央行视角下的金融领域网络攻击风险评估

◎曾繁荣

摘要：随着金融领域云服务和远程工作的普及，金融部门遭受网络攻击的风险随之增长，并对金融稳定构成了威胁，网络风险成为政策制定者的重要关注点。本文从全球层面和中央银行视角，基于对2021年全球网络弹性小组（GCRG）一项调查的分析，首次系统性地评估了金融领域面临的网络攻击风险及其带来的经济损失，以及应对准备情况，旨在进一步充实现有研究。

关键词：中央银行；金融领域；网络攻击；云服务；远程工作

中图分类号：F831　　**文献标识码：**A

近年来，金融领域的网络攻击日益频繁和复杂，加密货币世界的兴起又增加了金融领域遭受黑客攻击的可能性（尤其是金融机构和金融市场基础设施，FMI），金融业已被视为受网络攻击最严重的行业之一（Boissay et al., 2022）。

当前有关网络威胁的研究文献大多指向私营部门（主要是金融部门），关于中央银行对金融部门网络攻击评估的文献较少。刘贵辉（2017）阐述了金融网络攻击的行为动机、主要特征、发展趋势，分析了金融网络攻击给金融行业带来的新问题，总结了欧美国家和国际组织应对金融网络攻击的做法。Aldasoro et al.（2022）使用Advisen数据集，发现IT投资较高的行业遭受网络攻击的损失更低，尤其是金融和保险部门，比其他部门更能抵御网络风险。Duffie&Younger（2019）发现，最具系统重要性的美国金融机构拥有足够的高质量流动资产来应对极端网络事件期间的大规模资金流失。Eisenbach et al.（2022）的研究表明，美国关联度最高的五家银行中的任何一家因网络事件减值都可能对其他银行产生显著的溢出效应。

中央银行如何评估辖内金融领域的网络攻击风险，又采取了哪些应对措施？回答上述问题迫在眉睫，因为无论是直接针对中央银行还是针对金融部门的网络攻击都可能损害中央银行的履职能力并威胁金融稳定。鉴此，本文从全球层面和中央银行视角，基于对2021年全球网络弹性小组（GCRG）一项调查的分析，首次系统性地评估了金融领域面临的网络攻击风险及其导致的经济损失，以及应对准备情况，旨在进一步补充现有研究。

后文第一部分概述网络风险，分析金融领域采用云计算和远程工作对网络风险的关键影响；第二部分分析中央银行可能面临的网络攻击类型，对其

作者简介：曾繁荣，中国人民银行赣州市中心支行。

影响和损失进行评估，并提出防范措施；第三部分分析中央银行对金融部门网络风险的评估；第四部分概述中央银行在网络风险领域的合作；第五部分是研究结论与启示。

一、网络风险与形势评估

（一）网络风险

网络风险涵盖了因 IT 系统失败或被破坏所导致的各类风险。金融稳定委员会（2018）将网络风险定义为网络事件发生的概率及其影响的组合。其中，网络事件指在信息系统中发生的任何可观察到的事件，包括危及信息系统及其处理、存储、传输信息的网络安全，以及违反安全政策、安全程序或使用政策。网络事件又分为意外网络事件（如意外的数据泄露以及错误的实施、配置和处理）和蓄意网络事件两类。约 40% 的网络事件是蓄意和恶意而不是偶然的，即网络攻击（Aldasoro et al.,2020）。以下三类网络攻击尤为突出。

一是网络钓鱼。这是最常见的初始攻击载体。传统上，网络钓鱼邮件被用来欺骗用户运行恶意软件，从而将恶意软件安装到用户设备上。近年来，网络钓鱼攻击频率明显增加，2021 年 1 月—12 月全球针对云服务的网络钓鱼邮件的月均数量翻番。攻击者凭借有针对性和量身定制的恶意邮件入侵终端用户设备，或获得一个入口点，以获得访问本地基础设施或基于云服务的特权。这种未经授权的访问潜在伤害可能很大。其中，凭据网络钓鱼是一种新型的网络钓鱼诱饵。其攻击者先通过在电子邮件、即时消息或其他通信渠道中伪装成有信誉的或已知的实体，窃取受害者的登录名和密码组合，然后再攻击其他目标，以获得进一步的访问权限。

二是供应链攻击。当攻击者渗透到合法软件供应商的网络，并在供应商将软件发送给客户之前使用恶意代码破坏软件时，就会发生供应链攻击。这种攻击利用已建立的信任关系，并借助用于提供基本软件更新的机对机通信。供应链攻击的频率相对较低，但能产生潜在、巨大的系统性后果。

三是勒索软件。这是攻击者在受害者的计算机网络上部署的恶意软件，用于加密和持有他们的文件，以获取赎金。它往往从受感染的终端用户设备传播到整个组织的 IT 环境。其不仅会损害信息和 IT 资产的可用性，还会损害它们的机密性和完整性。近几年，勒索软件的使用量大幅增长，仅 2021 年一年就翻倍。

除上述类型外，还有工业间谍、黑客行动主义者或国家赞助的行动者等网络攻击。相应地，网络攻击既可能只为赚取利润（如勒索软件、工业间谍），也可能出于地缘政治（国家赞助的对关键基础设施的攻击）或普遍不满（黑客行动主义）而发生。

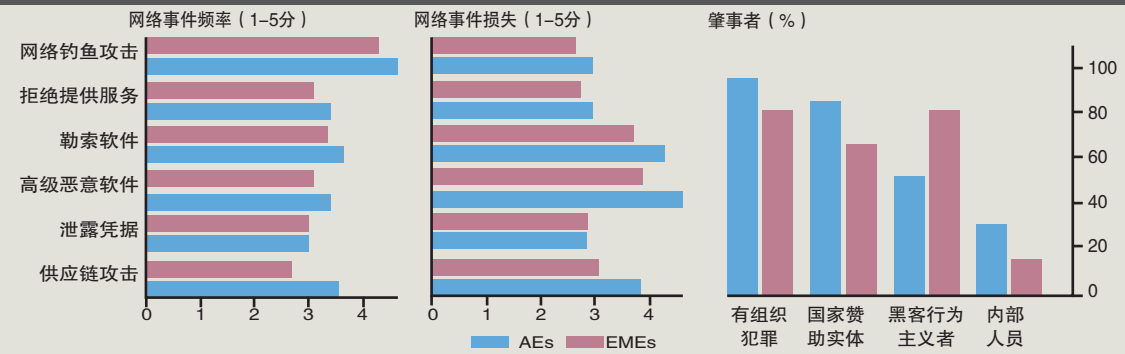
（二）网络风险对云应用和远程工作的影响

一是对云应用的影响。金融领域引入数字化工作方式，既促进了云计算的应用，也为网络攻击提供了新机会。尽管中央银行本身通常并不依赖云服务来运行其关键业务，但金融机构应用云也给金融业带来了新挑战，传统安全边界可能不再适合云技术时代。当前，敏感数据驻留在网络之外，网络攻击目标也转移到终端用户及其设备和身份，因而新的数字边界已经转移到对身份识别、用户、设备和数据实施有效的控制。

网络风险给云应用带来了三大挑战。第一，在无明确定义边界情况下，缺乏一套全面统一的信息安全控制措施，包括应用程序编程接口（API）易受攻击、配置不正确、身份和访问管理脆弱。第二，如何选择云提供商成了艰难抉择，尤其在面临数据主权问题时。在选择将哪些关键服务上传到云端时，关键看国家有关承载和处理数据的法律和监管框架。第三，存在较大技能差距。部分中央银行在招聘、留住和持续培训员工方面存在较大困难，尤其在劳动力供应有限、成本高和技术环境发生变化时。企业战略集团（ESG）和信息系统安全协会（ISSA）在 2020 年的一份报告中指出，70% 的网络安全专业人士表示，其所在组织面临网络安全技能短缺问题，超过 60% 的安全专业职位至少空缺了 3 个月。

二是对远程工作的影响。与云应用相关的挑战因远程工作的增加而加剧，例如，定向钓鱼邮件对家庭无线网络和工作中使用的个人设备的安全保障带来挑战。中央银行和金融机构云服务的广泛应用

图1 中央银行面临网络攻击的频率、损失和肇事者



资料来源：作者根据GCRG调查计算

注：左面板为中央银行受访者回答“贵机构如何评价自身遭受各种攻击媒介的概率，从1（非常低）到5（非常高）”的平均分；中间面板为回答“贵机构如何评价自身遭受各类攻击的损失（1—5分）”的平均分；右面板为回答“贵机构认为网络攻击的主要肇事者是谁”的百分比（可多选）。

以及向远程工作的转变，对网络安全战略提出了新要求。第一，组织的数字和物理边界的模糊需要制定新的战略。一种常见方法一是所谓的零信任概念。它假设不能信任外围防御，甚至不能信任内部网络，而应根据多种因素（如用户身份、端点属性、位置和行为指标）赋予用户对资源的访问权限。第二，应加强信息分类纪律以及与信息配置相关的自动化控制。这是因为信息资产在转移到云上时需要多技术协作。数据显示，云环境遭到破坏有近三分之二是由信息配置错误导致的（De Beck，2021）。第三，网络安全战略需要应对机构治理弱化的风险。当机构依赖云提供商的安全控制而缺乏对其基础设施的控制权时，会让其误以为云提供商负有维护基础设施安全的全部责任。事实上，机构和云提供商负有共同保障数据安全、安全配置和漏洞管理的责任。

二、中央银行自身面临的网络攻击状况

（一）网络攻击的类型及其带来的损失

中央银行负责管理和监督金融部门的关键基础设施（如支付系统），因此对中央银行及其关键基础设施的网络攻击不仅可能对央行造成重大的资金和声誉损失，还可能导致整个金融系统遭到破坏，最终付出重大的社会成本。此外，中央银行负责保护的大量敏感信息往往是网络攻击者的目标，例如，有关未来政策的机密材料可能成为参与网络间谍活动的犯罪分子和国家赞助实体的目标。因此，了解哪类网络攻击最频繁和最具破坏性，有助于确定和应对网络威胁。

从攻击类型看，根据 GCRG 对发达经济体（AEs）和新兴市场经济体（EMEs）中央银行的调查，网络钓鱼和社会工程攻击的概率均被 AEs 和 EMEs 中央银行排在第一位（见图 1 左）。可能是因为此类攻击只需通过向大众发送大量电子邮件就能显著提高攻击成功的概率，且不需要进行大量投资。而受勒索软件或拒绝服务攻击的概率，AEs 和 EMEs 中央银行相差不大，但 AEs 中央银行明显比 EMEs 中央银行更担心供应链攻击。

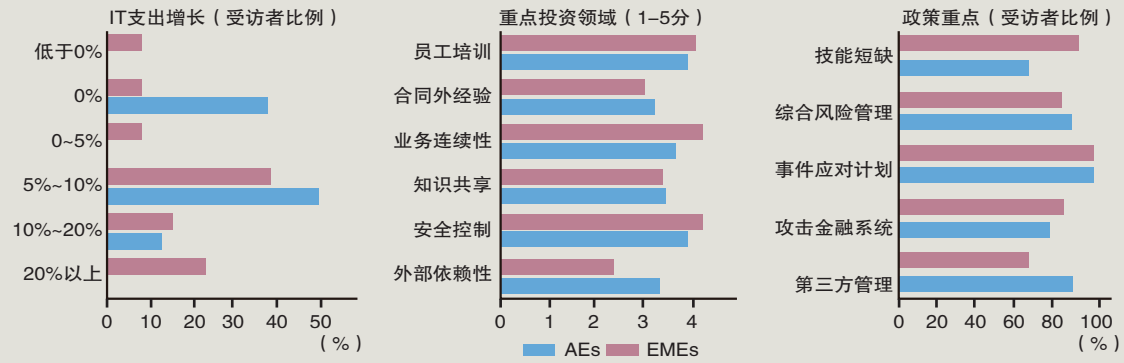
从攻击损失看，网络事件的损失是多方面的，不仅潜在的经济损失重大，潜在的操作影响和相关声誉（如对中央银行或支付系统的信任）损失也值得关注。其中，各中央银行受高级持久恶意软件和勒索软件攻击的损失最高；AEs 中央银行受供应链攻击的损失通常高于 EMEs 中央银行；而受拒绝服务攻击（DoS）和网络钓鱼造成的损失相对较低（见图 1 中）。

从攻击肇事者看，AEs 中央银行认为，攻击者主要是有组织犯罪和国家赞助的实体，而 EMEs 中央银行认为主要是有组织犯罪和激进分子；此外，少数 EMEs 中央银行和三分之一的 AEs 中央银行认为，内部参与者是重要肇事者（见图 1 右）。虽然内部威胁的发生概率较低，但其严重性不应被低估，因为内部人员可能是犯罪实体的教唆者。

（二）提高抵御网络攻击的能力

信息技术也是金融领域的核心，因而网络安全

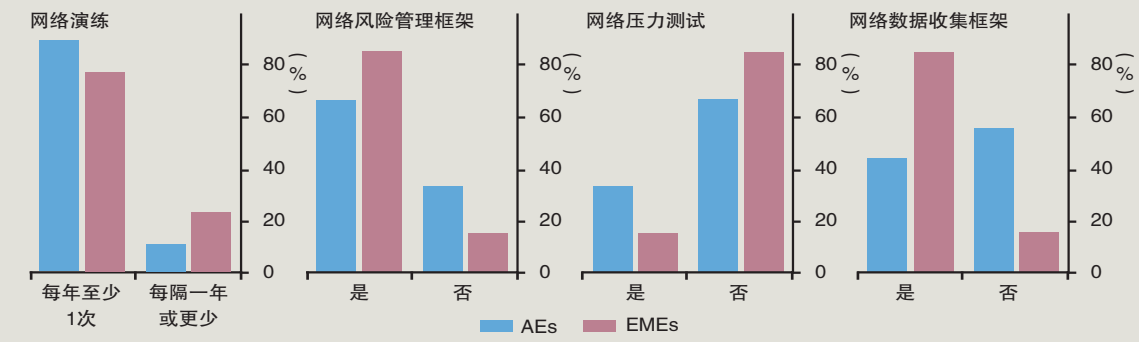
图2 中央银行投资于网络安全和政策问题的情况



资料来源：作者根据GCRG调查计算

注：左面板为中央银行受访者回答“2020年年初以来，贵机构的网络安全投资预算增长多少”的比例；中间面板为回答“贵机构的网络安全投资优先领域是哪些（1—5分）”的平均分；右面板为回答“贵机构对网络风险的分析和政策制定重点是什么”的比例（可多选）。

图3 中央银行模拟情景、演练和监督框架



资料来源：作根据GCRG调查计算

注：左1面板分别为中央银行受访者回答“贵机构多久进行一次模拟网络攻击的内部演练”的比例；左2面板为回答“辖区相关监管机构是否为金融公司提供网络安全风险管理框架”的比例；右2面板为回答“辖内监管机构是否对金融公司进行网络压力测试”的比例；右1面板为回答“辖内监管机构是否有收集金融机构网络攻击和损失信息的框架”的比例。

和威胁也是中央银行日常操作的关注重点。网络犯罪呈上升趋势促使网络安全成为监管部门的一个关键政策问题。下文将分析中央银行自身网络风险管理的关键方面以及应引起金融体系注意的政策问题。

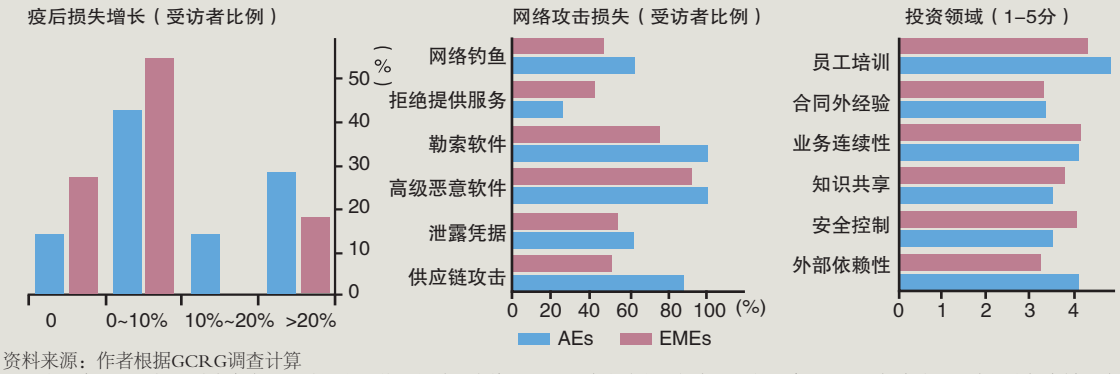
如图 2 所示，投资方面，自 2020 年年初以来，AEs 和 EMEs 多数中央银行的网络安全投资预算至少增长了 5%，四分之一的 EMEs 中央银行甚至增长 20% 以上，但也有约三分之一的 AEs 中央银行预算无变化（见图 2 左），投向技术安全控制和弹性的资金排名靠前。对现有员工进行网络安全培训或雇用具有相关技能的新员工也受到重视，其中，EMEs 中央银行更急需解决技能短缺问题，而 AEs 中央银行则更依赖于云提供商等外部管理（见图 2 中）。

除了投资，中央银行还制定了具体的政策应对措施。例如，所有中央银行都制定了事件应对计划，有些中央银行还在制定正式战略，以应对辖区金融体系受到的攻击（见图 2 右）。其中，有些政策已落实到位。例如，所有中央银行都进行了模拟应对网络攻击的内部演练，且多数中央银行每年至少一次（见图 3 左 1）。演练的最常见场景是中央银行系统受到攻击以及支付系统或其他关键金融市场基础设施出现故障。

多数司法管辖区（尤其是 EMEs）的中央银行已经或计划提供网络安全风险管理框架（见图 3 左 2），但定期对金融公司进行网络压力测试的情况不多见，仅三分之一的 AEs 中央银行和约 15% 的 EMEs 中央银行定期进行网络压力测试（见图 3 右 2）；而在尚未进行网络压力测试的中央银行中，三分之二的 EMEs 中央银行计划开展，不到 30% 的 AEs 中央银行计划开展。

多数 EMEs 的中央银行为收集金融机构遭受网

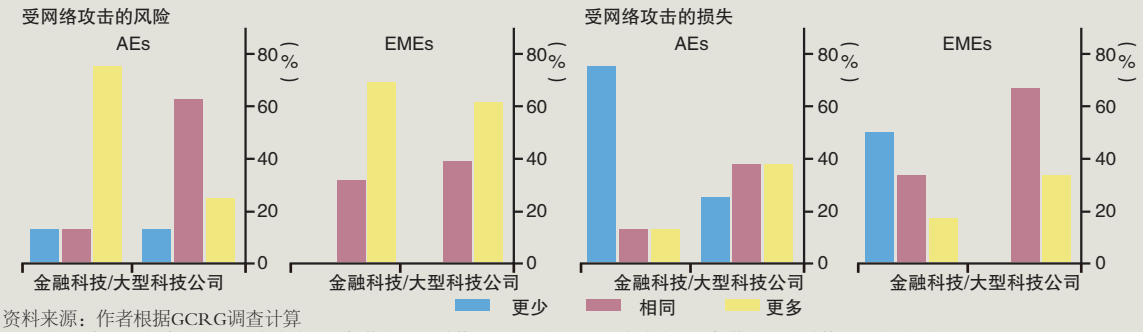
图4 中央银行评估辖内金融部门的网络攻击和损失



资料来源：作者根据GCRG调查计算

注：左、中、右面板分别为中央银行受访者回答“相对于疫情大流行之前的时代，辖内金融部门在2020–21年遭受网络攻击的损失增长多少”“哪类网络攻击事件导致金融机构的资金损失最大（可多选）”“贵机构所在辖内金融机构投资网络安全的优先领域是什么”的得分。

图5 传统金融机构与金融科技 / 大型科技公司受网络攻击的风险和损失比较



资料来源：作者根据GCRG调查计算

注：（1）每一面板中的左侧，为传统金融机构与金融科技公司的比较，右侧为传统金融机构与大型科技公司与的比较。

（2）左边的两个面板分别为AEs、EMEs中央银行回答“相对于传统金融机构，金融科技公司受网络攻击的风险更小/同等/更高，大型科技公司受网络攻击的风险更小/同样/更大”的百分比；右边的两个面板分别为AEs、EMEs中央银行回答“与传统金融机构相比，金融科技公司受网络攻击的损失更小/同样/更大（以GDP的最大损失百分比衡量），大型科技公司受网络攻击的损失更小/同样/更大”的百分比。

络攻击的信息提供了标准框架（见图 3 右 1），而一半多的 AEs 中央银行尚未建立。几乎所有 EMEs 中央银行都要求向监管机构报告网络攻击的损失，但仅三分之二的 AEs 中央银行要求这样做。所有中央银行均未要求公司公开披露网络攻击的损失。

三、中央银行对金融领域网络攻击的评估

在新冠肺炎疫情暴发之前，金融部门面临网络攻击事件时仍能保持比较稳健的状态。尽管如此，金融部门正成为越来越有吸引力的网络攻击目标。对此，金融部门在网络安全和 IT 系统防御方面投入了大量资源，也培养了相当多的相关人才。然而，随着金融部门逐渐将 IT 外包并更多地采用云技术，也给金融机构带来了新风险。

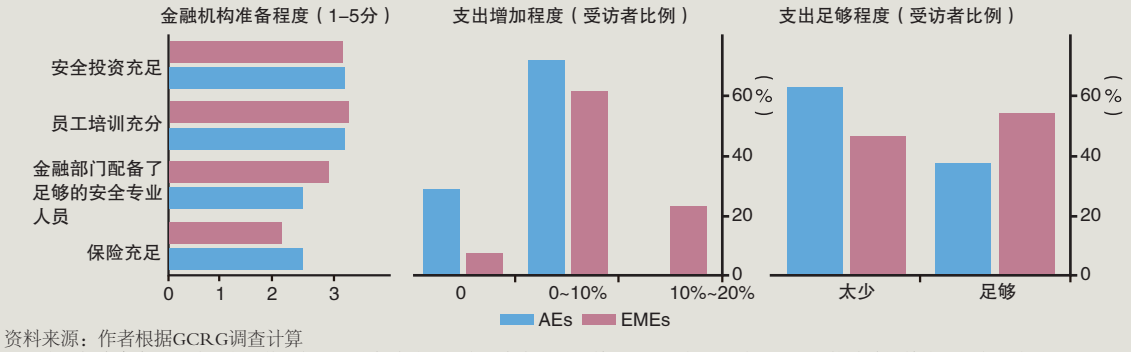
（一）传统金融机构受网络攻击损失评估

对于当金融机构遭受系统性网络攻击所遭受的损失，多数中央银行经评估后认为，可能占到一国 GDP 的 5%，有些 EMEs 中央银行估计甚至超过 10%。这说明，金融部门提供的关键金融基础设施的安全对于国家极其重要。

纵向来比，多数中央银行认为，金融部门在 2020—2021 年期间遭受网络攻击所造成的损失比疫情大流行之前有所增加（见图 4 左）。其中，近 30% 的 AEs 中央银行认为金融机构损失增长了 20% 以上，多数 EMEs 中央银行则认为损失增长在 10% 以下。这种损失的增长与其说是网络攻击的频率更高，不如说是网络攻击更趋严重。

从分类看，所有中央银行均认为，高级持久恶意软件和勒索软件攻击事件给金融机构造成的损失最大，而拒绝服务攻击造成的损失最小（见图

图6 金融部门的IT支出和网络保险



资料来源：作者根据GCRG调查计算

注：左面板为中央银行受访者回答“辖区金融领域的网络安全支出是否足够”“金融部门工作人员是否接受过足够的网络安全培训”“金融部门是否雇佣足够多的网络安全专业人员来保护自身免受网络威胁”“当前的保险政策是否足以补偿金融机构受严重攻击的后果”的得分；中间面板为回答“相对于疫情大流行之前，贵机构认为金融部门2020–2021年的网络安全投资方面增长多少”的比例；右面板为回答“贵机构在过去一年对网络安全的投资是否太少/足够/太多”的比例。

4 中）；相对而言，AEs 中央银行认为供应链攻击在金融机构中很突出，但 EMS 中央银行未将其置于突出位置。

从投资看，随着网络事件频度和严重性的上升，中央银行普遍认为金融机构应优先考虑在网络安全方面的投资，对员工进行网络安全培训，确保业务连续性，并管理其外部依赖性（见图 4 右）。

（二）金融科技行业受网络攻击损失评估

除了传统金融机构，网络安全也是金融科技行业的一个重要问题。金融科技行业是一个充满活力的创新领域，许多新提供商提供网络安全相关服务，但它们也面临特定风险，例如，在众筹中可能出现资金被盗或加密货币交易遭到黑客攻击，都不属于传统金融监管范围。此外，大型科技公司也是关键云基础设施提供商，从而使金融部门与大型科技公司形成了依赖关系。

从受攻击风险看，各中央银行普遍认为，金融科技行业受到网络攻击的风险较大。四分之三的 AEs 中央银行和三分之二的 EMEs 中央银行认为，相较于传统金融机构，金融科技公司更易成为网络攻击的目标（见图 5 左）。从受损失程度看，多数中央银行认为，金融科技公司受网络攻击所导致的损失程度与传统金融机构类似或更低，而大型科技公司的损失程度常常高于传统金融机构（见图 5 右）。

（三）应对网络风险的准备情况

目前，仅有少数中央银行认为，辖内金融机构已做好应对网络攻击风险的充分准备（见图 6 左）。其中，在网络安全支出和员工培训方面准备的平均得分为 3 分（1 分表示表示严重不足，5 分表示充分准备下，同）；在雇佣员工充足性准备方面的平均得分不足 3 分；在制定应对网络攻击造成严重损失的保险政策方面得分最低。

多数中央银行认为，辖内金融部门大幅增加了网络安全投资（见图 6 中）。约一半的 EMEs 中央银行和 40% 的 AEs 中央银行认为网络安全投资充足，其余认为投资太少（见图 6 右）。同样，多数中央银行表示，辖内不到一半的金融机构持有网络保险，多数认为保险市场还不够成熟，无法有效地对网络攻击损失进行定价和承保。

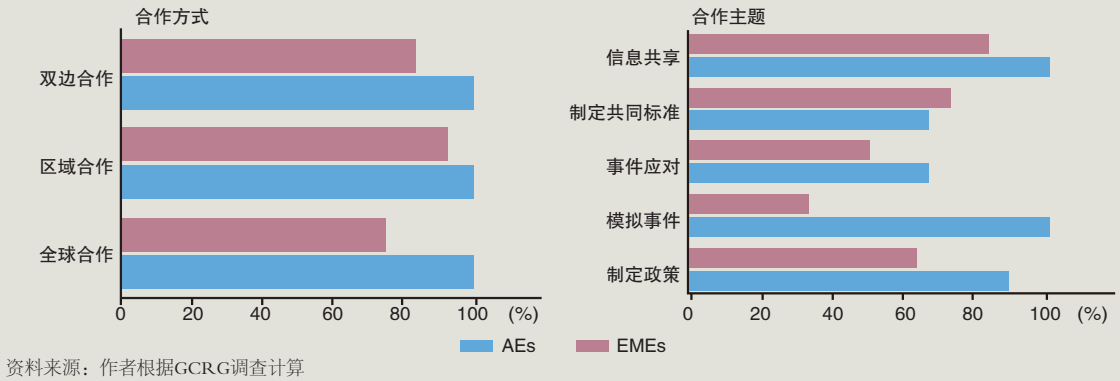
四、国际合作

网络安全领域的国际合作不仅有助于推广最佳实践和共同经验，还可以克服单家机构难以保障网络安全的问题，有效应对网络攻击导致的系统性影响（Kopp et al,2017）。当前在这方面已开展多项国际合作。

（一）中央银行之间的国际合作

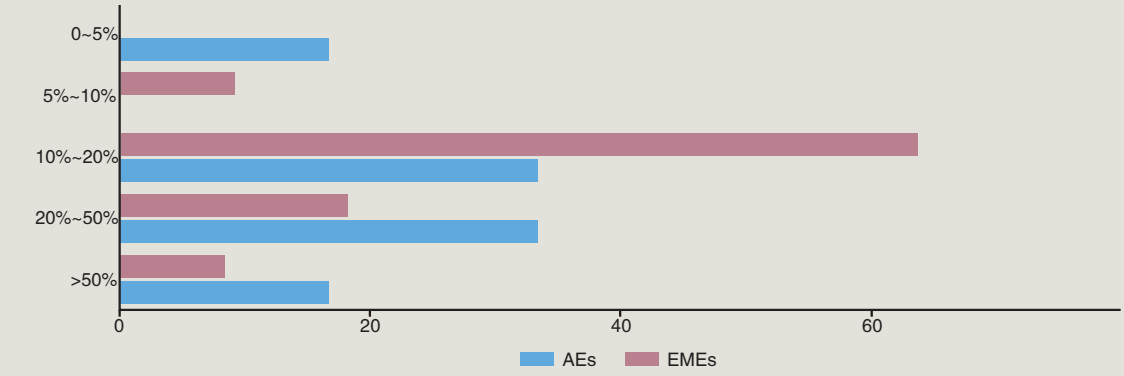
各中央银行已开展了一系列相关主题的广泛合作，包括双边合作以及全球和区域层面之间的合作（见图 7 左）。从合作主题看，AEs 中央银行对信息共享、联合桌面或网络演练、政策制定方面的合作更关注（见图 7 右）；相对而言，EMEs 中央银行在

图7 中央银行之间的国际合作



资料来源：作者根据GCRG调查计算
注：左、右面板分别为受访者回答“贵机构如何在网络安全方面开展国际合作”“贵机构在网络安全方面的国际合作主题是什么”的百分比（可多选）。

图8 引入CBDC所增加的网络安全预算



资料来源：作者根据GCRG调查计算
注：该图为中央银行受访者回答“引入CBDC是否大幅增加贵机构的网络安全预算”的百分比。

信息共享和政策制定方面的合作涉及较少。此外，超过三分之二的 AEs 和 EMEs 中央银行在推动制定共同标准和协议。

（二）国际清算银行支持中央银行合作的方式

国际清算银行通过多种方式支持各经济体中央银行在网络安全方面开展全球合作，并为此成立了国际清算银行网络弹性协调中心（CRCC）和国际清算银行创新中心（BISIH）。

1.CRCC

CRCC 成立于 2019 年，旨在为各经济体中央银行在网络弹性领域的知识共享、协作和运营提供结构化方法。其在积极促进技术交流、网络空间模拟和网络弹性评估方法等方面发挥了关键作用。为给各经济体中央银行合作提供安全服务，CRCC 组建了由一批资深的 IT 安全专家组成的 GCRG。GCRG 支持的一个关键项目是开发网络弹性评估，旨在为各中央银行提供一个通用框架，评估网络弹性态势并改善其在提供关键业务服务中的网络弹性实践。这种为中央银行量身定制的方法基于共同基准，有助于开展定量的自我评估。

2.BISIH

BISIH 旨在为中央银行合作提供平台，在开发应对与中央银行和更广泛的金融部门相关的网络威胁的技术方面，发挥了重要作用，并降低了相关运营成本。BISIH 下设多个二级中心。其中的欧元系统中心，正在研究后量子密码学对支付系统的影响；香港中心的 Sela 项目，由以色列银行和香港金融管理局合作，探索网络安全的两层零售中央银行数字货币（CBDC）架构的技术实施问题；北欧中心的 Polaris 项目，主要研究与离线使用 CBDC 相

关的弹性和安全问题。CBDC 的引入，增加了 IT 环境的复杂性，需要投入更多资源用于网络安全保障（见图 8）。

五、结论

随着金融领域云服务的广泛运用以及远程工作的增加，中央银行和金融部门所遭受的网络攻击也日趋频繁复杂。本文从全球层面和中央银行的视角，基于全球网络弹性小组 2021 年所开展的一项调查，首次系统性地评估了金融领域面临的网络风险及其带来的经济损失，以及应对准备情况，以进一步补充现有文献。现将研究结论小结如下。

（一）AEs 和 EMEs 中央银行对网络攻击频率和损失的评估不同

所有中央银行均认为，受网络钓鱼和社会工程攻击的频率最高，而 AEs 中央银行明显比 EMEs 中央银行更担心供应链攻击。所有中央银行均认为，受高级持久恶意软件和勒索软件攻击造成的损失最高。AEs 中央银行认为，有组织犯罪和国家赞助的实体是主要肇事者，EMEs 中央银行则认为肇事者主要是有组织犯罪和激进分子。

（二）各中央银行积极制定应对网络攻击政策，2020 年以来显著增加了相关投资

各中央银行均将投资于技术安全控制和弹性置于重中之重的地位，同时也十分关注对现有员工进行培训或聘用具有相关技能的新员工，尤其 EMEs 中央银行。此外，各中央银行均高度重视制定事件的应对计划，并通过内部演练来模拟网络攻击。

（三）各中央银行均认为金融领域面临网络攻击的潜在损失很大，且过去一年受网络攻击造成的损失有所增加

仅少数中央银行认为，金融部门做好了应对网络攻击的充分准备，超一半的中央银行的网络安全投资不足。各中央银行均认为，除传统金融机构外，金融科技公司受网络攻击的风险普遍更大。多数中央银行认为，大型科技公司受网络攻击造成的损失比金融科技公司高。

（四）各中央银行已经在一系列议题上进行了广泛合作

中央银行双边之间以及全球和区域之间的合作已成为常态。在具体议题上，AEs 中央银行在信息共享、模拟和政策制定方面尤为突出，EMEs 中央银行经常在信息共享和政策制定方面开展合作。此外，超三分之二的中央银行为金融部 s 门制定了共同标准和协议。国际清算银行通过多种方式支持各国中央银行在网络安全方面进行全球合作，并为此成立了网络弹性协调中心和创新中心的项目。

参考文献

[1] 刘贵辉．网络攻击对金融行业的影响及对策分析 [J]. 西南金融，2017（6）：72-76

[2]Aldasoro，I.，Gambacorta，L.，Giudici，P. and Leach，T. The Drivers of Cyber Risk[J]. Journal of Financial Stability，2022,60

[3]Aldasoro，I.，Frost，J.，Gambacorta，L.，Leach，T. and Whyte，D. Cyber Risk in the Financial Sector[R]. SUERF Policy Note，2020，No. 206

[4]Boissay，F.，G. Cornelli，S. Doerr and J. Frost. Blockchain Scalability and the Fragmentation of Crypto[R]. BIS Bulletin，2022,No. 56

[5]De Beck，C. IBM X-Force Report：No Shortage of Resources Aimed at Hacking Cloud Environments[j]. Security Intelligence，2021，September

[6]Duffie，D. and Younger，J. Cyber runs[R]. Hutchins Center Working Paper,2019 No. Brookings

[7]Kopp，E，L Kaffenberger，and C Wilson. Cyber Risk，Market Failures，and Financial Stability[R]. International Monetary Fund,2017

（责任编辑：辛本胜）