs, Popular Mechanics), but they agree with Mi2g's $38.5 billion estimate. SoBig has two groups of consistent estimates: $30 billion and $36-37.1 billion. The presence of an Mi2G estimate at the higher cluster – like MyDoom – drives the selection of the $37 billion estimate shown in Tables 5 and 6. This is also the case for the pair of clusters for Klez. One is in the range of $9-9.5 billion, and the other is $18.9-19.8 billion. The higher of the two sets of sources uses Mi2g, which is the only expert source available for Klez and is thus selected ($18.9 billion).

Table 6: Understanding Estimate Ranges (Excluding Outliers)

Event	Low End	High End	Average	Midpoint	Selected
ILOVEYOU	$7.7 bn	$15.5 bn	$10.6 bn	$11.4 bn	$15 bn
Klez	$9 bn	$19.8 bn	$14.3 bn	$14.4 bn	$18.9 bn
Nimda	$635 mn	$1.5 bn	$1.1 bn	$1.1 bn	$1.5 bn
SoBig	$30 bn	$37.1 bn	$34 bn	$33.6 bn	$37 bn
MyDoom	$4 bn	$38.5 bn	$31 bn	$21.3 bn	$38 bn
MOVEit	$1 bn	$15.8 bn	$8.9 bn	$8.4 bn	$1 bn
Crowdstrike	$1 bn	$5.4 bn	$3.2 bn	$3.2 bn	$1.7 bn

The situation with historical estimates for ILOVEYOU is more nuanced. Three of the nine estimates are at the high end of the range ($15 billion), although that could come from the republication of prior estimates. The low end is an outlier at $7.7 billion, which

34 Greenberg, 2018.

is roughly $3 billion below the average in Table 5. There needs to be a binary decision – as with SoBig – on which grouping is more likely to be accurate, after which an estimate can be selected, and the preponderance of estimates at the high end proved impossible to ignore, although the estimate should be contemplated within the context of uncertainty. Nuance was necessary for MOVEit and Crowdstrike, as well. The former had only dubious estimates that were easily countered by an analysis of the underlying data provided in the TechCrunch article (see Appendix B),[35] and the latter came down to a choice between two expert sources – Cyence[36] and Parametrix.[37] Cyence was chosen, largely because the high estimate offered by Parametrix conflicted significantly with insurance industry estimates for the insured loss from the event (see Appendix C).

Finally, only two estimates arose for Nimda: $635 million and $1.5 billion. Both are from questionable sources. The former is from Yahoo! Finance, and the latter is from Techopedia. The estimates are far apart and with no meaningful qualitative factors to consider. For this reason, the higher of the two was simply selected, with the understanding that the event is already small enough that the risk of a major over-estimation would have minimal impact on the overall data set.

Category 4. The Chernobyl Estimate

The final event remaining is for the earliest event on this list: 1998's Chernobyl. The range offered is wide, and it only comes from one source (Techopedia), which offers a range of $250 million to "Several Billion"[38] and no further explanation. For the high end, $2 billion was selected because it is the lowest number that satisfies the plural of "billions." As a result, the role of judgument in this case was significant, given the paucity fo information available. Although the estimate could be much higher, that would be doubtful given how low the low end of the range is $250 million, and the notion that a very high estimate likely would have had more specificity around it. Of course, there have been cases of wide ranges (e.g., for NotPetya[39]), but for the analysis of Chernobyl to proceed, a decision had to be made, even if seemingly arbitrary. Ultimately, an economic loss of $1 billion was selected because it fit within the range, reached the billion-dollar threshold, and settles roughly in the middle of an admittedly wide range. It would be fair to call this loosely ring-fenced guesswork, but there is little else to work with. This estimate, like any associated with the Chernyobyl event, should be treated with a significant amount of skepticism. However, it is important to remember that if the event had been profoundly impactful on an economic basis, there is the likelihood that more news coverage and analysis about the event (and its effects) would have been available.

35 Page, 2023.
36 Staff, 2024, "The Financial Impact of the CrowdStrike Global IT Outage," *Guidewire*, 26 July, https://www.guidewire.com/resources/blog/technology/the-financial-impact-of-the-crowdstrike-global-it-outage.
37 Parametrix, 2024, *CrowdStrike's Impact on the Fortune 500: An Impact Analysis*, n.d., https://www.parametrixinsurance.com/crowdstrike-outage-impact-on-the-fortune-500.
38 Beattie, 2012.
39 Welburn and Strong, 2022.

Summary

The twenty-four historical catastrophic cyber events captured by this study span a wide range of data problems, from insufficient sources to questionable sources, to wild divergence in estimates for an event. Because catastrophic cyber events have been relatively rare, the exercise of selecting the best estimates is a highly qualitative exercise that is significantly dependent upon the judgment of the analyst (for the purposes of this article, this author). The estimates in Table 7 represent a first formal and comprehensive attempt to develop a historical dataset of economic losses from catastrophic cyber events and provide a starting point for future analysis. The next section of this article discusses the importance of the newly formed dataset and how it can be used to improve the analysis of economic effects from catastrophic cyber events.

The process of understanding cyber risk in general – to include its potential impact in the future – begins with developing a view of how impactful past attacks have been. The gap in historical scholarship on this specific issue has impeded rigorous analysis. The debate over the potential economic implications of cyber war and other catastrophic events has had to proceed without the benefit of precedent and quantification, and firm footing with regard to how much catastrophic cyber events have cost stands to reshape the debate well into the future. While the possibility remains of a cyber catastrophe far more extreme than those that have occurred so far, what is most evident from the data on the twenty-four estimates collected – to include the final estimates used – is that they do not suggest that such extreme events would reach truly devastating levels. After all, society is quite experienced with extreme economic losses (e.g., from natural disasters), and the economic impacts of cyber catastrophe would have to scale profoundly to reach the familiar.[40]

Consequently, the first lesson from the estimates in Table 7 is that the economic consequences of major catastrophic cyber events may be significant, but they certainly do not appear to pose an existential economic security threat. There has been no world- or society-changing cyber attack, based on twenty-five years of experience. Further, the prior years not covered in this study coincide with the earliest days of the commercial internet – and the internet's pre-commercial period – suggesting that even the worst cyber events during that period, such as the Morris Worm, are not consequential within the context of study at the nexus of cyber security and economic security. Further, if time is seen as a proxy for maturation of the cyber domain as both a security priority and an economic environment, then it appears that maturity has become a security force in itself, as Figure 2 suggests.

Some may fear that the worst is yet to come, which could be true, but the data suggests that it is a much less likely prospect than it seems. The frequency and severity of catastrophic cyber events have declined precipitously since 1998 as Figure 2 below demonstrates. Fourteen of the twenty-four events tracked came from 1998 through 2004. Two more came in 2007, adding up to 67% of events by count. Of the years that followed, 2017 and 20224 were the only years with more than one event. By aggregate economic loss, the

40 Johansmeyer, 2024c.

Table 7: Summary of Final Estimates for Catastrophic Cyber Events*

Event	Year	Low	High	Range	No. Sources	Original Selected	Adj. (2025)
Chernobyl	1998	$250 mn	Several bn**	$1.75 bn	2	$1 bn	$2.3 bn
Melissa	1999	$80 mn	$1.5 bn	$400 mn	3	$1.3 bn	$2.9 bn
ILOVEYOU	2000	$7.7 bn	$15 bn	$7.3 bn	9	$15 bn	$32.3 bn
Klez	2001	$9 bn	$19.8 bn	$10.8 bn	4	$18.9 bn	$39.6 bn
CodeRed	2001	$2 bn	$2.5 bn	$750 mn	9	$2.25 bn	$4.7 bn
Nimda	2001	$635 mn	$1.5 bn	$865 mn	2	$1.1 bn	$3.1 bn
SirCam	2001	$750 mn	$1.25 bn	$100 mn	4	$1 bn	$2.1 bn
SoBig	2003	$30 bn	$37.1 bn	$7 bn	5	$37 bn	$73 bn
SQL Slammer	2003	$750 mn	$1.2 bn	$450 mn	7	$1 bn	$2 bn
Swen	2003	$9.15 bn	$10.4 bn	$1.25 bn	2	$9.2 bn	$18.1 bn
Minmail	2003	$8.85 bn	$8.85 bn	$0	1	$8.9 bn	$17.5 bn
Yaha	2003	$11.1 bn	$11.1 bn	$0	1	$11.1 bn	$21.7 bn
MyDoom	2004	$4 bn	$38.5 bn	$34.5 bn	8	$38 bn	$72.8 bn
Sasser	2004	$500 mn	$500 mn	$0	2	$500 mn	$960 mn
StormWorm	2007	$10 bn	$10 bn	$0	1	$10 bn	$17.5 bn
Conficker	2008	$9 bn	$9.1 bn	$0	4	$9.1 bn	$15.9 bn
Zeus	2007	$3 bn	$3 bn	$0	2	$3 bn	$5.2 bn
CryptoLocker	2013	$665 mn	$665 mn	$0	1 1	$665 mn	$980 mn
NotPetya	2017	$3 bn	$57 bn	$54 bn	5	$10 bn	$13 bn
WannaCry	2017	$4 bn	$4 bn	$0	3	$4 bn	$5.2 bn
MOVEit	2023	$1 bn	$15.8 bn	$14.8 bn	3	$1 bn	$1 bn
Change Healthcare	2024	$1.6 bn	$1.6 bn	$0	1	$1.6 bn	$1.6 bn
CDK	2024	$1 bn	$1 bn	$0	1	$1 bn	$1 bn
Crowdstrike	2024	$1 bn	$5.4 bn	$4.4 bn	2	$1.7 bn	$1.7 bn

Note: *The ranges in this table include outlier estimates.
**The range uses the $2 billion high-end estimate discussed earlier in this article.

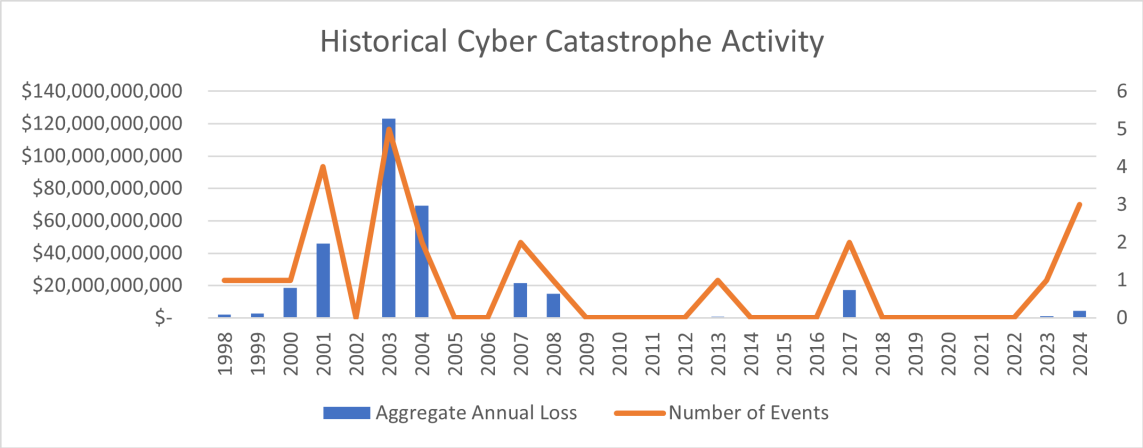

Figure 2: Annual Catastrophic Cyber Loss Activity

drop-off after 2007 is even more pronounced. In aggregate, $293 billion (82%) in economic losses, as shown in Table 7 and Figure 2, came from 1998 through 2004, with another $22.3 billion in 2007, bringing the 1998-2007 total to $315.8 billion. The historical data is difficult to ignore, even if one were to try to contend that it is not compelling. Clearly, there have been major historical cyber attacks with consequential economic effects, but there have been far fewer since 2007. Those that have occurred during this seeming dry spell have not been severe compared to those that came in a time of heavier attack frequency and economic consequence. No single event since 2009 has achieved the average per-event inflation-adjusted loss for the study of $14.8 billion. In fact, the only above-average aggregate loss year since then was 2017 (at $18.3 billion), which had two major events – WannaCry and NotPetya. For this reason, the events of 2017 seem to look like the extreme case going forward, particularly given that 2024 had multiple events, as well, with minimal accumulated economic effect.

Discussion: Future Uses of the Data Set for National Security Strategy

The power of the data set introduced in Table 7 is in its utility, particularly with regard to informing economic security concerns within the broader discussion of national security strategy. Although cyber security strategy reaches beyond economic concerns – to include espionage, societal and government disruption, and purely military matters – the data that the study has yielded is directly useful in contextualizing the effectiveness of cyber attacks, potentially informing and guiding future cyber security strategy.

Deterrence remains an important part of national cyber security strategy, even if it has been criticized as inappropriate for the cyber domain.[41] Although the 2023 U.S. national

41 James Lewis, 2023, "Deterrence and Cyber Strategy," *Center for Strategic & International Studies*, 15 November, https://www.csis.org/analysis/deterrence-and-cyber-strategy.

cyber security strategy does not use any form of "deterrence," the Department of Defense counterpart relies on it, going so far as to claim, "The Department will campaign in and through cyberspace to reinforce deterrence objectives while achieving informational and military advantages."[42] Further, the 2018 U.S. national cyber security strategy emphasized deterrence, which suggests the current administration (which was responsible for the 2018 strategy) could revive the priority.[43] However, deterrence requires the consent of the deterred,[44] and it is clear that consent has not been forthcoming. Cyber attacks have become frequent and mundane, with the fact that they have failed to rise to cataclysmic economic levels suggestive of the need for – let alone the effectiveness of – deterrence.

While it may be tempting to declare deterrence wholly inappropriate for the cyber domain, the lack of experience and lingering fear of a major, unprecedented event keeps the strategy relevant. Further, even if cyber-specific deterrence is downplayed (as it seemingly was in the 2023 U.S. national cyber security strategy), there remains the role that cyber plays in the broader integrated deterrence position adopted by the Department of Defense that same year.[45] That said, the data found in this study suggests that a broader strategic posture aside from the extreme cases for which deterrence is suited must be contemplated. In fact, cyber threats operating far short of the extremes are clearly the greater concern, according to the data.

Instead of focusing on prevention (which would be the aim of deterrence, as well as other models), the estimated economic loss quantum in Table 7 indicates that the economic effects of cyber attacks may be manageable, and while it certainly does not make sense to tolerate them without a robust defense, more effort on resilience and recovery could be a more effective use of cyber security strategy time and resources. Cyber attacks will happen, and they will cause economic harm. However, the economic harm that they can cause, as shown earlier in this article, can be absorbed. In fact, investing in the capabilities that minimize harm instead of trying to prevent it can make such attacks even less effective. This implies a pivot from focusing on security to the broader concept of cyber resilience, which consists of withstanding and recovering from attacks rather than simply preventing them.[46]

The distinction is important – and not just between security and resilience. Preparing for cyber attacks with the potential for catastrophic harm in a manner that accelerates recovery minimizes the potential harm that such events can cause. This approach is based on the assumption that prevention cannot achieve a success rate of 100%, an assumption supported by experience. The fact that some attacks will get through and that they could

42 Department of Defense, 2023, *Summary: 2023 Cyber Strategy of The Department of Defense*, n.d., https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.
43 Donald J. Trump, 2018, *National Cyber Strategy of the United States of America*, September, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
44 Colin Gray, 2000, "Deterrence in the 21st Century," *Comparative Strategy*, vol. 19, p. 257, https://doi.org/10.1080/01495930008403211.
45 Department of Defense, 2023, pp. 2-3.
46 Filipe Beato, Luna Rohland, Ioannis Agrafiotis, Sadie Creese, William H. Dutton, Patricia Esteve-Gonzalez, and Jamie Saunders, 2024, *Unpacking Cyber Resilience*, November, p. 8, https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf.

have major consequences suggests that it is advisable to prepare for such eventualities, particularly given that the prospective economic impacts are well within the levels already experienced routinely from such events as natural disasters[47]. The twenty-seven years of data in Table 7, frankly, are only slightly higher than the economic losses sustained from natural disasters in 2024 alone.[48] According to Figure 2, the worst year in history for cyber catastrophe losses – 2003, with more than $130 billion in estimated impact – is still well below 2024's $320 billion from natural disasters, chosen only for recency. It is clear that more economic impact from cyber catastrophe events could be absorbed.

If there are two keys to cyber resilience with regard to mitigating economic security vulnerability, they are time and capital. The economic effects of cyber attacks – particularly those catastrophic in nature – are largely a function of time. Elongating the unavailability of key systems impedes activity, which generally implies an increase in economic harm. Shortening that unavailability, conversely, reduces economic harm. The role of capital as a key to resilience is to enable not just the investments in prevention, as is often contemplated, but also to affect and accelerate post-event recovery. This is consistent with the role of insurance in economic security more broadly,[49] to include the use of contingent capital, such as insurance, in reducing the economic harm associated with cyber catastrophe events. In fact, cyber insurance has been identified as a useful tool in economic security strategy by several cyber powers, including the United States,[50] United Kingdom,[51] and the European Union.[52] The prospect of increased cyber insurance availability, through an improved understanding of cyber catastrophe risk,[53] could significantly reduce the effectiveness of major cyber attacks (including by adversary states) and improve resilience.

In addition to the granular efforts associated with increasing the flow of capital to the cyber insurance market, there is a broader set of uses for the estimated economic losses from cyber catastrophes in Table 7. Beyond calculating the past effects of cyber catastrophes to understand today's potential implications, the data can be used to revisit present as-

47 Johansmeyer, 2024c.

48 Munich Re, 2025, "Climate change is showing its claws: The world is getting hotter, resulting in severe hurricanes, thunderstorms and floods," *Munich Re*, https://www.munichre.com/en/company/media-relations/media-information-and-corporate-news/media-information/2025/natural-disaster-figures-2024.html.

49 Tom Johansmeyer, 2025, "Bad decisions have consequences: how cyber security could fall victim to climate change," *British Actuarial Journal*, vol. 30, no. 15, https://doi.org/10.1017/S1357321725000091.

50 Richard Forno, 2023, "What is the National Cybersecurity Strategy? A cybersecurity expert explains what it is and what the Biden administration has changed," *TheConversation*, 20 March, https://theconversation.com/what-is-the-national-cybersecurity-strategy-a-cybersecurity-expert-explains-what-it-is-and-what-the-biden-administration-has-changed-201122.

51 Rebecca Matyear, 2024, "Major UK insurance associations unite with National Cyber Security Centre to combat ransomware," *UKGI Insight*, May, https://insight.rwabusiness.com/blog/posts/2024/may/major-uk-insurance-associations-unite-with-national-cyber-security-centre-to-combat-ransomware/

52 Dimitra Markopoulou, 2021, "Cyber-insurance in EU policy-making: Regulatory options, the market's challenges and the US example," *Computer Law & Security Review*, vol. 43, November, https://doi.org/10.1016/j.clsr.2021.105627.

53 Tom Johansmeyer, 2024d, "Perception Shapes Reality: How Views on Financial Market Correlation Affect Capital Availability for Cyber Insurance," *Journal of Risk Management and Insurance*, vol. 28, no. 1, pp. 13-17, https://jrmi.au.edu/index.php/jrmi/article/view/287/189.

sumptions about the need for economic support in the face of catastrophic cyber attacks, to include the mechanisms by which such support would be conveyed. Nowhere is this more relevant than in the discussion about cyber backstops, public-private partnerships, and other government-specific roles to provide economic support in the wake of a catastrophic cyber attack.[54] While some organizations have seen the need for such a solution as a forgone conclusion,[55] the data set produced by this article suggests that pursuing government solutions may be hasty, and that states stepping back and enabling the insurance industry to fill the gap may have chosen a more prudent approach – an approach grounded in verifiable historical experience.[56]

The broader lesson from the narrow discussion about government backstops and relief programs following cyber catastrophes is that the data in Figure 8 can be used as a diagnostic for a wide range of strategic challenges. Gauging the potential economic effects of a cyber catastrophe relative to the cost, effort, and available resources necessary for remediation can improve strategic planning and execution. Decisions that once relied heavily upon assumptions without foundation could now be made following a much more robust analytical process.

Conclusion

The future scholarship focused on the nexus of cyber security and economic security should begin to integrate the data presented in this article, from what is enshrined in Table 7 to the underlying data that fed it – and indeed to any as-yet undiscovered sources of data relevant to historical catastrophic cyber events. There finally exists a stake in the ground with regard to economic impact. While the data present may be imperfect, imperfectly collected, and imperfectly analyzed, it provides a desperately needed starting point for further study of catastrophic cyber events. This article should be seen as an invitation for criticism and further research rather than a final statement on the economic effects of historical catastrophic cyber events. In this manner, study at the nexus of cyber security and economic security can proceed more rigorously and meaningfully.

The newly formed dataset in Table 7 is certainly open to interpretation, disagreement, and even dismissal, but the fact that it must be acknowledged in doing so stands to fundamentally change the debate over the potential economic security implications of major cyber attacks, to include cyber war. The data provides a clear view of past economic loss activity from major cyber attacks in a manner that has never before been presented and enabling a new approach to analysis of the economic security implications of cyber security. The problems with the data cannot be ignored, and how those problems shaped the

54 Tom Johansmeyer, 2024e, "The narrow case for cyber insurance backstops," *Binding Hook*, 22 October, https://bindinghook.com/articles-binding-edge/the-narrow-case-for-cyber-insurance-backstops/.
55 Graham Steele, 2023, "Remarks by Assistant Secretary Graham Steele at the Federal Insurance Office and NYU Stern Volatility and Risk Institute Conference on Catastrophic Cyber Risk and a Potential Federal Insurance Response," *U.S. Department of the Treasury*, 17 November, https://home.treasury.gov/news/press-releases/jy1922.
56 Josephine Wolff, 2024, "Insurers will help define the threshold for cyberwar," *Binding Hook*, 4 July, https://bindinghook.com/articles-hooked-on-trends/insurers-will-help-define-the-threshold-for-cyberwar/.

methodology further complicates the credibility of the dataset, but that is a small price to pay for a new starting point for analysis that has been impossible in the past.

More important than the data presented, though, is what comes next. The estimates accompanying the twenty-four events in Table 7 are formed through a process heavily reliant on both judgment and contextless data from questionable sources. For this reason, the underlying data has been provided in Appendix A to encourage further work on Figure 8 and the development of new and better sources and methods for addressing the problem of historical data for catastrophic cyber attacks. Again, to view this Conclusion as anything other than a series of possible next steps is to miss the point of this article and the study within it entirely.

Future scholarship using Table 7 and Appendix A could proceed along a number of dimensions. First, there is the possibility that the twenty-four events do not form a complete historical record. Either by modifying the $800 million threshold or simply conducting additional research, it may be possible to find additional events to be included. Further, one could look prior to 1998 for events like the Morris worm. Additionally, one could find publicly available estimates not found through the course of the study in this article, which could either affirm or call into question the estimates selected for Table 7. The evolution of estimates is not only possible but encouraged, as such refinement will help improve future study of cyber and economic security strategy. The methodology used in this article could be modified in ways that lead to different estimates – a possibility that is welcome, as well. Finally, future scholars may find ways to reverse engineer the estimates available in the public domain or create new ways to produce such estimates. There are many possibilities for future scholarship, and the most interesting are likely to disagree with the findings of this article.

For now, however, what is most important is to take the estimates in this article and use them to take a fresh look at the problem of economic security strategy with regard to cyber strategy. The historical record is no longer barren. Further, the newly formed historical record suggests that a new look at the potential impacts of catastrophic cyber events – to include cyber war – is necessary. How scholars perceive the cyber threat needs to evolve from doomsday prophecy to a view that at least contemplates twenty-seven years of experience.

Appendix A: Full List of Sources of Cyber Catastrophe Economic Loss Estimates

108 Congress, "Computer Viruses: The Disease, the Detection, and the Prescription for Protection," House Hearing, 6 November, 2003, https://www.govinfo.gov/content/pkg/CHRG-108hhrg90727/html/CHRG-108hhrg90727.htm.

Beattie, Andrew, "The Most Devastating Computer Viruses," Techopedia, 11 March 2012, https://www.techopedia.com/2/26178/security/the-most-devastating-computer-viruses.

Berr, Jonathan, "'WannaCry' ransomware attack losses could reach $4 billion," CBS News, 16 May 2017, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

Cyware Hacker News, "Most Expensive Computer Viruses of All Time," Cyware Hacker News. 30 August 2016, https://cyware.com/news/most-expensive-computer-viruses-of-all-time-de0d5fae.

Dignan, Larry, "UnitedHealth sees $1.35 billion to $1.6 billion hit in 2024 due to Change Healthcare cyberattack," Constellation Research, 16 April 2024, https://www.constellationr.com/blog-news/insights/unitedhealth-sees-135-billion-16-billion-hit-2024-due-change-healthcare.

Federal Bureau of Investigation (FBI), "Melissa Virus," FBI, n.d., https://www.fbi.gov/history/famous-cases/melissa-virus.

Gerencer, Tom, "The Top 10 Worst Computer Viruses in History," HP Tech Takes, 4 November 2020, https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history.

Greenberg, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Guidewire Staff, "The Financial Impact of the CrowdStrike Global IT Outage," Guidewire Blog, 25 July 2024, https://www.guidewire.com/resources/blog/technology/the-financial-impact-of-the-crowdstrike-global-it-outage.

Haury, Amanda, "10 Of The Most Costly Computer Viruses Of All Time," Yahoo! Finance, 31 May 2012, https://finance.yahoo.com/news/10-most-costly-computer-viruses-192415030.html.

Johansmeyer, Tom "How Bad Can Systemic Cyber Get?" ASTIN, 7th ASTIN Cyber Workshop – A market set for growth, 30 October 2023, https://doi.org/10.13140/rg.2.2.23767.48801.

Leman, Jennifer, "11 Malware Attacks That Nearly Wrecked the Internet," Popular Mechanics, 31 October 2019, https://www.popularmechanics.com/technology/security/g29625471/history-of-malware-attacks/?slide=11.

Lemos, Robert, "Counting the cost of Slammer," Cnet, 2 February 2003,

https://www.cnet.com/tech/tech-industry/counting-the-cost-of-slammer/.

Leyden, John, "Why is mi2g so unpopular?" The Register, 21 November 2002, https://www.theregister.com/2002/11/21/why$_i s_m i2g_s o_u npopular$/.

Mi2g, "MyDoom becomes most damaging malware as SCO is paralysed," Mi2g, 1 February 2004, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/010204.php.

Mi2g, "Minmail to become 4th worst malware over weekend," Mi2g, 21 November 2003, http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/211103.php.

Moes, Tibor, "Cybercrime Examples (2023): The 10 Worst Attacks of All Time, Software Lab, May 2023, https://softwarelab.org/blog/cybercrime-examples/.

Page, Carly, "MOVEit, the biggest hack of the year, by the numbers," TechCrunch, 25 August 2023, https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/.

Parametrix, Crowdstrike's Impact on the Fortune 500: An Impact Analysis, 2024, https://www.parametrixinsurance.com/crowdstrike-outage-impact-on-the-fortune-500.

Smith, Christopher, "Dealers Are Set to Lose Nearly $1 Billion Over CDK Cyberattack [UPDATE]," Motor1, 1 July 2024, https://www.motor1.com/news/725118/dealers-lose-1-billion-cdk-cyberattack/.

Appendix B: Discussion about MOVEit's estimated economic impact

The range for economic losses from MOVEit, for example, stretches from $9.9-15.8 billion, with two sources. Both sources – blog TechCrunch[57] and a report by cyber security company Emsisoft[58] – use the number of records as a blunt instrument and multiply that by a standard cost per record of $165 from IBM. The IBM methodology for "mega data breach" losses, which would cover MOVEit, is a bit thin, relies on simulations, and may not account for such issues as record duplication among victims. Further, there are cues as to the prospect that the estimates are inflated. Examples include Wilton Re and Nuance Communications.

Wilton Re's exposure to the MOVEit loss, per Emsisoft, would be approximately $198 million, based on the IBM estimate of $165 per record. That's nearly 80% of its 2022 life and health premium.[59] Additionally, it is an awfully large economic consequence for a breach sustained by a relatively small company. For reference, that's nearly 2% of the economic loss sustained worldwide by NotPetya (not indexed for inflation). It seems unrealistic.

Nuance Communications offers a unique opportunity for analysis, given that it was a named and publicly reported victim of NotPetya in 20217. At the time, Nuance experienced a $90 million economic loss which is equivalent to $107.5 million in 2023 at an annual

57 Page, 2023.

58 Zack Simas, 2023, "Unpacking the MOVEit Breach: Statistics and Analysis," *Emsisoft Blog*, 18 July, https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

59 Wilton Re, 2023, *Annual Statement for the Year Ended December 31, 2022 of the Condition and Affairs of the Wilton Reassurance Company*, n.d., https://www.wiltonre.bm/wp-content/uploads/2023/05/WREB-Audited-GAAP-Financial-Statements-2022.pdf.

inflation rate of 3%.[60] According to the analysis provided by Emsisoft, the economic loss Nuance Communications sustained by Nuance would have reached $198 million, because it was exposed to the same number of lost records (1.2 million) as Wilton Re. The obvious question is whether the economic damage caused by MOVEit could be compared to that of NotPetya, which seems unlikely given the magnitude and global impact of the latter.

Informal interviews with several insurers and reinsurers exposed to cyber insurance losses from MOVEit suggest an industry-wide insured loss estimate of approximately $700 million. Further, those discussions suggest an absence of "runaway losses" – economic consequences that far exceed the insurance protection available. When asked if they believed the economic loss to be below $1 billion, all agreed.

Appendix C: Discussion about Crowdstrike's estimated economic impact

The recent Crowdstrike loss has benefited from considerable analysis as a result of being high-profile, despite being relatively small on an economic basis. Two major economic loss estimates have been released. The first, $5.4 billion, came early after the event from cyber analytics firm Parametrix [61]. The second is also from a cyber analytics firm, Cyence, which features in the analysis for historical economic loss estimates earlier in this article. The Cyence range is $1-3 billion with a "best estimate" of $1.7 billion.[62] Both firms are credible, although the transparency offered by Cyence is helpful, if narrowly focused on the airline sector.

The industry-wide insured loss estimates for the cyber event may be helpful, although there is some noise. Four major estimate ranges are offered.[63] Cyber analytics firm CyberCube has $400 million to $1.5 billion, with Paramtrix at $500 million to $1.1 billion. Reinsurance intermediary Guy Carpenter estimates $300 million to $1 billion, and cyber insurer coalition estimates $300 million to $900 million, although for the United States only. The insured loss estimates are helpful in this regard. Taking the $500 million loss and applying the 10% insurance penetration estimate[64] leads approximately to the Parametrix economic loss estimate of $5.4 billion. However, a straight market share analysis may not make sense, given the other 2023-4 losses, where economic impacts are believed not to have far outpaced insurance exposure (see MOVEit, Change Healthcare, and CDK, above). In evaluating Crowdstrike within the context of recent losses, Cyence's $1.7 billion economic loss estimate seems far more realistic.

60 Ionut Arghire, 2018, "Nuance Estimates NotPetya Impact at $90 Million," *SecurityWeek*, 2 March, https://www.securityweek.com/nuance-estimates-notpetya-impact-90-million/.
61 Parametrix, 2024.
62 Staff, 2024.
63 Catrin Shi, 2024, "Microsoft/Crowdstrike industry loss likely in low single-digit billions: Beazley's Cox," *Insurance Insider*, 8 August, https://www.insuranceinsider.com/article/2dlod250b03y26yx2uvb4/london-market/microsoft-crowdstrike-industry-loss-likely-in-low-single-digit-billions-beazleys-cox.
64 Gareth Mott, Sarah Turner, Jason R.C. Nurse, Jamie MacColl, James Sullivan, Anna Cartwright, and Edward Cartwright, 2023, "Between a rock and a hard(ening) place: Cyber insurance in the ransomware era," *Computers & Security*, vol. 128, p. 11, https://doi.org/10.1016/j.cose.2023.103162.

Author

Tom Johansmeyer is co-lead of the economic and legal warfare project at the Irregular Warfare Institute, an early research member of the Institute of Cyber Security for Society (iCSS), and a Ph.D. candidate at the University of Kent, Canterbury, where he is researching the nexus of economc and cyber security with regard to cyber war. Based in Bermuda and also working in the reinsurance industry, he previously led Property Claim Services at Verisk, estimating the cost of disasters worldwide. Tom also has an M.A. in global diplomacy from SOAS, University of London; an M.B.A. in accounting from Suffolk University (Boston), and an A.B. in philosophy and history from Ripon College (Wisconsin). He is a veteran of the U.S. Army.