CENTER FOR
SECURITY, INNOVATION,
AND NEW TECHNOLOGY

Insuring the Unseen: Closing the Protection Gap in Economic Cyber-Espionage

Tom Johansmeyer

CSINT Policy Paper Series · Fall 2025

TABLE OF CONTENTS

Abstract

Intellectual property (IP) theft compromises a company's ability to compete and, in aggregate, can erode a country's economic security, allowing adversaries to close commercial and technological innovation gaps. The insurance industry lacks a solution for economic cyber espionage, exposing companies to a $9 trillion risk. The absence of relevant insurance protection does not appear to be a problem of insurability but rather of execution. This paper explores a broadened view of the economic cyber espionage threat, one that includes identifying the financial harm that can come from a wide range of cyber espionage scenarios for both "competent" and "incompetent" actors. The research then uses this expanded scope to identify the current protection gaps in insurance for this increasingly frequent risk and offers recommendations toward closing them.

About the Author

Tom Johansmeyer is a POLIR Ph.D. candidate at the University of Kent, Canterbury. Based in Bermuda, where he also works in the reinsurance industry, Tom is co-lead of the economic and legal warfare project at the Irregular Warfare Initiative and an early career member of the Institute of Cyber Security for Society. His research has largely focused on economic security in the face of large natural, cyber, and political violence events – with a specific concentration on impact quantification. Additionally, Tom proudly pushed paper in the U.S. Army in the late 1990s.

Introduction

Economic cyber espionage represents an ongoing threat to both nations and markets, yet unlike other cyber threats, it remains largely uninsured. This does not have to be the case. The underinsurance for economic cyber espionage is more of a mechanical problem, with coverage gaps hinging on proving damage to intangible assets. In fact, this protection gap persists even when attackers are “incompetent” (i.e., unable to use the IP they steal), since victims still incur measurable, indemnifiable costs.

It is not easy to manage the economic effects of cyber espionage. If cyberattacks themselves are often called “borderless,”[1] then cyber espionage can involve months or years of virtual invisibility, with consequences that victims may never fully recognize. After all, the use of stolen IP, for example, can have implications for several years.[2] While straightforward cyberattacks can range from causing visible damage (e.g., defacement) to requiring defined payment amounts (e.g., ransomware) and even the possibility of widespread damage (e.g., LockerGoga[3] and NotPetya[4]), espionage involves the theft and possible use of IP, itself an “intangible asset” that defies straightforward valuation and, as such, difficult to calculate economic harm.[5]

The nebulous effects of economic cyber espionage—even if large enough to be visibly impactful—have made this threat difficult to insure. Cyber insurance may provide a starting point, but it is unfit for purpose for economic cyber espionage. As it exists today, according to the International Association of Insurance Supervisors (IAIS), cyber insurance “is designed to provide first party and third party coverage to mitigate risk exposure by offsetting costs involved with recovery of cyber losses,” and specific coverage can consist of losses related to “network security breaches, data and systems recovery costs, legal expenses and third-party indemnification related to data breaches, as well as business interruption costs.”[6] This requires identifying and quantifying the damage, a process more difficult with cyber espionage than with other cyberattack forms, like ransomware.

[1] Tom Johansmeyer et al., “Invisible Lines, Visible Impact: How Territorial Security Influences Russian Cyber Security Strategy,” Ñ ă Ư̦ Å Ö É ƒ,170, 9 ǵ ɀ 1 ȓ (Ǫ ȼ Ǧ February 2025): 20–31, https://doi.org/10.1080/03071847.2025.2458143.
[2] “The Damaging Effects of IP Theft,” Ö 9̦ 7 Ư ȓ Ǣ Ư Ğ Ư ɀ̦ É զ ă ǵ (blog), August 24, 2018, ȓ Ǭ ȼ Ƞ Ǒ ǵ ǫ https://ischoolonline.berkeley.edu/blog/damaging-effects-ip-theft/.
[3] Tom Johansmeyer, “Look Again: Learning from Smaller Cyber Catastrophes,” Ñ ă Ư̦ զ Ƞ ɀ ȼ March 7, 2025, https://www.theactuary.com/2025/03/07/look-again-learning-smaller-cyber-catastrophes.
[4] U.S. Government Accountability Office (GAO), 9 ɀ ơ Ư ȓ̦ ƒ ǫ û ɀ ȓ ȼ ǫ զ Ư̦ ̦ զ Ƞ Ǒ ǵ ǫ̦ Ư Ư Σ Ư Σ̦ Ƞ ǵ̦ û û Ư û Å Ư û Ȑ ǵ ǫ û Ư̦ Ƞ ǵ̦ 9 ȼ Ƞ (GAO, June 2022), 40, Ƞ Ƞ ȼ զ Ǣ û https://nsarchive.gwu.edu/themes/custom/nsarchive/templates/pdfjs/web/viewer.html?file=https%3A%2F%2Fnsarchive.gwu.edu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Frl07a4-i5cwe%2FGAO-Cyber-Insurance-gao-22-104256-June-2022.pdf.
[5] HM Treasury,] Ư Ƞ Ƞ Ǒ ǫ Ǉ̦ É Ǭ ȼ ȓ Ƞ̦ ȼ ơ ǵ ɀ Ƞ̦ ƒ ǫ Ƞ Ư Ğ Ğ Ư զ Ƞ ɀ ȼ Ǧ̦ Â ȓ ǵ Ȑ Ư ȓ Ƞ ɀ̦ ȼ ǫ Σ̦ § Ƞ ă Ư ȓ̦ ƒ (HM Treasury, October 2018), 3, https://assets.publishing.service.gov.uk/media/5bd4391140f0b604cbff22e5/Getting_smart_about_intellectual_property_and_other_intangibles_in_the_public_sector_-_Budget_2018.pdf.
[6] International Association of Insurance Supervisors (IAIS), 9 ɀ ơ Ư ȓ̦ Å Ǒ û Ǣ̦ Ö ǫ Σ Ư ȓ Ⱥ ȓ Ǒ Ƞ Ǒ ǫ Ǉ̦ ̦ ƒ Σ Ư ǫ Ƞ Ǒ ɘ Ư É ɀ Ȑ Ư ȓ ȸ Ǒ û ǵ ȓ ɀ̦ 9 ǵ ǫ û Ǒ Σ Ư ȓ ȼ Ƞ Ǒ ǵ ǫ û̦ dž ǵ ȓ (IAIS, December 2020), 9, Ğ Ư̦ ~ ȼ ȓ Ǣ Ư Ƞ̦ ? Ư ȸ Ư Ğ ǵ Ȑ Ǭ Ư https://www.iais.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf.

The challenges associated with determining cyber espionage damage have created a gap in the insurance market spanning both cyber and IP. The existing market structure, while not specifically excluding it, does overlook coverage for economic cyber espionage. Consequently, only partial insurance protection exists today—specifically, where clear economic cyber espionage damage is quantifiable and in the limited cases where IP insurance is available.

This paper makes two novel contributions to the literature on economic cyber espionage and cyber insurance protection. The first expands the understanding of how cyber espionage can impact victims by probing how this threat can result in time and resource demands on victims, even when states engaging in espionage are not competent to use what they stole. The notion that IP is a target of state actors capable of integrating what they steal into their respective domestic industries for increased global competitiveness may still be the prevailing case. Yet, economic cyber espionage by actors incapable of productively using stolen IP can also have detrimental impacts. This paper draws a distinction between "competent" and "incompetent" actors and shows that economic cyber espionage, even by the latter, can result in meaningful economic harm to victims.

Additionally, this paper examines the process by which cyber espionage operations unfold relative to available insurance protection—identifying where insurance would respond, what gaps exist, and where insurance market depth may be insufficient to meet the needs of prospective insureds. New and innovative insurance structures can help fill the gaps identified, potentially enabling companies to secure protection that might not be available today.

Cyber Espionage and the Economic Impact

The most successful economic cyber espionage cases may remain unknown,[7] given that the intent is to remain undetected. Moreover, in cases with discovery, the damage more than likely exists by the time the victim identifies the breach. Economic cyber espionage has been "leveraged by state-owned and favoured private enterprises to boost economic competitiveness at the expense of adversaries."[8] States use economic cyber espionage to accelerate their efforts at innovation and commercialization, and as clandestine work-arounds to restrictive trade policies enacted by adversaries (including sanctions and embargoes).[9] China, for example, has a gap in semiconductor demand relative to domestic production capabilities and has engaged in economic cyber espionage to reduce the cost, time, and effort necessary to improve its competitive standing. The security implications are clear, given its reliance on adversaries—Taiwan alone is responsible for 36 percent

[7] U.S. Government Accountability Office (GAO), [illegible] (GAO, January 2022),13–14, https://www.gao.gov/assets/gao-22-104746.pdf.
[8] William Akoto, "Who Spies on Whom? Unravelling the Puzzle of State-Sponsored Cyber Economic Espionage," [illegible] 61, no. 1 (2024): 59–71, https://doi.org/10.1177/00223433231214417.
[9] For example see: Antonia Hmaidi, "[illegible] (Mercator Institute for China Studies November 22, 2023), 6, https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals.

of China's semiconductor imports.[10] When a competent actor engages in economic cyber espionage, the implications can be significant and long-lived. However, there are meaningful consequences related to operations conducted by incompetent actors, as well.

Economic cyber espionage is not just about seeking to narrow the advantage enjoyed by adversary states. Even when not executed successfully, operations can impose costs on adversaries, create uncertainty, and cause distractions that may benefit the actor. A victim of economic cyber espionage, regardless of the actor's competence, would still face determining what was stolen, alongside understanding its prospective uses, the financial and liability impacts to the business, and the required changes in commercial strategy—all this on top of the range of activities necessary following a cyber breach of any kind, including information technology (IT) forensics, crisis communications, and remediation.[11] Thus, even when an actor is not competent to use the targeted IP, the victim sustains some economic effect and a protracted period of uncertainty.

Effectively, economic cyber espionage can range from a conventional espionage (via the cyber domain and for economic advantage) to an unconventional approach to the imposition of "costs on adversaries," which the US Office of the Director of National Intelligence (ODNI) explicitly notes as a prospective form of retribution.[12] This broadened range of economic cyber espionage impact increases the potential importance of insurance as part of a solution.

Insurability of Cyber Espionage

The motivation of company executives and boards of directors to find an insurance solution to economic cyber espionage stems from their need for a financial security tool to help them address a significant threat to important, difficult-to-value intangible assets. Insurance provides a predictable and reliable form of protection,[13] which compensates economic harms under certain pre-agreed conditions. Insurance is unique in that policy negotiations specify the security acquired in advance with specificity, as opposed to after an attack from a weakened bargaining position.[14]

[10] Seamus Grimes and Debin Du, "China's Interdependent Positioning in the Semiconductor Global Value Chain," [illegible] 9, no. 4 (September 2024): 591–613, https://doi.org/10.1080/23792949.2024.2397973.
[11] "Guide to Cyber Insurance," Coalition, accessed August 17, 2025, https://www.coalitioninc.com/en-gb/topics/cyber-insurance.
[12] National Counterintelligence and Security Center, [illegible] (Office of the Director of National Intelligence, 2018),15, https://www.odni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.
[13] Matthew Flug and Thomas Johansmeyer, "Leveraging Contingent Capital as a Non-Traditional Discipline of Economic Warfare," Joint Special Operations University, (JSOU Report 25–22), September 4, 2025, https://www.jsou.edu/Press/PublicationDashboard/291.
[14] Tom Johansmeyer, "Why Parametric Insurance Could Be a Climate Disaster Aid Solution in the Global South," World Economic Forum, February 28, 2024, https://www.weforum.org/stories/2024/02/why-parametric-insurance-could-be-the-solution-to-uncertain-relief-capital/.

For economic cyber espionage, the question of insurability remains largely overlooked, unlike other cyber risks, such as war, which have received extensive debates.[15] This is likely not because economic cyber espionage is uninsurable. To meet the criteria for insurability, there must be a sufficiently large and broad collection of "exposure units" (colloquially, separate independent risks) so that "losses of the few can be **distributed** across the entire population of policyholders [emphasis in the original]."[16] Additionally, that large base of exposure units should be "**accidental** or random and unintentional in nature [emphasis in the original]."[17] The fortuitous nature of losses does not require pure accident as opposed to an intentional act, given that risks could impact anyone policyholder, resulting in fortuity for the insurer, even if the underlying victim was indeed a target.[18]

Regarding the quantification and scale of loss as it affects insurability, there is no rigid threshold. Risks considered uninsurable are those exposed to catastrophic or potentially ruinous events.[19] Ruinous, in this context, refers to widespread loss that can strain insurance capital for a company or across the industry. The classic examples tend to be natural disasters, although kinetic war (i.e., traditional combat with direct physical force) is also among them. Since insurers do not hold a dollar of capital for every dollar of risk they assume, there is the theoretical risk that a major event could require more capital than an insurer keeps on hand. Using cyber insurance as a reference point, the 2025 industry forecast is $16.3 billion in premiums.[20] A single loss causing insured losses of that amount would not be ruinous, as it would merely wipe out the full year's top-line revenues from that class of business. Given the other costs associated with running an insurance business, the overhead above the major event loss—along with any other losses accumulating—would make cyber unprofitable for the year. However, a ruinous event would have to have a much greater impact, impairing capital to the point where it affects the entire business.[21]

Such broad and potentially ruinous exposure is not inherently disqualifying; it just requires additional risk management, such as the use of reinsurance.[22] This practice is quite common in other classes of re/insurance ("reinsurance") contracts, with insurers transferring catastrophic

[15] See for example: Frank Cremer et al., "On the Insurability of Cyber Warfare: An Investigation into the German Cyber Insurance Market," 9 ǵ Ǭ Ȁ ẓ ŋ Ư ȓ û̦ 142, no. 103886 (2024), https://doi.org/10.1016/j.cose.2024.103886.
[16] Howard Kunreuther and Jason Schupp, "A Framework for Defining a Role for Insurers in 'Uninsurable' Risks: Insights from COVID-19," s ǵ ẓ ȓ ǭ ƈ Ğ̦ ǵ ǆ̦ f ǭ û ẓ 40, no. 10 (2021): 5, Ǉ ẓ Ğ ƈ ŋ Ŏ ǵ ǭ https://content.naic.org/sites/default/files/JIR-ZA-40-10-EL.pdf.
[17] Kunreuther and Schupp, "A Framework for Defining a Role for Insurers," 5.
[18] Tom Johansmeyer, "If Cyber Is Uninsurable, the United States Has a Major Strategy Problem," s ǵ ẓ ȓ ǭ ƈ Ğ̦ ǵ ǆ̦ Å Ŏ û Ǣ̦ ~ ƈ ǭ ƈ Ǉ Ư Ǭ Ư ǭ ŋ̦ ƈ ǭ 28, no. 2 (2024): 10, https://jrmi.au.edu/index.php/jrmi/article/view/291/190.
[19] Kunreuther and Schupp, "A Framework for Defining a Role for Insurers," 5.
[20] "Cyber Insurance: Risks and Trends 2025," Munich Re April 3, 2025, https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.item-63b78dc6572d54d4c380b34189b6c273.html.
[21] Tom Johansmeyer, "Bad Decisions Have Consequences: How Cyber Security Could Fall Victim to Climate Change," 7 ȓ Ŏ ŋ Ŏ û ă̦ ɋ ŋ ẓ 30, (May 2025): 15, https://doi.org/10.1017/S1357321725000091.
[22] "What is Reinsurance?" Reinsurance Association of American, accessed September 9, 2025, https://www.reinsurance.org/RAA/RAA/About-the-RAA/what-is-reinsurance.aspx.

risk to reinsurers for widespread events ranging from hurricanes to cyber catastrophes.[23] As part of the hedging process, such risk-transfer activity fundamentally reframes the quantum associated with insurability, simply by reducing significantly the quantum of potential loss to which a reinsurer is exposed. For example, in the current cyber insurance market structure, insurers cede approximately 36 percent of their business to reinsurers.[24] Only two years prior, the amount ceded was as high as 50 percent,[25] with the reduction showing progress toward market maturity and stability. The quantification of insurability is a moving target and is thus as much art as science. However, a dynamic marketplace could and should move with the perception of insurability levels.

Finally, affordability is part of insurability. If an insurer cannot transfer risk on an economically beneficial basis,[26] then it is effectively not transferable (i.e., uninsurable). For extremely remote and severe potential threats, the cost to hedge might be disproportionately expensive for what seems beyond the realm of possibility, and for frequent risks that have manageable economic effects, it may be more beneficial simply to retain the risk. Risk transfer is economically beneficial when the cost of protection frees up capital or otherwise allows for further business activity that generates a return greater than the cost of protection.[27]

Insurance exists to make the insured whole in the event of a loss,[28] not to provide a more favorable economic state post-loss than before the occurrence. For this reason, the concept of damage is fundamental to insurance recoveries. When seeking to claim on a policy, the insured generally must show some sort of loss or economic damage that the stated coverage would remedy. If there is no such damage, then there is no way to make them whole—because the insured is presumably still whole. This is the crux of the mechanical problem, identified above, from which economic cyber espionage suffers with regard to insurability.

Economic cyber espionage, itself, does not appear to be uninsurable, concerning the criteria delineated above. Yes, challenges exist—as they do in other areas of cyber insurance—from the

[23] Darren Pain, [illegible] (The Geneva Association, [illegible] November, 2023), 31, https://www.genevaassociation.org/sites/default/files/2023-11/cyber_accumulation_report_91123.pdf.
[24] Howden Re, “Into the Cyberverse,” (Howden Re, April 2025), 11, https://www.howdenre.com/sites/howdenre.howdenprod.com/files/2025-04/howdenre_into_the_cyberverse_report_april_2025.pdf.
[25] Adam Banas et al., “The Risk of a Cyber Catastrophe: Solving for Insurers’ Fear of the Unknown, [illegible]Gallager Re (n.d.), 9, accessed October 23, 2025, https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/the-risk-of-a-cyber-catastrophe.pdf.
[26] Kai-Uwe Schanz, [illegible] (Geneva Association, April [illegible] 2018), 6, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/understanding_and_addressing_global_insurance_protection_gaps.pdf.
[27] This is something of an oversimplification, in that the return would likely have to exceed a range of costs beyond the cost of insurance protection, to include the cost of capital and other operational expenses.
[28] Philippe P. F. M. van de Calseyde et al., “The Insured Victim Effect: When and Why Compensating Harm Decreases Punishment Recommendations,” [illegible] 8, no. 2 (2013): 161–73, [illegible] https://doi.org/10.1017/S1930297500005088.

availability of historical data and precedent to modeling and pricing.[29] However, cyber catastrophe has not been flagged as a catastrophic risk that would overwhelm the industry (e.g., as feared with cyber war[30]). In fact, it seems likely to have overlooked the risk rather than explicitly excluded it. The publications, articles, reports, and other statements offered by cyber insurance industry stakeholders are relatively quiet on the subject. Rather than explicit uninsurability, the lack of coverage for economic cyber espionage appears to come from a mechanical problem, particularly with the identification and quantification of damage.

Where Economic Cyber Espionage Falls in

When viewed as a mechanical problem, economic cyber espionage could be partially recoverable through insurance, at least given the nature of the insurance industry as it stands today. Some of its aspects fall within the domain of traditional cyber insurance; meanwhile, there are elements within economic cyber espionage that a niche form of IP insurance specifically designed to address the theft or operational compromise of intangible assets could cover. Other risks covered by cyber insurance have overlapping implications with some aspects of cyber espionage. While ransomware, for example, culminates in a potential ransom payment (which itself could have insurance ramifications), the engagement of incident response services, counsel, and crisis communications professionals applies to many forms of cyberattack. As Table 1 illustrates, there are aspects of many cyberattacks—like intrusion and any damage to systems or data—that are agnostic to the purpose of the attack. What differentiates activities like ransomware, defacement/destruction, and cyber espionage only matters in certain aspects of an attack. The divergence in intent, regarding cyber espionage, is what results in some of the economic impact falling through the cracks.

In addressing economic cyber espionage, cyber insurance would likely concentrate on the operational aspects of accessing, using, and potentially damaging the victim's systems. However, it would stop short of the IP itself. IP insurance, on the other hand, consists of a collection of underlying specific coverages that include disputes, enforcement of rights, and infringement liability.[31] Within this collection of coverages is trade secret value insurance, which "can protect an insured from loss due to the misappropriation (theft) or unauthorized disclosure of its own trade secrets."[32] This last area of IP insurance is the aspect that is relevant to cyber espionage risk. It is also a small subset of the already small IP insurance category—a niche within a niche.

As Section 3 notes, damages are fundamental to the process of recovery from insurance—if there is no damage, then there can be no recovery. In identifying how insurance can respond to economic cyber espionage operations, therefore, it is necessary to see where and when damage can occur,

[29] Pain, 9 ʐ ơƯ r̂ ÅǑûǢ , 16.ǫ.ɳ ʐ Ǭ ʐ Ǧ ƈ ŋ Ǒ ǵ ǭ
[30] Cremer, et al., "On the Insurability of Cyber Warfare."
[31] "Intellectual Property Insurance," Gallagher Industries, accessed August 17, 2025, https://www.ajg.com/uk/corporate-insurance/intellectual-property-insurance/.
[32] "IP Protect," MarshMcLennan, accessed 28 August 2025 https://www.marsh.com/en/services/financial-professional-liability/expertise/ip-protect.html.

with the understanding that undiscovered operations do not lead to insurance recovery. If a victim does not know it has been affected by a breach, then there would be no way to assess possible damages and no reason to place a claim, making the insurance discussion irrelevant. Table 1, which breaks down economic cyber espionage into five phases, shows at each one what type of insurance could engage and where the gaps in protection may exist.[33] The first point at which victims might realize a breach is in Phase III, although the attack could go through all five phases undetected, leaving victims ignorant that an intrusion, theft, or subsequent sale of data has occurred. In such cases, by definition, there is no possibility of an insurance recovery without the knowledge of a reason to claim.

Table 1: The Five Phases of Cyber Espionage Operations[34]

Phase	Description	Potential Insurance Implications
I. Objective	The actor sets objectives for the operation.	None
II. Recognition	The actor "employs various recognition techniques to identify attack vectors."[35]	None
III. Infiltration	This is where the actor compromises the target, gains access, and identifies relevant information.	Cyber insurance
IV. Extraction	Extraction may not refer to extracting data or other assets, but rather an actor's departure from the system accessed, often with an eye to returning in the future.	Cyber, IP insurance
V. Sale	The actor sells to prospective buyers of stolen IP, who "consider this expense as the cost of knowledge transfer because they could obtain third-party technologies at a lower cost."[36]	IP insurance

[33] Richard Rivera et al, "An Analysis of Cyber Espionage Process," in ?ƯȸƯĞǵȒŌƯǭῃû, ƈǭΣ, ΣȸƈǭɋƯû, Ŏǭ, ÉƯɋ ʐ, ed. Á. Rocha, C.H. Fajardo-Toro, J.M.R. Rodríguez, vol. 255, ÉŌƈȓῃ, fǭǭǵȸƈῃŎǵǭ, Éʐûῃ ƯŌû, ƈǭ (Springer, 2022), 3–4, https://doi.org/10.1007/978-981-16-4884-7_1.
[34] Rivera, et al, "An Analysis of Cyber Espionage Process," 3–4.
[35] Rivera, et al, "An Analysis of Cyber Espionage Process," 3–4.
[36] Rivera, et al, "An Analysis of Cyber Espionage Process," 3–4.

Not all phases are relevant to the insurance process, even though they do imply unspecified harm to the victim. For example, setting objectives is an intentional act that suggests a future effort to cause harm. However, there has been no operation, as yet, and thus no impact, which means that Phase I is irrelevant within the context of insurance recoveries—and, in general, only implies the earliest stages of a threat. Phase II, likewise, is a preparatory stage in which the threat actor begins to plan an operation, but still, no damage has occurred. For the purposes of identifying and preventing threats, Phases I and II are relevant. A target that can prevent threat actor efforts at the "Recognition" stage would indeed protect itself from the potential for harm. Such efforts are more likely the domain of either state actors, as part of a broader national cybersecurity effort, or of highly capable specialist technology companies. As a potential victim of economic cyber espionage contemplating risk management alternatives, the process really begins with Phase III.

Phase III involves infiltration, when threat actors directly engage with targets, and at this point, the targets indeed become victims. The reason for this is that there are economic damages to realize upon the discovery of the threat actor in the company's systems. For example, simply discovering a breach demands an array of costs. The company would need to engage counsel, IT services (audit, forensics, remediation), and potentially crisis communications firms for both the public and (if publicly traded) its institutional investors.[37] Resulting costs could include "a direct (or first party) financial loss to you or your business arising from a cyber event" or "investigation and defence costs, civil damages, compensation payments to affected parties."[38] The fact that the attack was economic cyber espionage is effectively incidental, as the focus would be on the unauthorized entry and use of the system—and the attendant expense necessary to recover from this breach.

Phase IV is when a threat actor could extract system data from the target—this is the point at which company information leaves its control. Once extracted, threat actors have the data outside the company environment and can use it as they see fit, from sales to third parties to extortion against the victim. In addition to the insurance ramifications for Phase III, Phase IV would add the further potential for customer notification and attendant expenses, which likely would still fall to the cyber insurance market. Notably, Phase IV is the stage at which economic cyber espionage becomes differentiated from other forms of cyberattack. If the information extracted is company IP (e.g., trade secrets), then something of intangible value has left the victim's control, and the ramifications are far different from those associated with the theft of customer information and the need for notification.

The fifth and final phase is the sale of stolen IP. Of course, threat actors reach this phase only if they have successfully negotiated the first four. Even then, the need for Phase V depends on the

[37] Whether there are any payments, and the extent to which such payments would occur, is subject to policy terms and conditions, on which the details can vary. This is a discussion involving a hypothetical event and a discussion of possible outcomes.
[38] "What Does Cyber Insurance Cover?" Association of British Insurers, accessed 17 August 2025, https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/what-does-cyber-insurance-cover/.

actor's objectives. If the actor is a state seeking IP for its own security purposes (economic or otherwise), then it would not necessarily need or want to sell them. Also, if the theft intent were simply to distract or destabilize an adversary, then a sale would not necessarily follow an extraction. However, if sold, then the theft itself becomes potentially more impactful, as the sale implies a buyer who could use the stolen IP for a competitive advantage and ensuing market impact (e.g., the impairment of the victim's value). Like Phase IV, there is the potential for IP insurance engagement at this stage, in which the victim is able to claim on the lost value of the IP, within the pre-agreed terms of the insurance policy.

Cyber insurance and IP insurance are different tools that engage at distinct points in the cyber espionage process. Neither is a fit-for-purpose cyber espionage insurance policy, and their use may cause gaps in protection, of which a buyer should at least be aware. Without requirements for insurers to maintain support of these products, national security policies treat Cyber and IP insurance as "found object[s],"[39] not designed with to address economic cyber espionage and unlikely to be repositioned to do so. The gaps described above, however, represent only part of the problem. In addition to not being naturally suited to the risk of economic cyber espionage, the insurance products available lack the depth necessary to fully address the risk.

Mind the Gap (in the Insurance Market)

The insurance protection gap is the "difference between the amount of insurance that is economically beneficial and the amount of coverage actually purchased."[40] The concept is an insurance industry standard, with high-profile protection gaps for natural catastrophes and, of course, cyber.[41] Regarding IP, companies and states should see the protection gap as an impediment to "[s]elf-defense."[42] Given the importance of insurance to the national economic security strategy,[43] it is necessary to determine the size and nature of the protection gap, as a whole, for economic cyber espionage to determine how to narrow it. The trillions of dollars at stake comprise only part of a broader threat that ranges from the ability of the private sector to fuel economic growth through national competitiveness and faith in the national economic system itself.

[39] Johansmeyer, "If Cyber Is Uninsurable," 4.

[40] Kai-Uwe Schanz, "Understanding and Addressing Global Insurance Protection Gaps," 6.

[41] Kai-Uwe Schanz, "Understanding and Addressing Global Insurance Protection Gaps," PowerPoint presented at 6th Polish Insurance Association Congress, Sopot, Poland (May 2018), 6–7, https://piu.org.pl/wp-content/uploads/2021/03/K.U.Schanz-Understanding-and-addressing-global-insurance-protection-gaps.pdf.

[42] Glenn Chafetz, "How China's Political System Discourages Innovation and Encourages IP Theft," Ñ ă Ư̦ É f É̦ Å Ưȸ Ǒ Ư Ą̦ ǵ dž̦ f ǭ Ƞ Ư ȓ ǭ ƈ Ƞ July 31, 2023, https://saisreview.sais.jhu.edu/how-chinas-political-system-discourages-innovation-and-encourages-ip-theft/.

[43] Johansmeyer, "If Cyber Is Uninsurable," 1–19.

The cyber insurance protection gap is relatively easy to ascertain, with an estimated insurance penetration rate of 10 percent worldwide[44] —likely higher in the United States due to market maturity—and an estimated $1.76 trillion in protection outstanding.[45] This leaves an exposure of $15.84 trillion. The IP protection gap may add as much as $9 trillion, with cybercrime believed to have reached $9.22 trillion in economic impact in 2024,[46] for which the amount covered by insurance is potentially $760 billion, discussed below, although that is at the high end of a wide range. These numbers warrant some skepticism, given that the $9.22 trillion cybercrime estimate in 2024 represents 8.23 percent of that year's global gross domestic product, or GDP, calculated by the World Bank at $111.3 trillion.[47]

Table 2: Understanding IP Insurance Protection in the Market

	Worldwide Premium	**Price/ROL**	**Total Insurance Protection Outstanding**
Low premium, high price	$1.09 billion	2.5%	$43.6 billion
Low premium, low price	$1.09 billion	0.5%	$218 billion
High premium, high price	$3.8 billion	2.5%	$152 billion
High premium, low price	$3.8 billion	0.5%	$760 billion

Table 2's projections for outstanding IP insurance protections calculate annual aggregate market premiums at $1.09 billion and $3.8 billion,[48] against low and high rates on line (ROL),[49] at 0.5 percent and 2.5 percent, respectively.[50] Assuming a 2.5 percent ROL and $1.09 billion premium

[44] Elena Jelmini Cellerini et al., 9ζơƯȓ fǭûζȓƈǭɋƯ ÉŋȓƯǭǇŋăƯǭǑǭǇ ÅƯ(Zurich: ǑƯǭɋƯ džǵȓ Swiss Re Institute, November 7, 2022), 15, https://www.swissre.com/institute/research/topics-and-risk-dialogues/digital-business-model-and-cyber-risk/cyber-insurance-strengthening-resilience.html.

[45] Howden Re, "Into the Cyberverse," 6.

[46] Anne Fleck, "Cybercrime Expected to Skyrocket in Coming Years," ÉŋƈŋǑûŋƈ February 22, 2024, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.

[47] "GDP (current US$)," World Bank Group, accessed September 11, 2025, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

[48]]Ğǵơƈ Ğ fǭŋƯĞĞƯɋŋζƈĞ ÂȓǵȒƯǭɋζȓƈǭûƯȓÑζȒƯ ¬ÂƈĒƯǭŋÉǑǭƯζƈζǭɋƯ Ñ 7ζ ÂǵĞǑɋζ ÑζȒƯ ¬ÉŋƈǭΣƈĞǵǭƯ ÂǵĞǑɋǑƯǭΣζǭŋƯǇȓƈÑƯζăǭǵĞǵɋǑƯûÂăƈ]ƯǵǇȓƈȒăǑɋ ÉɋǵȒ, Verified Market Research, July 2025, https://www.verifiedmarketresearch.com/product/intellectual-property-insurance-market/; cf. "Intellectual Property Insurance Market by Type of Coverage, and by End-User, Global Market Size, Share, Growth, Trends, Statistics Analysis Report, by Region, and Segment Forecasts 2024 to 2033," DataHorizzon Research accessed 18 August 2025, https://datahorizzonresearch.com/intellectual-property-insurance-market-43255 :

[49] An ROL represents the premium paid as a percentage of total protection offered. For example, paying a $1 premium for $100 of insurance protection translates to a 1 percent ROL.

[50] Ayesha Venkataraman, "IP insurance: Learning Points from the Early Foray into Intangibles," fǭûζȓƈǭɋƯ fǭûǑΣƯȓ March 13, 2024, https://www.insuranceinsider.com/article/2cyq5oypiw3mnr6yh7l6o/global-insurers-section/ip-insurance-learning-points-from-the-early-foray-into-intangibles.

yields $43.6 billion in IP insurance protection outstanding, and an ROL of 0.5 percent applied to a $3.8 billion premium results in an estimated $760 billion in IP insurance protection outstanding. Although that range might appear too wide to be useful, only a small subset of it concentrates on protections for IP theft. Conversations with a London-based market underwriter suggest that the subset of IP insurance covering the protection of patents and trademarks ("protected IP") amounts to only about $100 million in premiums worldwide, indicating that the amount of insurance outstanding would range from $4 billion to $20 billion. Additionally, there is insurance for unprotected IP, known as trade secret value insurance (among other similar categorizations), which "can protect an insured from loss due to the misappropriation (theft) or unauthorized disclosure of its own trade secrets."[51] The market for this type of protection is "vanishingly small," consisting of only "a handful of policies."[52]

Table 3: Cyber and Intangible Asset Insurance Coverages

	Worldwide Premium	Worldwide Insurance Outstanding	Notes
Cyber	$1.76 trillion	$17.6 trillion	90% protection gap is well documented; sources are generally accepted and considered reliable
IP (Protected and Not)	$1.09–3.8 billion	$43.6–760 billion	Sources are not from industry participants and warrant skepticism; protection outstanding is likely toward the lower end of the range
Protected IP	$100 million	$4–20 billion	Considered a niche within the broader IP market, which itself is a niche insurance segment[53]
Trade Secret IP	< $100 million	< $4 billion	Very little hard information available because the sector is "vanishingly small"[54]

What is clear from the amount of protection available in the insurance market for both cyber and IP risks is that much of the market remains underinsured. The cyber insurance sector, itself considered relatively new, has an estimated protection gap of 90 percent. While it is a bit more

[51] "IP Protect," Marsh, accessed August 28, 2025, https://www.marsh.com/en/services/financial-professional-liability/expertise/ip-protect.html.
[52] Conversation with an IP underwriter in the Lloyd's of London insurance market environment, conducted by phone on September 12, 2025.
[53] Conversation with an IP underwriter, September 12, 2025.
[54] Conversation with an IP underwriter, September 12, 2025.

difficult to understand the gaps in the IP insurance market, the protection gap could stretch from $8.5 trillion to $9 trillion, although the subset for trade secrets would be a bit smaller. Using high-end estimates yields a protection gap of 90 percent, although low-end estimates bring the gap to more than 99 percent, as Table 4 shows.

Table 4: Cyber and IP Insurance Protection Gaps

	Cyber Insurance	**IP Insurance (High)**	**IP Insurance (Low)**
Addressable Economic Exposure	$17.6 trillion	$9.22 trillion	$9.22 trillion
Available Insurance Protection	$1.76 trillion	$760 billion	$43.6 billion
Unaddressed Economic Exposure	$15.84 trillion	$8.5 trillion	$9.18 trillion
Â ȓ ǵ Ƞ Ư ɋ Ƞ Ǒ ǵ ǭ. Ŀ	Ƃ h ɡ,	Ƃe : ɡ Ƃ	Ƃ Ƃ : ę e ɡ,

Cybercrime (to include cyber espionage) has been called “the greatest transfer of economic wealth in history.”[55] This may not be accurate, given the likely exaggeration of the $9.22 trillion estimate, but the stakes are nonetheless high. Economic security relies, in part, on the ability of companies to use their investments in trade secrets and other IP to fuel economic growth and support the communities around them. This becomes more challenging when economic cyber espionage erodes their competitive advantages and corporate strategies.

Case Studies: Evaluating the Impact of

Economic cyber espionage begins with motivation and intent. A state seeks to gather information for use in advancing its “national security.”[56] It differs from “traditional espionage” in that “the cyber variety is an area where third parties, uncontrolled by either side, can play a major role and cause serious damage to relations,”[57] and ostensibly, the “[i]nformation targeted is often useful in some way to furthering the state’s national security interests” (or at least is intended to be useful).[58] Moreover, as Section 2 discusses, there are cases where the theft of information is in fact not directly useful to the actor, but the simple fact that stealing the information would impose costs on the victim and produce non-economic uncertainty effects. This represents the difference between a “competent actor”—a state that can use effectively the IP it steals—and an “incompetent actor”—a

[55] “The CEO’s Guide to Data Security: Protect Your Data Through Innovation,”. Ñ ᴘ Ñ. 9 ɀ ơ Ư ȓ û Ư ɋ ɀol. Ǒ Ƞ ɀ. f ǭ û ǑǇ ă (AT&T, 2021), 2, https://cybersecurityventures.com/wp-content/uploads/2021/01/attceocyberreport_compressed.pdf.
[56] Akoto, “Who Spies on Whom? Unravelling the Puzzle,” 59.
[57] Anatol Lieven, “A Lesson in Cyber Spying vs. Cyber Attack,” Responsible Statecraft, January 13, 2021, https://responsiblestatecraft.org/2021/01/13/a-lesson-in-cyber-spying-vs-cyber-attack/.
[58] Akoto,” Who Spies on Whom? Unravelling the Puzzle,” 59.

state that cannot use what it steals but may see value in destabilizing an adversary and requiring it to spend time and resources responding to a cyber espionage operation.

Although there is little data available for evaluation, the damage from competent actor attacks is intuitively more concerning than that from incompetent actors. The reason for this is that the economic harm associated with operations conducted by incompetent actors is limited to the core issues associated with cyberattacks in general—such as Phase III issues, like IT forensics and remediation, crisis communications, and legal counsel (see Section 4, Table 1). There may be additional costs associated with the determination of the actual information stolen, the extent to which the actor can use it productively, and how the theft could affect the company's strategy. What differentiates the economic harm caused by competent actors, though, is that the IP stolen is useful. Thus, the value of the IP becomes part of the loss quantum, and that includes months or even years of downstream economic impact.

Competent Economic Cyber Espionage: Chimera APT Group

China's advanced persistent threats (APTs) may have been responsible for $225–600 billion in 2017, an amount that "has likely increased since then."[59] While the broad threat posed by China's economic cyber espionage is profound, the country's focus on semiconductor IP is particularly concerning. Semiconductors power an artificial intelligence market forecasted to approach $5 trillion worldwide by 2033—with the United States and China among those coveting greater and greater market share[60]—and that is one of many applications of a technology in which the United States invested $62.7 billion in research and development in 2024.[61] In addition to the value of the IP, China relies on key adversaries for much of its $385 billion in semiconductor imports and trails them in market share,[62] as Table 5 shows. Taiwan alone is responsible for 36 percent of China's imports.[63]

[59] Grayce McCormick, "Investors, Lawmakers Call for Crackdown on IP Theft amid China Trade War," 9 7 É ʐ û ŋ Ŏ ǫ April 11, 2025, https://cbsaustin.com/news/nation-world/investors-lawmakers-call-for-crackdown-on-ip-theft-amid-china-trade-war-intellectual-property-tariffs-retaliatory-kevin-oleary-thom-tillis-investors-markets-hackers-espionage.
[60] United Nations Conference on Trade and Development (UNCTAD), Єһ Єҿ Ñ Ư ɋ ă ǫ ǵ Ğ ǵ Ǉ ʐ ƈ ǫ Σ ƒ ǫ ǫ ǵ ȸ ƈ ŋ Ŏ ǵ ƒ ǫ ɋ Ğ ʐ û Ŏ ȸ Ư ȓ ŋ Ŏ ɘ ɋ Ŏ ƈ Ğ ƒ ǫ (Geneva: UNCTAD, 2025), 6, https://unctad.org/system/files/official-document/tir2025_en.pdf.
[61] Semiconductor Industry Association (SIA), É ŋ ƈ ŋ Ư ǵ ǆ ŋ ă Ư Ö : É : (SIA, 2025), 10, Σ ʐ ɋ ŋ ǵ ȓ ƒ ǫ Σ ʐ û ŋ ȓ ʐ https://www.semiconductors.org/wp-content/uploads/2025/07/SIA-State-of-the-Industry-Report-2025.pdf.
[62] Ben Jiang, "China's 2024 Chip Imports Surged 10.4% to US$385 billion Amid Tighter US Tech Sanctions," É ǵ ʐ ŋ ă 9 ă Ŏ ǫ ƈ ~ ǵ ȓ, January 13, 2025, https://www.scmp.com/tech/tech-trends/article/3294570/chinas-2024-chip-imports-surged-104-us385-billion-amid-tighter-us-tech-sanctions?module=perpetual_scroll_0&pgtype=article.
[63] Grimes and Du, "China's Interdependent Positioning," 599.

Table 5: Semiconductor Industry Market Share by Country[64]

Country/Region	Semiconductor Market Share
United States	54%
South Korea	22%
Taiwan	9%
Europe	6%
Japan	6%
China	4%

For China, economic cyber espionage—among other forms of espionage[65]—provides a potentially cost-effective alternative to attempting direct competition with much larger market players. China's economic cyber espionage operations in the semiconductor industry have been fruitful,[66] particularly the work of the so-called "Chimera APT Group" in Taiwan from 2018 to 2019,[67] which affected at least seven companies in the "Hsinchu Science-based Industrial Park in Taiwan," including the Taiwan Semiconductor Manufacturing Company (TSMC). Though a financial impact estimate has not been estimated, Chimera APT's compromise, dubbed "Operation Skeleton Key,[68] jeopardized more than 30,000 semiconductor company endpoints, in an attack positioned as more impactful than WannaCry,[69] which caused an estimated $256 million in damages to TSMC alone.[70] A more sophisticated attack, some fear, "has the potential to cripple the entire industry," with a week's outage having "global implications."[71]

The insurance industry's experience with Chimera APT and the Taiwanese semiconductor market—if anything at all—would have been too small to reach any meaningful materiality threshold. The impact experienced was strictly economic; therefore, with no insurance hedge able to absorb some of the loss. There are several reasons for this, including the fact that the global insurance industry in 2018 and 2019 was still at the early edge of its maturity cycle—and only

[64] Grimes and Du, "China's Interdependent Positioning," 599.
[65] Hmaidi, *Ð C Ư î Ư ŋ ĺ ǵ ǥ ă Ē Õ ŋ ǫ ư ẓ û Ŀ ǐ ç É Ğ ŋ Ǒ ç ŋ ŋ Ư Σ*, 6 *c ơ ɋ Ǣ Ǒ ǭ LJ*
[66] Hmaidi, *Ð C Ư î Ư ŋ ĺ ǵ ǥ ă Ē Õ ŋ ǫ ư ẓ û Ŀ ǐ ç É Ğ ŋ Ǒ ç ŋ ŋ Ư Σ*, 6 *c ơ ɋ Ǣ Ǒ ǭ LJ*
[67] CyCraft Research Team, *Â Ñ] î ǵ ẓ Ȑ ǀ 9 Å Ñ Ǭ Ş Ȑ Ư î ơ ŋ Ǒ ǵ ǭ É Ǣ Ư Ğ Ư ŋ ǵ ǭ u Ư ẓ Ñ ơ î LJ Ư ŋ û Ñ ơ Ǒ é Ư ǭ Σ* (CyCraft, February 2020), 1, https://www.cycraft.com/en/white-paper/apt-group-chimera-semiconductor-vendors.
[68] Thomas J. Shattuck, "Stuck in the Middle: Taiwan's Semiconductor Industry, the U.S.-China Tech Fight, and Cross Strait Stability," *§ î o* 65, no. 1 (November 2021): 101–17, https://doi.org/10.1016/j.orbis.2020.11.005.
[69] CyCraft Research Team, *Â Ñ] î ǵ ẓ Ȑ*, 2 *9 ă Ǒ Ǭ Ư î ơ*
[70] CyCraft Research Team, *Â Ñ] î ǵ ẓ Ȑ*, 1 *9 ă Ǒ Ǭ Ư î ơ*
[71] Shattuck, "Stuck in the Middle," 115.

beginning to respond to the effects of NotPetya, the defining event for cyber insurance industry growth.[72]

Nonetheless, even the later cyber insurance market evolution likely would not have addressed much of the loss from Chimera APT and economic cyber espionage. Returning to Table 1's phases (Section 4), the only aspects of Chimera APT's espionage operations that the cyber insurance market would have addressed were Phase III (infiltration) and Phase IV (extraction). Although it is difficult to estimate the effects of these two phases on the seven companies in the Taiwan Industrial Park, the economic damage from such actions, when discovered, can be much smaller than the value of the IP affected. After all, the Colonial Pipeline ransomware attack's economic impact stayed within the company's reported $15 million insurance policy.[73] In fact, the prospect of IP representing the bulk of the potential loss in this case received validation via the adjacency of consumer notification costs, with personally identifiable information signaling the potential costs of intangible assets. Notification represented the bulk of the insured losses from the data breaches to Marriott in 2018,[74] and Capital One in 2019,[75] two of the largest single-risk insured losses the affirmative cyber insurance market has sustained.[76]

Notably, the amount of economic impact was not what prevented Chimera APT's victims from securing insurance. In fact, it is unlikely that traditional cyber insurance would have provided any meaningful protection, given that it would have covered only a small portion of the economic loss. Absent specialized IP insurance—which Section 3 describes as a niche within a niche—the victims would still have remained exposed. It is evident, in this case, though, that insurance could have been helpful. Yet, the current lack of relevant insurance protection limits the ability to remedy the near-term problems and invest in the efforts necessary to prevent or mitigate future effects. An event with economic implications stretching into the hundreds of millions of dollars is well within the insurance industry's ability to absorb.[77] The problem is that there is no coverage product directly relevant to the attack sustained by TSMC and its peers in Taiwan in 2018 and 2019.

[72] Jon Bateman, "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions" (Carnegie Endowment for International Peace ̇ Ọctober, 2020), 21, https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_-_Cyber_Insurance_-_Final.pdf.
[73] John Hewitt Jones, "Axa XL and Beazley on risk for Colonial Pipeline Cyber Attack," ƒ ǫ û ʐ ȓ ƈ ǫ ƣ Ư̦ May 12, û Ǒ Σ Ư ȓ 2021, https://www.insuranceinsider.com/article/28issali53wu2wus5s5j5/axa-xl-and-beazley-on-risk-for-colonial-pipeline-cyber-attack.
[74] Staff Writer, "Marriott Data Breach to Be Tracked as PCS Global Cyber Loss," Å Ư Ǒ ǫ û ʐ ȓ ƈ ǫ ƣ Ư̦ December 3, Ư Ⱥ û 2018, https://www.reinsurancene.ws/marriott-data-breach-to-be-tracked-as-pcs-global-cyber-loss/; PCS DISCLOSURE: Tom Johansmeyer led PCS from 2016 to 2023, to include the development of PCS Global Cyber and other industry-wide insured loss estimate tools. See Luke Gallin, "Tom Johansmeyer leaves PCS to join reinsurance broker Inver Re as Global Head of Index," Å Ư Ǒ ǫ û ʐ ȓ ƈ ǫ ƣ Ư̦ May 1, 2023, Ư Ⱥ û https://www.reinsurancene.ws/tom-johansmeyer-leaves-pcs-to-join-reinsurance-broker-inver-re-as-global-head-of-index/.
[75] Steve Evans, "Capital One Data Breach Puts $400m Insurance Tower on-Watch," Å Ư Ǒ ǫ û ʐ ȓ ƈ ǫ ƣ Ư̦ July 31, Ư Ⱥ û 2019, https://www.reinsurancene.ws/capital-one-data-breach-puts-400m-insurance-tower-on-watch/.
[76] "Catastrophe Claims Data: PCS Global Specialty Lines," Verisk, accessed September 30, 2025, https://www.verisk.com/products/pcs-global-specialty-lines/.
[77] Tom Johansmeyer, "Why Natural Catastrophes Will Always Be Worse than Cyber Catastrophes," ì ƈ ȓ̦ ǵ ǫ̦ ŋ ă Ư̦ Å ǵ ƣ, Ⱥ û April 5, 2024, https://warontherocks.com/2024/04/why-natural-catastrophes-will-always-be-worse-than-cyber-catastrophes/.

Incompetent Economic Cyber Espionage: The F-35 and the J-20

While the conventional motivation for state economic cyber espionage actors focuses on stealing IP they can put to direct and productive use,[78] there are cases where actors are not competent—whether or not they believe themselves to be so. The threat actor has a plan to steal IP (and may have a plan to use it), but in the end, the actor is unable to use the stolen property to productive effect. Even if the lack of productive use is unintentional, the net effect nonetheless involves the imposition of costs by the actor, and although the long-term effects may not be as severe, they may linger. This exact problem arose from the theft of IP related to the F-35 Joint Strike Fighter's self-diagnostic system."[79]

From 2009 to 2013,[80] China engaged in cyber espionage operations related to the F-35, ultimately stealing files "focused on the design and performance statistics of the fighter, as well as its electronic systems," which could serve to "reduce the efficiency of the fighter jet by understanding its limitation and performance weaknesses."[81] The implications of this operation are vast. First, some of it would not fall within economic cyber espionage, given that the information stolen would have uses to develop military capacities, as noted, to reduce the effectiveness of the US capability. However, there is an economic aspect to the operation, as well.

Lockheed Martin was among those identified as hacked as part of the theft of F-35 files.[82] Regarding the theft's economic ramifications, reports, at the time, indicated a "consensus that escalating costs, reduced annual purchases and production stretch-outs are a reflection to some degree of the need for redesign of critical equipment."[83] This is a clear case where insurance recoveries would have been directly relevant, given that there were business and engineering activities required as a result of the cyber espionage operation, presumably with additional costs that could be tracked and shown to an insurer in support of a claim. While the future costs would not be as easy to determine, a partial solution for remediation based on compromised IP would have been possible.

[78] Akoto, "Who Spies on Whom? Unravelling the Puzzle,"59.

[79] Benjamin Jensen, ÉηƈηƯǬƯǭη, ơƯdžǵȓƯ, ηăƯ, cǵẓûƯ, sẓΣǑɋǑƈȓẓ, ÉẓơɋǵǬǬǑηηƯƯ, ǵ fǭηƯ.“ȓcǭǵƯAη ηăƯ, 9ăǑǭƯûƯ, 9ǵǬǬẓǭǑûη, ÂƈȓηẓǑûƯû, 9ẓơƯȓ, ,”E118th ǑǵǭƈLJƯ, ηǵ Cong. (October 19, 2023) (Written testimony by Dr. Jensen as senior fellow, International Security Program, Center for Strategic and International Studies), 4,https://www.congress.gov/118/meeting/house/116383/witnesses/HHRG-118-JU03-Wstate-JensenB-20231019.pdf.

[80] Associated Press, "Chinese Man Charged with Hacking into US Fighter Jet Plans," ÑăƯ,]ẓƈȓΣǑƈǭ July 11, 2014, https://www.theguardian.com/technology/2014/jul/12/chinese-man-charged-with-hacking-into-us-fighter-jet-plans.

[81] Jensen, ÉηƈηƯǬƯǭη, ơƯdžǵȓƯ, ηăƯ, cǵẓ, 4.ƯƯ, sẓΣǑɋǑƈȓẓ, ÉẓơɋǵǬǬǑηηƯƯ

[82] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," The Diplomat, January 27, 2015, https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

[83] David Fulghum et al., "China's Role In JSF's Spiraling Costs," ȸǑƈηǑǵǭ February 3, 2012, https://www.key.aero/forum/modern-military-aviation/117596-china-s-hacking-into-f-35-led-to-spiraling-costs.

As with Chimera APT, the use of conventional cyber insurance—even if it had been more widely available in 2013—would have provided little economic protection relative to the "full" loss experience resulting from the economic cyber espionage operation and its effects. After all, it would have responded only to the initial entry by the actors and potentially some subsequent forensic and remediation activity. As the comparison between Chimera APT and such loss events at Marriott, Capital One, and Colonial Pipeline shows, this tends to be small relative to IP or IP-like economic impacts. The cyber losses from the F-35 espionage likely would have looked more like those from Colonial Pipeline than at Marriott or Capital One because the losses would have been overwhelmingly first-party (i.e., covering economic harm caused to Lockheed Martin itself and not requiring payment to engage in the protection of impacted third parties).

To respond to this case, IP insurance would have been necessary to supplement the conventional cyber coverage available even by today's standards, let alone the limited market penetration achieved in 2013. The cyber insurance market reached only $1.7 billion in worldwide premiums in 2015,[84] suggesting that previous years' results are effectively too small to estimate credibly. With Table 3 (Section 5) showing that trade secret protection outstanding today is minimal, it is virtually impossible to ascertain what would have been available at the time to respond to the F-35 event. However, estimates put the costs resulting from the operation at potentially exceeding $100 million,[85] suggesting a meaningful loss even by today's standards.

The economic cyber espionage operation in the F-35 theft is unique in that it reveals the associated economic effects when an incompetent actor conducts the attack, highlighting that being "incompetent" to use the stolen material does not mean that the damage is small. In this case, an impact of $100 million is the result of work necessary to address the entry and use of systems by the actor, as well as to identify the nature and extent of the damage caused.

Even without the ability to use what it stole, China was able to cause a large amount of damage with this cyber espionage operation. The fact that China was not a competent actor is likely why the impact remained so low, and had it been competent, the military security implications of the theft could have far exceeded the economic consequences. While visible similarities between the F-35 and China's J-20 may have "fueled speculation" about the cyber espionage operation,[86] underlying capabilities are a different matter entirely. China had not developed a solution for material science challenges like the development of "Radar Absorbent Material."[87] Although there was concern that the J-20 "is likely to be a serious threat to U.S. aircraft, ships, and bases for the

[84] Aon, "Global Cyber Market Overview: Uncovering the Hidden Opportunities" (AON, June 2017), 4, https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf, accessed 1 June 2025.
[85] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," *Ñ ă Ư̦ ? Ŏ Ř ĕ ǵ ǫ ƞ*, January 27, 2015, https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.
[86] Gady, 2015
[87] Harrison Kass, "China Has A F-35 Fighter 'Problem' It Might Never Be Able Fix," *Ñ ă Ư̦ ƈ Ƞ Ŏ ǵ ǭ* (blog), *f ǭ Ƞ Ư ȓ Ư ȗ Ƞ̦* November 6, 2024, https://nationalinterest.org/blog/buzz/china-has-f-35-fighter-problem-it-might-never-be-able-fix-210811.

foreseeable future,"[88] it appears that the full fruits of the cyber espionage operation may not have been as productive as initially feared. Nonetheless, this case shows both that the threat exists and that even an incompetent actor can inflict a measurable economic effect.

A Review of Insurability

The cases—Chimera APT Group and the F-35 IP—show the wide spectrum of potential impacts of economic cyber espionage, and in both, the economic effects are within the insurance industry's ability to absorb them, which the representative large single-risk losses in Table 6 suggest. Further, catastrophic risk is no greater than that posed by the broader cyber threat environment, which, while certainly an area of disagreement among insurance industry stakeholders,[89] the market has settled enough at least to deliver $1.76 trillion in sector-wide insurance protection.[90] Given that insurance covers, in part, economic cyber espionage (e.g., cyber and IP; see Table 1, Section 4), the other criteria of insurability have at least generally been met. The fact that economic cyber espionage cases fall into the protection gap does not mean that they are insurable; it just means that the risk warrants more attention.

Table 6: Major Insured Single-Risk Losses

Event	Year	Insured Loss	Description	Sources
Merck (NotPetya)	2017	$1.7 billion ($1.4 billion in property insurance, $275 million in cyber insurance)	Cyber attack	Reinsurance News (property)[91] Artemis.bm (cyber)[92]
Abu Dhabi National Oil Company (ADNOC)	2017	< $2 billion	Onshore energy	Insurance Insider[93]

[88] Mark B. Schneider, "Professional Notes: The U.S. F-35 versus the PRC J-20," Ö : É :, ̛ȡ̛Ğ, ̙ ǫ û ŋ143, ŋ ẓ ŋ Ư, , Â ȓ ǵ
no. 10 (October 2017), https://www.usni.org/magazines/proceedings/2017/october/professional-notes-us-f-35-versus-prc-j-20.

[89] Tom Johansmeyer, "How Cyber Model Vendors See Their Role in Closing the Cyber Insurance Protection Gap," ȿ ǵ ẓ ȓ ǫ ̛Ğ, ǵ dž, ̙ ǫ 40, no. 1 (2024): 118–34, https://www.jstor.org/stable/48770675.

[90] Howden Re, "Into the Cyberverse," 6.

[91] Luke Gallin, "Merck Reaches Settlement With Insurers Over $1.4bn NotPetya Cyber Attack," Å Ư Ŏ ǫ û ẓ ȓ ̛ ǫ ɋ Ư, Ư Ⱥ û 10 January 10, 2024, https://www.reinsurancene.ws/merck-reaches-settlement-with-insurers-over-1-4bn-notpetya-cyber-attack/.

[92] "PCS Puts Merck Malware Cyber Loss Estimate at $275m," ȓ ŋ Ư, October 18, 2017, https://www.artemis.bm/news/pcs-puts-merck-malware-cyber-loss-estimate-at-275m/.

[93] "Adnoc Refinery Claim Soars Towards $2bn," ̙ ǫ û ẓ ȓ ̛ ǫ ɋ Ư, January 26, 2018, https://www.insuranceinsider.com/article/2876fnf4db62x2r85demd/adnoc-refinery-claim-soars-towards-2bn.

Jubilee/Kwame offshore energy	2016	~$1.5 billion	Offshore energy	Artemis.bm[94]
Tianjin port explosion	2015	$1.6–3.3 billion	Port (onshore/offshore)	Artemis.bm[95]
Costa Concordia	2012	$2 billion	Ocean marine	PCS Global Marine and Energy[96]
Deepwater Horizon	2010	$3.3 billion	Offshore energy	PCS Global Marine and Energy[97]

Addressing the protection gap associated with economic cyber espionage does not require the immediate creation of a new insurance product or line of business, and it does not necessarily call for radical changes to the scope of coverage currently available within the cyber or IP insurance markets. Section 7 offers a series of policy recommendations based on the existing capabilities and without significant regulatory or structural market changes.

Early Solutions to Long-Term Market Opportunity

In its current form, the insurance market does not offer much support for economic cyber espionage risks beyond the core cyber insurance product. Table 1's five phases of cyber espionage provide a sense of what types of insurance would help at different points in a cyber espionage operation. To address those gaps, innovation and new market entrants could change the landscape over time—and, indeed, such efforts are ongoing.[98] However, the tools needed to narrow the protection gap do exist, and they have been used for other risks covered by insurance (including cyber). Existing practices simply need redirection toward a new problem— i.e., economic cyber espionage.

Self-Financing and Self-Insuring

Self-insurance remains an option, and it can take on several forms. The simplest, of course, is for a company to gauge the potential uncovered and unrecoverable costs associated with an economic cyber espionage event and keep sufficient funds available. It may be more effective to form a captive insurer—an insurance company that is within the control of its insured(s) and exists solely

[94] Steve Evans, "Jubilee Oil Field FPSO Business Interruption Loss Creep Slows," *Artemis*, July 25, 2019, https://www.artemis.bm/news/jubilee-oil-field-fpso-business-interruption-loss-creep-slows/, accessed 28 June 2025.
[95] "Tianjin Blasts Insurance Loss as Much as $3.3bn: Guy Carpenter," *Artemis*, September 4, 2015, https://www.artemis.bm/news/tianjin-blasts-insurance-loss-as-much-as-3-3bn-guy-carpenter/.
[96] Tom Johansmeyer and Ted Gregory, "PCS® Global Risk Loss Report FY2017" (Verisk, 2017), 2, https://www.verisk.com/492c36/siteassets/media/pcs/pcs-global-risk-loss-report-2017.pdf.
[97] Johansmeyer and Gregory, "PCS® Global Risk Loss Report FY2017," 2.
[98] "Trade Secret Insurance," Alvarez & Marsal, February 9, 2021, https://www.alvarezandmarsal.com/insights/trade-secret-assets-value-valuation.

for the purpose of insuring its owner(s).[99] Companies may use captives to self-insure for unique or difficult risks that cannot be served easily by the broader insurance market. While there are still some requirements around how much capital the company has to put into (and then maintain in) the captive, what risks it can cover, and how to calculate and justify the insurance rates the captive can charge, the mechanism can provide a company with increased flexibility for one of the most important day-to-day cyber risks that the traditional market does not cover fully.

Although for cyber risk in general rather than economic cyber espionage, the use of captives for cyber risk began to increase significantly in 2022,[100] a period during which the "ransomware epidemic" led to a sharp increase in the cost of traditional cyber insurance.[101] Additionally, the use of captives regarding the cyber insurance protection gap speaks to the utility of this form of risk transfer for other protection gaps,[102] as well, including economic cyber espionage. Captive insurers offer a way for companies with insurance needs that the mainstream market cannot satisfy to customize for themselves the risk-transfer solution they need.

Alternative and Bespoke Insurance Covers

The fact that captives can work for individual companies implies that these mechanisms do not scale easily. Each company needs to undertake the effort on its own (although with the help of advisors). A broad and easily adopted solution would need to come from insurers. While this may sound like an extensive process, innovative and creative solutions could enter the market relatively quickly for certain types of risk. This is particularly true of parametric insurance covers, which unlike traditional insurance, pay a pre-agreed amount based on the magnitude of a pre-defined event.[103]

Parametric insurance is most common for natural disaster events, with examples including coverage for an earthquake of a given magnitude (e.g., 6.5Mw) occurring in Istanbul or the Marmara Sea,[104] or a Category 5 hurricane making landfall in Miami.[105] There are even parametric covers designed for crop yields.[106] However, parametric covers are indeed possible for man-made events,

[99] "What Is Captive Insurance?" International Risk Management Institute (IRMI), accessed August 28, 2025, https://www.captive.com/captives-101/what-is-captive-insurance.
[100] Emma Sansom and Thomas Clayton, "Why and How Cyber Is Increasingly Being Insured by Captives," f Å ~ f 9 ƯẤ, August 1, 2022, https://www.airmic.com/news/why-and-how-cyber-increasingly-being-insured-captives.
[101] Jamie MacColl et al., 9 ʐ ơ Ư ȓ f ǭ û ʐ ȓ ơ ǭ ɋ Ư ơ ǭ Σ ŋ ă (London: Royal United Services Institute for Defence and Security Studies, July 2023), 73, https://static.rusi.org/OP-cyber-insurance-ransomware-challenge-web-final.pdf, accessed 29 June 2025.
[102] Gordon Thompson, "Captives: A Solution Built for Cyber Risk," Captive International, October 3, 2023, https://www.captiveinternational.com/captives-a-solution-built-for-cyber-risk.
[103] Flug and Johansmeyer, "Leveraging Contingent Capital."
[104] Tom Johansmeyer, "Money Talks and Hunger Walks: Buying Down State-Actor Influence Risk," f ȓ ȓ ƯǇ ʐ Ğ ơ ȓ ì ơ ȓ dž ơ ȓ f ǭ Ŏ ŋ Ŏ November 21, 2024, https://irregularwarfare.org/articles/money-talks-and-hunger-walks-buying-down-state-actor-influence-risk/.
[105] Johansmeyer, "Why Parametric Insurance."
[106] Steve Evans, "Parametric Crop-Yield Risk Transfer Product Launched by Praedictus & Speedwell," ȓ ŋ Ư Ǭ Ŏ û February 23, 2021, https://www.artemis.bm/news/parametric-crop-yield-risk-transfer-product-launched-by-praedictus-speedwell/.

as well, with cyberattacks and terrorism represented among historical transactions.[107] For economic cyber espionage, a parametric instrument would likely be structured to pay when a series of pre-defined and independently verifiable events occurs, such as the extraction of IP, determination of the threat actor's credibility in being able to use or sell the stolen IP, and then evidence of that IP's having been used. Initial structures would require close collaboration between insurer and insured in their development.

There are some shortcomings with parametric insurance for economic cyber espionage. Finding mutually agreed, independently verifiable indicators of key espionage events having occurred may be difficult and require creativity, and the nuance associated with attributing to a threat actor, quantifying the credibility of that threat actor in using or selling the stolen IP, and then finally determining, on an independent basis, the misuse of the IP has been detrimental to the insured can get complicated. A simplified structure that pays a mutually agreed amount on a binary basis would mitigate such challenges and obviate the need to tackle much of the nuance discussed here. Simplicity does bring the risk of a potentially more expensive—or less predictable—protection instrument, which relates to the challenge of insurability Section 3 raises.[108]

Further research is necessary—both in scholarly and commercial communities—to understand the parameters that may be effective in developing a parametric IP cover. Yet, if ascertained, there are insurers interested in creative, bespoke, and niche opportunities. An innovative solution would have openings to match with interested capital.

Conclusion

Economic espionage may represent a multi-trillion-dollar worldwide problem, but a solution is possible—even in the near term. The lack of insurance products for company IP, as this paper shows, is less an issue of insurability and more one of overlooked opportunities. Cyber insurance addresses some aspects of economic cyber espionage impact, and for the value of the IP at risk, there are niche forms of insurance from which a company could recover, provided it could get the support it requires from a small segment of an already small insurance market. The capital may not be in place, but the elements of a solution are indeed present.

Economic cyber espionage first requires recognition as the multidimensional threat it is, rather than simply the theft of IP that results in presumed long-term competitive harm through eroded market advantage. As this paper identifies, the different threats posed by both competent and

[107] Kane Wells, "Parametrix Launches New Cyber Insurance Solution for Digital Interruption," *Å Ư Ŏ ǫ û ɀ ȓ ƈ ǫ ɋ Ư̦ Ư Ӓ û* November 7, 2024, https://www.reinsurancene.ws/parametrix-launches-new-cyber-insurance-solution-for-digital-interruption/; Rachel Anne Carter et al., *ƒ ǫ û ɀ ȓ Ŏ ǫ Ǉ̦ c ǵ û Ƞ Ŏ Ğ Ư̦ 9 ɀ ơ Ư ȓ̦ ɋ Ƞ Ŏ ȸ Ŏ Ƞ*(The̦ *ƒ ǫ̦ É Ư ƈ ȓ ɋ ă̦* Geneva Association, January 2022), 29, https://www.genevaassociation.org/sites/default/files/cybersolutions_web.pdf.
[108] As with any other form of IP insurance, determining the amount to insure is at the buyer's discretion. This requires conducting valuation activities to reach that determination, although some valuation information may also be necessary to demonstrate insurable interest.

incompetent actors can impose costs on the firms targeted, necessitating different forms of recoverability. There is a spectrum of potential impact from the remediation of IT harm and diagnosis of an ultimately unsuccessful or unusable theft event to the worst-case scenario, in which a competent actor gains access to sensitive IP that has a truly market-disrupting effect. Both are possible; moreover, both are relevant to the problem of economic security and insurance recoverability.

The insurability of economic cyber espionage is not the problem. Rather, what has been missing is a focus on the gaps in the insurance market relative to the phases of economic cyber espionage. What comes next is a necessary market activity, in which risk managers and company executives identify the gaps in cover they have relative to economic cyber espionage and determine the sorts of insurance protection that would help them narrow the gap in cover. This activity at a company level ultimately accumulates to improved national cyber and economic security, given that US investments likely exceed the 2022 level of $655 billion and are foundational to US global economic competition and leadership in key industries ranging from communications to biotechnology to artificial intelligence.[109]

It has come to be accepted as fact that IP theft "is inevitable"[110]—and that economic cyber espionage remains a vital capability for some states in seeking to improve their competitive standing worldwide.[111] Prevention is always important but never assured, making it vital that companies develop and implement security measures that help them recover from economic cyber espionage operations. The rapid, direct, and predictable injection of capital that can come from insurance following a qualifying event provides resources that companies can count on and use when victimized. Companies must put locks on their virtual doors—and have a plan for when an adversary pushes through them.

[109] Kirti Gupta et al., *Â ȓ ǵ Ƞ Ư ɋ Ƞ Ŏ ǫ Ǉ ƒ ǭ Ƞ Ư Ğ Ğ Ư ɋ Ƞ ʐ ƈ Ğ Â ȓ ǵ Ȑ Ư ȓ Ƞ ʐ ǆ ǵ ȓ ƈ Ƞ Ŏ ǵ ǭ ƈ Ğ É Ư ɋ ʐ ȓ Σ Ǭ Ŏ ǫ Ŏ û* (Center for Strategic and International Studies, March 2025), 6, https://www.csis.org/analysis/protecting-intellectual-property-national-security-transition-report.
[110] Sean Lyngaas, "FBI Aims for Stronger Cyber Strategy as US Grapples with SolarWinds Fallout," *9 ʐ ơ Ư ȓ É ɋ ǵ ǵ Ȑ* January 13, 2021, https://cyberscoop.com/fbi-cyber-strategy-solar-winds-matt-gorham/.
[111] Juma Mdimu Rugina, "Economic Cyber Espionage: The US-China Dilemma," *s ǵ ʐ ȓ ǭ ƈ Ğ ǵ ǆ ƒ ǭ Ƞ Ư ȓ ǭ ƈ Ƞ Ŏ ǵ ǭ ƈ Ğ É Ƞ ʐ* 3, no. 2 (2023): 78, https://doi.org/10.5152/JIRS.2023.23014.

Acknowledgements

The author would like to thank the participants of the CSINT roundtable series on cyber espionage for their review of this report, as well as their insights and suggestions.

CENTER FOR
SECURITY,
INNOVATION,
AND NEW
TECHNOLOGY

Our mission is to examine the geopolitical implications of emerging technologies for security, democracy, and society. Based at American University's School of International Service, we conduct original research that advances theory and informs evidence-based policymaking, while also training the next generation of thought leaders and practitioners.

Visit the **Center for Security, Innovation, and New Technology** website for more information about our work and team.

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Center for Security, Innovation and New Technology or American University.

For publication inquiries, please contact **csint@american.edu**