研究简讯

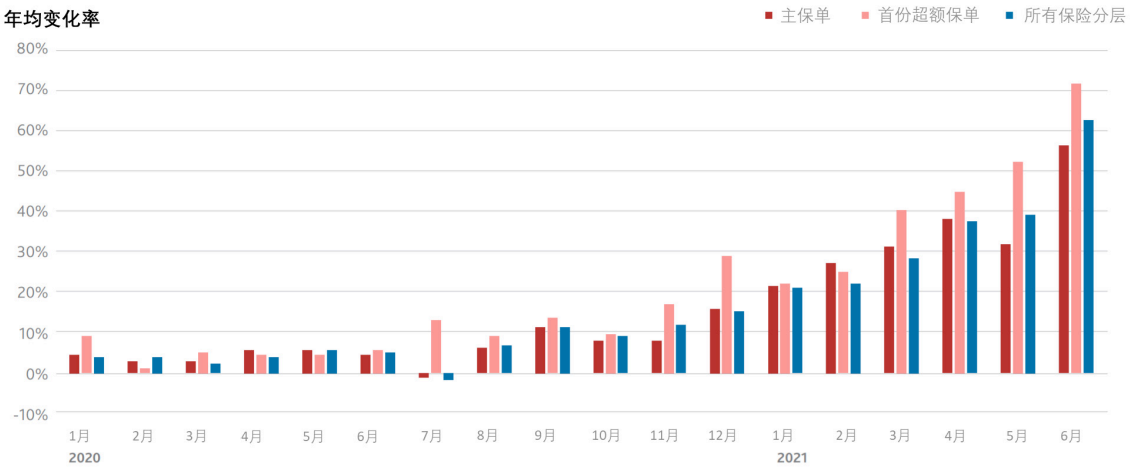
为恶意网络行为投保：寻求可持续的解决方案

Rachel Anne Carter, Carter 保险创新公司，董事总经理
Darren Pain, 日内瓦保险协会，“网络和演变中的责任险”专题主管
Julian Enoizi, Pool Re 首席执行官、恐怖主义风险共保体国际论坛秘书长

网络环境正在迅速演变中，数字化进程更是扩大了威胁和漏洞的范围。这个过程被此次新冠疫情带来的工作和商业行为的转变所放大，而其中一些变化可能会在疫情之后继续存在。自疫情爆发以来，勒索软件和对供应链的攻击变得更加猖獗，人们更广泛地认识到恶意网络事件可能会造成大规模的经济破坏。

随着时间的推移，一个网络保险的专门市场已经发展起来，涉及的风险类别逐渐扩大，包括第一方和第三方的损失。然而，近来独设的网络保险（即专门特定的保障）的损失率急剧上升，促使（再）保险人重新标定网络风险。再加上从传统的财产和意外保险中剔除非列明网络风险的举措（即隐含网络），市场上的（再）保险能力变得更加稀缺。持续强劲的需求引发了网络保险成本的急剧上升以及条款和细则的收紧（图 1）。

图1：在合同续转时网络保险费率按保险分层的增长



在美国等网络保险市场，希望获得1000万或1500万美元以上保障的被保险人通常会分层或叠加保险方案。第一层（或主保单）将为整个计划设定一般条款和条件。超额保单则提供任何所需的额外限额。主保险人承担100%的损失风险，直至其限额。然后，第一个超额保险人将承担上一个分层100%的风险，以此类推。

资料来源：Aon[1]

恶意网络攻击行为 (Hostile Cyber Activity, HCA) 和保险

近来严重的供应链入侵和勒索软件事件凸显了网络保险公司面对的一个长期问题：当此类攻击的肇事者与国家相关联时，保险能够和应该提供多大的保障？传统的战争或类似战争事件的保单免责条款未能充分涵盖国家被怀疑是网络攻击的幕后主使或至少为黑客提供安全港的情况，

[1] Aon 2021.

特别是在攻击动机不明的情况下。此类归属和定性的问题给保险公司带来了巨大的合同不确定性，这加剧了最近网络保险市场条件的收紧。

对网络事件进行更细化的分类——包括恶意网络攻击行为 HCA 术语，该术语规定对国家介入的举证责任比目前广泛使用的定义要低——这将有助于为保险公司提供更大的清晰度，并提高应对风险敞口的便易程度。然而市场需要时间才能接受针对已投保网络事故的更严格的保单措辞，但即便如此，也可能仅会走到这一步而已。

最新的网络事件凸显了在建立清晰明确的界限方面，即界定哪些符合 HCA 的规定，哪些不符合时所面临的挑战。国家层面的参与差异很大，从被报道过的默许赞助，包括为开发复杂但易于使用的恶意软件营造环境（如黑客组织 Dark Side 对美国燃油管道公司 Colonial Pipeline 的攻击），到据称一个主权国家的政府对黑客活动进行直接了当的督管和提供资源（如 SolarWinds 事件）。在这种情况下，直接归因于 HCA 的一些难题就重新浮出水面，特别是如果与犯罪团伙有联系的国家行为者使用假旗战术来隐藏踪迹，指责他人或以其它方式破坏任何关于攻击最终来源的国际共识。

量化网络风险仍具挑战性

网络风险建模和量化方面的进展，以及再保险的可获性和分担风险的其它机制，将是鼓励现有和未来的保险公司为 HCA 和其它恶意网络行为提供更多保险保障的关键。与自然灾害（如飓风）或恐怖袭击等人为灾害不同，网络风险没有地理边界；整个世界都可能成为一个网络灾难地带。除了归因和特征问题外，评估 HCA 的发生频率和严重程度，特别是大量累积损失的潜在可能性，仍然是一个特别严重的挑战。

表1：现有网络风险场景分析

场景描述	广泛的影响	可保性	损失估测的不确定性	经济损失估算（单位：10亿美元）	保险损失估算（单位：10亿美元）
传染性恶意软件的广泛传播[2]	扰乱性的	在网络市场上投保/可投保	高	193	27
重大的云计算故障[1]	扰乱性的	在网络市场上投保/可投保	高	53	8
基础设施的中断或故障（如停电）[2]	破坏性的/扰乱性的	在网络市场上未被投保/不可保	非常高	1,024	71（主要由财产险领域的非肯定性风险敞口所驱动）

注释：(1)导致无法运用的近因有很多，包括技术故障、分布式拒绝服务（DDoS）攻击以及恶意软件的感染。此外，该场景还考虑了受影响的客户无法自行恢复服务的情况。(2) 引发停电的可能触发因素包括众所周知的实体风险（如严重的风暴或地震）、人为错误，但也包括恶意行为。

注释：(1)导致无法运用的近因有很多，包括技术故障、分布式拒绝服务（DDoS）攻击以及恶意软件的感染。此外，该场景还考虑了受影响的客户无法自行恢复服务的情况。[3] (2) 引发停电的可能触发因素包括众所周知的实体风险（如严重的风暴或地震）、人为错误，但也包括恶意行为。[4]

资料来源：日内瓦保险协会和慕尼黑再保险

[2] Lloyd's and University of Cambridge 2019.
[3] Lloyd's and Cyence 2017.
[4] Lloyd's and University of Cambridge 2015.

确定性场景分析表明，一些恶意的网络事件，如云服务的暂时中断，可能会引发与某些历史上的自然灾害大致相当的经济损失（见表 1）。但更极端和持久的网络攻击，包括大范围的 IT 或运营基础设施的服务中断或故障，可能会造成更大的预期损失。此外，围绕这些估计的不确定性非常大，这意味着潜在的总损失可能大大高于这些“猜测”，很容易耗尽（再）保险行业的风险吸纳能力。这在 HCA 事件中尤其如此，因为黑客的动机、策略和威胁载体的模糊性，以及相对较小的、孤立的攻击升级为全面网络战的可能性，都会导致网络风险的量化更加复杂化。

政府支持的作用

在收集网络威胁情报方面的进展，包括企业和政府之间的合作，将提高风险意识和防备，这是建立网络复原力的重要因素。这些信息将使保险公司能够发现漏洞并促进网络风险建模的改进。同样，执法机构在追踪和追捕攻击行为的实施者以及追回被勒索的资金方面取得的进展，可能会在一定程度上震慑网络犯罪分子，而且便于提高保险公司所提供的风险吸纳能力。

然而，最终，一些网络风险的系统性特征，特别是单一事件或与 HCA 相关的攻击活动可能造成的多重损失，意味着累积损失的规模可能超过非公营（再）保险部门可以安全、合理吸纳的水平。围绕着大规模的恶意网络攻击，往往会有附带的损害；甚至非预期的目标也会遭受损失。在某种程度上，近期一连串的攻击也可以被看作是险象环生；如果情况发生了不利变化的话，损失可能会更大。

与目前关于疫情大流行相关风险的辩论相呼应，应该考虑由政府支持的解决方案，为应对这些尾部（极端）网络风险进行融资，以提高整个经济的复原力。一个设计良好的公私合作伙伴关系（PPP）可以提高保障能力，并鼓励网络市场创新，以扩大对 HCA 风险的覆盖面。这不应该仅仅是一项财政上的解决方案，还应该通过与保险行业合作，推广采用网络安全的最佳实践，包括购买适当的保险保障，以减轻社会对此类风险的脆弱性。

设计一个公私合作伙伴关系（PPP）

设计这种由政府支持的解决方案比较复杂。任何公私合作伙伴关系的重要考虑因素包括该计划是强制性的还是自愿性的，触发机制是参数型的还是损失赔偿型的，或者该计划是否建立在互惠性或共同分担原则之上。从财政和可行性的角度来看，也有必要确保采取适当的措施来为该类计划提供资助，并确保在事件发生前或发生后有足够的资金支撑。在采纳特定的方案特征方面，会有一些权衡；此外，如何确定投保人、私营（再）保险公司和政府之间各自应分担多少峰值损失也是一个难点（见表 2）。

这种设计挑战在国际层面上更是被放大了。理想情况下，鉴于网络风险的相互关联性和全球性，合作性的国际解决方案将成为覆盖 HCA 风险的一种选项。然而，法律限制、文化差异、获得资本的途径以及对各国政府是否愿意在不同司法管辖区之间分担风险的疑虑，意味着全球解决方案实际上仍不可行，至少在短期内是这样。因此，应优先考虑在国内制定应对大规模网络风险的 PPP 解决方案。

保险业在理解网络恐怖主义、HCA 和网络战争以及评估如何为此类风险投保方面已经取得了长足的进步。为了扩大可保范围，保险公司需要积极主动地评估分担网络风险的可行性方案，包括通过 PPPs 与政府合作。保险业与政府之间的这种合作努力将有助于缩小网络保障方面的缺口，并确保网络空间的全部社会效益得以实现。

表2：PPP计划可能特征的利弊概括

方案特征	可能的利与弊
 多重风险（相对于单一风险）	***利：*** *多元化的机会* ***弊：*** *管理成本较高*
 强制性（相对于自愿性）	***利：*** *扩大保费汇集，避免逆向选择* ***弊：*** *监控和强制执行的复杂性*
 预先资助（相对于事后资助）	***利：*** *激励预防和缓解风险，且手头有可供支付的资金* ***弊：*** *拨付应急资金所需的政治支持通常具有挑战性*
 参数型（相对于损失赔偿型）	***利：*** *更快、更有效地提供灾难事件后的流动性* ***弊：*** *赔款可能与实际发生的损失有出入*
 共同分担（相对于互惠性原则）	***利：*** *为那些原本可能无法负担的人提供网络保险* ***弊：*** *通常需要配套完善并具强制性*
 永久性（相对于临时性）	***利：*** *便于为获得资金和积累资本制定长期发展战略* ***弊：*** *可能会排挤私人市场参与者并扼杀未来的潜在创新*

资料来源: 日内瓦保险协会

参考文献

Aon. 2021. *Cyber Insurance Snapshot. A Focused View of 2021 Risk and Insurance Challenges*.

Lloyd's and Cyence. 2017. *Counting the Cost. Cyber Exposure Decoded*.

Lloyd's and University of Cambridge. 2015. *Business Blackout. Insurance Implications of a Cyber Attack on the US Power Grid*.

Lloyd's and University of Cambridge. 2019. *Bashe Attack. Global Infection by Contagious Malware*.