全球网络威胁

金融系统面临的网络威胁问题日益严峻，国际社会必须开展合作，共同保障金融系统的安全稳定。

蒂姆·毛瑞尔和亚瑟·纳尔逊

2016 年 2 月，黑客利用环球银行金融电信协会（SWIFT，即全球金融系统的主要电子支付信息系统）存在的安全漏洞，设法以孟加拉国央行为攻击目标，窃取 10 亿美元。尽管孟加拉国央行冻结了大部分交易，但仍有 1.01 亿美元不知去向。这起网络盗窃案件给全球金融界敲响了警钟，我们严重低估了金融系统中存在的系统性网络风险。

如今，重大网络攻击事件对金融稳定构成的威胁不言而喻，人们在评估网络威胁时，关注的问题不再是网络攻击会不会发生，而是什么时间发生。然而，全球目前尚未明确设立具体的责任机构，负责保障金融系统的安全稳定、抵御网络威胁，这使世界各国政府以及企业都在竭力防范这种威胁。重要人物们对网络威胁愈发关注，并为人们敲响了警钟。2020 年 2 月，欧洲央行行长、国际货币基金组织前总裁克里斯蒂娜·拉加德（Christine Lagarde）警告说，网络攻击可能会引发严重的金融危机。2020 年 4 月，金融稳定理事会（FSB）警告称，“如不能得到妥善控制，一

重大网络攻击事件对金融稳定构成的威胁不言而喻，人们在评估网络威胁时，关注的问题不再是网络攻击会不会发生，而是什么时间发生。

场严重的网络事件就有可能会对金融系统造成严重干扰，破坏重要金融基础设施，对金融稳定产生更广泛的影响。”这类网络事件会产生巨大的潜在经济成本，严重损害公众对金融系统的信任和信心。

然而，两大持续发酵的趋势加剧了这种风险。首先，全球金融系统正在经历前所未有的数字化转型，新冠疫情更是加快了这一进程。银行与科技公司之间相互竞争。与此同时，新冠疫情使得老百姓在网络金融服务方面的需求不断上涨，并促使居家办公常态化。目前，世界各地的央行都在考虑支持数字货币和推动支付系统现代化。在转型期间，网络安全事件可以轻而易举地破坏公众对金融系统的信心，中断创新之路，因此，网络安全比以往任何时候都更加重要。

其次，恶意破坏分子正在利用这种数字转型，日益威胁着全球金融系统、金融稳定和公众对金融系统完整性的信心。新冠疫情甚至为黑客提供了新的攻击目标。根据国际清算银行的数据，在新冠疫情相关的网络攻击事件中，金融行业占比第二，仅次于医疗行业。

谁是幕后主使?

未来，严重的网络攻击事件以及随之而来的网络冲击会越来越多。最令人担忧的是，网络攻击事件会损坏金融数据的完整性，如破坏记录、算法和交易等；目前，全球几乎还没有针对此类攻击事件的技术解决方案，公众对金融系统的信任和信心也可能会因此受到更加广泛的影响。隐藏在网络攻击背后的恶意破坏分子，不仅包括愈发猖獗的罪犯——例如，2013 至 2018 年间，以金融机构为攻击目标、窃取超过 10 亿美元的 Carbanak 团伙——还包括国家及国家资助的黑客（见表）。例如，在过去五年，朝鲜至少从 38 个国家不当获得了约 20 亿美元。

网络攻击是一个全球性问题。虽然高收入国家发生的网络攻击事件会被人们大肆宣传，但针对低收入和中低收入国家等弱势目标的网络攻击事件越来越多，且被较少关注。然而，正是在这些国家，普惠金融的推广工作最为显著，这使许多国家跨越式地实现了移动支付这类数字金融服务。这些数字金融服务确实推动了普惠金融的发展，但也为黑客提供了诸多攻击目标。例如，2020 年 10 月，乌干达最大的移动支付网络 MTN 和 Airtel 遭遇到了黑客攻击，交易服务中断长达 4 天。

责任鸿沟

尽管全球金融系统越来越依赖数字基础设施，但全球目前尚未设立专门负责保护金融系统、抵御网络攻击的责任部门。在某种程度上，造成

深究网络攻击事件

攻击事件背后的破坏分子不仅包括日益猖獗的罪犯，还包括国家及国家资助的黑客团队，他们的攻击目标和犯罪动机各有不同。

网络攻击破坏分子	动机	目标	案例
国家、国家资助的黑客团队	地缘政治、意识形态	干扰、破坏、损害、盗窃、间谍活动、经济利益	永久数据损坏、定向物理攻击、切断电网、中断支付系统、诈骗转账、间谍活动
网络犯罪分子	敛财	盗窃/经济利益	窃取现金、诈骗转账、窃取密码
恐怖组织、黑客活动分子、内部威胁	意识形态、不满情绪	干扰	泄露信息、诽谤、分布式阻断服务攻击

Source: European Systemic Risk Board. 2020. “Systemic Cyber Risk.” https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

设计：ISTOCK/YOUR_PHOTO

随着创新、竞争和新冠疫情进一步推动数字革命向前发展，如果没有专项行动，全球金融系统只会变得越来越易于遭受攻击。

这种局面的原因在于环境瞬息万变。随着创新、竞争和疫情进一步推动数字革命向前发展，如果没有专项行动，全球金融系统只会变得越来越易于遭受攻击。尽管多数网络攻击破坏分子的主要目的是窃取财富，但纯粹以干扰和破坏为目的开展的网络攻击活动的数量一直在增加；此外，那些掌握网络盗窃技术的破坏分子会不断学习金融系统的网络和运作知识，目的是在将来发动干扰性和破坏性更强的网络攻击活动（或者，将这些网络盗窃技术和知识出售给他人）。这种风险环境的快速演变，使原本成熟且井然有序的金融系统的反应能力有所下降。

想要更好地保障全球金融系统的安全稳定，最首要的是应做好组织工作。加强防御和监管固然重要，但随着网络攻击风险越来越大，仅仅是做好防御和监管工作，还远远不够。与多数行业不同，大多数金融服务群体并不缺乏实施技术解决方案的资源或实力。主要问题在于实现集体行动：如何在各国政府、各金融主管当局及各行业之间，以最 优形式组织保护整个金融系统，以及如何有效、高效地利用这些资源。

当前，各利益相关方和措施之间存在的割裂现象，这部分源于网络风险的独特性以及其不断演变的风险性质。不同的群体各行其是，仅根据自身职能来应对问题。针对金融监管界而言，它关注的是金融系统的稳健性；对外交官而言，他们关注的是国家的行为规范；对国家安全机构而言，它关注的则是设法阻止网络攻击活动；而会业内高管而言，他们则往往侧重公司而非整个行业所面临的风险。随着金融服务企业和科技公司之间的界限变得越来越模糊，安全责任的界限也很可能正变得越来越模糊。

金融界、国家安全部门和外交人士之间的脱节现象尤其明显。金融主管当局通常面临着特有的网络威胁，但同时，它们与国家安全部门之间的联系又十分微弱，而有效应对网络攻击风险离不开国家安全部门的参与。各方在责任问题上存在，在保护全球金融系统中的角色和职能持续存在不确定性，这都进一步加剧了上述风险。这种不确定性，部分来源于当前的地缘政治环境和各方之间的高度不信任，同时阻碍了国际社会的往来合作。网络安全涉及敏感的国家安全利益，因此，国际合作常常困难重重，阻力繁多，多数情况下，都局限于相互信赖的小团体内部。开展国际合作以及多个利益相关方之间的合作不是一件“锦上添花”的事情，而是一件“势在必行”的事情。

国际战略

为了更加有效地保护全球金融系统免受网络威胁，2020 年 11 月，卡内基国际和平研究院联合世界经济论坛共同发表了一份题为《关于更好地保护全球金融系统免受网络威胁的国际战略》的报告。报告建议，各国应当在国际社会、政府机构、金融企业、科技公司等层面加强合作，共同采取措施，缓解全球经济碎片化问题。

这项国际战略坚持四项原则：第一，务必明确角色和职责。只有少数国家明确了国内金融行业监管机构、执法部门、外交部门、其他有关政府官员、产业主体等对应的角色和职责，搭建起了有效的往来联系。当前，全球经济的碎片化趋势，阻碍了各国之间的国际合作，削弱了全球金融系统的集体抗风险能力、恢复能力和应对能力。

第二，国际合作十分必要和紧迫。考虑到网络威胁的范围、全球金融系统需要相互依存的本

质，任何政府、金融公司和科技公司单打独斗，都无法有效地防范网络威胁。

第三，缓解各国应对的碎片化问题，将释放出力量来应对网络威胁。为了更好地保障金融机构免受威胁，各国采取了多种应对措施，但往往都是各行其是。相互之间的重复性工作增加了交易成本。从全球范围来看，少数几项举措已经足够成熟，完全可以分享给其他国家，更好实现多国协调，进一步推动全球化发展。

第四，保护国际金融系统，可以为其他行业树立典范。即使是在地缘政治高度紧张的情况下，金融系统仍然是为数不多的各方存在明确共同利益的领域之一。聚焦金融行业，可以为全球社会提供一个起点，也可以为未来更好保护其他行业铺平道路。

除了增强网络抗风险能力的措施外，报告还建议，金融稳定理事会应当制定一项用以监督金融机构网络风险管理的基本框架。政府和金融行业应当效仿以色列的 FinCERT，共享网络威胁信息、建立金融计算机紧急响应小组（CERT），借以加强网络安全保障。

金融主管部门还应当优先提高金融行业抵御数据和算法攻击的抗风险能力。具体措施包括安全数据异地存储、加密数据异地存储，允许会员快速安全地备份客户的账户数据。同时以模拟网络攻击演习的方式，识别系统漏洞，制定行动计划。

为了强化国际规范，报告建议，各国政府应当明确国际法在数字行业的实施办法，并强化有关规范，以保障金融系统的完整性。澳大利亚、荷兰和英国政府已经率先发表了声明，表示可能将境外势力的网络攻击视同非法动用武力、干涉别国内政的行为。

增加网络韧性、强化国际规范，有助于开展执法行动，联合业界多方参与抵御网络攻击，推动集体应对措施。具体应对措施包括制裁、逮捕以及扣押资产。

各国政府可以建立实体机构来协助评估网络威胁、协调应对措施，为威胁抵御工作提供支持。情报收集应侧重金融系统所面临的威胁，政府应当与盟国、志同道合的国家共享网络威胁情报。

能力建设

反过来，想要落实卡内基报告中概述的全面战略，就要搭建网络安全人才队伍，扩大金融行业的网络安全能力，保障数字转型所带来的普惠金融利益。

新冠疫情造成失业率上升，这为培训和招聘网络人才、加强网络安全人才队伍建设提供了重要的契机。金融服务公司应当面向高中生、学徒培养计划、高校项目投入资源，搭建人才输送管道。

建设网络安全能力意味着要着眼于为有需求的领域提供援助。国际货币基金组织及其他国际组织曾收到过成员国有关网络安全的众多请求，这在 2016 年孟加拉国事件之后尤其如此。G20 政府和央行也可以为金融业网络安全能力建设建立一个国际机制，指定像国际货币基金组织这样的国际机构协调这项工作。经济合作与发展组织以及国际金融机构应当将网络安全能力建设纳入到一揽子发展援助计划内，大幅增加对有需求国家的援助。

最后，要维护我们在普惠金融领域的发展成果，就必须加强普惠金融与网络安全之间的联系。这一点对非洲国家尤其如此——非洲大陆上的许多国家正在推广普惠金融服务，普及数字金融服务，因此金融业正在经历重大变革。国际组织应当专门针对非洲的网络安全问题成立一个专家网络。

包括各国政府、央行、监管机构、业界、其他利益相关方在内的整个国际社会，亟须携手应对这一紧迫而重要的挑战。一项缜密且周全的战略——如我们上文介绍的全面战略——可以为我们绘制一幅美好蓝图，引领我们将倡议转化成行动。FD

蒂姆·毛瑞尔（Tim Maurer），担任卡内基国际和平研究院网络政策项目的联席主任、技术和国际事务项目高级研究员。

亚瑟·纳尔逊（Arthur Nelson）担任卡耐基网络政策项目研究分析师。