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

Could a Cyber Attack Meaningfully Impact GDP?
Using Natural Disasters to Better Understand the Economic Effects of Cyber Attacks

Tom Johansmeyer[1]

Abstract

Fears that a major cyber event – a "cyber catastrophe" – could cause significant impairment to gross domestic product (GDP) has long been implied through discussion of potential severity. However, this article is the first to test the effects of historical cyber catastrophe on GDP. Using GDP as a common reference point, the study uses a comparison of cyber catastrophe economic losses to those from natural disasters in order to show how severe the economic consequences of a cyber catastrophe would have to become in order to achieve materiality. Building on limited prior research in the space, this article offers the first formal comparison of cyber catastrophe and natural disaster economic losses as a signal regarding potential impact, which can be used to inform cyber security strategy.

Keywords: Security strategy, cyber security, economic security, natural disasters

1 Co-director, Economic and Legal Warfare Project, Irregular Warfare Initiative; editor-in-chief, Journal of Strategic Competition; early career researcher, Institute of Cyber Security for Society (iCSS), University of Kent; PhD Candidate; University of Kent, Canterbury.

Introduction

Some—such from insurance marketplace Lloyd's of London[2] to insurance scholars Martin Eling, Mauro Elvedi, and Greg Falco[3] and even the (first) Trump administration[4]—believe the economic damage possible from cyber attacks could reach profound levels. Moreover, the hypothetical quanta suggested can get frighteningly large. From the potential for $3.5 trillion in economic harm[5] to the concern that "[w]e are witnessing the rapid unfolding of an international cyber arms race,"[6] there has been no shortage of cataclysmic predictions. Of course, there is a real threat. The cyber domain has legitimately been called a "a field of confrontations,"[7] and in 2016, the North Atlantic Treaty Organization (NATO) identified cyber as "an operational military domain."[8] States regularly engage in offensive cyber operations, and the increased professionalization of cyber forces suggests that commitments to this domain are only poised to grow.

However, the extent to which economic harm can be affected via this field of confrontations is a different matter. There have been plenty of instances of fear-mongering and hyperbolizing,[9] but little to show that the economic effects of major cyber attacks can reach the levels feared. The gap between fear and empirical evidence is what led to the research question for this article: Could a cyber attack have sufficiently large economic consequences to meaningfully impact on a country's gross domestic product (GDP)?

Through original research and the novel application of recently developed data sets, this article shows that the GDP effects of major cyber attacks have been relatively small. Relative to GDP, cyber attacks have failed to achieve materiality. To make this determination, historical cyber catastrophe data as a percentage of GDP is compared to an independent threshold of GDP materiality developed by insurance scholars Eling, et al,[10] Further, the GDP impacts of major natural disasters are compared against the same scale, making it possible to understand more fully how short cyber attacks have fallen in severity in this regard. The limited effects of major cyber attacks suggest this threat could be

2 Lloyd's of London, n.d., "Counting the economic cost: How vulnerable could you be?" *Lloyd's*, https://www.lloyds.com/news-and-insights/futureset/futureset-insights/systemic-risk-scenarios/illuminating-cyber-crime/economic-impact.

3 Martin Eling, Mauro Elvedi, and Greg Falco, 2022, "The Economic Impact of Extreme Cyber Risk Scenarios," *North American Actuarial Journal*, vol. 27, no. 3, pp. 429-443, https://doi.org/10.1080/10920277.2022.2034507.

4 Press Secretary, 2018, "Statement from the Press Secretary," *Trump White House Archives*, 15 February, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

5 Lloyd's of London, n.d., "Counting the economic cost."

6 Mette Eilstrup-Sangiovanni, 2018, "Why the World Needs an International Cyber Convention," *Philosophy and Technology*, 31, p. 2, https://doi.org/10.1007/s13347-017-0271-5.

7 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.

8 Douzet and Gery, 2021, p. 99.

9 Tom Johansmeyer, 2024, "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/.

10 Eling, et al., 2022, p. 429.

reprioritized, at least within the context of economic security strategy. As an economic threat, cyber may be more manageable than previously believed.

Their use as a reference point for understanding the effects of natural disasters goes at least as far back as 2004, with the work of Cashell, et al.,[11] has appeared in a study focused on the cost of cyber attacks in Japan,[12] more recently has been applied globally.[13] The comparison reveals that historical cyber disasters – the worst of which occurred more than twenty years ago – had minimal GDP impact, which is objectively verifiable. Meanwhile, major natural disasters have led to economic devastation, a fact that is also objectively verifiable. The fact cyber losses have been far smaller than those from noteworthy natural disasters indicates generally that the ability to absorb economic shock events is far greater than the impacts caused by even the most severe cyber events.

The national security implications of this article's findings are both relevant and applicable. Economic security forms an important aspect of national security strategy, as one of the five security "sectors" offered by Buzan, et al.[14] As a result, the misunderstanding of the potential economic threat possible from major cyber attacks could lead to suboptimal national security strategy and policy. The quantification of past cyber events and their comparison to non-cyber events of much larger economic magnitude contextualizes the threat, allowing for improved strategy formulation and resource allocation in execution.

Literature Review

Security strategy has evolved from a discipline once focused on military matters to a more expansive set of concerns that includes environmental, societal, political, and economic security.[15] Specifically, according to Nye, economic security requires the balancing public welfare benefits against a reduction of autonomy.[16] While economic security can be interpreted broadly,[17] Buzan keeps the focus on "access to the resources, finance and markets

11 Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, 2004, "The Economic Impact of Cyber attacks," *CRS Report for Congress*, 1 April, p. 38, https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf.

12 Akiyoshi Kokaji and Atsuhiro Goto, 2022, "An analysis of economic losses from cyberattacks: based on input–output model and production function," *Journal of Economic Structures*, vol. 11, no. 34, p. 2, https://doi.org/10.1186/s40008-022-00286-4.

13 For precedent in measuring cyber attacks against natural disasters, please see Tom Johansmeyer, 2025, "Bad decisions have consequences: how cyber security could fall victim to climate change," *British Actuarial Journal*, vol. 30, e15, pp. 1-15, https://doi.org/10.1017/S1357321725000091. See also Tom Johansmeyer, 2025, "Lights Out: What Hurricanes Reveal about Cyberattacks and Blackouts," *Cyber Defense Review*, vol. 10, no. 1, pp. 73-92, https://doi.org/10.55682/cdr/qw13-9v8c.

14 Barry Buzan, Ole Waever, and Jaap de Wilde, 1998, *Security: A New Framework for Analysis*, Boulder: Lynne Rienner Publishers, p. 7, https://doi.org/10.2307/2586187.

15 Buzan, et al., 1988, p. 7.

16 Joseph S. Nye, 1974, "Collective Economic Security," *International Affairs*, vol. 50, no. 4, p. 588, https://doi.org/10.2307/2615925.

17 Matteo G. Richiardi and Zhechun He, 2020, "Measuring economic insecurity: A review of the literature," *CeMPA Working Paper Series*, June, p. 2, https://www.iser.essex.ac.uk/wp-content/uploads/files/working-papers/cempa/cempa1-20.pdf.

necessary to sustain acceptable levels of welfare and state power."[18] Economic security has been included in national security strategies,[19] with the connection between economic and cyber security established both by the economic effects of impeded business activity due to cyber attacks but also through the reliance of technology systems to support economic activity in general.[20]

Because of the clear links among cyber, economic, and national security, the fear of a major cyber attack and its potential economic consequences have become well established in the historical literature. Concerns about runaway malware,[21] spillover from offensive cyber operations,[22] and prolonged outages of key utilities and services[23] (from the power grid[24] to the water supply[25]) have led to the imagination[26] of cataclysmic scenarios and vast economic consequences. The end result involves the prospect of a single catastrophic cyber attack bearing sufficient weight to impact the victim state's GDP. However, recent research with regard to the potential economic quantum of major cyber attacks provides the foundation for a robust debate about the potential economic effects of catastrophic cyber attacks and whether they could reach sufficient size to have a meaningful impact to GDP.

Perceptions of a heightened threat

The notion that the economic effects of major cyber attacks can be benchmarked to any measure is relatively new. Historically, the prevailing view has been that the cyber domain's history in general has been short, as it is a new environment.[27] There has been a perceived paucity of historical events,[28] none of which have reached any meaningful level of

18 Barry Buzan, 1991, "New Patterns of Global Security in the Twenty-First Century," *International Affairs*, vol. 67, no. 3, p. 433, https://doi.org/10.2307/2621945.

19 Tom Johansmeyer, Gareth Mott, and Jason R.C. Nurse, 2024, "Cyber Strategy in Practice: The Evolution of US, Russian and Ukrainian National Cyber Security Strategies through the Experience of War," *RUSI Journal*, vol. 169, iss. 3, pp. 43-4, https://doi.org/10.1080/03071847.2024.2377544.

20 Johansmeyer, et al., 2024, pp. 46-7.

21 Cambridge Centre for Risk Studies, Lloyd's of London, and Nanyang Technological University, 2019, *Bashe attack: Global infection by contagious malware*, pp. 12-18, https://assets.lloyds.com/assets/pdf-bashe-attack-cyrimbasheattack-finalbashe-attack/1/pdf-bashe-attack-CyRiMBasheAttack_FINALbashe-attack.pdf.

22 Alexander Braun, Martin Eling, and Christoph Jaenicke, 2023, "Cyber insurance-linked securities," *ASTIN Bulletin: The Journal of the IAA*, vol. 53, iss. 3, p. 685, https://doi.org/10.1017/asb.2023.22.

23 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 (IJSPTM)*, vol. 12, no. 1, p. 9, https://doi.org/10.5121/ijsptm.2023.12101.

24 Johansmeyer, 2025, "Lights Out."

25 Alexander Martin, 2025, "Hackers are attacking Britain's drinking water suppliers," *The Record*, 3 November, https://therecord.media/britain-water-supply-cybersecurity-incident-reports-dwi-nis.

26 James Lewis, 2020, "Dismissing Cyber Catastrophe," *Center for Strategic and International Studies*, 17 August, https://www.csis.org/analysis/dismissing-cyber-catastrophe.

27 Gallagher Re and CyberCube, 2024," *A History of Near Misses: Utilizing counterfactual analysis to understand cyber risk*, n.d., p. 2, https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/2024/gallagherre-a-history-of-near-misses-counterfactual-analysis.pdf.

28 Tom Johansmeyer, 2024, "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, p.

materiality.[29] It is difficult to study a problem for which there is very little data and a short history, where a "lack of data restrains the quality" of potential cyber catastrophe "statistical and actuarial examinations,"[30] making it necessary to accept considerable conjecture and extrapolation from what little is known and accepted.[31] Because of this prevailing perception, there is an ongoing problem of relatability. Absent intuitive reference points, it is difficult to describe the impact of cyber attacks, as they are not "as intuitively relatable as bomb craters and war ruins."[32]

It is generally accepted that the lack of historical precedent has made the problem of "cyber catastrophes" more difficult to study. In fact, the cyber catastrophe label is itself not without controversy. This article uses the definition set by Johansmeyer[33] – and based generally on insurance industry catastrophe event designation bodies like PCS[34] – that a cyber catastrophe should affect a large number of victims (qualitative threshold) and result in an aggregate economic loss of at least $800 million from a single cause.[35] This definition, which is designed to maximize the number of historical events captured,[36] still leaves researchers with a thin historical record, which in turn frustrates the use of traditional statistical methods.

Further, within the context of cyber catastrophes, is the belief that what has happened so far is not indicative of the severity that future cyber catastrophe events could achieve. Pain, for example, advances the notion that there has not been a true cyber catastrophe "yet,"[37] although he adds that part of this may be a problem of terminology and language, given how new cyber catastrophe risk is and how little attention it has received so far.[38] Past research and analysis on cyber catastrophe quantification thus generally has been limited to specific scenarios against limited sets of data at best,[39] forecasts relying heavily on extrapolation, and declarations of magnitude with lean attendant analysis or support. Historical views of the economic damage that can come from cyber attacks dates back at least to the Morris Worm of 1988,[40] and what followed included a period of contemplating

7, https://jrmi.au.edu/index.php/jrmi/article/view/287/189.

29 Johansmeyer, 2025, "Bad Decisions."

30 Daniel Zangerle and Dirk Schiereck, 2023, "Modelling and predicting enterprise-level cyber risks in the context of sparse data availability," *The Geneva Papers on Risk and Insurance – Issues and Practice*, vol. 48, p. 435, https://doi.org/10.1057/s41288-022-00282-6.

31 Tom Johansmeyer, 2024, "How Cyber Model Vendors See Their Role in Closing the Cyber Insurance Protection Gap," *Journal of Insurance Issues*, vol. 47, no. 1, p. 126, https://www.jstor.org/stable/48770675.

32 Johansmeyer, 2024, "Cyber Attacks in Perspective."

33 Tom Johansmeyer, 2026, "Rewriting History: Understanding Historical Catastrophic Cyber Economic Losses," *Journal of Strategic Competition*, vol. 2, no. 1, p. 5, https://strategiccompetition.org/index.php/josc/article/view/22/3.

34 Tom Johansmeyer, 2024, "Surprising stats: the worst economic losses from cyber catastrophes," *The Loop: ECPR's Political Science Blog*, 12 March, https://theloop.ecpr.eu/surprising-stats-the-worst-economic-losses-from-cyber-catastrophes.

35 Johansmeyer, 2024, "Surprising stats."

36 Johansmeyer, 2024, "Surprising stats."

37 Darren Pain, 2023, *Cyber Risks Accumulation: Fully tackling the insurability challenge*, November, p. 32, https://www.genevaassociation.org/sites/default/files/2023-11/cyber_accumulation_report_91123.pdf.

38 Pain, 2023, p. 16.

39 E.g., Eling et al., "Economic Impact," 2023.

40 Johansmeyer, 2024, "Perception Shapes Reality," p. 3.

the potential impacts to shareholder value from cyber attacks. For example, early studies of the effects of cyber attacks on company share price (from before the year 2000 and even for a few years after) can be seen as overstating impact, even when one accounts for such factors as novelty and fear. Share price movements post-attack were studied over a period of days and parsed by attack type (e.g., denial of service versus website defacement) to examine what would be most problematic.[41] However, a shortcoming of the study of share price impacts in the days after a cyber attack is that they "do not attempt to determine if there is any persistent change in stock prices, or if the drop in stock prices is temporary."[42]

Even if, as Cashell, et al., observe, meager decline could translate to hundreds of millions of dollars in lost shareholder value, such losses may be transitory, and a recovery in price necessarily obviates the impact of the attack. In fact, meaningful and enduring impacts to share price have been reserved for cases where the victim company has other factors that lead to investor concerns, such as the large amount of personally identifiable information compromised during the 2017 Equifax breach[43] and the national security implications of the 2020 attack on SolarWinds. Given that the effects of single-company victims as meaningful percentages of market capitalization are rare, systemic effect is necessarily rarer.

In parallel with the analysis of cyber attack impacts on shareholder value came the development of more rigorous and specific estimated economic impacts from cyber events seems to have begun with a 2015 Lloyd's report that suggested a cyber-induced blackout could leave 93 million without power and cause economic losses of $243 billion to "more than" $1 trillion.[44] The low end of that range would have constituted 1.33 percent of U.S. GDP, with the high end of economic impact at 5.46 percent.[45] While the estimate speaks to the prevailing perspective at the time, it should be noted that the reference event used for the Lloyd's study was the 2003 blackout in the northeastern United States and southern Canada, although it did not result from a cyber attack.[46] The event cut power for approximately 50 million[47] for up to twenty-nine hours. Despite affecting 54 percent of the 93 million people used in the 2015 Lloyd's scenario, for the 2003 event, the economic impact was far less severe, at less than $10 billion.[48]

More recently, a 2023 Lloyd's study developed with the Cambridge Centre for Risk

---

41 Cashell, et al., 2004, p. 5.

42 Cashell, et al., 2004, p. 5.

43 Kelly Sheridan, 2021, "How Much Do Cyberattacks Affect Stock Price? Depends on The Breach," *Dark Reading*, 27 April, https://www.darkreading.com/threat-intelligence/do-cyberattacks-affect-stock-prices-it-depends-on-the-breach.

44 "Business blackout," *Lloyd's*, last modified July 6, 2015, https://www.lloyds.com/news-and-insights/risk-reports/library/business-blackout.

45 "GDP (current US$) - United States," *World Bank Group*, 2026, n.d., https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US.

46 As a reference event, the 2003 is the base event, and the scenario then uses a cyber attack as the hypothetical cause. This is different from what transpired, but it could be said to provide enough of a basis in reality to be useful as a model event. As the analysis shows, however, the reference event's consequences are far less severe than those in the hypothetical.

47 Eyewitness News, 2023, "'From lights out to lights on': 20 years since the 2003 blackout," *abc7NY*, 14 August, https://abc7ny.com/2003-blackout-nyc-20-years-power-outage/13646160/.

48 Electricity Consumers Resource Council (ELCON) *The Economic Impacts of the August 2023 Blackout*, 9 February, p. 1, https://www.nrc.gov/docs/ml1113/ml111300584.pdf.

Studies estimated that a systemic cyber attack on the global financial system could cause \$3.5 trillion in economic damage over five years.[49] Again, presumably heavy on extrapolation and with little foundation in historical data, it is noteworthy for its reflection of sentiment as to the potential effects of a systemic cyber event. Given the five-year scope of the impact, taking 20 percent of the estimate (\$700 billion) represents more than 7 percent of 2023 global GDP, the last year for which data is available from the World Bank. This approach is conservative, because the impact would likely be more significant in the earlier years, and even on this conservative basis, the forecast is extreme (with no transparency as to the methodology used or other aspects of the study). Finally, the low-end estimate of \$2.2 trillion has been assigned a return period of 1-in-30,[50] meaning it could be expected to occur once every thirty years. Compared to the historical economic cyber catastrophe loss experience to be revealed below, this is questionable.

The hypothetical scenario published by Lloyd's provides an economic impact that deviates significantly from the historical record, although in the years that followed, estimates of economic severity from catastrophic cyber attacks have tended to move downward. For example, a scenario published by Lloyd's of London with cyber analytics firm puts the potential economic effects of a range of major cyber events at more reasonable levels. The estimates for the cloud scenario, for example, range from "large" at an economic loss of \$46 billion to "extreme" at \$53.05 billion, and those for the mass vulnerability interruption stretch from \$9.68 billion to \$28.72 billion.[51] While the results are lower than the other examples above – and thus indicative of a smaller GDP effect – they show the perils of extrapolation and estimation without the availability of a stable and widely accepted historical record.[52]

Some progress has been made toward a more uniform starting point for the underlying analysis supporting such forecasts. A recent body of work developed since 2019 provides the ability to address the problems with cyber catastrophe loss quantification and comparison in the historical literature. It has yielded what has become the first historical database of cyber catastrophe economic losses[53] – a data set that features below in this study. What exists now (and is used in Table 1, below) began as an informal list of historical cyber catastrophe events produced in 2019 by PCS, a division of insurance analytics firm Verisk, to show past scale in order to help the cyber insurance and reinsurance ("re/insurance") market better understand systemic risk.[54] At the time, this exercise was simply conducted to provide an example. The methodology and data set were formalized

49 "Lloyd's systemic risk scenario reveals global economy exposed to \$3.5trn from major cyber attack," *Lloyd's*, 2023, 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.

50 I.e., on average, it is the sort of event that can be expected to occur once in a thirty-year time horizon.

51 Lloyd's and Cyence, 2017, *Counting the cost: Cyber exposure decoded*, n.d., London: Lloyd's, p. 7, https://assets.lloyds.com/assets/pdf-emerging-risk-report-2017-counting-the-cost/1/pdf-emerging-risk-report-2017-counting-the-cost.pdf.

52 Johansmeyer, 2024, "How Cyber Model Vendors," p. 126.

53 Tom Johansmeyer, 2024, "Surprising stats."

54 Tom Johansmeyer, 2019, *Could NotPetya's Tail Be Growing?* n.d., Jersey City: Verisk, p. 1, https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf.

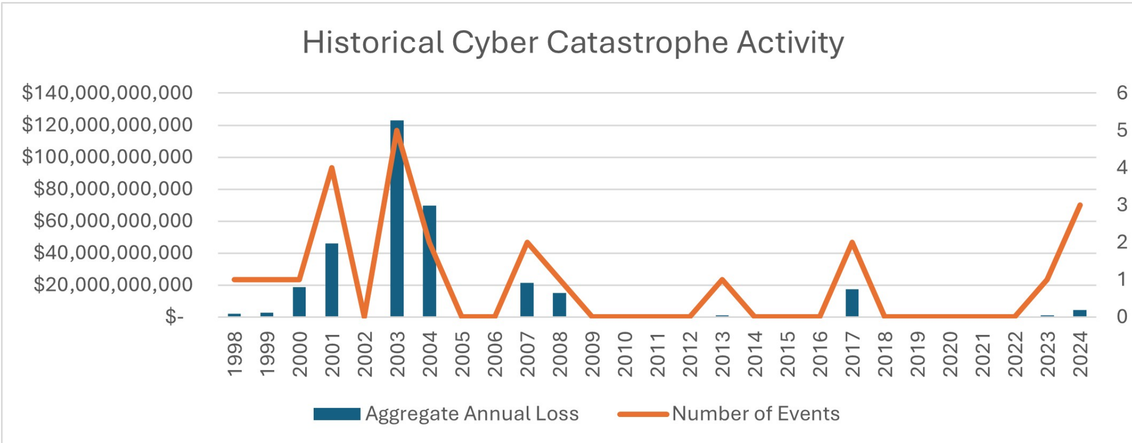

Figure 1: Annual Economic Losses from Cyber Catastrophe (Source: Johansmeyer, 2026).

and released in 2024,[55] with the inclusion of four new cyber catastrophe events: MOVEit, Change Healthcare, CDK, and Crowdstrike[56]).

As Figure 1[57] reveals, major cyber events – as measured by economic impact (and requiring a significant number of victims[58]) – have not reached the cataclysmic levels historically feared, with aggregate economic losses of only $326.4 billion (adjusted for inflation) since 1998.[59] Although there have been some difficult years (particularly 2003 and 2004), the economic effect of major cyber events has tended to be manageable, and the quanta of loss feared were never realized. However, the future potential remains an open question, despite the salient downward trend in Figure 1. Generally, this fear is rooted in the notion that the "big one"[60] simply has not happened "yet"[61] – and it is a matter of time until it does.[62]

55 Tom Johansmeyer, 2024, "Recent cyber catastrophes show an intensifying trend – but they are manageable," *The Loop: ECPR's Political Science Blog*, 25 September, https://theloop.ecpr.eu/recent-cyber-catastrophes-show-an-intensifying-trend-but-they-are-manageable/.

56 Tom Johansmeyer, 2024, "Crowdstrike reveals a 'small catastrophe' pattern in cyber insurance," *Binding Hook*, 23 August, https://bindinghook.com/crowdstrike-reveals-a-small-catastrophe-pattern-in-cyber-insurance/.

57 Although there is a robust debate over the effects of first-, second-, and further-order effects in the study of the economic impacts of cyber catastrophes, this article uses a pre-existing data set, obviating the need for this discussion. The data set used is built upon publicly available estimates of economic catastrophe events that imply a representation of the full economic loss, not just first- or second-order effects. Further, with regard to effects other than first order, there is evolving thinking that downstream effects may not be as robust as originally feared. See, for example, Howden, 2024, *Cyber insurance: Risk, resilience and relevance*, June, p. 25, https://www.howdengroupholdings.com/sites/default/files/2024-06/howden-2024-cyber-report.pdf.

58 Johansmeyer, 2026, p. 5.

59 Johansmeyer, 2024, "Recent cyber catastrophes."

60 Elizabeth Blosfield, 2021, "The Really, Really Big One: The Likelihood of a 1-in-100 Year Cyber Catastrophe," *Insurance Journal*, 12 May, https://www.insurancejournal.com/news/2021/05/12/613489.htm.

61 Pain, 2023, p. 32.

62 Peter Hoekstra and Brian Finch, 2013, "In dread of a cyber Pearl Harbor," *Politico*, 19 February,

Evolving Perspectives on Economic Harm from Major Cyber Attacks

The hypothesis that a major cyber attack could cause cataclysmic economic damage is common, but not uniformly accepted in existing literature. In fact, a body of work has emerged to address the limitations on the potential effects of cyber attacks and cyber weapons, suggesting that the potential for economic harm is actually quite limited. First, and most important, is the fact that no such cataclysmic event has occurred.[63] If the capabilities for a catastrophic cyber attack do exist, and if such attacks are indeed attempted regularly, then one is left to wonder why the economic effects of the attacks that have transpired have been so small (see Figure 1, above).

Despite the fears of a "cyber 9/11"[64] or a "cyber Pearl Harbor,"[65] nothing has come close to that sort of effect. In fact, even a "cyber Hurricane Andrew"[66] (although "cyber Katrina" is a better comparison[67]), has failed to materialize. One can contend that such an event has not occurred – if the capabilities for affecting one do exist – because of the potential for reprisals. The fact that an attack occurs via the cyber domain does not mean that the response will. Max Smeets emphasizes Erik Gartzke's claim that a cyber war "is not likely to serve as the final arbiter of conflict in an anarchic world,"[68] if for no other reason than Gartzke's other observation that "[t]here will not be a cyber Pearl Harbor, except possibly when and if a foreign power has decided it can stand toe-to-toe with conventional U.S. military power."[69] Further to this point, Lindsay contends, "Those who worry about a digital Pearl Harbor would do well to remember Japan's experience after the real Pearl Harbor."[70]

While the dynamics above exist regardless of whether offensive capabilities are sufficiently robust to do the sort of damage feared, there is scholarship to suggest that offensive cyber capabilities are inherently limited in their ability to inflict enduring harm. Smeets describes the effects of cyber weapons as "short-lived" and "temporary," going so far as to contrast them with the "Kalashnikovs mass-produced in the early 1950s."[71] For van Puyvelde and Brantly, the limitation of cyber weapons is that their effects are easier to reverse than the physical damage caused by kinetic attacks.[72] The reversibility of those

---

https://www.politico.com/story/2013/02/the-looming-certainty-of-a-cyber-pearl-harbor-087806.

63 Lewis, 2020.

64 Clifford S. Magee, 2013, "Awaiting Cyber 9/11," *Joint Force Quarterly*, vol. 73, 3rd Quarter, p. 78, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_76-82_Magee.pdf.

65 James J. Wirtz, 2017, "The Cyber Pearl Harbor," *Intelligence and National Security*, vol. 32, no. 6, p. 764, https://doi.org/10.1080/02684527.2017.1294379.

66 Johansmeyer, 2024, "Natural Catastrophes."

67 Andrew Lauland, 2016, "Rather Than Fearing 'Cyber 9/11,' Prepare for 'Cyber Katrina,'" *RAND*, 30 March, https://www.rand.org/pubs/commentary/2016/03/rather-than-fearing-cyber-911-prepare-for-cyber-katrina.html.

68 Max Smeets, 2018, "A matter of time: On the transitory nature of cyberweapons," *Journal of Strategic Studies*, vol. 41, nos. 1-2, p. 92, https://www.tandfonline.com/doi/full/10.1080/01402390.2017.1288107.

69 Erik Gartzke, 2013, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, vol. 38, no. 2, p. 68, https://www.jstor.org/stable/24480930.

70 Lindsay and Kello, 2014, p. 184.

71 Smeets, 2018, p. 6.

72 E. Lincoln Bonner III, 2014, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly*,

weapons remains a key constraint,[73] because, as Gartzke observes, "[t]o the degree that damage can be repaired quickly, there is not much leverage in raising" threats of force.[74]

While the developments in this area of research, described above, are encouraging with regard to a more realistic view of the potential effects of cyber catastrophe events, they do not use reference points of known economic impact from extreme events to make the point. Rather, they discuss the factors limiting the propagation of economic harm from cyber attacks, such as reversibility[75] and response dynamics. What has been missing has been a basis for comparison that shows the limited effects of cyber attacks with regard to economic impact.

Research Methodology

The decision to compare the effects of cyber attacks to natural disasters may not seem immediately intuitive. Cyber attacks are, by definition, intentional, and they inhabit a digital environment, which is both man-made and believed to be highly interconnected, resulting in the risk that impact can spread easily without regard to physical geography.[76] Natural disasters, on the other hand, are constrained geographically, both in terms of scope and in their likelihood to occur at all. For example, the prospect of a hurricane reaching the central United States (not in degraded form) is extremely remote, and earthquakes follow fault lines. They are also not intentionally conceived and executed.

The study of both thus is necessary to answer this article's research question: Could a cyber attack have sufficiently large economic consequences to meaningfully impact on a country's gross domestic product (GDP)? There are several reasons for this. First, natural disasters offer a useful basis for comparison because they are vast in economic effect, occur quite frequently (particularly compared to cyber catastrophes), and have a robust historical record. In fact, the estimation of economic loss from natural disasters dates back more than fifty years (per the data sets to be discussed below) and has been widely accepted in academic research and practitioner use. Both are extreme events believed to cause widespread economic effect. Further, both cyber catastrophes and natural disaster require human impact.

According to the United Nations Office for Disaster Risk Reduction (UNDRR), a disaster is "a serious disruption of a community or a society at any scale due to hazardous events interacting with conditions of exposure, vulnerability and capacity, leading to one or more

---

vol. 74, 3rd Quarter, p. 103, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_102-109_Bonner.pdf.

73 Josiah Dykstra, Chris Inglis, and Thomas S. Walcott, 2020, "Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat," *Joint Force Quarterly*, vol. 74, 3rd Quarter, p. 103, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_102-109_Bonner.pdf.

74 Gartzke, 2013, p. 56.

75 Dykstra, et al., 2020, p. 103.

76 Tom Johansmeyer, Gareth Mott, and Jason R.C. Nurse, 2025, "Invisible Lines, Visible Impact: How Territorial Security Influences Russian Cyber Security Strategy," *RUSI Journal*, vol. 170, iss. 1, p. 20, https://doi.org/10.1080/03071847.2025.2458143.

of the following: human, material, economic and environmental losses and impacts."[77] This is relevant both to natural and cyber events, with each simply being the manifestation of a core concept involving the widespread impact to a community or society. Further, Eling, et al., propose that for the economic effect of a disaster – natural or cyber – to be meaningful, it should at least impact a range of 0.2-2 percent of GDP, with those above 2 percent of GDP particularly severe.[78]

The process by which this article addresses the research question is first to gather historical economic loss data on both cyber catastrophes and natural disasters. The former uses the underlying research produced by Johansmeyer, as discussed in the literature review above, to provide the twenty-four historical cyber catastrophes that occurred from 1998-2025 (see Table 1 in the next section). The latter comes from the EM-DAT database, which contains more than 13,000 historical records.[79] Where necessary, EM-DAT is supplemented with data from Munich Re NatCatSERVICE[80] and Swiss Re sigma.[81] Natural disaster data going back to 1999 is considered, in order to align with the availability of the cyber economic loss data. Historical losses across both categories are adjusted for inflation using a forced 3 percent per year rate. While the process of adjusting for inflation is subject to debate, the use of this rate for both historical cyber and natural disaster events at least provides for a similar basis for comparison. Finally, the event loss data (both natural and cyber) is compared to GDP (and each other), relative to the threshold set by Eling, et al.

Historical Analysis

To understand calamitous events, one must turn to research done by Eling and colleagues. They suggest that a cyber event would have to affect 0.2-2 percent of a state's GDP to be truly impactful.[82] In their analysis of hypothetical cases of cyber catastrophe, the largest they can conceive has a 0.17 percent impact to global GDP, which translates to an economic loss of $35 billion in 2019 dollars.[83] As a result, even the hypothetical cases they fear would fail to become material on an economic loss basis, even with that hypothetical loss of $35 billion far exceeding anything that has transpired since at least 2008 (see Table 1, below).

Major cyber events and their economic implications

As Table 1 shows, there have been twenty-four cyber catastrophes since 1998. A basic review of the event history shows that over the twenty-six years from the beginning of

77 United Nations Office for Disaster Risk Reduction (UNDRR). n.d., "Disaster," *United Nations Office for Disaster Risk Recovery*, https://www.undrr.org/terminology/disaster.
78 Eling, et al., 2022, p. 429.
79 Centre for Research on the Epidemiology of Disasters (CRED), 2022, "EM-DAT Public Data," *EM-DAT: The International Disaster Database*, 1 February, https://public.emdat.be/data.
80 Munich Re, 2025, "Data on natural disasters since 1980: Munich Re's NatCatSERVICE," *Munich Re*, n.d., https://www.munichre.com/en/solutions/for-industry-clients/natcatservice.html.
81 Swiss Re, 2025, "sigma explorer," *Swiss Re Institute*, n.d., https://sigma.swissre.com/.
82 Eling, et al., 2022, p. 429.
83 Eling, et al., 2022, p. 430.

1999 through 31 August 2024, the average annual number of events was only 0.93, and the average annual aggregate economic loss, adjusted for inflation, reached a mere $12.1 billion. Further, there is some amount of unevenness, with only thirteen of the twenty-six years represented having any major cyber events at all, as shown in Figure 1, earlier in this article. The last year with an above-average annual aggregate loss was 2017 – and before that, 2007 and 2008.

Table 1: Historical Cyber Catastrophe Losses (1998-2025)

Event	Year	Loss at the Time	Inflation Adj. Econ. Loss (2025)
SoBig	2003	$37 billion	$73 billion
MyDoom	2004	$38 billion	$72.8 billion
Klez	2001	$19.8 billion	$41.5 billion
Yaha	2003	$11.1 billion	$73 billion
ILOVEYOU	2000	$15 billion	$32.3 billion
Swen	2003	$9.2 billion	$18.1 billion
StormWorm	2007	$10 billion	$17.5 billion
Minmail	2003	$8.9 billion	$17.5 billion
Conficker	2008	$9.1 billion	$15.9 billion
NotPetya	2017	$10 billion	$13 billion
Zeus	2007	$3 billion	$5.3 billion
WannaCry	2017	$4 billion	$5.2 billion
CodeRed	2001	$2.4 billion	$4.7 billion
Nimda	2001	$1.5 billion	$3.1 billion
Melissa	1999	$1.3 billion	$2.9 billion
SirCam	2001	$1.3 billion	$2.6 billion
SQL Slammer	2003	$1.2 billion	$2.4 billion
Chernobyl	1998	$1 billion	$2.3 billion
Change Healthcare	2024	$2 billion	$2 billion
CDK	2024	$2 billion	$2 billion
Crowdstrike	2024	$1.7 billion	$1.7 billion
MOVEit	2023	$1 billion	$1 billion
CryptoLocker	2013	$665 million	$980 million
Sasser	2004	$500 million	$960 million

Note: Source: Johansmeyer, 2026, p.16. Estimates not included in that article which have been added here by way of updated are individually sourced in Table 1.

On a standalone basis, it is difficult to understand what the economic impacts in Table 1 mean. One can see trends forming – such as the general decline in economic severity since 1998 – and it is easy to assume that impacts stretching into the billions of dollars are somehow "big." To assign richer meaning to the most significant cyber catastrophes by economic effect, though, it is necessary to compare them to other significant economic events, and that is facilitated by the GDP threshold of 0.2-2 percent set by Eling, Elvedi, and Falco, which is where they forecasted cyber catastrophe economic harm could land. Table 2 shows just how rarely this occurs.

Table 2: Historical Cyber Event Losses Relative to U.S. GDP

Event	Year	Economic Loss	Loss as a Percentage of GDP
Chernobyl	1998	$1 billion	0.01%
Melissa	1999	$1.3 billion	0.02%
ILOVEYOU	2000	$15 billion	0.15%
Klez	*2001*	*$19.8 billion*	*0.18%*
CodeRed	2001	$2.4 billion	0.02%
Nimda	2001	$1.5 billion	0.01%
SirCam	2001	$1.3 billion	0.01%
SoBig	**2003**	**$37 billion**	**0.32%**
SQL Slammer	2003	$1.2 billion	0.01%
Swen	2003	$9.2 billion	0.08%
Minmail	2003	$8.9 billion	0.08%
Yaha	2003	$11.1 billion	0.1%
MyDoom	**2004**	**$38 billion**	**0.32%**
Sasser	2004	$500 million	0.004%
StormWorm	2007	$10 billion	0.07%
Conficker	2008	$9.1 billion	0.06%
Zeus	2007	$3 billion	0.02%
CryptoLocker	2013	$665 million	0.004%
NotPetya	2017	$10 billion	0.05%
WannaCry	2017	$4 billion	0.02%
MOVEit	2023	$1 billion	0.004%
CDK	2024	$2 billion	0.007%
Change Healthcare	2024	$2 billion	0.009%
Crowdstrike	2024	$1.7 billion	0.006%

Note: Sources: Johansmeyer, 2026, p. 5, and Countryeconomy.com, 2023.

Simply by expressing economic effect relative to GDP, it becomes easier to understand by reference. However, this leads to the question of which country's GDP to use. Given that cyber events are often considered "borderless" – although sometimes erroneously[84] – it may be tempting to use global GDP. Doing so, unfortunately, would mask any localized concentration of effect (given that cyber is not as diffuse as some might believe), which in turn could make the effects look less onerous. Because cyber events have been relatively small on an economic basis – even if in comparison to the hypothetical case provided by

84 Johansmeyer, Mott, and Nurse, 2025, p. 20.

Eling, et al., of $35 billion[85] – the analysis in Table 2 intentionally stresses the scenarios considered by comparing them only to the GDP of the United States only, even though some are multinational in scale. Even with this artificially narrowed constraint, shown in Table 2 below, only two reach the GDP threshold set by Eling, et al. – SoBig (0.32%) and MyDoom (0.32%). Another one, Klez, comes close to the bottom end, at 0.18%. Even in the most severe cases of cyber catastrophe, though, it appears that natural catastrophes are far more impactful – and that more impactful natural catastrophes are far more frequent.

Major natural disaster events and their economic implications

The direct economic losses associated with natural disasters are staggering in scale, particularly in comparison to the cyber data above. Moreover, the problem is not limited to developed and mature markets. Natural disasters exact an economic toll in countries large and small, those with developed and emerging economies, and those of different sizes, locations, and populations. While it may be tempting to look at large economies on fault lines or in water-adjacent tropical areas, the expensive reality is far broader. In 2022 alone, Munich Re reports worldwide economic losses of US$270 billion, and although most of it comes from the United States, due to Hurricane Ian.[86]

A review of the historical natural disaster loss data in EM-DAT makes immediately clear the difference in scale between this risk and cyber. Just the major events in Table 3 below – only twenty since 1999 of more than 13,000 in EM-DAT since 1970, add up to $1.7 trillion in economic impact (adjusted for inflation to 2025). The largest is the 2011 Tohoku earthquake and tsunami, which using 3% inflation (as in the analysis of cyber event losses above) yields a total economic loss of $318 billion in 2023 dollars. Hurricane Katrina, which struck the United States in 2005, is next at an inflation-adjusted $207 billion. Adjusted for inflation, three more events exceed $100 billion, as shown in Table 3 below. Further, all of them are over $20 billion on that basis (compared to just the four largest cyber events in Table 1).

Table 3 shows the loss events span eight regions – seven countries with the eighth region, Europe, not broken down by country in the data available in EM-DAT. The United States is affected most frequently with nine events, followed by China with four and Japan with three. Economically, the United States is again most affected, with US$800 billion in losses from the events in Table 3, followed by Japan with half that. Of course, these three countries are among the world's largest by GDP, with the United States first, China second, and Japan fourth.[87] The fact that they are also disaster-prone and their sheer size makes it unsurprising that they would suffer the greatest absolute economic effects from natural disasters. However, the fact that there are smaller countries by GDP in Table 3 –

85 Eling, et al., 2022, p. 430.

86 Brittney Meredith-Miller, 2023, "Munich Re: Natural disasters caused losses of $270B in 2022," *PropertyCasualty360*, 12 January, https://www.propertycasualty360.com/2023/01/12/munich-re-natural-disasters-caused-losses-of-270b-in-2022/?slreturn=20230523063133.

87 World Bank, 2025, "GDP (Current US$)," *World Bank Group — Data*, n.d., https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true.

Table 3: Largest Historical Natural Disasters by Economic Loss

Event	Country	Year	Original Econ. Loss	Adjusted Econ. Loss	Loss as % of GDP
Tohoku earthquake	Japan	2011	$210 billion	$318 billion	3.37%
Hurricane Katrina	United States	2005	$125 billion	$226 billion	0.97%
Sichuan earthquake	China	2008	$85 billion	$140 billion	1.86%
Hurricane Harvey	United States	2017	$95 billion	$120 billion	0.49%
Hurricane Ina	United States	2022	$100 billion	$109 billion	0.49%
Hurricane Maria	United States	2017	$68 billion	$86 billion	0.35%
Hurricane Sandy	United States	2012	$50 billion	$73 billion	0.31%
Hurricane Irma	United States	2017	$57 billion	$72 billion	0.3%
Floods	Thailand	2011	$40 billion	$61 billion	11.73%
European flash floods	Various Euroope	2021	$54 billion	$61 billion	N/A
Earthquake	Japan	2004	$28 billion	$52 billion	0.57%
Hurricane Ike	United States	2008	$30 billion	$50 billion	0.2%
Earthquake	Chile	2010	$30 billion	$47 billion	13.82%
Izmit earthquake	Türkiye	1999	$20 billion	$43 billion	7.8%
Winter storm	China	2008	$21 billion	$35 billion	0.46%
Hurricane Ivan	United States	2004	$18 billion	$33 billion	0.15%
Earthquake	Taiwan	1999	$14 billion	$30 billion	4.64%
Hurricane Charley	United States	2004	$16 billion	$30 billion	0.13%
Floods	China	2016	$22 billion	$29 billion	0.2%
Riverine flood	China	2010	$18 billion	$28 billion	0.3%
Earthquake	Japan	2016	$20 billion	$26 billion	0.4%

Note: Sources: CRED, 2022; Countryeconomy.com, 2023; and Office of Management and Budget (OMB), 2023, "Historical Tables," White House, n.d., https://www.whitehouse.gov/omb/budget/historical-tables/, accessed 18 November 2025.

such as Chile and Türkiye – indicates that significant economic effects are not limited to the world's largest economies.

As to how natural disaster economic losses compare to those from cyber catastrophes, the difference in scale is immediately evident. The twenty largest natural disasters by economic impact caused nearly US$1.5 trillion in losses, adjusted for inflation, with the top ten responsible for 78% of that. This far exceeds the aggregate $326.4 billion from cyber catastrophes in Table 1. Quite simply, natural disaster losses are so much larger than those from cyber catastrophe that meaningful comparison is virtually impossible. When linked to GDP as a reference point, this becomes even clearer. While only two events in Table 1 reached the low end of the threshold set by Eling, et al., natural disasters routinely exceed the high end of their threshold, as Table 4 reveals.

Table 4: Natural Disasters with Economic Impacts that Exceed 2% of GDP

Event	Country	Year	Original Econ. Loss	Loss as % of GDP
Earthquake	Chile	2010	$30 billion	13.82%
Floods	Thailand	2011	$40 billion	11.73%
Izmit earthquake	Türkiye	1999	$20 billion	7.8%
Earthquake	Taiwan	1999	$14 billion	4.64%
Tohoku earthquake	Japan	2011	$210 billion	3.37%

Note: Sources: CRED, 2022; Countryeconomy.com, 2023; and OMB, 2023.

Table 4 shows that while only two cyber events reached the lower end of the threshold set by Eling, et al., five natural disasters exceeded the high end, and thirteen more fell within their 0.2-2% range (see Table 3). The nations most affected relative to GDP – Chile, Thailand, and Türkiye – could be characterized as emerging markets (at least relative to the United States, China, and Japan), supporting the belief that major natural disasters would have a disproportionate impact on smaller and more fragile economies. Taiwan, while perhaps not an emerging economy, is still relatively small, and thus could be subject to the same dynamic. Japan, on the other hand, is one of the largest economies in the world – and was in 2011, when the Tohoku earthquake occurred. This is indicative of the impact a natural disaster can have on a developed state.

Although they did not pierce the top of the range given by Eling, et al., some of the thirteen that fell within the range still show economic losses as a percentage of GDP were still much larger than MyDoom and SoBig (i.e., the only two cyber catastrophes to exceed 0.2% of U.S. GDP). Seven of the thirteen events falling in the 0.2-2% range reached at least 0.4% of GDP. Overall, thirteen of the twenty events in Table 3 had GDP impacts larger than that of SoBig or MyDoom, with another three close at 0.3-0.31%. Further, it is important to remember that SoBig and MyDoom were intentionally stressed, with the comparison of their economic effects coming relative only to U.S. GDP.

Economic Security Implications

The analysis above suggests that the ability of economies to absorb major losses has been tested thoroughly since at least 1998. Although many have expressed skepticism about whether the "big one"[88] is "yet"[89] to happen, historical activity reveals that far greater tests of economic capacity to absorb harm have been endured – and far more frequently. As a result, the economic security threat posed by major cyber events is likely far lower than some fear. Rather than plan for "cybergeddon,"[90] it may make far more sense to approach the risk within the context of its potential economic scale and adjust security strategy appropriately.

Resetting expectations for "cybergeddon"

Natural disaster economic losses have been profoundly greater than those caused by cyber catastrophes to a degree that makes comparison difficult. The twenty-four cyber catastrophe events since 1998, in aggregate, are only a bit larger than the economic loss from just the Tohoku earthquake represent well under 10% of natural disaster economic losses for the same period.[91] The difference in scale is instructive when trying to gauge the size of a cyber attack necessary to strain economic capacity to absorb it. At a minimum, such an event likely would have to exceed the aggregate economic losses of the twenty-four events in Table 1, because a total of that magnitude would be the approximate equivalent of the 2011 Tohoku earthquake economic loss in Japan (see Table 3). Further, the effects of such an event would likely have to be reasonably concentrated in one or a small number of economically mature countries in order to mirror the nature of the economic effects of the costliest natural disasters (by GDP). Distributing $318 billion in economic effect is much different when compared to global GDP of $111 trillion than to U.S. GDP of $29 trillion or Japanese GDP of $4 trillion.[92]

If a cyber catastrophe were to cause economic losses of US$318 billion today (i.e., the level reached by the Tohoku earthquake), it would cause a material GDP impact as long as the aggregate GDP affected added up at least to what was present in Japan in 2011 (not much different from 2024). Given that Tohoku impaired GDP at a rate of 3.37% (see Table 3), one could even argue that such an event could have a GDP impact in a region with aggregate GDP ten times greater than that of Japan in 2011. After all, what is 3.37% in a $4 trillion GDP would be approximately 0.337% in when affected against $40 trillion in GDP. Given the historical record, it is difficult to conceive of a cyber catastrophe scenario

88 Blosfield, 2021.

89 Pain, 2023, p. 32

90 Jennifer Daffron, 2019, "CYBERGEDDEN VS. CYBERTOPIA: FUTURE OF CYBER RISK," *The Future of Cyber Risk Conference 2019*, n.d., https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/192407-cyberconference-presentation-daffron.pdf.

91 Tom Johansmeyer, 2024, "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/.

92 World Bank, 2025.

that could occur and reach sufficient economic impact to test the ability of a more mature economy to absorb it.

In addition to the difficulties in achieving necessary scale simply due to the delta between historical size of impact and that necessary to register even in comparison to natural disasters, the historical trend evident in economic impact from cyber catastrophes suggests that even a larger event relative to other cyber catastrophes is unlikely. Since 1998, as shown in Figure 1, eight major events have occurred since 2008, with one of them (CryptoLocker) in 2013 two (WannaCry and NotPetya) in 2017, one in 2023, and three in 2024. Together, they represent only 8.54 percent of the aggregate economic loss from cyber catastrophes since 1998. Moreover, the four most recent events are by far the smallest in Table 2 as measured by U.S. GDP effect, with even 0.01 percent. Thus, in addition to having to achieve an as yet unreachable level, such a cyber catastrophe would also have to represent an abrupt change in a trend that has persisted since 2008. While one could contend that such a change from the prevailing state is not impossible, making such a claim credibly would require the provision of detailed scenarios, experience, and risks that have not yet been furnished.

Realistic cyber and economic security concerns

The relatively low economic impact from even the most severe cyber attacks should not be interpreted as justification for complacency or the significant redirection of resources currently allocated to cyber security. After all, improvements in security have contributed to the decline in the economic effects of major cyber events since 2008,[93] and continuing to invest in cyber capabilities will help maintain a favorable "offence-defence balance."[94] Even without rising to the GDP levels achieved by natural disasters, cyber attacks can have important economic consequences, and there are non-economic consequences requiring strategic attention, as well.

First, the economic effects of cyber attacks can have targeted and localized effects (either geographically or to workforces and business networks linked by key companies and relationships). This was demonstrated by the Jaguar Land Rover ransomware attack, which started in late August 2025 and halted operations for several weeks. It led to a 28.6 percent drop in the manufacture of automobiles[95] and caused the UK's Office for National Statistics revised their UK GDP growth forecast from an initial estimate of 0.1 to 0.0 percent.[96] The breach also caused protracted supply chain disruption, with vendors who were heavily reliant on JLR and potentially risking insolvency. Arguably, the secondary harms (for instance, for impacted employees and their families) represent more tangible and more politically salient indicators of real-terms economic security risk than the near-rounding error shift in GDP,[97] recalling the concerns about economic security at the household level,

93 Johansmeyer, 2026, pp. 16-7.

94 John Halstead and Luca Righetti, 2025, "Assessing The Risk Of AI-Enabled Computer Worms," *GovAI*, 10 September, https://cdn.governance.ai/Assessing_The_Risk_of_AI-Enabled_Computer_Worms.pdf.

95 Johansmeyer, 2026, pp. 16-7.

96 Stewart, 2025.

97 Jason R.C. Nurse, Tom Johansmeyer and Gareth Mott, 2025, "Jaguar Land Rover cy-

raised by Richiardi, et al.[98] Further, it aligns with existing research that has advocated for greater focus on the 'holistic' harms of cyber breaches, beyond and behind the bottom-line economic cost.[99]

There are considerations for cyber security beyond economic security as well – or at least within the context of direct action. The fears of cataclysmic cyber events have focused on the destruction of economic value, but other objectives may be more relevant. Espionage remains a key cyber domain concern within the sphere of strategic competition,[100] even if the potential economic effects remain relatively limited.[101] Cyber operations can also be used to "buy time for diplomacy" and otherwise engage in coercive activity with adversaries,[102] although such efforts are likely to stay below the threshold of war.[103] In fact, only three of the twenty-four major cyber events (in economic terms) recorded since 1998 resulted from state-actor offensive cyber operations, and they only amounted to approximately $40 billion in economic effect (adjusted for inflation to 2025).[104] The space for cyber operations, therefore, seems likely to lie in intelligence operations, limited disruption and interference (e.g., sabotage), and in coercive diplomacy. While direct action with scale may be seem like a concern given the cyber threat scenarios that have been imagined, such economic effects are likely far too difficult to achieve.

Conclusion

Comparing cyber events to natural disasters, perhaps counterintuitively, can help change how cyber security risks are perceived, resulting in a savvier approach to cyber and economic security strategy, given the improved understanding of the potential economic consequences of cyber catastrophe – even in the most severe possible cases. Given the limited experience society has had with the cyber domain, natural disasters provide a known quantity and useful reference point for economic impact, which then can be used to inform how the prospect of cyber catastrophe is treated.

berattack shows that governments must provide post-incident support," *Binding Hook*, 7 October, https://bindinghook.com/jaguar-land-rover-cyberattack-shows-that-governments-must-provide-post-incident-support/.

98 Richiardi, et al., 2020, p. 2.

99 Jamie MacColl, Pia Husch, Gareth Mott et al., 2024, "Ransomware: victim insights on harms to individuals, organisations and society," *RUSI, Occasional Papers*, 16 January, https://www.rusi.org/explore-our-research/publications/occasional-papers/ransomware-victim-insights-harms-individuals-organisations-and-society.

100 Anatol Lieven, 2021, "A lesson in cyber spying vs. cyber attack," *Responsible Statecraft*, 13 January, https://responsiblestatecraft.org/2021/01/13/a-lesson-in-cyber-spying-vs-cyber-attack/.

101 Tom Johansmeyher, 2025, "Insuring the Unseen: Closing the Protection Gap in Economic Cyber-Espionage," *American University Center for Security, Innovation, and New Technology Policy Paper Series*, Fall, pp. 14-9, https://www.au-csint.com/publications/insuring-the-unseen.

102 John R. Lindsay, 2025, "Stuxnet revisited: From cyber warfare to secret statecraft," *Journal of Strategic Studies*, vol. 48, iss. 4, p. 3, https://doi.org/10.1080/01402390.2025.2481447.

103 Thomas Rid, 2012, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, vol. 35, iss. 1, p. 7, https://doi.org/10.1080/01402390.2011.608939.

104 Johansmeyer, 2026, p. 16.

The concern that there is still a major cyber event yet to happen – the "big one" – reinforces the fear of the unknown. The prospect of a major cyber event that causes an unprecedented level of economic harm persists, making cyber risk take on a larger-than-life nature. It is time to use the data available to push back against that narrative. Cyber has not been so bad. It could get worse, and based on what we know about natural disasters, it could get profoundly worse and still not pose a major economic threat.

Ultimately, the biggest fear in cyber appears to be fear itself. Fear of the unknown, fear of the potential magnitude of the risk and fear of something new have made cyber risks to appear much larger and menacing than they really are. Meanwhile, natural disaster risk is far more frequent and severe, and it is not seen as nearly as great an economic threat. The fact that several indicators suggest the inability of cyber events to cause meaningful economic losses should help push through the fear, making cyber risk easier to understand, manage, and hedge.

Author

Tom Johansmeyer is co-lead of the economic and legal warfare project at the Irregular Warfare Initiative, 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 economic 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.