CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

OCTOBER 2020

War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions

Jon Bateman

War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions

Jon Bateman

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Summary

Insurance is one of the most promising tools for addressing pervasive cyber insecurity. A robust market for insuring cyber incidents could, among other things, financially incentivize organizations to adopt better cyber hygiene—thereby reducing cyber risk for society as a whole. But cyber insurance is not yet mature enough to fulfill its potential, partly due to uncertainty about what kinds of cyber risks are, or can be, insured.

Uncertainties in cyber insurance came to a head in 2017, when the Russian government conducted a cyber attack of unprecedented scale. Data-destroying malware called NotPetya infected hundreds of organizations in dozens of countries, including major multinational companies, causing an estimated $10 billion in losses.[1] NotPetya showed that cyber risk was greater than previously recognized, with higher potential for "aggregation"—the accumulation of losses across many insurance policies from a single incident or several correlated events.

NotPetya also exposed a serious ambiguity in how insurance policies treat state-sponsored cyber incidents. Some property and casualty insurers declined to pay NotPetya-related claims, instead invoking their war exclusions—long-standing clauses that deny coverage for "hostile or warlike action in time of peace and war" perpetrated by states or their agents.[2] War exclusions date back to the 1700s, but they had never before been applied to cyber incidents.

This novel use of the war exclusion, still being litigated, has raised doubts about whether adequate or reliable coverage exists for state-sponsored cyber incidents. Some observers have asked whether such incidents are insurable at all, given the potential for aggregated cyber losses even more catastrophic than those of NotPetya.[3] And while the war exclusion has attracted the most attention, another exclusion—for terrorism—presents similar challenges to cyber claims.

Three years after NotPetya, it is still unclear how insurance can or should cover state-sponsored cyber incidents and other large-scale cyber risk. This fundamental uncertainty continues to inhibit the development of robust, socially beneficial cyber insurance markets. New frameworks are needed. Developing and implementing these frameworks requires laying a strong intellectual foundation, bringing more stakeholders into the conversation, and publicly airing fresh ideas to stimulate critique and debate.

Most discussions to date have happened inside the insurance industry, with only limited engagement from outside experts in geopolitics, cyber statecraft, or cybersecurity public policy. Yet the war exclusion challenge is interdisciplinary by its nature. Industry-led reforms must be firmly grounded in the realities of state-sponsored cyber operations—including why and how states use such tools and

the role of cyber conflict in a changing global security environment. Conversely, national policymakers charged with addressing state-sponsored cyber threats must understand the role of insurance—including its potential benefits for society and its ongoing limitations. An independent think tank specializing in international affairs like the Carnegie Endowment for International Peace is well-positioned to help bridge these gaps.

This paper seeks to diagnose the problem, establish criteria for a solution, evaluate potential options, and present new models of alternative cyber exclusions. The proposed exclusions aim to better address catastrophic and state-sponsored cyber risk than today's war and terrorism exclusions do. But whether or not these proposals are adopted, the underlying analysis will hopefully provoke debate and stimulate other creative new ideas. The key points from this analysis are as follows:

- **Traditional war and terrorism exclusions should be abandoned for cyber claims.** Applying these exclusions requires resolving very hard questions: Who perpetrated an incident, what state authority did they have, and how was the incident related to broader military or political aims? Litigating these issues is time-consuming, expensive, and unpredictable. Many organizations may come to doubt the utility of buying cyber insurance with such ambiguous and potentially sweeping exclusions. Yet, despite their breadth, these exclusions were not actually designed to protect insurers from catastrophic cyber risk as such. War exclusions still leave insurers exposed to various non-state-sponsored, catastrophic cyber scenarios, suggesting a basic disconnect between these exclusions and risk itself.

- **Suitable remedies will require new thinking.** Many hope that pending NotPetya litigation will provide valuable guidance, but those cases may not establish binding, generally applicable precedents anytime soon. And litigation is inherently backward-looking: it cannot tell insurers, insureds, or regulators how future contracts should be written. The industry has promising efforts under way to clarify "silent cyber" coverage—a major source of uncertainty—and explore alternative exclusions, but these will take time to bear fruit. Meanwhile, the underlying threat of state-sponsored cyber incidents continues to grow. Instituting reforms across a diverse insurance marketplace will require engaging a broad universe of stakeholders with fresh analyses and proposals.

- **Solutions should aim for clarity and practicability, while also defining a manageable zone of coverage.** Insurers, insureds, and regulators need shared expectations about what kinds of claims would be excluded from coverage. Litigation cannot be avoided altogether, but its impacts can still be minimized through careful exclusion design. Yet clarity and ease of application are not

enough. There is also a business case for, and a public interest in, providing adequate coverage to meet the needs of insureds. This requires a financially sustainable and balanced transaction that protects insurers' profitability and solvency, with government support if necessary.

- **One approach would be to deal separately with catastrophic and war-related or other state-sponsored cyber risks using two complementary exclusions.** The first exclusion would address uninsurable cyber catastrophes based on the scale and nature of losses, regardless of the perpetrator or any connection with war. In fact, a cyber catastrophe exclusion could apply even to nonmalicious cyber events, like those caused by malfunctions or natural disasters. This exclusion would be insurers' first line of defense against aggregated cyber losses during times of both peace and war. With such an exclusion, "war" would no longer be needed as a crude proxy for catastrophic risk. The second exclusion could therefore focus more narrowly on certain unique insurance problems raised by war and state-sponsored cyber incidents.

- **A new exclusion for cyber catastrophes should be limited to extreme scenarios, yet flexible enough to address a variety of causal mechanisms.** The starting point for designing such language is today's infrastructure exclusions, which deny coverage for cyber losses resulting from electricity and telecommunications outages. To better account for the unpredictable ways that modern cyber catastrophes can arise, a new exclusion could be based on impact rather than limited to cyber incidents affecting specific infrastructure types. But the exclusion cannot be so open-ended that it becomes all-encompassing. Caveats and examples can help to confine a cyber catastrophe exclusion to truly uninsurable scenarios.

- **A separate new war exclusion for cyber claims could then deal specifically with cyber losses arising from kinetic war.** With high-impact scenarios already addressed by a cyber catastrophe exclusion, the new war exclusion would have more modest objectives: to equalize the insurance treatment of wartime kinetic and cyber losses, reduce moral hazard for nation states, and account for correlated cyber events involving geopolitical adversaries. Limiting the objectives of a revised war exclusion makes it possible to avoid the thorniest questions about cyber actors' identities, authority, or intent. One version would simply exclude all cyber losses suffered inside known areas of hostilities, where kinetic military activity has reached a substantial threshold of violence.

- **Scenario analysis is vital for clarifying and testing these and any other proposed exclusions.** Insurers, insureds, and regulators will distrust proposals that do not transparently reveal how they would operate in practice. Moreover, different stakeholders have different risk appetites and perceptions of cyber risk, and there is likely no set of exclusions that can earn universal agree-

ment in the near term. Scenarios can therefore stimulate frank conversations about the appropriate insurance treatment of key cases and then test the limits of proposed solutions. This paper presents eight scenarios to clarify the intent and functionality of its proposed exclusions.

- **Government backstops may be necessary to support the market for insuring state-sponsored and catastrophic cyber risk.** With cyber insurance in an immature state, no settled consensus exists on the boundaries of insurability. So long as insurers and other players tread cautiously, private capital may be insufficient to fund a purely market-based solution. Government backstops could help attract more private capital while actually saving taxpayer money in the long run, as is already the case for traditional terrorism risk insurance. The coronavirus pandemic once again shows that governments remain politically accountable for major catastrophes, and financial frameworks should be in place before disaster strikes.

Introduction

The Societal Benefits of Cyber Insurance

One of the most promising developments in cybersecurity has been the growth of cyber insurance. For insurance buyers, called insureds, cyber coverage can help hedge against a rising business risk. For the insurance industry, this emerging line of business represents a potentially large new market and source of long-term profits. But there is a larger public interest at stake, too: cyber insurance can help address the global challenge of pervasive cyber insecurity. A well-developed cyber insurance industry could collect the right information, and create the right incentives, to improve cybersecurity and reduce cyber risk on a vast scale.[4]

Insurance is not just a financial tool for the business community; it is an essential mechanism for economies and societies to manage risk. Mature, healthy, and competitive insurance markets are critical infrastructure.[5] They help companies assure their continued survival in the face of unpredictable events, inspiring confidence and encouraging investment. Insurers are also uniquely positioned to understand risks at a systemic level—leveraging claims data and other proprietary information to identify emerging risk patterns and warn of systemic vulnerabilities that no individual client could see.[6]

Armed with this data, the insurance industry has unique opportunities to help reduce the risks that it discovers. Through incentives like rate-setting, insurers can encourage their clients to behave more responsibly. Cyber risk reduction by individual organizations has many positive externalities. Data held by third parties would be better protected, supply chains would become more resilient, and the overall reduction of cyber vulnerability would lessen incentives to carry out malicious cyber activity. Robust insurance markets are therefore beneficial to society at large, not just to insurers and insureds.

Unrealized Potential

However, this potential remains largely unrealized.[7] The cyber insurance market is growing but still quite small compared to other insurance lines.[8] Only a small fraction of cyber losses is currently insured.[9] Part of the reason is that demand for cyber coverage remains limited. Many companies do not yet appreciate the full extent of cyber risk, or they assume that traditional insurance lines will protect them.[10] Others recognize the risk but see cyber insurance coverage as too narrow or ambiguous to guarantee adequate recovery.[11]

On the supply side, insurance companies are treading cautiously, expanding their offerings at a conservative pace.[12] Most cyber insurers offer only low coverage limits and high deductibles, and they may limit coverage in areas like business interruption, because cyber risk is difficult to estimate and price accurately.[13] For one thing, there is too little actuarial data to draw on. For another, traditional actuarial techniques are poorly suited to gauging cyber risk.[14] The risks at play evolve continuously based on unpredictable changes in digital technology itself, patterns of technological use, and threat actors' capabilities and intentions.[15]

Governments also have a stake in both the demand for and supply of cyber insurance. Many governments are interested in nurturing the cyber insurance market for its obvious economic benefits.[16] More government policymakers have also realized that cyber insurance has national security benefits, such as improving a country's resilience to hostile cyber attacks.[17] But at the same time, governments are wary of insurers becoming overly exposed to a poorly understood set of risks that could lead to their insolvency.[18] Insurer insolvency could cause claims to go unpaid or force governments themselves to pick up the tab.

These and other challenges of covering cyber risk are well-known in the insurance world.[19] Insurers, insureds, and governments have worked steadily and incrementally to address them. As a result, more cyber insurance coverage is sold each year—including policies specifically created for cyber risk (known as "standalone" cyber coverage), as well as some traditional lines, like property and casualty insurance, that are revised to include cyber alongside other risks (adding a "cyber endorsement" to a broader policy).[20] This growth in premiums collected has been accompanied by institutional maturation, as insurers develop more cyber expertise and refine their cyber practices.[21] The overall sense has been one of optimism.

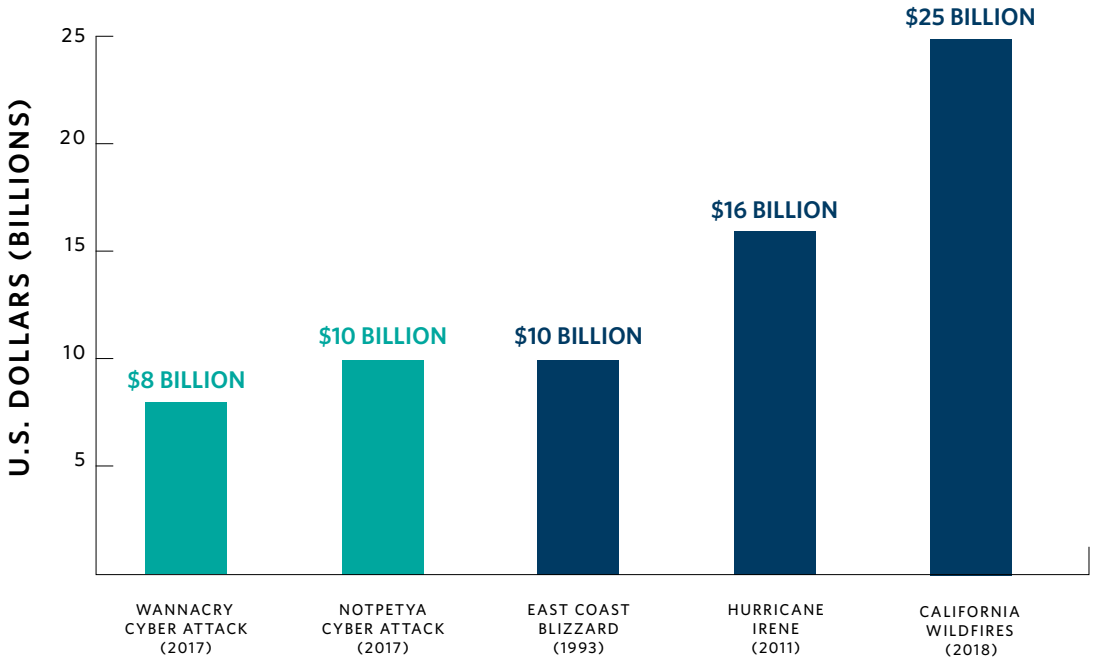
The NotPetya Challenge

But in 2017, an unprecedented cyber attack shook this optimism.[22] NotPetya, data-destroying malware released by Russian military intelligence, struck Ukraine and quickly spread around the world. Many called it the largest and most damaging cyber attack in history—costing hundreds of global businesses an estimated $10 billion, according to the leading insurance industry loss estimation service (see figure 1).[23] Victims lost access to data and needed to replace physical hardware. In addition, many faced substantial disruptions to business operations, resulting in lost revenue and damaged relationships.

The vast majority of losses—about $7 billion—were not covered by any insurance policy.[24] But the $3 billion of insured losses, and the overall magnitude of event, surprised many in the insurance market.[25] Industry leaders had considered the possibility of such a broad-based, high-impact cyber

FIGURE 1

Global Cyber Attacks Compared With Select U.S. Natural Disasters



SOURCE: Luke Gallin, "Re/insurance to Take Minimal Share of $8 Billion WannaCry Economic Loss: A.M. Best," Reinsurance News, May 23, 2017, https://www.reinsurancene.ws/reinsurance-take-minimal-share-8-billion-wannacry-economic-loss-m-best/; PCS, "Could Not-Petya's Tail Be Growing?," 2019, https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf; and National Oceanic and Atmospheric Administration, "Billion-Dollar Weather and Climate Disasters: Events," 2020, https://www.ncdc.noaa.gov/billions/events.

NOTE: The cost of these U.S. disasters is calculated in 2020 dollars.

event, but not every insurer had fully appreciated or planned for it.[26] NotPetya and a similar 2017 cyber attack called WannaCry were the first modern cyber incidents to inflict such high levels of simultaneous losses on hundreds of victims in dozens of countries. This phenomenon is known in the insurance industry as "aggregation": the risk of a single peril or trigger leading to many claims at once. Aggregation risks are financially dangerous for insurers, particularly when they cut across multiple geographic regions and economic sectors.[27] In such cases, it is difficult for insurers to limit, diversify, or swap portions of their exposure, as they might do for natural disasters.[28]

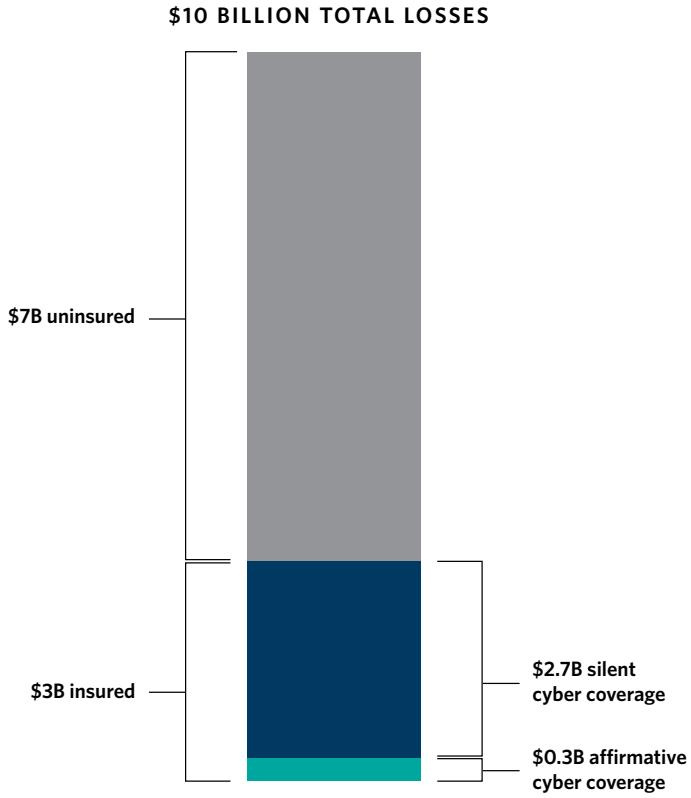
Faced with the unexpected NotPetya problem, insureds and insurers scrambled to respond. Insureds found themselves sifting through a patchwork of policies to find adequate coverage for their losses. The pharmaceutical company Merck, for example, claimed at least $1.3 billion in losses—mostly from business interruption, including disrupted sales and drug manufacturing.[29] Merck had dozens of policies that it hoped might apply.[30] Some of them specifically covered cyber incidents

("affirmative" cyber insurance), but as is often the case, these policies had relatively low limits.[31] Merck therefore turned to its property and casualty insurance, which were all-hazards policies with higher limits.[32]

Some of Merck's insurers paid its NotPetya claims.[33] This was the historical norm for high-profile, state-sponsored cyber attacks, like North Korea's 2014 hack of Sony Pictures Entertainment.[34] But other insurers saw huge claims that fell beyond the traditional ambit of their property and casualty policies and therefore did not pay. These policies, like many property and casualty policies, were silent about cyber risks—neither affirmatively covering them nor specifically excluding them. They may not have been written with cyber incidents in mind.

This "silent cyber" phenomenon can tacitly expose insurers to cyber risks they never collected premiums to cover, threatening their profitability and even solvency.[35] Silent cyber is also vexing for insureds because it leaves the scope of their coverage uncertain. Yet despite the ambiguities of such

FIGURE 2
NotPetya's Estimated Global Losses and Insurance Impact



SOURCE: Valeria Ermakova and Catherine Thomas, "Scrutiny of Management Approach Increases as London Cyber Insurance Market Grows," AM Best, March 2, 2020, http://www3.ambest.com/bestweekpdfs/sr774997420811full.pdf.F.

policies, insureds have strong incentives to invoke them following an extremely costly cyber event. Property and casualty policies simply tend to provide much higher coverage limits than standalone cyber policies do (see figure 2).[36]

Silent cyber was already a concern among insurers and regulators, but NotPetya showed the problem's scale to be far larger than many previous estimates.[37] The back-to-back occurrence of NotPetya and WannaCry suggested that additional incidents of this kind were possible. Subsequent modeling by the insurance industry found that a future global malware event, the so-called Bashe scenario, could be twenty times as costly as NotPetya (resulting in up to $193 billion in losses).[38] The threat of unpredictable, massive, correlated losses across many policyholders is an actuarial nightmare.[39]

Given the sheer scale of NotPetya and potential future incidents, it is no surprise that multiple insurers resisted Merck's claims. There is now ongoing litigation over the claims filed by both Merck and Mondelez, a food and beverage company that suffered at least $100 million in losses due to NotPetya.[40]

The War Exclusion Controversy

Facing silent cyber claims of a wholly new scale, Merck's and Mondelez's insurers made several legal arguments. One has drawn particular attention. The insurers argued that NotPetya, widely attributed to the Russian government, was excluded from coverage under clauses that address "hostile or warlike action" by states or their "agents."[41] Such clauses are commonly called war exclusions, though this particular language applied "in time of peace or war."[42] War exclusions have a long history in insurance but had not yet been applied to cyber incidents.[43]

The war exclusion clause offered a powerful legal defense in the face of unexpected and disputed losses, but it also raised problems of its own. The exclusion requires identifying the perpetrators, showing they acted as agents of a government, and characterizing the incident as "hostile or warlike." This type of analysis can be difficult with cyber incidents for technical, analytical, and legal reasons discussed below. Centering a coverage exclusion on these factors is an invitation to costly, time-consuming, and highly uncertain litigation. Moreover, applying war exclusions to a new class of perils raises many unanswered questions about the scope of the exclusion, as detailed in the next section.

Such uncertainty and transaction costs are harmful to all stakeholders and destabilizing to the marketplace as a whole. For insureds, the possibility that major state-sponsored cyber losses could be excluded suggests a large gap in the heart of their cyber coverage—placing them in a precarious position and reducing their motivation to purchase insurance for cyber claims. For insurers, the potential exposure to extraordinary, potentially correlated cyber losses poses a threat to their balance sheets.

Governments are caught in between—wanting to ensure that adequate coverage exists but not at the expense of insurer solvency. Failure in either direction could cost governments directly. If major cyber losses are uninsurable or uninsured, then victims of cyber incidents may expect governments to step in and make them whole. But if insurers offer too much coverage and become insolvent after a major event, governments may also be left holding the bag.

The war exclusion controversy is really a symptom of more fundamental challenges in the cyber insurance market that NotPetya helped to expose. First, cyber risk in general—and state-sponsored risk in particular—is greater than previously understood. Second, such risks remain difficult to estimate and price. Third, societies have yet to devise a comprehensive, sustainable set of mechanisms to allocate financial responsibility for major cyber risks. Fourth, this state of affairs leads to reliance on short-term solutions—with some insureds turning to ambiguous silent cyber policies, and some insurers invoking antiquated war exclusions in response.

Verdicts in the Merck and Mondelez lawsuits may help bring some clarity, but they will not solve these underlying problems. Instead, a new framework is required to address the insurance treatment of state-sponsored and other large-scale cyber incidents.

Understanding the Problem

War exclusions have existed since the 1700s and serve a recognized set of purposes. War has been called "the 'perfect storm' of actuarial nightmares: a correlated catastrophic, ongoing clash event."[44] It is highly destructive, potentially far-reaching in its geographic scope, and can have a broad impact on diverse civilian interests and industries. War therefore poses aggregation risks that are difficult for insurers to manage. Moreover, war cannot be predicted using actuarial analysis.

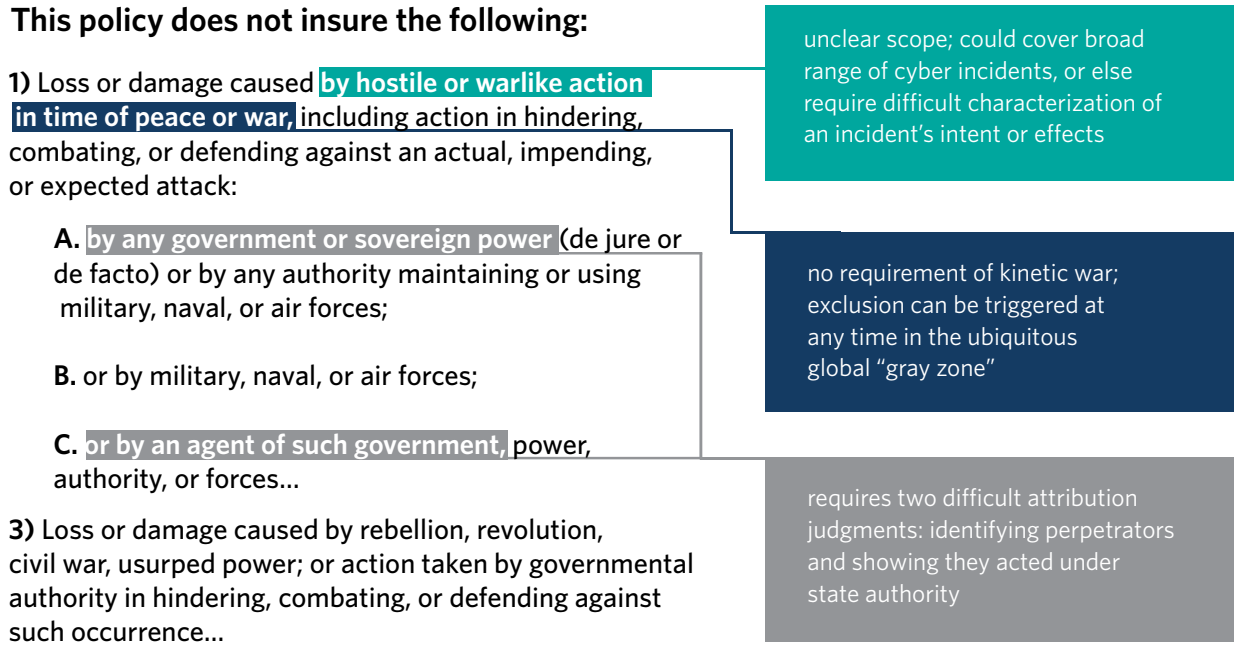
Insurance companies therefore came to exclude certain war-related claims to protect their overall financial viability.[45] In addition, there is a moral basis for war exclusions: some insurers are wary of encouraging aggression by helping to offset the costs of any blowback suffered by an aggressive state.[46]

These same rationales could arguably apply to "cyber war," or more precisely, to state-sponsored cyber operations. NotPetya showed that state-sponsored cyber operations can cause correlated and potentially catastrophic losses. Like kinetic wars, cyber incidents can also have cascading consequences—spreading from one victim to another and disrupting businesses or entire supply chains. And insuring against state-sponsored cyber operations can also pose a moral hazard. Governments could be more likely to launch them—or to take other aggressive actions that invite retaliation in cyberspace—if any cyber blowback is mitigated by insurance payouts.[47]

The specific language of war exclusions varies, but they are generally written in broad terms, especially in property and casualty policies. Merck's and Mondelez's property and casualty policies are particularly broad, excluding any "hostile or warlike action in time of peace or war," whether carried out by a government or its "agent" (see figure 3).[48] The umbrella term "war exclusion" can therefore be misleading. It can conflate war-specific clauses with others that apply during both war and peace, and some clauses may not even require any act of violence. In the cases of Merck and Mondelez, broadly written exclusions enabled insurance companies to argue that NotPetya fit their literal terms and intent.

FIGURE 3

Merck's War Exclusion as Applied to Cyber Claims



SOURCE: Response of Generali in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

However, there are several challenges in applying war exclusions to cyberspace. Some challenges, like attribution, are well-known but often poorly understood. Others are rarely highlighted. A comprehensive and detailed account of these problems is crucial to ensuring that any potential solution aims in the right direction and avoids repeating old mistakes.

Attributing Cyber Incidents

Applying a war exclusion clause requires "attribution"—determining who is responsible for an incident. For cyber incidents, attribution is a complex topic often clouded by misunderstandings. Many people falsely assume that cyber attribution is close to impossible. National leaders have even promoted this fiction to cast doubt on truthful allegations of state-sponsored operations.[49] In reality, the most capable intelligence agencies and private firms have become adept at attribution and can now make near-certain judgments under the right circumstances. Development of this capability has been a crucial step on the long journey toward establishing greater accountability for state-sponsored cyber operations.

But the most successful cases of cyber attribution can lead people to make the opposite error—thinking the challenge of cyber attribution has been largely "solved" through technical advances.[50] The truth is that no two attributions are alike, and no cyber incident is guaranteed to yield a highly confident or persuasive attribution. Cyber attribution depends on at least three factors: the quantity and quality of evidence available, the technical and analytical sophistication of investigators, and the credibility of the investigative process in the eyes of key audiences and decisionmakers. These factors vary greatly from one situation to the next.

Attribution in insurance litigation. Such variance is a fact of life for national policymakers and cybersecurity researchers, but it can pose major legal and financial challenges in the insurance industry. While attribution will be straightforward for some cyber insurance claims, in other cases it will be fuzzy and contested or not possible at all. Those cases may lead to costly, time-consuming, and uncertain litigation. Allowing billion-dollar insurance decisions to turn on attribution is therefore a costly gamble for insurers, insureds, and regulators alike. In fact, the pending Merck case may possibly represent the most amount of money ever wagered on proving cyber attribution in court.

At first blush, any difficulties in establishing attribution would seem to benefit insureds. Insurers bear the legal burden of showing that an exclusion applies; invoking the war exclusion therefore requires insurers to prove attribution.[51] However, the situation is more complicated than that. Large international insurers and reinsurers could have their own advantages. They might become repeat litigators, and in some cases, they would have a resource advantage over their policyholders. If a major cyber incident were to leave an insured scrambling for cash, it might not be able to afford the time and expense of a lawsuit. It is therefore unclear which party would most benefit from these uncertainties; the answer may vary from case to case.

The question of who benefits is ultimately too narrow. The whole system suffers when coverage is uncertain and disputes are costly to resolve. Moreover, insurance requires a sustainable long-term bargain between insurers and insureds (with governments, reinsurers, and other market players all exerting influence). Ambiguous insurance contracts that skew the transaction toward one side or the other will hinder overall market development. In other words, everyone has a stake in preventing insurance disputes from being unnecessarily bogged down in difficult matters like attribution.

Process and purpose. No universal, generally applicable process exists for cyber attribution. The evidence considered, methodology used, and standard of proof required in any given instance depends on who is performing attribution and what purposes they have. For example, U.S. criminal cases against hackers apply different burdens of proof at each stage of the legal process—from "reasonable suspicion" to "beyond a reasonable doubt"—and such cases follow well-defined rules of evidence.

By comparison, intelligence agencies might render judgments with what they deem "high," "moderate," or "low" degrees of confidence, and they can draw on unique information sources unavailable in open court.[52] Unlike courts, different intelligence services might offer competing assessments of the same incident and may update their judgments continuously as more evidence emerges.

Diplomacy is another story entirely. No matter what courts or intelligence agencies conclude, national leaders must decide for themselves what level of certainty is enough to hold another sovereign state accountable for a cyber incident. Such subjective political decisions have no formal criteria.[53]

Since different elements within the same government have different approaches to attribution, it stands to reason that different governments around the world will vary even more. International organizations and private companies also have diverse approaches to performing attribution, based on what they each seek to accomplish.

For the insurance industry, attribution would be grounded in specific contract language as interpreted and applied by courts of jurisdiction. No court has ever ruled on how war exclusions apply to cyber claims, so no one yet knows what sort of attribution will be required. That said, the contracts at issue in NotPetya litigation offer some clues.

The Merck and Mondelez war exclusion clauses seem to require two layers of attribution: first, identifying the perpetrator of the cyber incident in question (a person or organization), and second, showing that the perpetrator acted under state authority. (A related but distinct problem, characteriz-

ing the perpetrator's actions as "hostile or warlike," is discussed later.) Both layers can be challenging depending on the circumstances, particularly if a judge or jury is the ultimate decisionmaker.

Challenges in identifying perpetrators. Cyber actors tend to leave technical and behavioral footprints that can help to distinguish them from other hacking groups and potentially identify them. Their patterns and occasional mistakes provide clues to investigators, and the clues from many incidents can be synthesized to track actors over time and across victims. Of course, identifying the perpetrators of a cyber incident requires overcoming their own active efforts to obscure or sow confusion about their identities and locations.

Sophisticated cyber actors typically operate through multiple layers of compromised third-party networks residing in other countries. They may use generic tools and tactics to avoid a clear technical fingerprint, or they may even repurpose malware and digital infrastructure associated with other actors to masquerade as someone else.[54] Many hacking techniques are designed to complicate forensic analysis—for example, the wiping of log files, encryption of exfiltrated data, or use of stolen credentials and local executables to obviate the need for malware.[55]

These challenges to attribution can be overcome. Through painstaking detective work and careful analysis, governments and private cybersecurity firms have made great strides in the science and art of cyber attribution.[56] This progress has enabled legal, diplomatic, and military responses to malicious cyber activity, helping to bring more accountability to the chaotic domain of cyberspace. Continued investments in attribution are critically important.

Nevertheless, attribution remains an uncertain process; the quality of its results varies significantly from case to case. In addition, many of the attribution methods used by governments and private firms were not designed to resolve insurance claims and do not translate readily to this new arena.

For example, cybersecurity firms can often attribute multiple cyber incidents to a common group of actors and a suspected national affiliation, but they may not know the actors' true names or the specific government agency that sponsors them. Hence, these threat groups receive pseudonyms, like Charming Kitten, or Advanced Persistent Threat 37 (APT37).[57] It remains unclear whether this level of specificity will satisfy courts adjudicating cyber-related insurance claims.

Attribution can also be a highly technical exercise, involving detailed analysis of technical signatures. Juries and even judges can have difficulty navigating this unfamiliar terrain, forcing them to rely on expert witnesses. In high-stakes litigation, each side has ample incentive to find friendly experts—or at least someone who can cast doubt on the other side's position. Juries and judges may fail to prop-

erly weigh the competing claims of experts, leading to unpredictable verdicts, as happens in other areas of complex litigation.[58] Such randomness then alters litigation incentives. It encourages parties with weaker cases to try their luck in court, or to extract more in a settlement than they might really deserve.

Challenges in establishing state authority. When a cyber incident is successfully attributed to specific perpetrators, showing that they acted as state "agents" is yet another matter. Many states employ proxy forces in cyberspace for the express purpose of maintaining plausible deniability. These proxy relationships vary greatly in their nature and the level of government oversight.[59]

Some states exercise strict command-and-control in a military-type setting. In such cases, it can be possible to reliably infer state authorization for specific cyber operations. But other states broadly tolerate cyber actors who behave in the government's interest and signal their desires indirectly. In between these two extremes is a murky middle ground that poses difficult line-drawing problems. To cite a few examples, governments might provide general guidance but not oversee individual operations, state-affiliated cyber actors could sometimes act on their own initiative or moonlight on the side, and both parties may use subtle forms of coercion or enticements to influence the other.

Under which of these circumstances would an "agent" relationship exist for the purpose of insurance claims? Intelligence analysts investigating malicious cyber incidents are well-versed in complicated proxy relationships. And national leaders enjoy the flexibility to decide, on a situational basis, when attribution is sufficient for their diplomatic or public policy purposes. But courts must aim for a predictable, consistent set of legal rules, and they have yet to develop a jurisprudence for cyber attribution in insurance disputes over the war exclusion.

Critically, just because a cyber actor often works at a state's behest does not mean he or she does so in all instances. For example, FireEye, a leading cyber intelligence firm, has assessed that a threat group it calls APT41 "carries out Chinese state-sponsored espionage activity *in addition to* financially motivated activity *potentially outside of state control* [emphasis added]."[60] This kind of moonlighting is not unusual among state-sponsored cyber actors, and it indicates the difficulties of applying conventional attribution techniques to resolve cyber insurance claims. If APT41 were found responsible for an insurable cyber incident, it would still remain to be determined whether that specific incident was state-directed.

Courts would face evidentiary challenges in resolving such questions. While hackers themselves can be tracked with forensic techniques, finding evidence of government foreknowledge or authorization can require active intelligence collection, like recruiting human sources or intercepting communica-

tions.[61] Even for intelligence agencies, this evidence is hard to collect and parse. Governments that oversee offensive cyber operations may actively thwart outside investigations by using strict security measures and limiting knowledge of sensitive operations to a close-knit inner circle.

Compared to intelligence agencies, private firms retained by insureds or insurers are much less equipped to monitor foreign leaders' decisionmaking. They must often make informed inferences about a cyber actor's state sponsorship—for example, by comparing a cyber actor's known targets to presumed geopolitical interests of the suspected state sponsor.[62] Reliance on such inferences can lead to less confident assessments. In some cases, cybersecurity companies may settle for a "suspected attribution" or describe hackers as generally "affiliated with" a foreign government but decline to assess the nature of that affiliation.[63] Whether these hedges would be enough to legally establish an agent relationship under the war exclusion is unknown and may be a question that requires extensive litigation to resolve.

Limits of government attribution. In the face of these challenges, it is tempting to defer to government attribution—such as the coordinated statements by the United States, the United Kingdom (UK), and five other governments attributing NotPetya to the Russian government.[64] After all, governments have access to unique intelligence sources and are often best positioned to establish firm attribution. However, this approach would have several drawbacks.

Most fundamentally, deference to governments would be a piecemeal solution. Governments do not make public attributions of most cyber incidents. They may lack conclusive evidence, may want to avoid jeopardizing intelligence sources, or may believe public statements would be diplomatically or politically counterproductive. The public statements they do make sometimes lack detail, like the recent warning by the Federal Bureau of Investigation (FBI) that actors "affiliated" with the Chinese government were targeting coronavirus-related research data.[65]

When governments do go public with their attributions, the raw intelligence information underlying their assessments typically remains classified. U.S. courts do have procedures for hearing classified evidence in secret, and the government has sometimes offered classified evidence to help resolve war exclusion disputes.[66] Some commentators have therefore proposed new mechanisms to facilitate this practice for cyber insurance litigation involving the war exclusion.[67] But the U.S. government has been reluctant to share its most sensitive intelligence, even in a judge's chambers without any litigants present.[68] It is unclear whether courts would give credence to partial or conclusory government statements, particularly if they were contested by other public evidence.

Government attribution is not always beyond dispute. In 2014, the FBI publicly attributed the Sony hack to North Korea, and then president Barack Obama personally confirmed this attribution at a press conference.[69] Nevertheless, many outside experts treated this attribution with great skepticism based on alleged weaknesses in the FBI's public case.[70] Four years later, the U.S. Department of Justice released a detailed, 179-page indictment accusing a North Korean named Park Jin Hyok of involvement in the Sony hack, WannaCry, and other incidents.[71] Yet a number of Sony executives and other people directly affected by the hack continue to doubt the North Korea attribution.[72]

Over time, most analysts have come to accept the U.S. government's attribution of the Sony hack. The cyber attribution process of U.S. intelligence agencies has earned substantial public credibility, and the Department of Justice laid out a powerful "speaking indictment," filled with more persuasive detail than was legally necessary, to make its case. But if a Sony executive can remain skeptical despite the weight of evidence, then so might an average juror who hears from dueling experts in a cyber insurance lawsuit.

The NotPetya public attribution and the Park indictment were highly credible, but other government attributions could be dubious. Public attributions offered by governments may sometimes be colored by ulterior strategic or domestic political motives—the cyber equivalent of the 1964 Gulf of Tonkin incident, an alleged torpedo attack by North Vietnam that U.S. leaders mischaracterized to justify military escalation.[73] And some governments might simply lack the analytical or technical capacity to support sound attributions. Not every government has a pool of well-trained cyber investigators or an institutional culture that rewards critical thinking.

Like governments, private cybersecurity companies that perform attribution vary greatly in their credibility and motivations. Some are highly credible, while others have questionable or unknown practices.[74] A single cyber incident could therefore lead to competing attributions by multiple governments and/or cybersecurity firms.[75] One attribution may be much more sound than the others and convince the vast majority of credible experts. Even so, a sliver of doubt could be exploited in litigation. This dynamic could be costly and unpredictable for insurers and insureds.

Finally, there is risk of a distorting feedback loop between governments and the insurance industry. If insurers and insureds come to routinely invoke government attribution statements in high-stakes litigation, this could influence whether governments speak in public and what they choose to say. Obama's decision to label the Sony hack as "cybervandalism," rather than "war," was partly intended to avoid prejudicing Sony's insurance claims.[76] In the future, governments might be even more reticent—or worse, overeager and biased—based on the domestic or international political implications of specific cyber-related insurance disputes.

Institutional reforms might help to overcome some aspects of the attribution challenge. An international consortium of insurers and insureds could fund its own best-in-class attribution capability, or it could designate a group of elite cybersecurity companies to perform this function and then mutually agree to abide by whatever assessments emerge. This consortium might also set out criteria for considering highly credible government attributions. But such reforms would reinforce the war exclusion's undue focus on state sponsorship, a problem discussed later. Moreover, attribution is not the only challenge in applying war exclusions to cyber claims.

Characterizing Cyber Incidents as Hostile or Warlike

When the perpetrator of a cyber incident is identified and known to be acting under state authority, a third question remains: whether the cyber incident can be characterized as "hostile or warlike," per the language of Merck's and Mondelez's war exclusions. This language is ambiguous and so far lacks any judicial precedent to clarify its scope in cyberspace.

Unclear scope in cyberspace. On its face, "hostile or warlike action" can be read quite broadly. The phrase "hostile action" has been particularly ill-defined by courts.[77] In the cyber context, some commentators believe this wording could encompass a wide range of state-sponsored incidents—not only rare destructive or coercive cyber attacks but also everyday breaches carried out for intelligence gathering and data theft.[78] Such breaches could be deemed part of a "hostile" campaign of economic espionage, for example.[79] This broad interpretation would be relatively easy for courts to apply, as it would not require making fine distinctions between cyber incidents. But such an interpretation would create a gaping hole in cyber insurance coverage by excluding nearly any state-sponsored incident.

Other experts believe the war exclusion should be read narrowly in cyber cases. They cite long-standing legal precedents—from noncyber cases—that limit war exclusions to insurance losses closely associated with kinetic military conflicts.[80] U.S. courts, for instance, have ruled that actions against "civilian citizens of non-belligerent powers and their property at places far removed from the locale or the subject of any warfare" would not qualify as "warlike operations."[81] That is a good description of NotPetya, suggesting the war exclusions might not apply in such cases under this interpretation.

That being said, pre-digital concepts like "the locale of warfare" would be open to interpretation in the era of cyber conflict. For now, that question leaves insureds, insurers, and governments to guess about which kinds of state-sponsored cyber operations will be excluded under traditional war clauses.

If a narrow interpretation of the clause prevails, then courts would eventually need to fashion rules for differentiating "hostile or warlike" cyber operations from other kinds. In particular, they might look to the intent of the perpetrator or the effects of a cyber incident. Both routes would bring challenges.

Challenges in assessing intent. If courts look to intent, the first question would be *whose* intent matters: that of the cyber actor sitting at the keyboard, the government handler issuing guidance, or the senior political leader setting national policy for cyber operations? These individuals may have varying intents, especially in states with loose command and control of cyber operations.

For example, the Russian government has a national policy of allowing domestic cyber criminals to freely target Western companies. The government does not necessarily direct their day-to-day activities, though it does actively support them by obstructing foreign law enforcement.[82] In exchange for this protection, Moscow bars Russian cyber criminals from targeting domestic entities and requires them to accept government tasks when needed. An individual Russian cyber actor stealing corporate data may view himself as committing simple theft against one company. But in Moscow's eyes, he may be participating in general economic warfare against the West and helping to fund a cyber reserve corps on call to defend the Russian state. Whether this activity is considered "hostile or warlike" may depend on whose intent counts.

A single actor can also have mixed motives for conducting a cyber operation, with some being more "hostile or warlike" than others. For example, the U.S. Department of Justice recently indicted two Chinese hackers for stealing trade secrets and conducting other hacking activities on behalf of China's Ministry of State Security. By itself, corporate espionage might not be deemed "hostile or warlike," even if state-sponsored. But the prosecutors in this case argued that China's policy was more sweeping in nature—"using cyber-enabled theft as part of a *global* campaign to 'rob, replicate, and replace' non-Chinese companies in the global marketplace."[83] In other words, a self-interested criminal intent allegedly coexisted with a larger strategic intent. Cases involving mixed motives would create more legal uncertainty.

Finally, intent can change over time. State actors may spend months or even years inside a single victim's network, and during this time they may pursue a number of different objectives.[84] For example, a state-affiliated cyber actor might first penetrate a network on his or her own initiative, then assess what data is available, and only later decide what to do with it—commit cyber crime for

personal gain, contact a government agent to negotiate joint work, or sell the network access to another cyber actor. Even under strict government oversight, cyber operations can evolve based on shifting state priorities. Network access originally obtained and exploited for espionage may be repurposed for more destructive ends during a foreign policy crisis.

In fact, cyber actors and their government overseers do not always have fully formed intents at all; they sometimes target whatever networks seem vulnerable, with a general goal of developing options for unforeseen contingencies. The U.S. military even has a doctrinal term, "operational preparation of the environment," to describe network penetrations that are not themselves destructive but would enable future destruction.[85] Changes in intent could complicate insurance litigation when complex cyber breaches are discovered years after the fact. Losses of different kinds, triggered at different points in time, might need to be individually litigated to determine whether each one was "hostile or warlike."

Then there are the evidentiary challenges. The most compelling evidence of intent comes from direct access to the cyber actors or their government sponsors—for example, interception of their private communications, or a human source who elicits a confession. Acquiring such evidence generally requires active intelligence collection by governments. In its absence, courts might need to infer intent from the perpetrator's actions—an uncertain enterprise.

After all, cyber actions do not always reliably reveal intent. For example, a cyber actor who intends to inflict damage and disruption often behaves in much the same way as someone aiming merely to collect data.[86] Both actors might begin by probing a vulnerable system and finding an initial access point, then move laterally within the network and escalate user privileges, while also working to secure a persistent presence and extract any files of interest. Any disruptive intent may only become apparent in the final moment—for example, when the cyber actor deploys malware that deletes critical data. Depending on when a breach is discovered and remediated, the actor's true intent may never be revealed.

Challenges in assessing effects. Given the difficulties of assessing intent, courts might look instead (or in addition) to the actual effects of a cyber incident. Effects can be observed more directly and reliably. However, the effects of an incident can also diverge from what the perpetrators intended. This disconnect could mean that actions meant as merely malicious could be classified by courts as "hostile or warlike," or vice versa.

For example, businesses often choose to shut down their networks to contain and remediate a major breach. The perpetrators may have done nothing intentionally disruptive, yet the victim could still suffer severely from business interruptions.[87] Cyber operations can also unwittingly cause much greater harm than intended if malware spreads unexpectedly or if consequences cascade in unforeseen ways. In other cases, seemingly ordinary data thefts could threaten a company's reputation, competitiveness, or liquidity—perhaps well beyond what the perpetrator envisioned.[88]

Conversely, cyber operations actually intended as "hostile or warlike" might not produce effects that demonstrate this clearly. For example, a hostile government might seek to distract, confuse, and destabilize an adversary state through a broad-based campaign of cyber intrusions. Individually targeted companies might not discern—let alone be able to prove in court—that apparently run-of-the-mill cyber incidents were actually part of a covert operation targeting society as a whole. In other cases, the perpetrating state might carry out "loud" cyber operations in hopes of being discovered and thereby sending a signal of warning or displeasure.[89] The intent may be hostile even if the effects are marginal or transitory.

In sum, characterizing a cyber incident as "hostile or warlike" is more difficult than recognized. A broad interpretation could sweep in most state-sponsored cyber incidents. A narrow interpretation could require assessing the perpetrators' intent (which can be elusive) or its effects (which may be unexpected or misleading). While the war exclusion's attribution problem has received the most attention, its separate characterization problem may be just as difficult to litigate, if not more so.

The Overinclusiveness of War Clauses

Attribution and characterization problems are not wholly unique to cyberspace. Covert or proxy attacks in the physical realm may raise similar challenges when war exclusions are invoked. But there is at least one essential difference: kinetic attacks are much rarer than cyber operations. Most companies will never be victims of war or other state-sponsored kinetic attack. Those at greatest risk, because of their operations in contested territories, know to take protective measures. As a result, the challenges of applying war exclusions for kinetic attacks have only limited practical consequence.

State-sponsored cyber operations, however, are quite common. They happen with increasing regularity during peacetime in all countries. Almost any company is at risk from state-sponsored cyber operations, whether purposeful or opportunistic. The prevalence of state-sponsored cyber operations magnifies the impact of war exclusions, including their ambiguity and uncertainty.

Value for insureds. For insureds, an entire class of routine cyber threats (those sponsored by states) could lack reliable insurance protection due to the war exclusion. Yet these threats are a primary rationale for purchasing cyber insurance, especially for large organizations. Consider that most cyber incidents cause relatively small losses, enabling large organizations to self-insure.[90] It is the outlying events that call for insurance—those that cause exceptional losses and that are difficult or impossible to prevent or predict. A disproportionate number of these incidents are state-sponsored. State actors have been behind many of the most expensive cyber incidents documented in recent years—including NotPetya; WannaCry;[91] and the breaches affecting Equifax,[92] Yahoo!,[93] and Marriott.[94]

If war exclusions are used to deny claims for state-sponsored cyber incidents, then organizations will be unable to insure themselves against the most important part of today's cyber risk landscape. This would be particularly true if war exclusions are interpreted broadly to include state-sponsored data thefts and breaches of personally identifiable information. If that happens, large organizations could conclude that insurance for cyber incidents is not very valuable.

Without reliable insurance coverage, organizations would lack adequate means to manage the serious and growing threat of state-sponsored cyber operations. They could always invest more in cyber defenses and resilience, of course. But state-sponsored cyber incidents can be extraordinarily difficult to prevent, detect, and remediate—even for large, sophisticated organizations.

Many state-sponsored cyber actors are highly skilled, organized, well-resourced, and persistent.[95] Unlike ordinary hackers, some can leverage the tools of national power to carry out complex, blended operations—for example, using human and signals intelligence to facilitate network access, or collaborating with state media to amplify leaks of stolen data.[96] And state-sponsored cyber actors enjoy near-immunity from legal recourse.[97] In contrast, victims themselves are typically constrained from "hacking back" or other forms of active cyber defense under domestic law.[98]

Private entities, in short, are seriously overmatched by state-sponsored cyber threats. This is clear from the long list of global companies and organizations that have been compromised to date. And the potential impact of a state-sponsored cyber incident can be substantial. Among small businesses, it is not uncommon for cyber incidents (whether state-sponsored or not) to result in bankruptcy or liquidation.[99] Among large businesses, the most serious cyber incidents have caused billions of dollars in direct expenses, liability, lost shareholder value, and reputational damage.[100]

Given the limitations of preventive measures and self-help, insurance becomes a critical tool for organizations to hedge against state-sponsored cyber threats. Blanket exclusions on coverage for state-sponsored incidents, or even significant uncertainty about coverage, would leave many organizations overexposed. Financial harm could occur well in advance of an actual cyber incident, because creditors and investors increasingly estimate cyber risk and incorporate it into capital allocation decisions.[101]

Insurers' interests and the government's role. Of course, what insureds view as an overly broad exclusion may look to insurers like prudent risk management. Most insurers are taking a conservative approach in the cyber market, as they have done in the past for other emerging risks. But in the long run, growth in this market will require coverage to be adequate and clear. Insurers have an interest in establishing viable ways to cover the most salient risks, and in persuading insureds that coverage is reliable. These risks arguably include state-sponsored cyber incidents.

Some insurers may take a principled position against covering any state-sponsored cyber incidents. There is a philosophical argument that governments, not private entities, should bear the financial burden of hostile international acts. And there is a practical case that state-sponsored cyber incidents are too difficult to insure—for example, they may not qualify as independent or chance events. Still, insurers with this viewpoint should not necessarily be satisfied with traditional war exclusions. Depending on how terms like "hostile or warlike" are interpreted, they may fail to exclude coverage for some state-sponsored cyber incidents, like many data breaches.

So far, governments have chosen not to assume financial responsibility for state-sponsored cyber incidents suffered by private organizations. And the historical precedents set by kinetic wars reveal that different governments at different times have had varying policies on compensation for domestic war victims. These range from no compensation at all, to public-private insurance programs, to government indemnification for some losses.[102] Government insurance backstops, discussed later, offer a promising middle path for cyber losses. Without backstops in place, insurers' appetite for covering state-sponsored cyber risk remains an open question.

The Underinclusiveness of War Clauses

Whether or not insurers seek any exposure to state-sponsored cyber risk, they and their regulators must remain mindful of other forms of catastrophic risk that could also threaten solvency. War exclusions may be broad, but they do not entirely protect insurance companies from all large-scale,

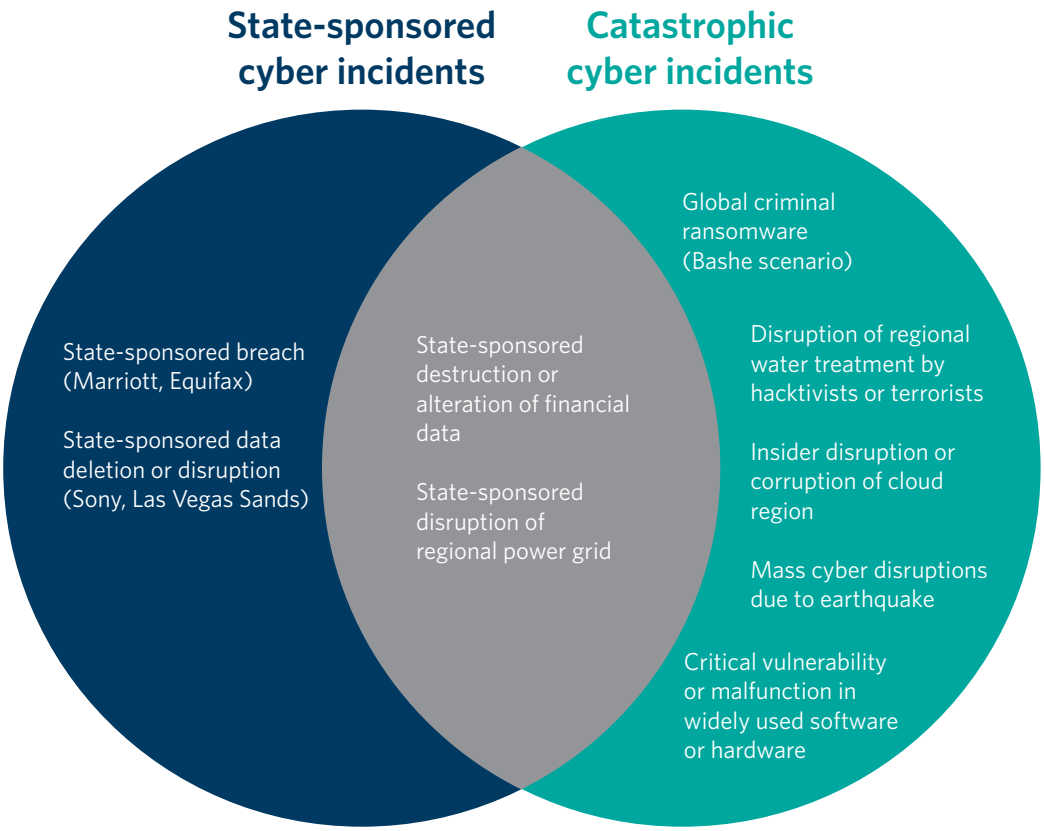
aggregated events (see figure 4). It is possible to imagine a future NotPetya-like attack, or something even more devastating, being carried out by nonstate actors, happening by accident, or being caused by a natural disaster. War exclusions would be no help to insurers in those cases.

Independent cyber criminals can be as capable as some state-sponsored actors and have conducted many large-scale extortion and data theft operations.[103] In 2019, an insurance consortium surmised that cyber criminals could launch a ransomware attack many times more costly than NotPetya.[104] Hacktivists and terrorist groups, traditionally less capable, may some day acquire powerful cyber tools sold on the black market or accidentally released by states.[105] Insiders with privileged access to cloud servers and other valuable digital assets can inflict tremendous costs, as demonstrated in the 2019 CapitalOne hack.[106]

A NotPetya-style cyber incident could even occur by accident. A faulty software update, for instance, could disable or damage millions of devices.[107] Alternatively, a physical trigger like an earthquake could damage or disrupt computer equipment and cause cascading cyber-related consequences.

FIGURE 4

Imperfect Correlation Between State Sponsorship and Catastrophic Cyber Risk



As these various scenarios illustrate, insurers should not mistake war exclusions for general exclusions of cyber catastrophes. War exclusions only apply to state-sponsored incidents, not other triggers that can lead to similar impacts. Of course, war exclusions were never designed to do any more than that. But the spotlight on NotPetya makes it easy to lose sight of other important cyber risks. If NotPetya is seen as the paradigmatic cyber catastrophe, then state sponsorship will be wrongly conflated with extreme cyber risk itself. The two are only partially correlated, with war exclusions serving as a crude proxy for catastrophic risk. To effectively manage the risk of cyber catastrophes, insurers need tools tailored to that purpose.

Comparison With Terrorism Exclusions

The NotPetya litigation has focused attention on war exclusions, but these are not the only clauses at issue in the lawsuits. Some of Merck's insurers have also invoked a terrorism exclusion, which presents very similar difficulties (see figure 5).[108] A general discussion of terrorism exclusions is beyond the scope of this paper. For present purposes, the key point is how terrorism exclusions reproduce many of the same problems discussed above.

FIGURE 5

Merck's Terrorism Exclusion as Applied to Cyber Claims

Notwithstanding any provision to the contrary within this insurance or any endorsement thereto it is agreed that this insurance excludes loss, damage, cost or expense of whatsoever nature directly or indirectly caused by, resulting from or in connection with any act of terrorism regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

For the purpose of this endorsement an act of **terrorism means an act, including but not limited to the use of force or violence and/or the threat thereof,** of **any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organization(s) or government(s), committed for political, religious, ideological or similar purposes** including the intention to influence any government and/or to put the public, or any section of the public, in fear.

This endorsement also excludes loss, damage, cost or expense of whatsoever nature directly or indirectly caused by, resulting from or in connection with any action taken in controlling, preventing, suppressing or in any way relating to any act of terrorism.

violence not required; cyber incidents can trigger exclusion

state-sponsored acts can trigger exclusion

state-sponsored cyber operations inherently have political purposes

SOURCE: Response of Atrium in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

Merck's terrorism exclusion, for example, refers to "any act, including but not limited to the use of force or violence."[109] No kinetic attack is required; a cyber incident could trigger the clause, just as with the war exclusion. The terrorism exclusion is also similarly broad. It excludes coverage of any acts "committed for political . . . purposes," which almost by definition applies to state-sponsored cyber operations. Whether governments have strict or loose oversight of these operations, their objectives are inherently political, namely advancing national or economic security. The terrorism exclusion, then, could apply to most if not all state-sponsored cyber operations—much like the war exclusion in its broadest interpretation.

If phrases such as "political purposes" are interpreted more narrowly, then courts would need to characterize the intent behind a cyber incident to distinguish truly "political" incidents from others. The difficulties of such characterization analysis were discussed above. Moreover, determining the perpetrators' intent often depends on knowing their identity—one aspect of the attribution problem.

In short, Merck's war and terrorism exclusions have a similar scope and raise similar problems when applied to cyber claims. It is therefore no surprise they are both being litigated in parallel. Unfortunately, the terrorism exclusion has received much less attention in this context. This paper will primarily refer to the war exclusion for the sake of simplicity. Its analysis and recommendations apply to both clauses unless stated otherwise.

Assessing Current Industry Efforts and Trends

The war exclusion is not well-tailored to today's cyber risk landscape. It is overinclusive in some ways, underinclusive in others, and leads to costly and uncertain lawsuits. Another approach is needed.

Since Merck and Mondelez filed suit in late 2018, the insurance industry has grappled with these issues. The lawsuits themselves are among several efforts to seek clarity and stability for the marketplace. Insurance experts have also been exploring alternatives to traditional war exclusions. Industry discussions have laid an important foundation, but no single proposal will solve this problem in the short run. Reforming the marketplace likely calls for multiple new ideas and concerted action over time from a broad range of stakeholders.

The NotPetya Litigation

For almost two years, the Merck and Mondelez cases have been focal points for discussions about cyber risks and war exclusion clauses.[110] As the first live cases to test these issues in court, the two lawsuits have generated much suspense.[111] Clear and consistent rulings in both cases would reduce

uncertainty about how war exclusion clauses apply to cyber claims—clarifying interpretive issues like the scope of the clauses, as well as practical issues like how to handle attribution and characterization. Even if the rulings leave one or more parties unsatisfied, they could still provide a baseline. Such an outcome would help settle expectations and create a starting point for further negotiations among insurers, insureds, and regulators about the future of cyber insurance.

The judges in these cases could also provide an important intellectual contribution by publishing thoughtful analyses of the difficult issues at stake. Given the litigation's scale and complexity, both courts will hear strong arguments from skilled advocates who have conducted deep research. The judges will have opportunities to weigh practical concerns too, like how various rulings might impact insurance markets. At the end of this intensive, adversarial process, they may be able to offer fresh perspectives and perhaps identify legal approaches not previously considered.

While there is reason to be hopeful, the insurance industry should temper its expectations for these cases. Most obviously, the two cases could produce inconsistent verdicts, further fueling uncertainty. Short of that, there are several reasons why the NotPetya litigation might still fail to provide broad, timely guidance to the marketplace.

Precedent may be elusive. First, the insurers in these cases have invoked a broad array of defenses—including not only the war and terrorism exclusions but also various other contract wordings and legal arguments.[112] Some disputes involve the specific conduct of the parties.[113] It is quite possible that these lawsuits will be resolved on grounds other than the war or terrorism exclusions. Such verdicts would leave the industry no more informed than before about how to interpret these clauses for cyber incidents.

Second, any legal precedents emerging from these cases would be somewhat limited by their facts. This limitation starts with the specific language of Merck's and Mondelez's respective war exclusions, which is not exactly the same; such language can vary widely in insurance contracts.[114] Additionally, the courts may well look to other communications between the parties, or the insurers' specific marketing and underwriting practices, to parse their intentions—potentially limiting the precedential value of any decisions.[115] Future cyber incidents may also be different from NotPetya, inviting new rounds of legal arguments. For example, it is rare for multiple Western governments to make coordinated public statements of attribution, as happened with NotPetya. A future case with more ambiguous attribution could yield different results.

Third, trial judgments could still be many months or even years away, and they would not be legally binding on other judges in future cases. Binding precedents in the U.S. judicial system require appellate rulings, and appeals in these cases would create additional delays and uncertainty.

Meanwhile, the parties always have the option to settle privately—before, during, or even after a trial.[116] Settlement might benefit both plaintiffs and defendants, but it would also defer a public reckoning of the legal issues at stake.

Litigation looks backward. Fourth, and most importantly, this litigation is backward-looking in nature: it addresses the historical meaning of previously agreed-upon contract language. The legal issues at stake in the cases are completely distinct from the forward-looking question of how insurance contracts *should* handle future cyber incidents. The forward-looking policy question must be decided by insurers, insureds, and regulators themselves. While the Merck and Mondelez cases grind on, insurers already are issuing new contracts and renewing old ones—raising an immediate question of what language should govern state-sponsored cyber incidents. Once the judges have ruled in the NotPetya cases, the industry will then need to evaluate whether their decisions provide useful, agreeable means of resolving future cyber claims.

A verdict, after all, reflects a judge's legal interpretation—not necessarily the policy consensus of all stakeholders, including other government agencies. This reality brings political and regulatory risks. For example, an insurer victory in court could be fleeting if regulators or legislatures countermand the ruling with new requirements to cover NotPetya-like incidents.

There is ample history of such regulatory blowback. After Hurricane Andrew devastated Florida in 1992, the insurers that survived sought to curtail their exposure to future hurricanes.[117] The Florida legislature responded by restricting this curtailment for several years. California took similar action in the wake of recent devastating wildfires.[118] There are now ongoing discussions in Congress and in state legislatures over some form of mandatory pandemic insurance to cover outbreaks like the novel coronavirus.[119] Given the possibility of regulatory or legislative action, court rulings in the NotPetya cases cannot be taken as definitive. Insurers must reach a durable understanding with both insureds and governments about the underlying policy issues.

Silent Cyber Reforms

Some observers view the war exclusion controversy as solely a silent cyber problem, and therefore something that could be solved by clarifying policies that are silent on cyber coverage.[120]

The significance of silent cyber coverage. War exclusions have yet to be invoked in any standalone cyber insurance policies.[121] Merck's and Mondelez's disputes involve only their all-hazards property and casualty policies, which are allegedly silent about cyber risks.[122] Perhaps these insurers never intended to provide any cyber coverage and are now understandably motivated to press every possible legal defense against a massive cyber claim.

Conversely, issuers of affirmative cyber coverage have good reason not to invoke war exclusions: it might scare off potential customers. Affirmative cyber policies have historically paid many claims stemming from state-sponsored cyber operations, including instances of major data deletion and interrupted business operations.[123]

The different incentives and behavior of silent cyber issuers and affirmative cyber issuers suggests that eliminating silent cyber could mitigate the war exclusion problem. If insurers clearly indicated their appetite for cyber risk, then some all-hazards property and causality insurers would impose blanket cyber exclusions, while others would add affirmative cyber endorsements. The net result would be to funnel all cyber risk exposure to affirmative cyber issuers, which have less incentive to invoke war exclusions. These issuers would also be able to collect premiums that reflect the estimated risk of state-sponsored incidents. Higher premiums would improve their financial positions and make them less likely to use war exclusions as emergency safety valves for unplanned losses.

Efforts to clarify silent cyber coverage are already under way.[124] Lloyd's of London, at the behest of UK regulators, aims to eliminate silent cyber coverage among its syndicates by mandating greater clarity in property and casualty policies issued during 2020–2021.[125] However, this is an ambitious timeline.[126] Elimination of silent cyber coverage requires clear definitions of cyber risk in its many forms and clear decisions on whether and how to cover these risks.[127] Given the varied perspectives among insureds, insurers, and government regulators, it could take years to negotiate new terms for the hundreds of billions of dollars of property and casualty coverage currently outstanding.

Beyond silent cyber coverage. Even the total elimination of silent cyber coverage would not solve the war exclusion controversy once and for all. While silent cyber policies represent the most urgent problem and are the focus of Merck's and Mondelez's lawsuits, war exclusions also exist in most affirmative cyber policies.[128] They simply have not yet been enforced. And this non-enforcement may be temporary.

Affirmative cyber policies have low coverage limits and are generally very profitable for insurers, reducing their incentives to enforce exclusions of all kinds.[129] These incentives will shift as the market grows and insurers thereby accumulate more risk exposure. Issuers of affirmative cyber coverage may someday face their own NotPetya moment: a new state-sponsored cyber incident of a wholly unexpected scope and scale. They might then consider invoking war exclusions too.[130]

From the insureds' perspective, lax enforcement of exclusions is far short of guaranteed coverage. Insureds' investors and creditors will also want greater clarity, especially as they seek larger amounts of cyber coverage. The risks of confusing, ambiguous, and impractical war exclusions cannot be fully mitigated by insurers' enforcement discretion.

Granted, war exclusions in many affirmative cyber policies are narrower than the Merck and Mondelez clauses.[131] Yet they tend to share some fundamental problems, like requiring attribution and characterization. And cyber-specific war exclusions come with their own distinctive kinds of ambiguity.

Recall that the Merck policy has exclusions for both war and terrorism, which seem to overlap as applied to state-sponsored cyber incidents. Many affirmative cyber policies also cite both war and terrorism, but invert their relationship. They exclude war, then create an exception to this exclusion (a "write-back" or "carve-back") that restores coverage for "cyber terrorism."[132] In other words, while the Merck policy excludes both war and terrorism, many affirmative cyber policies exclude war *except when it is* terrorism.

Because of how easy it is to categorize state-sponsored cyber operations as terrorism, there is a basic tension between cyber war exclusions and cyber terrorism write-backs. Cyber war exclusions may sweep a broad array of state-sponsored incidents out of coverage, only to have them swept back in again with a broad cyber terrorism write-back. The tension between these clauses raises questions about their intended application.[133] This tension has never been resolved in court, and it seems like a ticking time bomb for litigation.

Research and Dialogue on New Exclusions

Thankfully, there are promising efforts within the insurance industry to develop alternatives to war and terrorism exclusions for cyber claims. Last year, Capsicum Re published a framework for discussion and offered two potential models to replace traditional war exclusions for cyber claims.[134] In July 2020, the Geneva Association (GA) and the International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP) released the first of several papers on cyber war and cyber terrorism, debuting some interesting new concepts intended to standardize language and promote insurability.[135] (Both of these proposals will be discussed later.) Meanwhile, the Lloyd's Market Association is reexamining the war exclusion and weighing new model language for cyber claims.[136]

This work is very encouraging. It demonstrates that key market players recognize the centrality of the war exclusion problem, understand the status quo is unworkable, and are generating new ideas. Efforts to convene insurers, reinsurers, insureds, brokers, and regulators together are particularly valuable. Given the many dimensions of the war exclusion challenge, it must be understood from

multiple vantage points. The risk perceptions and interests of different parties often overlap but rarely align in full. Surfacing disagreement is therefore the first step in building toward shared understanding.

Consensus, however, remains unlikely for now. There is probably no universal solution to the war exclusion challenge that would satisfy all stakeholders. If such a solution did exist, there is no global authority to impose it. Individual insurers and insureds ultimately negotiate their own contract language (although large reinsurers and regulatory agencies in key jurisdictions still wield outsized influence). Given the fractured and decentralized nature of the insurance industry, change is likely to emerge in slow, piecemeal fashion. No single paper or working group can drive this process alone. Rather, many actors must be educated and engaged over time.

Most discussions to date have happened inside the insurance industry, with only limited engagement from outside experts in geopolitics, cyber statecraft, or cybersecurity public policy. Yet the war exclusion challenge is interdisciplinary by nature. Industry-led reforms must be firmly grounded in the realities of state-sponsored cyber operations—including why and how states use such tools and the role of cyber conflict in a changing global security environment. Conversely, national policymakers charged with addressing state-sponsored cyber threats must understand the role of insurance—including its potential benefits for society and its ongoing limitations. An independent think tank specializing in international affairs like the Carnegie Endowment for International Peace is well-positioned to help bridge these gaps.

Trends in State-Sponsored Cyber Operations

While insurers and insureds grapple with these issues, the underlying threat of state-sponsored cyber incidents continues to grow. Offensive cyber capabilities that were formerly held by just a few major governments are proliferating widely. Dozens of governments now have offensive cyber programs—which leverage the international black market, homegrown hacking communities, sophisticated turnkey tools sold by private companies, partnerships among likeminded governments, and repurposing of cyberweapons unwittingly disclosed by adversary states.[137] And many countries are motivated to target global corporations for espionage, sabotage, or influence.

The impact of state-sponsored cyber operations also appears to be growing. Events like the 2015–2016 Ukrainian power disruptions,[138] the 2017 NotPetya attack, and the 2017 WannaCry attack illustrate how state-sponsored actors continue to set new precedents for damaging civilian systems.

These actors are encouraged by a climate of tolerance—a widespread perception that states and their cyber proxies have not suffered significant consequences and can keep pushing the envelope.[139]

Finally, cyber actors are exploring new ways to thwart attribution. There are more frequent reports of state-sponsored cyber actors masquerading as other actors and taking other sophisticated measures to complicate attribution.[140] Meanwhile, more governments are turning to shadowy proxy forces to make their actions more plausibly deniable.

To counter these trends, intelligence agencies and private firms have invested more in cyber attribution capabilities. These investments have yielded concrete new insights and helped create somewhat more accountability for malicious cyber activity than existed before. Nevertheless, attribution is a cat-and-mouse game between two highly determined and adaptive groups (perpetrators and investigators). The long-term trajectory of this contest is unknown, and the balance of advantages may shift from time to time based on technological and tactical innovations. While attribution capabilities may well improve, insurers must also consider the possibility that attribution could be harder at points in the future than it is today.

Evaluating Potential Solutions

New language should replace traditional war exclusions in both affirmative and silent cyber coverage. Language alone cannot solve all the underlying challenges in cyber insurance that NotPetya exposed, but language reforms can work alongside broader reforms to support market growth and maturation. To balance the interests of insurers, insureds, and governments, solutions should focus on two overarching goals.

The first goal must be *clarity and practicability* in insurance coverage rules. To the greatest extent possible, insurers, insureds, and regulators should have shared expectations about what kinds of claims would be excluded. Moreover, the contract language should not require costly, lengthy, and uncertain litigation to apply.

The second goal should be *a manageable zone of coverage* that provides adequate value for insureds without jeopardizing the profitability or solvency of insurers. Threading this needle would require financially sustainable and balanced transactions among insurers, insureds, and possibly governments to ensure that cyber risk coverage is both sufficient and actuarially sound. If such a coverage zone

could be defined, it would offer profits to insurers, protection to insureds, and broad benefits for society at large. A manageable zone of coverage would foster growth and maturation in the marketplace, enabling insurers to do more over time to shape the risk environment.[141]

Overview of Proposed Approach

A crude approach would be to eliminate war and terrorism exclusions entirely for cyber claims, in both affirmative and silent coverage. But removal of these exclusions without adequate replacements would create its own problems, discussed below. This section therefore focuses on designing replacement exclusions that would address the known disadvantages of traditional war exclusions, while avoiding or at least minimizing new problems. In the end, all possible exclusions bring trade-offs, and market players must choose how to balance them.

As discussed, the war exclusion is both overinclusive and underinclusive with respect to cyber claims. That is because war exclusions are preoccupied with a variable—state sponsorship—that is only indirectly related to risk. A better approach would begin with a new exclusion for catastrophic cyber risk, having nothing to do with war or state sponsorship. This exclusion would align with basic principles of insurability, denying coverage for cyber incidents—whether in war, peace, or anywhere in between—that threaten aggregated losses beyond what insurers could bear.

Designing such an exclusion is no easy task. But if successful, a cyber catastrophe exclusion would be clearer and more practical than war exclusions for cyber claims, and it would provide a more manageable zone of coverage. Such a clause would then be paired with a revised "war" exclusion, as described later. The two exclusions would work in tandem. The catastrophe exclusion could be insurers' first line of defense against extraordinary cyber losses regardless of cause or perpetrator. This arrangement would relieve pressure on the "war" exclusion, which could then focus narrowly on its specific historical purposes as applied to cyberspace.

Designing a Cyber Catastrophe Exclusion

Insurers already have many mechanisms in place to limit their exposure to catastrophic risk. They can curtail their exposure to high-risk coverage areas, scrutinize potential clients during underwriting, and set limits or sublimits on individual policy amounts. Insurers can also offload some amount of risk onto others through tools like reinsurance, retrocession (reinsurance for reinsurers), or—for some lines of coverage—insurance pools, insurance-linked securities, and various forms of government backstopping.

But NotPetya helped to illustrate how these mechanisms might still fall short in cyber insurance. Meanwhile, some risk-limiting mechanisms in cyber coverage—like low ceilings on individual policy amounts—have reduced its appeal for insureds, inhibiting demand and slowing market growth.

An exclusion specifically tailored for cyber catastrophes could help insurers and reinsurers manage the risk of extreme cyber events—whether malicious or nonmalicious, including those with physical triggers—more effectively than traditional war exclusions. The major challenge in designing a cyber catastrophe exclusion is predicting what kinds of perils or triggers could result in catastrophic losses and therefore how the exclusion should be worded.

Challenges of defining cyber catastrophe. Catastrophe is a subjective concept. Different insurers and reinsurers will have different views on what qualifies as an uninsurable cyber catastrophe based on their unique risk appetites and varying estimates of cyber risk itself. The goal is not a single uniform exclusion, but a palatable menu of options.

Crafting this menu means considering the diverse and ever-changing cyber risk landscape. Use of digital technology by insureds and third parties is constantly evolving, and no one has a complete or accurate view of where risk lies or will lie in the future. For example, parties signing a one-year cyber insurance contract in late 2019 could not have anticipated how the coronavirus pandemic would drastically change the technology usage and cyber vulnerabilities of most insureds.

Changing patterns of technology usage mean that a once-obscure software platform, data repository, or hardware subcomponent can quickly become critical to millions of people, sometimes without anyone noticing or being able to assess the implications.[142] High-stakes vulnerabilities in critical systems can be discovered years after the fact, while patching them can be both time-consuming and challenging.[143] Moreover, sophisticated cyber threat actors innovate their tactics continuously and take active measures to frustrate monitoring and analysis by network defenders.

Taking these factors together, it is very challenging to predict what sorts of triggers could lead to uninsurable cyber catastrophes, let alone to find magic words that describe these risks with clarity. This is not an unfamiliar challenge to insurers, but it is particularly complex in the cyber realm.

Specific or infrastructure-oriented definitions. There are at least two basic approaches to the problem. One is to exclude specific event types that are most likely to cause catastrophic damage and losses. For example, Munich Re excludes cyber losses stemming from electrical grid outages and failures of

core internet infrastructure such as the Domain Name System. It reasons that these scenarios carry "a systemic accumulation risk" due to the large number of affected parties and cannot be adequately modeled.[144] This sort of "infrastructure exclusion" is used by many affirmative cyber issuers.[145]

Infrastructure exclusions help to manage some classic sources of catastrophic risk, namely electricity and telecommunications outages not under the insured's control. With such centralized utilities, a single system failure can have direct downstream impacts on many customers and third parties. But in the modern era, new kinds of catastrophes can develop in unexpected places and spread in nonlinear ways. Interconnected computer systems and supply chains create a web of complexity in which systemic risks can lie undetected.[146] Such risks, once triggered, may then cascade in multiple directions.

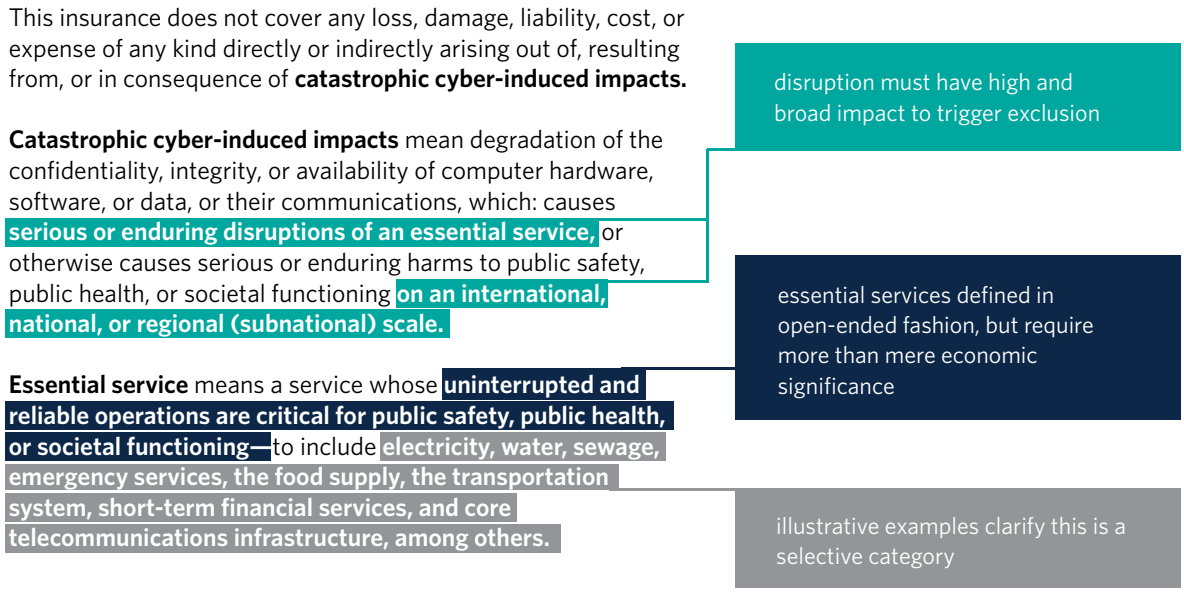
NotPetya, for example, spread among large multinational corporations via compromised Ukrainian tax preparation software—no one's definition of critical infrastructure.[147] Similarly, major cyber vulnerabilities with global consequences have been found in widely used encryption algorithms or microprocessors.[148] Incidents connected to these vulnerabilities would be outside the scope of most infrastructure exclusions, as the vulnerable software and hardware was locally installed and operated by end users—meaning it was under control of the insured. These cases illustrate how the compromise of millions of identical software or hardware components could be just as devastating as the compromise of a single centralized service supporting millions of users.

General or impact-oriented definitions. A second approach would be to use broad language to exclude general categories of high-consequence risk, beyond electrical and telecommunications infrastructure. Umbrella terms such as "essential services" or "critical infrastructure" can indicate a larger category of assets whose disruption or damage could lead to uninsurable losses.

These assets can be defined by their societal function, rather than their specific industry or infrastructure type, to account for the inherent unpredictability of future cyber catastrophes. Of course, a flexibly worded exclusion should not become all-encompassing. Carefully worded examples (which would be illustrative but not exhaustive) can help to signal focus and intent. An exclusion could also be bounded in some quantitative way. For instance, it could be triggered for cyber incidents causing a certain level of loss or damage in a certain number of countries.

FIGURE 6

Proposal for a New Cyber Catastrophe Exclusion



A proposed cyber catastrophe exclusion. Figure 6 is a proposed model of a cyber catastrophe exclusion for affirmative and silent cyber coverage. It seeks to combine the best of both approaches: electricity and telecommunications outages are encompassed within broader categories of catastrophic risk, while caveats and illustrations help to clarify the boundaries of the exclusion.

Compared to traditional war exclusions, this model language is meant to better match risk and be less technically demanding or fact-intensive to apply. It also sets an intentionally high bar for triggering the exclusion. It aims to exclude the starkest and most disastrous cases, while leaving others covered. Three aspects of this proposal help to clarify its intent.

First, it defines essential services as those whose failure, even if temporary, could threaten life or "societal functioning." Thus, it suggests a cyber catastrophe would be something more than mere economic disruption. Second, its illustrative examples are selective and focused on the most sensitive or time-critical infrastructure. For example, "short-term financial services" might include ATMs or clearinghouses, but not mortgage origination or student loan servicing. Third, the exclusion is only triggered if disruptions to an essential service are "serious or enduring" or cause harms beyond just one locality. All these caveats help to bound what is otherwise meant to be a flexible, open-ended description of cyber catastrophe that could apply to any number of triggers.

Implied risk tolerance. This language helps to draw a line between cyber incidents on the scale observed to date and future incidents that potentially could be many times more devastating. NotPetya, the high-water mark of historic cyber incidents, would not trigger this exclusion. Although NotPetya

caused vast losses from property damage and interrupted business operations, it did not disrupt essential services critical for public safety, public health, or societal functioning. By covering NotPetya-scale events, this language implies a certain level of risk tolerance.

More risk-averse insurers or reinsurers might view this definition of cyber catastrophes as too narrow and wish to broaden the exclusion. For example, the specific illustrative examples of essential services could become more general: "the food supply" could be expanded to cover "food and agriculture," "core telecommunications infrastructure" could become "communications and digital infrastructure," and so on. These sorts of changes would further reduce insurers' exposure to catastrophic losses, compelling insureds to retain more risk. Broadening the exclusion would offer more financial security to insurers and reinsurers, while potentially lowering demand and increasing litigation.

Quantitative approaches. Any attempt to describe catastrophic risk in words will be imperfect. Catastrophic scenarios cannot be entirely predicted. It is also possible for a series of events to cause extreme, aggregated damage even when each event individually falls just short of the exclusion threshold. For these reasons, qualitative efforts to craft exclusion language could be paired with quantitative efforts to cap exposure (in dollar terms or the number of insurable events in a single year) and to attract new capital to help shoulder the risk.

Promising avenues include insurance-linked securities, parametric risk transfer contracts, and government backstops.[149] Each of these risk-limiting mechanisms has proven effective in other coverage areas but remains nascent or experimental for cyber coverage. While these mechanisms will take time and effort to fully establish, they are likely essential for cyber insurance to catch up with cyber risk itself.

Designing a New "War" Exclusion for Cyber Claims

The cyber catastrophe exclusion discussed above has important advantages over today's war exclusions. It is better tailored to risk and does not require any painful lawsuits over attribution. At first blush, it might seem appealing to eliminate war exclusions for cyber claims and allow a catastrophe exclusion to stand on its own. But insurers may wish to retain something like a "war" exclusion for cyber claims. Even so, it should look quite different than traditional war exclusions.

Why retain a "war" exclusion? There are at least three arguments for supplementing a cyber catastrophe exclusion with some kind of exclusion for war-related or state-sponsored cyber operations. First, war exclusions help to absolve insurers of moral hazard. If wartime and other state-sponsored cyber attacks are always insured, states might tend to act more aggressively, knowing that insurers would help bear the cost of any cyber retaliation. An exclusion could at least mitigate this hazard.[150]

Second, war exclusions for cyber claims can ensure fair treatment for wartime losses of different types. Kinetic war will and should remain excluded from most standard insurance lines, due to its high cost, aggregation risk, and unpredictability. Yet kinetic wars increasingly have cyber dimensions, as more militaries adopt cyber tools to complement or directly enable kinetic operations. If the war exclusion clause is eliminated for cyber incidents but retained for other perils, there would be a major disconnect in insurance treatment of kinetic and cyber attacks suffered during the same war.

Third, a state of war or even lower-level conflict between two states might lead to a series of cyber incidents that individually fall below the threshold of the catastrophe exclusion but collectively cause large-scale aggregated losses. A revamped war exclusion could seek to account for this type of loss correlation.

Today's war exclusions should not be the model for cyber claims. Instead something more specific and narrower is needed. Its primary purpose would not be to exclude massive, uninsurable cyber losses arising from war or state-sponsored cyber incidents, because the cyber catastrophe exclusion would already do that. The catastrophe exclusion is focused on insurability in war as well as in peace, regardless of the perpetrator. Rather, a new exclusion would fulfill the three purposes identified above.

As with the cyber catastrophe exclusion, designing a new "war" exclusion for cyber claims is no easy matter. Quite a few challenging questions must be answered along the way.

Is "war" still a relevant term, in or out of cyberspace? The traditional distinction between war and peace has been challenged by many observers as increasingly irrelevant.[151] Legally, formal declarations of war have been largely replaced with undeclared armed conflicts. Meanwhile, many countries have developed foreign policies and military doctrines that deemphasize large-scale armed conflict. Instead they elevate other forms of contestation and confrontation—involving more sporadic and low-intensity violence, more covert and deniable actions, greater use of proxy actors, less adherence to clearly defined battlefields, and more integration of military activity with other tools of national power.

Experts disagree on how to describe these phenomena. The "gray zone," "hybrid warfare," and "geopolitical competition" are just a few of the proposed terms.[152] Within the insurance industry, GA/IFTRIP has offered "hostile cyber activity" as a way to describe state-sponsored cyber operations that fall short of war.[153] But regardless of the terminology, there is general consensus on the overall direction of the international security environment.

This new environment defies simple categorization. For example, U.S. military doctrine since 2018 has rejected "the obsolete peace/war binary" in favor of a "competition continuum" that includes

"cooperation, competition below armed conflict, and armed conflict."[154] Importantly, the different parts of this continuum "are not mutually exclusive conditions" and "can exist concurrently." In this nonlinear worldview, military tools are not reserved for an ultimate state of armed conflict. Rather, military operations of varying kinds are used continuously to influence adversaries and allies and shape the security environment.[155] Cyber operations exemplify this approach.

In national security circles, cyberspace is often cited as a paradigmatic arena of gray-zone competition. Many governments view cyber operations as ideally suited for pursuing national interests short of war. Cyber operations are stealthy, deniable, cost-effective, have global reach, and seem less likely to trigger damaging blowback than other tools. These incentives have led to the pervasive use of cyber operations—initially by a small group of elite cyber powers like the United States and Russia, and now by scores of countries. The vast majority of these activities have occurred outside the context of any armed conflict.

As a result, some governments and experts are paying less attention to long-running debates about what might qualify as "cyber war," "acts of war in cyberspace," or an "armed attack equivalent."[156] This school of thought holds that states should focus less on distinguishing "war" from peace in cyberspace, and more on how to compete in the cyber gray zone.[157] For example, U.S. cyber strategists now embrace "persistent engagement" with adversaries—a never-ending series of maneuvers designed to create transitory strategic advantages.[158] The trend is broadly similar in other countries.

With military thinkers and cyber conflict experts both shifting away from "war" and even armed conflict as their dominant paradigm, does it make sense for the insurance industry to stick with those terms? And if the term "war" is no longer adequate for cyber insurance, how can it be replaced or refined?

One answer is to retain the concept of war but define it in more objective terms. For example, Capsicum Re has proposed an exclusion for cyber incidents linked to "kinetic military action," regardless of any formal declaration or public acknowledgment by the belligerent states.[159] Another approach would be to introduce new terms for capturing the cyber gray zone short of war, like GA/IFTRIP's "hostile cyber activity."[160]

Both ideas have different implications but reflect the same key insight: the language of insurance policies must evolve to better reflect real-world realities of conflict. These proposals, and other possibilities, are compared in greater detail below.

What is the role of attribution? Any reform proposal must somehow account for twin challenges that plague war exclusions: attribution (who was responsible) and characterization (the nature or intent of

the incident). Interestingly, war exclusion reformers tend to accept attribution as a necessary evil. Capsicum Re describes it as "the unavoidable problem."[161] GA/IFTRIP called attribution a basic limitation that "will inevitably be difficult."[162]

However, it is possible to imagine new kinds of war exclusions that sidestep attribution. One approach would be geographically based. In maritime shipping, the Lloyd's Market Association operates a Joint War Committee that designates high-risk geographic areas where special rules and rates may apply.[163] Something similar could be devised for cyber claims. Kinetic combat zones or other territories at high risk of state-sponsored cyber operations could be identified. Losses suffered in these areas could then be excluded from cyber coverage, regardless of the perpetrator's identity. Model language for this geographic approach is offered later.

What is the role of characterization? Whether attribution is required or not, the characterization problem must be tackled separately. Traditional war exclusions involve characterizing whether a cyber incident is "hostile or warlike," a tricky determination that would probably mean assessing the intent or effects of an operation. As with attribution, war exclusion reformers often retain some form of characterization requirement.

For example, GA/IFTRIP offers several ways that "hostile cyber activity" might be defined. Some definitions look to the intent behind a cyber incident (such as whether it is carried out "in the interest of a state"), and some look to the incident's ultimate effects (certain types of government or business disruptions, or specified economic or political damage).[164] Capsicum Re takes a more general approach, excluding cyber incidents that are "in connection with a state of war" or "part of, directly connected to, or in support of kinetic military action."[165] Courts would presumably develop more detailed rules for assessing connections between specific cyber incidents and military conflicts, perhaps by looking at intent or effects.

NotPetya illustrates how difficult characterization can be. On the one hand, insurers could certainly argue that NotPetya is connected to kinetic military action and therefore excludable under some proposed approaches. The cyber attack was conducted by the Russian military and coincided with Russian kinetic operations in eastern Ukraine. NotPetya helped to advance Russian military objectives for its kinetic conflict in Ukraine—namely, eroding Ukrainian popular will to resist Russia and Russian-aligned militants (by damaging the Ukrainian economy), as well as driving a wedge between Ukraine and its Western allies (by punishing foreign companies involved in Ukraine).

On the other hand, insureds would have strong counterarguments. NotPetya was not a battlefield action or synchronized at the tactical level with any Russian kinetic maneuvers. It was designed to target civilian companies, most of which were based in other countries far from the Ukraine-Russia

conflict.[166] And given its global scale, perhaps NotPetya was meant to support Russia's global strategic objectives, rather than (or in addition to) its military operations in Ukraine. These wider objectives include fostering a sense of chaos and insecurity in the Western world, signaling Russia's cyber capabilities for deterrence purposes, and forcing other powers to respect Russia's interests and great power status by posturing as a spoiler.[167]

The characterization problem invites lengthy litigation featuring expert testimony from dueling military and cyber experts, with unpredictable outcomes. While difficult to avoid, alternatives are possible. A geographically based exclusion offers one potential path. If all cyber incidents within a certain kinetic conflict zone are excluded, there would be no need to characterize any individual incident. Instead, the focus would shift to characterizing the conflict itself (to establish a geographic zone of exclusion). This approach would come with its own challenges but would likely be easier and cheaper to litigate. Such zones could even be publicly pre-declared, like the Joint War Committee's high-risk areas.

When does a "war" or conflict state begin and end? A new cyber exclusion might be conflict-independent—that is, encompassing a broad range of cyber incidents in the gray zone short of "war." Or it might be conflict-dependent, applying only when some state of kinetic military conflict exists. GA/IFTRIP's concept of hostile cyber activity takes the former approach, while Capsicum Re's framework and this paper's proposal for a geographically based exclusion are examples of the latter.[168]

Conflict-dependent exclusions must set a clear threshold for recognizing that a kinetic conflict state has begun. This means distinguishing minor military exchanges from more substantial combat. Without such a distinction, a single minor use of force might trigger the exclusion. Moreover, there must be a clear termination condition that indicates when a conflict state, once begun for insurance purposes, would subsequently expire. For example, Capsicum Re's model language looks to the connection between a cyber incident and kinetic military action ("usually, but not necessarily, including lethal force").[169] Courts would need to develop caselaw on when such a connection begins and ends.

In the international gray zone, kinetic military action can arise quite frequently, depending on how this term is interpreted. Would an unintended collision between U.S. and Chinese military aircraft, as occurred in 2001, qualify and therefore trigger an exclusion?[170] What about China seizing a small U.S. undersea drone, as it did in 2016?[171] Or Russia's frequent unsafe, unprofessional intercepts of U.S. aircraft and naval vessels—which have not yet caused kinetic damage but are designed to create risk of damage?[172] These examples show the need for, and difficulty of, defining a clear lower bound of kinetic conflict.

The termination condition raises similar challenges. Consider the U.S. killing of Qassem Soleimani in January 2020, an apparent act of kinetic military action. This kind of event could conceivably trigger an exclusion for any losses arising from immediate Iranian cyber retaliation. But as more time passes without new U.S.-Iran military engagements, the connection with any subsequent cyber incidents would become harder to assess, and the exclusion would become more ambiguous.

If Iran were to launch a retaliatory cyber attack six months later, would an exclusion still apply? Such delays are not uncommon, as states require time to develop complex cyber operations and may wish to avoid escalatory spirals. In 2014, Iran conducted a data deletion attack on the Las Vegas Sands Corporation in apparent retaliation for comments that its chairman had made more than three months earlier.[173]

These gray-zone scenarios are both diverse and pervasive, indicating the benefits of a clear and substantial minimum threshold so as to avoid an overbroad exclusion. Some possible language is offered later.

What are the territorial boundaries of "war" or hostility in cyberspace? Unlike kinetic military operations, cyber operations can have simultaneous impacts across multiple countries or regions. This raises complicated questions about the territorial remit of any "war" exclusion. A geographically based exclusion would need to define clear and meaningful territorial boundaries. And once these boundaries are set, applying them would require somehow geolocating cyber losses and defining them as inside or outside the exclusion zone. Geolocation may not be straightforward. An insured corporation that suffers a cyber attack might have its headquarters in one country; its affected business operations in another country; and its impacted hardware, software, and data spread among multiple countries.

The difficulties of parsing such geographic nuances can be avoided by a global rule, like the GA/IFTRIP concept of "hostile cyber activity." However, a global exclusion could sweep quite broadly—applying to the losses of so-called bystanders far away from any conflict or belligerent state.[174] In the case of NotPetya, most losses were collateral damage suffered outside of Ukraine.

Below, this paper offers model language for a geographically based exclusion that would apply only to losses experienced within zones of kinetic conflict (for example, Ukrainian territory in the case of NotPetya). To geolocate cyber losses, such an exclusion relies on the fact that all cyber activity ultimately has a physical reality in hardware.

What types of actors can trigger "war" exclusions? Traditional war exclusions apply only to acts committed by states and their agents. Courts have held that de facto states can trigger war exclusions,

but they have interpreted this term somewhat narrowly. For instance, a U.S. federal appeals court ruled last year that Hamas is not a de facto state and therefore cannot trigger war exclusions.[175]

Yet in the modern world, Hamas and other statelike entities like Hezbollah and the self-proclaimed Islamic State can amass significant military and cyber capabilities. They can fight kinetic wars and conduct sophisticated cyber operations.[176] Such actions might or might not trigger terrorism exclusions (or write-backs), depending on the actions' nature and the clauses' wording. As the insurance industry rethinks war and terrorism exclusions for cyber claims, it might more explicitly address statelike entities with demonstrated capabilities to make "war" in and out of cyberspace.

A proposed geographic exclusion. These questions posed above do not have definitive answers. Rather, they indicate complexities and trade-offs that will likely require years of negotiation and refinement. To stimulate these discussions, figure 7 gives model language for a new, geographically based war exclusion for cyber claims in both affirmative and silent cyber coverage.

FIGURE 7

Proposal for a New Cyber Catastrophe Exclusion

This insurance does not cover any loss, damage, liability, cost, or expense of any kind directly or indirectly arising out of, resulting from, or in consequence of **wartime cyber-induced impacts.**

Wartime cyber-induced impacts mean degradation of the confidentiality, integrity, or availability of computer software or data, or their communications, **where such software, data, or communications is stored or processed on hardware physically located within an area of hostilities.**

Area of hostilities means **the entire sovereign territory of a state,** provided that anywhere within such territory, major combat operations are taking place at the time of the wartime cyber-induced impacts or are **initiated, in whole or in part, by the wartime cyber-induced impacts.**

Major combat operations mean regularly recurring or large-scale military operations between at least two states or statelike entities, including any forces under their direct control, which result in **significant loss of life or widespread destruction of physical property.**

Statelike entity means a nonstate organization that **exercises enduring, de facto political authority in a definable physical area and controls substantial conventional military capability.** Examples include Hamas in Gaza, Hezbollah in parts of Lebanon, and formerly the so-called Islamic State in parts of Iraq and Syria.

no attribution or characterization required; exclusion is geographically based, with a rule for how cyber losses are assigned geography

clear geographic boundary

cyber blitz or decapacitation attack could trigger exclusion

substantial minimum threshold of violence required to trigger exclusion

statelike entities can trigger the exclusion

This proposal tests some possible answers to the questions raised above. First, it retains the concept of "war" while narrowing its scope to specific, high levels of violence. The intent is to avoid excluding gray-zone cyber activities, which occur daily. This language would instead exclude cyber incidents only in cases widely recognized as wars—where large-scale physical destruction or loss of life gives rise to the core actuarial challenges that historically justified war exclusions. Such an arrangement would greatly shrink the scope of excluded incidents compared to today's war exclusions. With a smaller universe of cases at stake, litigation over its terms would become less common. (The cyber catastrophe exclusion would bear more of this burden.)

Second, this proposal limits the geographic scope of the exclusion to a defined place called an "area of hostilities" and provides concrete but flexible conditions for a state of conflict to begin and end. These conditions are stated as clearly as possible, while still accounting for the fact that each conflict has unique and sometimes unpredictable contours. The language captures two distinct types of kinetic engagement—an ongoing exchange of violence, and a single episode of massive violence. To create even further clarity, an insurance industry body akin to the Joint War Committee could make periodic public declarations of where such areas of hostilities exist.

Of course, there are inherent limits on precision in such a diverse arena as war. Courts would still need to develop jurisprudence to apply these terms. But large-scale kinetic conflict tends to occur in plain sight, obviating the need for the kind of costly evidence and expert testimony essential to litigating traditional war exclusions for cyber claims. Legal debates over the nature of a given military conflict should be simpler and cheaper affairs than the NotPetya litigation.

Beyond attribution. The third and most radical element of this proposal is that it completely eliminates the need for attributing the cyber incident or characterizing its connection to the kinetic conflict. It simply excludes all losses tied to computer systems inside a conflict zone. This means that difficult judgments about the identity and state authority of perpetrators, their intent, or the political and military significance of a cyber incident become irrelevant. Instead, there is a blanket exclusion for all cyber claims within certain territories. This blanket exclusion would not be particularly harsh for insureds because "major combat operations" as defined in this language would be a rare condition.

Note that the "area of hostilities" is based on where major combat operations are occurring, not which countries are fighting the conflict. For example, the United States has conducted major combat operations in multiple countries since 2001, but these have all been expeditionary missions—not conducted on U.S. soil. Had this exclusion been in effect, it would not yet have

applied within U.S. territory. For that matter, the exclusion would not have applied within other countries that fought alongside or hosted U.S. troops (except those countries, like Iraq, that actually experienced major combat operations).

This definition of "area of hostilities" is intended to geographically link any cyber exclusion to the physical occurrence and sites of combat. A geographic link helps to focus the exclusion on its core purposes and confine it to a clear, manageable set of scenarios.

Admittedly, this may involve some moral hazard for expeditionary military operations. A country's decision to conduct major combat operations abroad will often increase the risk of retaliatory cyber attacks against private entities within its home territory. Underwriting this form of cyber risk might, in the eyes of some insurers, encourage governments to pursue riskier, possibly destabilizing foreign policies. On the other hand, launching a foreign military campaign is a weighty decision based on many factors; the influence of cyber insurance coverage on such decisions is therefore debatable. Insurers that do consider this an important risk would probably reject or modify the proposed exclusion.

Fourth, the proposed language treats statelike entities as equivalent to states. Given the emergence and resilience of statelike entities, and the significant cyber and kinetic capabilities they have accumulated, it seems inevitable that they will participate in future conflict of both kinds. This language anticipates that likelihood.

The proposal is no doubt novel and is intended to provoke debate and inspire other imaginative solutions. It introduces terms that are unfamiliar to the insurance industry. But as other proposals have recognized, the world is changing and insurance concepts must change in response. The model language also involves some ambiguity and would result in litigation. Though ambiguity can never be eliminated, it can be managed by replacing more harmful with less harmful forms. Litigation over this proposal should be simpler, less fact intensive, and more likely to result in meaningful precedents that help settle market expectations.

Testing Solutions With Scenarios

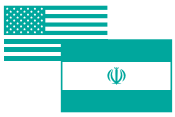
The test of any proposal is how it applies to specific scenarios. Insurers, insureds, and government regulators will distrust any language that is not transparent about how it would operate in practice. Below are eight scenarios illustrating how the two proposed exclusions—for cyber catastrophes and

war—would function together. These scenarios are neither exhaustive nor the most extreme or damaging scenarios imaginable. They aim to clarify the intent of these exclusions and reveal their limitations.

Scenario 1: A NotPetya Sequel

Russia conducts another data destruction attack—first striking Ukraine, then spreading globally—with roughly the same impacts.

Losses within Ukraine would be excluded as wartime cyber-induced impacts, because Ukrainian territory qualifies as an area of hostilities due to Russia's combat operations there. (Whether a loss is considered "within Ukraine" would depend on whether the affected hardware is physically located there.) However, losses in all other countries would not be excluded. This scenario illustrates how the proposed exclusions would lead to a clear result in the NotPetya litigation. The catastrophe exclusion would not come into play because NotPetya and its hypothesized sequel did not disrupt essential services.



Scenario 2: A Retaliatory Iranian Cyber Attack

Iran conducts a data deletion attack on U.S. companies in response to Soleimani's killing.

The wartime exclusion would not apply because no major combat operations are taking place in U.S. territory. This scenario illustrates how the proposed wartime exclusion is narrowly focused in its geographic scope and would not implicate gray-zone situations short of war. (The catastrophe exclusion might still come into play if, for example, Iran succeeded in shutting down hospitals or electric power grids on a substantial scale.)

If the United States retaliates against Iran's cyber attack by conducting large-scale military operations against Iranian forces, major combat operations would then exist in the operative territories—perhaps Iran itself, Syria, Iraq, and/or Yemen. Future cyber losses of all kinds inside those specific territories would then be excluded until the end of major combat operations. The United States would not qualify as an area of hostilities unless significant kinetic combat took place there.

Scenario 3: A Ransomware Attack in Syria

A criminal ransomware attack disrupts a multinational company's operations in Syria.

Losses inside Syria could be excluded, depending on whether Syria is deemed an area of hostilities at the time. The extraordinary complexity and fluidity of the Syrian war provides a difficult test case for proposed definitions of conflict.

From at least 2014 until 2019, the Islamic State was a statelike entity engaged in major combat operations with a variety of national militaries inside Syrian territory. The Islamic State ceased to exist as a statelike entity when it lost its last territory in 2019.[177] However, since late 2019, Turkey and its proxies have conducted incursions into northern Syria and periodically clashed with the Syrian military.[178] It can therefore be argued that Syria has been an area of hostilities since 2014, and if that is the case, any cyber losses within the country would trigger the proposed exclusion of war-time cyber impacts.

Although the perpetrator in this scenario is a mere criminal without any known goal of influencing the war, the exclusion would still operate, as it does not depend on attribution or characterization. Cyber losses outside of Syria would not be excluded, unless they resulted from disruptions of essential services and therefore triggered the catastrophe exclusion.

Scenario 4: Sabotage at a Water Treatment Plant

A hostile insider sabotages the computer systems of a water treatment plant, causing illnesses and, later, the interruption of the water supply.

Losses would be excluded based on their catastrophic nature, as water and water treatment are essential services and their disruption creates serious threats to public health. This scenario illustrates how the cyber catastrophe exclusion operates regardless of perpetrator, requiring no connection to war or state sponsorship.

Scenario 5: A State-Sponsored Data Breach

Chinese military hackers steal personal data from a German company.

Despite its state sponsorship, this act would not trigger the wartime cyber exclusion because German territory is not an area of hostilities. The incident also would not qualify as catastrophic, unless the victim company operates an essential service and remediation of the breach were to require system shutdowns that significantly disrupt that service. This scenario illustrates how the most common types of state-sponsored operations (network penetration and data theft) would generally not trigger the proposed exclusions.

Scenario 6: A Decapitation Cyber Attack

Russia launches a debilitating cyber attack on Georgia immediately prior to a ground invasion.

Losses would be excluded. Although an area of hostilities had not yet existed at the time of the cyber attack, the wartime exclusion also applies to cyber attacks that "initiated" major combat operations. This scenario illustrates one way the wartime condition could be triggered.

Scenario 7: A Disruption of Cloud Services

A major cloud service provider suffers a forty-eight-hour disruption, causing widespread second- and third-order impacts.

Application of the cyber catastrophe exclusion would depend on whether the disrupted cloud services are deemed "essential services." This determination, in turn, depends on the nature of these impacted cloud services and the cloud customers being served. For example, if a regional hospital chain relies on certain cloud services to make many life-saving treatment decisions, those specific cloud services could be considered "essential" under the proposed exclusion terms. On the other hand, many cloud services are not critical for public safety, public health, or societal functioning and

would therefore presumably not trigger the exclusion (though considerations of aggregation and cascade effects require further analysis). The same data center might provide both essential and non-essential cloud services.

This scenario illustrates how the proposed definition of "essential services" is nuanced in application. It also reveals some challenges in insurance treatment of the cloud, which go beyond the scope of this paper. More work must be done to understand cloud resiliency, identify aggregation potential, prioritize risks, and work toward standard requirements for insurance coverage.[179] These tasks will require additional coordination among insurers, regulators, essential service operators, and providers of cloud and other information technology services.

Scenario 8: A Cyber 9/11

Hackers inspired by the Islamic State carry out large-scale ransomware attacks that shut down hospitals and public transportation in multiple countries.

Losses would be excluded under the cyber catastrophe clause, given the disruption to essential services (hospitals and transportation). The wartime exclusion would not come into play, unless the victim countries were already considered areas of hostilities.

This scenario illustrates how the proposed exclusions compare with existing ways of treating terrorist acts in cyberspace. Under Merck's property and causality policy, this incident would be excluded as terrorism. Under many affirmative cyber policies, however, it would be covered through a cyber terrorism write-back.

Backstopping the Market

This paper's proposals are meant to create a manageable zone of coverage, while being clear and practical in their application. But their true financial impact is difficult to estimate. With cyber insurance in an immature state, no settled consensus exists on the boundary between insurable and uninsurable cyber risks.[180] Any proposed dividing line will be controversial, and its actuarial viability may be doubted.

Reinsurers, which specialize in understanding catastrophic and aggregated risks, will play a central role in assessing actuarial viability. The broader investment community will weigh in, too, as tools

like insurance-linked securities or private pool mechanisms seek to draw in alternative sources of capital.[181] Insurance regulators, whose expertise is in financial soundness, are also key players.

The Role of Government Backstops

But market players may prove unable to address catastrophic or state-sponsored cyber risk on their own, given the amount of risk and uncertainty. Even if the insurance industry devises clear and practical alternatives to traditional war exclusions, reinsurers, investors, and regulators could still deem these alternatives too financially risky. In that case, a government backstop for cyber insurance might be needed.

Government backstops help pay claims that are too catastrophic for private markets to bear on their own. As of 2010, the governments of nine members of the Organization for Economic Cooperation and Development offered terrorism insurance backstops of various kinds.[182] The U.S. Terrorism Risk Insurance Act (TRIA) and the UK's Pool Re are just two models among many possible approaches.[183] The precise design of any government cyber backstop is a complex question that will be explored in an upcoming Carnegie paper. For current purposes, it appears likely that a cyber backstop in some form will be needed. The major challenge will be uniting private sector stakeholders and lobbying governments.

Terrorism backstops have been created after extraordinary attacks created crises that demanded political action. The United States passed TRIA after the 9/11 terrorist attacks led most insurance companies to exclude terrorism coverage entirely; in response, property developers halted major new real estate projects.[184] This situation galvanized the U.S. political system. There has been no comparably dramatic cyber emergency to rally support for a cyber backstop. NotPetya was very costly, but its costs were spread among many companies in multiple countries and did not lead to the total freeze-up of insurance markets or investment seen after 9/11.

Cyber backstops have been debated for years, yet no coalition has emerged to forcefully advocate for one.[185] Insurers themselves are sometimes wary of backstops, which come with many strings attached and impose the government's views of risk onto the industry.[186] But insurers may be better off negotiating backstop terms before a major catastrophe occurs, rather than afterward, when political momentum is on the side of swift and forceful legislative action.

In recent years, more industry stakeholders have warmed to the idea of government cyber backstops.[187] However, there is not yet a clear vision or strong public advocacy. Effective advocacy would, among other things, demonstrate how the industry had taken all reasonable steps within its power to develop the cyber insurance marketplace without government financial support.

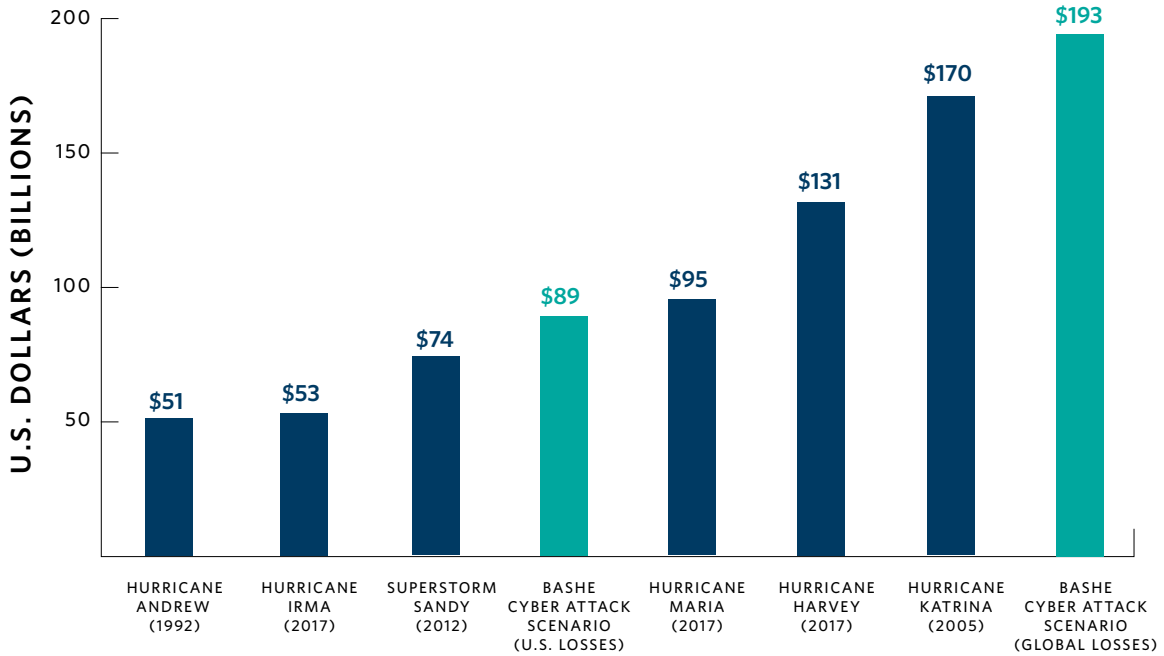
Persuading Governments

Many governments would be skeptical of the potential cost of cyber backstops. But politically speaking, governments are already expected to serve as de facto backstops for major disasters. In the United States, for example, there is a political consensus that local areas cannot fairly or effectively absorb the costs of natural disasters and that the federal government should therefore provide recovery funds. Although meeting such expectations often requires specific action by Congress, it has become routine.[188]

Cyber attacks can cause losses equivalent to those of natural disasters. NotPetya cost an estimated $10 billion dollars globally.[189] By comparison, natural disasters of that scale strike the United States only once or twice a year on average.[190] And future cyber incidents could be much more costly than NotPetya. An extreme global ransomware outbreak could cost as much as $193 billion, including $89 billion in U.S.-based losses, according to insurance industry modeling.[191] Such a cyber event would be one of the costliest disasters in modern history (see figure 8).[192]

FIGURE 8

Extreme Cyber Scenarios Compared with Select U.S. Disasters



SOURCES: Lloyd's, Aon Centre for Innovation and Analytics, MSIG, SCOR TransRe, and Cyber Risk Management (CyRiM), "Bashe Attack: Global Infection by Contagious Malware," January 2019, https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2019/cyrimbasheattack_final.pdf; and National Oceanic and Atmospheric Administration, "Billion-Dollar Weather and Climate Disasters: Events," 2020, https://www.ncdc.noaa.gov/billions/events.

NOTE: The cost of the U.S. disasters is calculated in 2020 dollars. The hypothetical costs of the Bashe scenario are calculated in 2019 dollars.

The devastation such a cyber attack would unleash—and the inability of insurance to adequately compensate victims or fund recovery—could force governments to pay. Already, multiple U.S. states have declared disasters or states of emergency in response to ransomware attacks and at times have even activated their National Guard units for assistance.[193] Larger cyber attacks could lead Congress to provide emergency appropriations, much like it often does after a hurricane. The alternative would be to leave victims undercompensated, or more drastically, to mandate that insurance companies provide after-the-fact coverage.[194] The former approach may be politically unpalatable, while the latter would meet fierce resistance and have grave unintended consequences.

In the wake of a major cyber disaster, there would be louder calls for a formal cyber backstop. It would be smarter and cheaper to create one in advance. A RAND study estimated that TRIA actually saves taxpayers money because the law attracts private capital into the insurance marketplace.[195] This initial base of private funds ultimately reduces the government's share of the financial burden following terrorist attacks, which might otherwise have been shouldered solely by congressional appropriations. A properly designed cyber insurance backstop could function in the same way.

There are encouraging signs that some governments are entertaining the idea of developing cyber backstops. In the United States, the congressionally chartered Cyberspace Solarium Commission recently proposed a study of the issue that would consider specific design parameters.[196] And the coronavirus pandemic has focused attention on other forms of catastrophic risk, spawning new calls for a government backstop to support expanded pandemic insurance.[197]

Proposals for cyber backstops and pandemic backstops may intersect and influence one another in unpredictable ways. Governments exhausted by the fiscal demands of the coronavirus pandemic and potential future pandemics may balk at accepting more ownership of cyber risk. Alternatively, policymakers may realize their societies face multiple catastrophic risks—including cyber incidents, pandemics, and more—and resolve to address each more proactively. In the latter scenario, there might be a decision between peril-specific backstops or some kind of all-hazards backstop.

Looking Ahead

Cyber insurance has significant unrealized potential to serve the needs of insureds, insurers, and society at large. Nearly everyone has a stake in the healthy development of cyber insurance. Insurance could someday incentivize better cyber hygiene and lower cyber risk on a broad scale. Such improve-

ments could help to chip away at pervasive cyber insecurity and thus provide economic, national security, and privacy benefits, among others. However, these benefits will not be realized without purposeful effort by many stakeholders. The cyber insurance marketplace has made great strides, but fundamental challenges revealed by NotPetya have not yet been solved. Three years later, it is clear that new ways of thinking and doing business are needed.

War exclusions that trace their lineage to the eighteenth century do not provide good answers for twenty-first-century cyber threats. They are ambiguous, poorly tailored to cyber risk, and naturally result in expensive, time-consuming, uncertain litigation. This paper has sought to diagnose the problem, establish criteria for a solution, evaluate potential options, and present new models of alternative cyber exclusions. The proposed exclusions aim to better address catastrophic and state-sponsored cyber risk than today's war and terrorism exclusions do. But whether or not they are adopted, these proposals will hopefully provoke debate and stimulate other creative new ideas. It will be years before insureds, insurers, and governments reach consensus on how to handle key aspects of cyber risk. More public discussion and fresh proposals can help bring that day forward.

Above all, the war exclusion challenge calls for broader discussion. Cyber insurance exclusions may seem arcane to non-experts, but they raise profound questions about how societies manage risk. Malicious cyber incidents are among the most significant and fastest-growing sources of risk to organizations and nations. And state-sponsored operations may be the foremost kind of cyber threat. Despite years of international attempts to encourage restraint or impose deterrence, state-sponsored cyber operations have only grown in volume and severity. Yet the private and public mechanisms for managing this risk remain woefully underdeveloped.

Insurance will be a key tool for countries seeking to better address cyber risk. But the insurance industry does not have all the answers, nor does it have all the resources needed to implement a comprehensive risk management framework. Ideas should draw upon expertise in a wide range of areas, including cyber conflict, warfare, international affairs, technology, cybersecurity public policy, disaster management, catastrophic risk, and more. Experts in these fields should recognize the stakes they hold in the development of cyber insurance. Likewise, the insurance industry should do more to educate outside stakeholders about the possibilities and limitations of cyber insurance. This paper represents one small step toward bridging these gaps and an invitation for further dialogue across disciplines and communities of interest.

About the Author

Jon Bateman is a fellow in the Cyber Policy Initiative at the Carnegie Endowment for International Peace. He previously worked as a senior intelligence analyst, policy adviser, and speechwriter in the U.S. Defense Department, most recently serving as special assistant to the Chairman of the Joint Chiefs of Staff.

Acknowledgments

This paper could not have been written without Ariel (Eli) Levite. His knowledge and perspective shaped every aspect of the paper's conception, development, and refinement. Special thanks also go to Wyatt Hoffman for helping to frame the problem, to George Perkovich for sharpening the writing and ideas, and to Evan Burke and Alexandria Hayman for valuable research assistance.

Outside of Carnegie, many experts generously shared their insights and provided feedback on versions of this paper. The author is immensely grateful to Nick Beecroft, Eric Durand, Franz Gromotka, Scott Kannry, Julian Miller, Jürgen Reinhart, Sasha Romanosky, and others who wish to remain anonymous. The paper makes no attempt to represent any consensus among their disparate views, and the final text is the author's sole responsibility.

Notes

1 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; and PCS, "Could NotPetya's Tail Be Growing?," 2019, https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf.

2 Response of Generali in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

3 Merryn Somerset Webb, "Cyber Breaches Expose the Limits of the Insurance Market," *Financial Times*, January 25, 2019, https://www.ft.com/content/41672a22-2005-11e9-b126-46fc3ad87c65.

4 For an overview, see Ariel (Eli) Levite, Scott Kannry, and Wyatt Hoffman, "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance," Carnegie Endowment for International Peace, November 7, 2018, https://carnegieendowment.org/2018/11/07/addressing-private-sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622.

5 For example, the U.S. Department of Homeland Security has designated insurance services as one of fifty-five "national critical functions" considered "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Cybersecurity and Infrastructure Security Agency (CISA), "National Critical Functions Set," May 13, 2020, https://www.cisa.gov/national-critical-functions-set.

6 Unless stated otherwise, the term insurers in this paper refers to both primary insurers and reinsurers.

7 CISA, "Assessment of the Cyber Insurance Market," July 2019, https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf.

8 Swiss Re, "Cyber Risk," November 21, 2018, https://www.swissre.com/institute/research/topics-and-risk-dialogues/digital-and-technology/topic-cyber-risk.html.

9 Lloyd's, Aon Centre for Innovation and Analytics, MSIG, SCOR TransRe, and Cyber Risk Management (CyRiM), "Bashe Attack: Global Infection by Contagious Malware," January 2019, https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2019/cyrimbasheattack_final.pdf.

10 "Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance," *Insurance Journal*, May 31, 2017, https://www.insurancejournal.com/news/national/2017/05/31/452647.htm.

11 "Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance," *Insurance Journal*.

12 Katherine Chiglinsky and Sonali Basak, "Buffett Cautious on Cyber Insurance Because No One Knows Risks," *Bloomberg*, May 5, 2018, https://www.bloomberg.com/news/articles/2018-05-05/buffett-cautious-on-cyber-insurance-because-no-one-knows-risks?sref=QmOxnLFz.

13 Elizabeth Blosfield, "Data Deficit Remains Key Challenge for Cyber Insurance Underwriters," *Insurance Journal*, June 18, 2019 https://www.insurancejournal.com/news/national/2019/06/18/529663.htm; "2019 Information Security and Cyber Risk Management Survey," Advisen and Zurich, October 2019, https://www.advisenltd.com/2019-information-security-and-cyber-risk-management-zurich-cyber-survey/; and Elizabeth Blosfield, "Cyber Business Interruption Remains Area of Uncertainty for Insurance," *Insurance Journal*, June 12, 2018, https://www.insurancejournal.com/news/national/2018/06/12/491842.htm.

14 Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?," *Journal of Cybersecurity* 5 (2019): https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419#131678466; and U.S. Cyber Solarium Commission, "Report," March 2020, https://www.solarium.gov/report.

15 Ariel (Eli) Levite and Wyatt Hoffman, "A Moment of Truth for Cyber Insurance," *Lawfare*, February 7, 2019, https://www.lawfareblog.com/moment-truth-cyber-insurance.
16 CISA, "Assessment of the Cyber Insurance Market."
17 U.S. Cyber Solarium Commission, "Report."
18 Andrew Granato and Andy Polacek, "The Growth and Challenges of Cyber Insurance," *Chicago Fed Letter* No. 426, 2019, https://www.chicagofed.org/publications/chicago-fed-letter/2019/426.
19 For an excellent overview, see Daniel Woods and Andrew Simpson, "Policy Measures and Cyber Insurance: A Framework," *Journal of Cyber Policy* 2 (2017): https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1360927.
20 "State of the Cyber Insurance Market— Top Trends, Insurers and Challenges: A.M. Best," *Insurance Journal*, June 18, 2019, https://www.insurancejournal.com/news/national/2019/06/18/529747.htm.
21 Duffie Osental, "Verisk Launches New Cyber Underwriting Report," *Insurance Business America*, June 18, 2019, https://www.insurancebusinessmag.com/us/news/cyber/verisk-launches-new-cyber-underwriting-report-170271.aspx.
22 Levite and Hoffman, "A Moment of Truth for Cyber Insurance."
23 Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"; and PCS, "Could NotPetya's Tail Be Growing?"
24 Valeria Ermakova and Catherine Thomas, "Scrutiny of Management Approach Increases as London Cyber Insurance Market Grows," AM Best, March 2, 2020, http://www3.ambest.com/bestweekpdfs/sr774997420811full.pdf.
25 Patrick Howell O'Neill, "NotPetya Ransomware Cost Merck More Than $310 Million," Cyberscoop, October 27, 2017, https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/.
26 In 2016, the year before NotPetya, Lloyd's began including a cyber scenario in its insurance industry stress tests. The scenario was not identical to NotPetya but bore some resemblance to it and has continued to be used. Lloyd's, "Realistic Disaster Scenarios—Scenario Specification," January 2016, https://www.lloyds.com/market-resources/underwriting/realistic-disaster-scenarios-rds/scenario-specification-2016.
27 Daniel M. Hofmann, Steve Wilson, and Rachel Anne Carter, "Advancing Accumulation Risk Management in Cyber Insurance," Geneva Association, August 2018, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance_0.pdf.
28 Organisation for Economic Co-operation and Development, "The Contribution of Reinsurance Markets to Managing Catastrophe Risk," December 14, 2018, https://www.oecd.org/finance/the-contribution-of-reinsurance-markets-to-managing-catastrophe-risk.pdf; and Mark Synnott, "The Problem of Silent Cyber Risk Accumulation," Willis Towers Watson, February 25, 2020, https://www.willistowerswatson.com/en-US/Insights/2020/02/the-problem-of-silent-cyber-risk-accumulation.
29 "Munich Re the Latest Carrier to Settle Merck NotPetya Dispute," *Insurer*, July 13, 2020, https://www.theinsurer.com/news/munich-re-the-latest-carrier-to-settle-merck-notpetya-dispute/9717.article.
30 David Voreacos, Katherine Chiglinsky, Riley Griffin, "Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?," *Bloomberg*, December 3, 2019, https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war.
31 "Munich Re the Latest Carrier to Settle Merck NotPetya Dispute," *Insurer*.
32 Many of the property and casualty policies held by Merck specifically excluded certain data losses, though how these exclusions apply to NotPetya is a matter of pending litigation. This paper does not

take a position on the merits of the litigation or the parties' legal arguments over the scope of the insurance policies. For the sake of simplicity, the paper will refer to Merck's policy as silent cyber coverage.

33 Voreacos, Chiglinsky, and Griffin, "Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?"

34 Mary Millikin, "Insurance to Fully Cover Sony's Cyber Attack, Says CEO," *Insurance Journal*, January 12, 2015, https://www.insurancejournal.com/news/national/2015/01/12/353835.htm; and Daniel W. Woods and Jessica Weinkle, "Insurance Definitions of Cyber War," *Geneva Papers on Risk and Insurance – Issues and Practice*, May 6, 2020, https://link.springer.com/article/10.1057%2Fs41288-020-00168-5.

35 Bethan Moorcraft, "What Is Silent Cyber Risk?," *Insurance Business America*, November 26, 2018, https://www.insurancebusinessmag.com/us/guides/what-is-silent-cyber-risk-117150.aspx.

36 CISA, "Assessment of the Cyber Insurance Market."

37 Bethan Moorcraft, "AGCS Global Cyber Head Explains Stance on Silent Cyber," *Insurance Business America*, October 23, 2019, https://www.insurancebusinessmag.com/us/news/cyber/agcs-global-cyber-head-explains-stance-on-silent-cyber-189414.aspx; and Stefan Golling and Katja Weber, "Silent Cyber – A Journey Shared Across Industry Participants," Munich Re, September 7, 2019, https://www.munichre.com/topics-online/en/digitalisation/cyber/silent-cyber-risks.html.

38 Lloyd's, Aon Centre for Innovation and Analytics, MSIG, SCOR TransRe, and CyRiM, "Bashe Attack: Global Infection by Contagious Malware."

39 Levite and Hoffman, "A Moment of Truth for Cyber Insurance."

40 Adam Satariano and Nicole Perlroth, "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.," *New York Times*, April 15, 2019, https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

41 Response of Generali in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

42 Response of Generali in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

43 Exclusions for losses caused by "military or usurped power" have existed since 1720, according to a leading judicial analysis. See *Pan American World Airways Inc. v. Aetna Casualty and Surety Co.*, 505 F.2d 989 (2nd Cir. 1974), https://casetext.com/case/pan-american-world-air-v-aetna-cas-sur.

44 Adam B. Shniderman, "Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies," *Yale Law Journal* 129 (2019): https://www.yalelawjournal.org/forum/prove-it-judging-the-hostile-or-warlike-action-exclusion-in-cyber-insurance-policies.

45 With war risks excluded from most insurance policies, a niche industry has emerged to provide specific war coverage. In the United States, affirmative terrorism coverage has become more common since 2002, when the Terrorism Risk Insurance Act mandated equal treatment for terrorism losses in exchange for a government backstop.

46 Rachel Anne Carter and Julian Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability," Geneva Association and IFTRIP, July 2020, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_war_terrorism_commonlanguage_final.pdf.

47 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."

48 Response of Generali in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

49 Euan McKirdy and Mary Ilyushina, "Putin: 'Patriotic' Russian Hackers May Have Targeted US Election," *CNN*, June 2, 2017, https://www.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html; and Tal Kopan, "Is Trump Right? Could a 400-Pound Couch Potato Have Hacked the DNC?," *CNN*, September 27, 2016, https://www.cnn.com/2016/09/27/politics/dnc-cyberattack-400-pound-hackers/index.html.

50 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (2015), https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf.

51 Shniderman, "Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies."

52 Office of the Director of National Intelligence, "A Guide to Cyber Attribution," September 14, 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

53 Herbert Lin, "Attribution of Malicious Cyber Incidents," Hoover Institution Aegis Paper Series no. 1607, October 2, 2016, https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

54 Ellen Nakashima, "Russian Spies Hacked the Olympics and Tried to Make It Look Like North Korea Did It, U.S. Officials Say," *Washington Post*, February 24, 2018, https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html.

55 Mark Goudie, "Going Beyond Malware: The Rise of 'Living off the Land' Attacks," CrowdStrike, May 7, 2019, https://www.crowdstrike.com/blog/going-beyond-malware-the-rise-of-living-off-the-land-attacks/.

56 Office of the Director of National Intelligence, "A Guide to Cyber Attribution."

57 "Charming Kitten," MITRE ATT&CK, July 4, 2020, https://attack.mitre.org/groups/G0058/; and "APT 37," MITRE ATT&CK, June 23, 2020, https://attack.mitre.org/groups/G0067/.

58 Shari Seidman Diamond and Jessica M. Salerno, "Empirical Analysis of Juries in Tort Case," in *Research Handbook on the Economics of Torts*, ed. Jennifer H. Arlen (Northhampton, MA: Edward Elgar 2013), http://www.law.nyu.edu/sites/default/files/upload_documents/Empirical-Analysis-of-Juries-in-Tort-Cases.pdf.

59 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).

60 "Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation," FireEye, August 7, 2019, https://content.fireeye.com/apt-41/rpt-apt41/.

61 Julian E. Barnes, Adam Goldman, and David E. Sanger, "C.I.A. Informant Extracted From Russia Had Sent Secrets to U.S. for Decades," September 17, 2019, https://www.nytimes.com/2019/09/09/us/politics/cia-informant-russia.html.

62 For example, a report by FireEye states, "We assess with high confidence that this activity is carried out on behalf of the North Korean government given malware development artifacts and targeting that aligns with North Korean state interests." "APT 37 (REAPER)," FireEye, February 20, 2018, https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf.

63 "Advanced Persistent Threat Groups," FireEye, 2020, accessed August 3, 2020, https://www.fireeye.com/current-threats/apt-groups.html.

64 Stilgherrian, "Blaming Russia for NotPetya Was Coordinated Diplomatic Action," ZDNet, April 12, 2018, https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

65 Federal Bureau of Investigation and CISA, "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations," May 13, 2020, https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.

66 *Pan American World Airways Inc. v. Aetna Casualty and Surety Co.*, 505 F.2d 989 (2nd Cir. 1974), https://casetext.com/case/pan-american-world-air-v-aetna-cas-sur.

67 For a discussion of this problem and potential remedies in the U.S. context, see Shniderman, "Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies."
68 *Pan American World Airways Inc. v. Aetna Casualty and Surety Co.*, 505 F.2d 989 (2nd Cir. 1974), https://casetext.com/case/pan-american-world-air-v-aetna-cas-sur.
69 White House, "Remarks by the President in Year-End Press Conference," December 19, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.
70 Aarti Shahani, "Doubts Persist on U.S. Claims of North Korean Role in Sony Hack," NPR, December 26, 2014, https://www.npr.org/sections/alltechconsidered/2014/12/26/373303733/doubts-persist-on-u-s-claims-on-north-korean-role-in-sony-hack.
71 Criminal complaint in *U.S. v. Park Jin Hyok*, U.S. District Court for the District of Columbia, June 8, 2018, https://www.justice.gov/opa/press-release/file/1092091/download.
72 Tatiana Siegel, "Five Years Later, Who Really Hacked Sony?," *Hollywood Reporter*, November 25, 2019, https://www.hollywoodreporter.com/features/five-years-who-hacked-sony-1257591.
73 Lieutenant Commander Pat Paterson, "The Truth About Tonkin," *Naval History Magazine*, February 2008, https://www.usni.org/magazines/naval-history-magazine/2008/february/truth-about-tonkin.
74 Alex Cybulski, "Did Iran Launch a Cyberattack Against the US? Probably Not, New Report Says," *Motherboard*, April 27, 2015, https://www.vice.com/en_us/article/vvbj58/did-iran-launch-a-cyberattack-against-the-us-probably-not-new-report-says.
75 Florian J. Egloff, "Contested Public Attributions of Cyber Incidents and the Role of Academia," *Contemporary Security Policy* 41 (2020), https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1677324.
76 Satariano and Perlroth, "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong."
77 Shniderman, "Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies."
78 Shniderman, "Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies."
79 Department of Justice, "Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax," February 10, 2020, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.
80 Matthew McCabe, "NotPetya Was Not Cyber 'War,'" Marsh and McLennan, August 2018, https://www.mmc.com/insights/publications/2018/aug/notpetya-was-not-cyber-war.html.
81 *Pan American World Airways Inc. v. Aetna Casualty and Surety Co.*, 505 F.2d 989 (2nd Cir. 1974), https://casetext.com/case/pan-american-world-air-v-aetna-cas-sur.
82 Maurer, *Cyber Mercenaries: The State, Hackers, and Power*.
83 Department of Justice, "Assistant Attorney General John C. Demers Remarks for Press Conference on United States V Li, Et Al. (EDWA)," July 21, 2020, https://www.justice.gov/opa/speech/assistant-attorney-general-john-c-demers-remarks-press-conference-united-states-v-li-et.
84 According to FireEye, the average "dwell time" (period between network penetration and detection) is fifty-six days. Some dwell times are significantly longer. For small to midsized organizations, the average dwell time is over two years. FireEye, "M-Trends 2020," February 20, 2020, https://content.fireeye.com/m-trends/rpt-m-trends-2020; and Chris Gerritz, "2019 Mid-market Threat and Incident Response Report," Infocyte, 2019, https://www.infocyte.com/resources/mid-market-threat-and-incident-response-report/.
85 Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

86 Bruce Schneider, "There's No Real Difference Between Online Espionage and Online Attack," *Atlantic*, March 6, 2014, https://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/.

87 "Voluntary Shutdown: A New Normal for Cyber Business Interruption," Marsh, November 2018, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Insights%20Cyber%20Voluntary%20Shutdown.pdf.

88 Ed Dante, "Cybersecurity Breach Bankruptcy: It Does Happen," Fractional CISO, January 23, 2019, https://fractionalciso.com/cybersecurity-breach-bankruptcy/; and Jessica E. Vascellaro, Jason Dean, and Siobhan Gorman, "Google Warns of China Exit Over Hacking," *Wall Street Journal*, January 13, 2010, https://www.wsj.com/articles/SB126333757451026659.

89 Herb Lin, "Developing 'Loud' Cyber Weapons," *Lawfare*, September 1, 2016, https://www.lawfareblog.com/developing-loud-cyber-weapons.

90 Sasha Romanosky, "Examining the Costs and Causes of Cyber Incidents," *Journal of Cybersecurity* 2 (2016): https://academic.oup.com/cybersecurity/article/2/2/121/2525524.

91 "Cyber-Attack: US and UK Blame North Korea for WannaCry," BBC, December 19, 2017, https://www.bbc.com/news/world-us-canada-42407488.

92 Department of Justice, "Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax."

93 Andrew Griffin, "US Charges Two 'State-Sponsored' Russian Spies Over Yahoo Hack, the Biggest Cyber Attack in the World," *Independent*, March 15, 2017, https://www.independent.co.uk/life-style/gadgets-and-tech/news/us-russia-yahoo-hack-donald-trump-spies-state-sponsored-cyber-attack-a7631566.html.

94 Department of Justice, "Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax."

95 The National Institute of Standards and Technology (NIST)'s definition of "advanced persistent threat" provides a succinct explanation of why state-sponsored cyber operations can be so effective. NIST, "Advanced Persistent Threat (APT)," https://csrc.nist.gov/glossary/term/advanced_persistent_threat.

96 Kim Zetter and Huib Modderkolk, "Revealed: How a Secret Dutch Mole Aided the U.S.-Israeli Stuxnet Cyberattack on Iran," *Yahoo News*, September 2, 2019, https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html.

97 Allison Peters and Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime," Third Way, May 27, 2020, https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime.

98 Wyatt Hoffman and Ariel (Eli) Levite, "Rethinking Corporate Active Cyber Defense," *Lawfare*, July 17, 2017, https://www.lawfareblog.com/rethinking-corporate-active-cyber-defense.

99 "Small Business Cybercriminal Target Survey Data," National Cybersecurity Alliance, October 23, 2019, https://staysafeonline.org/small-business-target-survey-data/; and Dante, "Cybersecurity Breach Bankruptcy: It Does Happen."

100 Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf; Organisation for Economic Co-operation and Development, "Enhancing the Role of Insurance in Cyber Risk Management," December 8, 2017, https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf; Paul J. Jim, "Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far," Money.com, September 12, 2017, https://money.com/equifaxs-massive-data-breach-has-cost-the-company-4-billion-

so-far/; Dhanya Skariachan and Jim Finkle, "Target Shares Recover After Reassurance on Data Breach Impact," Reuters, February 26, 2014, https://www.reuters.com/article/us-target-results/target-shares-recover-after-reassurance-on-data-breach-impact-idUSBREA1P0WC20140226.

101 Kate Fazzini, "Equifax Just Became the First Company to Have Its Outlook Downgraded for a Cyber Attack," CNBC, May 22, 2019, https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html; Algirde Pipikaite and Martina Cheung, "Investors Have a Role in Securing Our Shared Digital Future," World Economic Forum, July 8, 2019, https://www.weforum.org/agenda/2019/07/why-cybersecurity-should-be-standard-due-diligence-for-investors/; and Owen Walker, "Cyber Governance Indices Identify Companies at Risk of Data Breaches," *Financial Times*, May 13, 2019, https://www.ft.com/content/59e7a623-e3da-3896-b1f7-aa5593643048.

102 Nehemiah Robinson, "War Damage Compensation and Restitution in Foreign Countries," *Law and Contemporary Problems* 16 (1951), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2490&context=lcp; and Jack Hirshleifer, "Compensation for War Damage: An Economic View," *Columbia Law Review 55* (1955), https://www.jstor.org/stable/1119680?seq=1.

103 Danny Palmer, "What's the Difference Between State-Backed Hackers and Cybercrime Gangs? Nothing at All," ZDNet, March 14, 2017, https://www.zdnet.com/article/whats-the-difference-between-state-backed-hackers-and-cybercrime-gangs-nothing-at-all/; and Ivan Kwiatkowski, Pierre Delcher, and Maher Yamout, "Lifting the Veil on DeathStalker, a Mercenary Triumvirate," Kaspersky Lab Securelist, August 24, 2020, https://securelist.com/deathstalker-mercenary-triumvirate/98177/.

104 Lloyd's, Aon Centre for Innovation and Analytics, MSIG, SCOR TransRe, and CyRiM, "Bashe Attack: Global Infection by Contagious Malware."

105 Dan Goodin, "Stealing Advanced Nations' Mac Malware Isn't Hard. Here's How One Hacker Did It," Ars Technica, February 28, 2020, https://arstechnica.com/information-technology/2020/02/why-write-your-own-mac-malware-when-you-can-rip-off-a-competitors-a-how-to/.

106 Kate Fazzini, "The Capital One Breach Is Unlike Any Other Major Hack, With Allegations of a Single Engineer Wreaking Havoc," CNBC, July 30, 2019, https://www.cnbc.com/2019/07/30/capital-one-hack-allegations-describe-a-rare-insider-threat-case.html. For a detailed analysis of cyber threats to the cloud, see Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace, August 31, 2020, https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597.

107 Zach Whittaker, "In Patches We Trust: Why Software Updates Have to Get Better," ZDNet, December 10, 2015, https://www.zdnet.com/article/in-patches-we-trust-why-software-updates-have-to-get-better/.

108 Response of Atrium in *Merck & Co, Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

109 Response of Atrium in *Merck & Co, Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

110 Oliver Ralph and Robert Armstrong, "Mondelez Sues Zurich in Test for Cyber Hack Insurance," *Financial Times*, January 9, 2019, https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e.

111 Satariano and Perlroth, "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong."

112 For example, insurers have questioned whether Merck satisfied the conditions of its coverage or acted to mitigate its damages. Response of Generali in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

113 Complaint in *Mondelez International, Inc. v. Zurich American Insurance Company*, Circuit Court of Cook County, Illinois, October 10, 2018.

114 For the range of language seen in affirmative cyber policies, see Daniel W. Woods and Jessica Weinkle, "Market Definitions of Cyber War," Proceedings of The Hague Conference on Cyber Norms, working paper, September 30, 2019, https://www.researchgate.net/publication/336134006_Market_Definitions_of_Cyber_War.

115 For an example of this fact-specific analysis, see Whitney L. Allen and Jonathan L. Schwartz, "What Is Modern Warfare? Ninth Circuit Rules War Exclusions Do Not Preclude Coverage for First Party Loss Caused by Hamas Rocket Attacks," Lexology, July 22, 2019, https://www.lexology.com/library/detail.aspx?g=a5a2f563-df61-4a9a-9885-24ab8b4adcdd.

116 At least four insurers sued by Merck have already settled. "Munich Re the Latest Carrier to Settle Merck NotPetya Dispute," *Insurer*.

117 Lynne McChristian, "Hurricane Andrew and Insurance: The Enduring Impact of an Historic Storm," Insurance Information Institute, August 2012, https://www.iii.org/sites/default/files/paper_HurricaneAndrew_final.pdf.

118 Saumi Shokraee, "Six Things to Know About the Recent Impasse Between Regulators and Insurers in the Aftermath of California's Devastating Wildfires," *Insurance Journal*, April 17, 2020, https://www.insurancejournal.com/blogs/corelogic/2020/04/17/565104.htm.

119 Tony Lathrop, "Pandemic Risk Insurance Act of 2020 Introduced in Congress – A Federal Backstop for Business Interruption and Event Cancellation Losses," JDSupra, June 11, 2020, https://www.jdsupra.com/legalnews/pandemic-risk-insurance-act-of-2020-27937/; and Claire Wilkinson, "Ohio Bill Would Force Insurers to Cover COVID-19 Interruption Losses," *Business Insurance*, March 26, 2020, https://www.businessinsurance.com/article/20200326/NEWS06/912333733/Ohio-bill-would-force-insurers-to-cover-COVID-19-interruption-losses-coronavirus.

120 Synnott, "The Problem of Silent Cyber Risk Accumulation."

121 This is based on publicly available information. It is possible that war exclusions in affirmative cyber policies have been invoked without being publicized by the insured or the insurer.

122 Whether these policies are indeed silent as to cyber risk is a matter under litigation, and this paper does not take a position on the merits. In the Merck case, for example, Munich Re cited an electronic data exclusion that applies to any "loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever." Munich Re has since settled with Merck. Response of Munich Re in *Merck & Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018; and "Munich Re the Latest Carrier to Settle Merck NotPetya Dispute," *Insurer*.

123 Woods and Weinkle, "Insurance Definitions of Cyber War."

124 "Cyber: Drivers of Change," Aon Benfield, September 2016, http://thoughtleadership.aonbenfield.com/Documents/201609-cyber-drivers-of-change.pdf.

125 "Lloyd's Moves to Address Silent Cyber Risk," CIAB, July 11, 2019, https://www.ciab.com/resources/lloyds-moves-to-address-silent-cyber-risk/.

126 "'Silent Cyber' — Frequently Asked Questions," Marsh, July 2020, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/silent-cyber-faq.pdf; and Synnott, "The Problem of Silent Cyber Risk Accumulation."

127 Andrew Hill, "Cyber Risk Poses Ongoing Challenge for First-Party Property Damage Lines of Business," Willis Towers Watson, January 28, 2020, https://www.willistowerswatson.com/en-US/Insights/2020/01/cyber-risk-poses-ongoing-challenge-for-first-party-property-damage-lines-of-business.

128 Romanosky, Ablon, Kuehn, and Jones, "Content Analysis of Cyber Insurance Policies"; and Woods and Weinkle, "Market Definitions of Cyber War."
129 Sam Hanig, Josie Novak, Fred Eslami, and Bob Skrabal, "Cyber Insurers Are Profitable Today, but Wary of Tomorrow's Risks," AM Best, June 17, 2019, https://www3.ambest.com/bestweekpdfs/sr507453119175full.pdf.
130 "Cry Cyber and Let Slip the Dogs of War," Capsicum Re, July 23, 2019, https://www.capsicumre.com/wp-content/uploads/2019/07/Capsicum-Re-Cry-Cyber.pdf.
131 Woods and Weinkle, "Market Definitions of Cyber War."
132 Mirza Salam Ahmed and Ben Dyson, "Cyber Insurers Wrestle With War Exclusions as State-Sponsored Attack Fears Grow," S&P Global Market Intelligence, January 30, 2020, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-wrestle-with-war-exclusions-as-state-sponsored-attack-fears-grow-56743302.
133 Woods and Weinkle, "Insurance Definitions of Cyber War"; "Cry Cyber and Let Slip the Dogs of War," Capsicum Re; and Ahmed and Dyson, "Cyber Insurers Wrestle With War Exclusions as State-Sponsored Attack Fears Grow."
134 "Cry Cyber and Let Slip the Dogs of War," Capsicum Re.
135 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."
136 Ahmed and Dyson, "Cyber Insurers Wrestle With War Exclusions as State-Sponsored Attack Fears Grow."
137 Anthony Craig, "Understanding the Proliferation of Cyber Capabilities," Council on Foreign Relations, October 18, 2018, https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities.
138 Andy Greenberg, "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction," *Wired*, September 12, 2019, https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.
139 U.S. Cyber Solarium Commission, "Report."
140 Jack Stubbs and Christopher Bing, "Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say," Reuters, October 21, 2019, https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK.
141 Levite, Kannry, and Hoffman, "Addressing the Private Sector Cybersecurity Predicament."
142 For example, COVID-19 created massive, abrupt changes in technology usage, causing some to dub collaboration tools like Zoom as "critical infrastructure." Drake Bennet and Nico Grant, "Zoom Goes From Conferencing App to the Pandemic's Social Network," *Bloomberg Businessweek*, April 9, 2020, https://www.bloomberg.com/news/features/2020-04-09/zoom-goes-from-conferencing-app-to-the-pandemic-s-social-network.
143 Lily Hay Newman, "The Leaked NSA Spy Tool That Hacked the World," *Wired*, March 7, 2018, https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.
144 Rory Egan and Cyrus Delarami, "What If a Major Cyber Attack Strikes Critical Infrastructure?," Munich Re, November 22, 2018, https://www.munichre.com/topics-online/en/digitalisation/cyber/silent-cyber.html.
145 A typical example is the Beazley InfoSec policy, which excludes losses arising from "Failure or malfunction of satellites or of power, utility, mechanical or telecommunications (including internet) infrastructure or services that are not under the Insured Organization's direct operational control." "Beazley InfoSec," Beazley, accessed August 16, 2020, https://www.beazley.com/documents/TMB/Policies/beazley-tmb-infosec-policy.pdf.

146 Ariel (Eli) Levite, "ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies," Carnegie Endowment for International Peace, October 4, 2019, https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974.
147 Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."
148 Josh Fruhlinger, "Spectre and Meltdown Explained: What They Are, How They Work, What's at Risk," CSO, January 15, 2018, https://www.csoonline.com/article/3247868/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html.
149 Martin Eling and Jan Hendrik Wirfs, "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class," Institute of Insurance Economics (University of St. Gallen), 2016, https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf.
150 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."
151 Colin Clark, "CJCS Dunford Calls For Strategic Shifts; 'At Peace Or At War Is Insufficient'," *Breaking Defense*, September 21, 2016, https://breakingdefense.com/2016/09/cjcs-dunford-calls-for-strategic-shifts-at-peace-or-at-war-is-insufficient/.
152 Frank G. Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," Heritage Foundation, October 2015, https://www.heritage.org/sites/default/files/2019-10/2016_IndexOfUSMilitaryStrength_The%20Contemporary%20Spectrum%20of%20Conflict_Protracted%20Gray%20Zone%20Ambiguous%20and%20Hybrid%20Modes%20of%20War.pdf.
153 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."
154 Joint Chiefs of Staff, "Joint Concept for Integrated Campaigning," March 16, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.
155 Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)," July 25, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.
156 "The Cyber Act of War Act: A Proposal for a Problem the Law Can't Fix," Council on Foreign Relations, May 12, 2016, https://www.cfr.org/blog/cyber-act-war-act-proposal-problem-law-cant-fix.
157 Wyatt Hoffman, "Is Cyber Strategy Possible?", *Washington Quarterly* 42 (2019), https://www.tandfonline.com/doi/abs/10.1080/0163660X.2019.1593665?journalCode=rwaq20.
158 Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.
159 "Cry Cyber and Let Slip the Dogs of War," Capsicum Re.
160 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."
161 "Cry Cyber and Let Slip the Dogs of War," Capsicum Re.
162 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."
163 "Joint War Committee," Lloyd's Market Association, 2020, accessed August 3, 2020, https://www.lmalloyds.com/lma/jointwar.
164 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."
165 "Cry Cyber and Let Slip the Dogs of War," Capsicum Re.
166 Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."

167 Daniel Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community," Statement for the Record to the U.S. Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf; and Paul Stronski and Richard Sokolsky, "The Return of Global Russia: An Analytical Framework," Carnegie Endowment for International Peace, December 24, 2017, https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003.

168 "Cry Cyber and Let Slip the Dogs of War," Capsicum Re.

169 "Cry Cyber and Let Slip the Dogs of War," Capsicum Re.

170 Minnie Chan, "How a Deadly Collision With a US Spy Plane 18 Years Ago Brought Big Changes to China's Air Force and Navy," *South China Morning Post*, April 4, 2019, https://www.businessinsider.com/collision-with-us-spy-plane-near-hainan-causes-china-military-advances-2019-4.

171 Camila Domonoske, "China Seizes U.S. Underwater Drone From International Waters, Pentagon Says," NPR, December 16, 2016, https://www.npr.org/sections/thetwo-way/2016/12/16/505850933/china-seizes-unmanned-u-s-underwater-vehicle-in-international-waters.

172 Luis Martinez, "Navy Plane Buzzed by Russian Fighter Over International Waters," ABC News, June 5, 2019, https://abcnews.go.com/International/navy-plane-buzzed-russian-fighter-international-waters/story?id=63493145; and BBC, "Russia and US Warships Almost Collide in East China Sea," June 7, 2019, https://www.bbc.com/news/world-asia-48553568.

173 Jose Pagliery, "Iran Hacked an American Casino, U.S. Says," CNN, February 27, 2015, https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html; and Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," *Bloomberg*, December 12, 2014, https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas?sref=QmOxnLFz.

174 Carter and Enoizi, "Cyber War and Terrorism: Towards a Common Language to Promote Insurability."

175 Allen and Schwartz, "What Is Modern Warfare? Ninth Circuit Rules War Exclusions Do Not Preclude Coverage for First Party Loss Caused by Hamas Rocket Attacks."

176 Ben Schaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018, https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

177 Sune Engel Rasmussen, "U.S.-Led Coalition Captures Last ISIS Bastion in Syria, Ending Caliphate," *Wall Street Journal*, March 23, 2019, https://www.wsj.com/articles/u-s-backed-force-says-islamic-states-caliphate-destroyed-in-syria-11553322489.

178 Carlotta Gall, "Turkey Declares Major Offensive Against Syrian Government," *New York Times*, March 1, 2020, https://www.nytimes.com/2020/03/01/world/middleeast/turkey-syria-assault.html.

179 Some of these issues are explored in Maurer and Hinck, "Cloud Security: A Primer for Policymakers."

180 Eling and Wirfs, "Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class."

181 Laurel Di Silverstro, Matthew Silley, and Rebecca Bole, "ILS and the Cyber Market: Unlocking Potential in the Capital Markets," CyberCube, January 2020, https://www.cybcube.com/wp-content/uploads/2020/01/ILS-Report-FINAL-1.pdf; and Gabriel Olano, "Singapore Launches First Commercial Cyber Risk Pool," *Insurance Business Asia*, October 31, 2018, https://www.insurancebusinessmag.com/asia/news/cyber/singapore-launches-first-commercial-cyber-risk-pool-115040.aspx.

182 Neil Robinson, "Incentives and Barriers of the Cyber Insurance Market in Europe," European Network and Information Security Agency, June 2012, https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe; and Baird Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress," Congressional Research Service, December 27, 2019, https://fas.org/sgp/crs/terror/R45707.pdf.

183 Webel, "Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress."
184 Tom LaTourrette and Noreen Clancy, "The Impact on Federal Spending of Allowing the Terrorism Risk Insurance Act to Expire," RAND Corporation, April 2014, https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR611/RAND_RR611.pdf.
185 Robert K. Knake, "Creating a Federally Sponsored Cyber Insurance Program," Council on Foreign Relations, November, 2016, https://cdn.cfr.org/sites/default/files/pdf/2016/11/CyberBrief_Knake_Cyber-Insurance_OR.pdf.
186 Susanne Sclafane, "P/C Insurers Back a Federal Pandemic Loss Fund But Not a Backstop Like TRIA," *Insurance Journal*, May 19, 2020, https://www.insurancejournal.com/news/national/2020/05/19/569115.htm
187 According to the author's off-the-record conversations with industry stakeholders.
188 LaTourrette and Clancy, "The Impact on Federal Spending of Allowing the Terrorism Risk Insurance Act to Expire."
189 Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"; and PCS, "Could NotPetya's Tail Be Growing?"
190 National Oceanic and Atmospheric Administration (NOAA), "Billion-Dollar Weather and Climate Disasters: Events," 2020, https://www.ncdc.noaa.gov/billions/events.
191 Lloyd's, Aon Centre for Innovation and Analytics, MSIG, SCOR TransRe, and CyRiM, "Bashe Attack: Global Infection by Contagious Malware."
192 Lloyd's, Aon Centre for Innovation and Analytics, MSIG, SCOR TransRe, and CyRiM, "Bashe Attack: Global Infection by Contagious Malware"; and NOAA, "Billion-Dollar Weather and Climate Disasters: Events."
193 Lee Mathews, "Louisiana Governor Declares State of Emergency After Ransomware Hits School Systems," *Forbes*, July 26, 2019, https://www.forbes.com/sites/leemathews/2019/07/26/louisiana-governor-declares-state-of-emergency-after-ransomware-hits-school-systems/#7db991f9b37a; Benjamin Freed, "How Texas Used Its Disaster Playbook After a Huge Ransomware Attack," *StateScoop*, October 15, 2019, https://statescoop.com/texas-ransomware-emergency-declaration-nascio-19/; and Kate Polit, "National Guard Called in to Help After SLG Cyber Attacks," MeriTalk, August 29, 2019, https://www.meritalk.com/articles/national-guard-called-in-to-help-after-slg-cyber-attacks/.
194 Wilkinson, "Ohio Bill Would Force Insurers to Cover COVID-19 Interruption Losses."
195 LaTourrette and Clancy, "The Impact on Federal Spending of Allowing the Terrorism Risk Insurance Act to Expire."
196 U.S. Cyber Solarium Commission, "Report."
197 Sclafane, "P/C Insurers Back a Federal Pandemic Loss Fund But Not a Backstop Like TRIA."

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org