网络风险：日益影响宏观金融稳定

在数字化发展、技术进步、地缘政治紧张局势加剧的背景下，过去二十年，尤其是自 2020 年以来，网络相关事件，特别是恶意事件变得更加频繁。主要金融机构的严重事件可能导致信心丧失、关键服务中断，并通过技术和金融联系对其他机构产生溢出效应，从而对宏观金融稳定构成严重威胁。

第三章表明，尽管网络事件迄今尚未形成系统性风险，但这些事件导致企业遭受极端直接损失（至少高达 25 亿美元）的风险有所增加。此外，网络事件造成的间接损失也很大，往往比企业报告的直接损失大得多。

了解导致网络事件发生或防止其发生的因素对于制定稳健的网络安全政策和战略至关重要。本章分析表明，数字化和地缘政治紧张局势大大增加了网络事件风险，而完善网络立法和加强企业网络治理有助于减轻此类风险。

金融部门的网络风险敞口很大，近五分之一的网络事件都对金融企业造成影响。高市场集中度和低可替代性，特别是在考虑支付服务和托管银行业务等关键服务时，可能会使金融企业遭遇的网络事件尤其具有破坏性，这突出表明必须加强网络安全和运营韧性。金融企业的运营往往依赖于共同的第三方信息技术提供商，这也增加了发生共同冲击和溢出效应的风险。

金融机构发生的严重网络事件可能会破坏人们对金融体系的信任，在极端情况下，还会导致市场抛售或银行挤兑。尽管目前尚未发生重大的网络挤兑事件，但实证分析表明，美国一些小型银行在网络攻击发生后出现了一定程度的存款持续流失。

由于全球金融体系面临着显著且不断增加的网络风险，政策和治理框架必须跟上形势。然而，对新兴市场和发展中经济体的中央银行和监管机构开展的一项调查显示，网络安全政策框架往往仍不健全。

应当采取措施加强金融部门的网络韧性，包括制定有效的国家网络安全战略，实施适当的监管框架，培养一支能干的网络安全队伍，以及建立国内和国际信息共享安排。为了更有效地监测网络风险，应加强对网络事件的报告。监管机构应当要求金融企业董事会成员对企业的网络安全管理负责，并促进有益的风险文化、网络卫生、网络培训和意识。为了限制网络事件可能造成的扰动，金融企业应制定和测试响应与恢复程序。国家当局应制定有效的应对方案和危机管理框架。

IMF 通过“金融部门评估规划”和各项能力建设举措，积极帮助成员国加强网络安全框架。请参见此处的英文报告全文：http://IMF.org/GFSR-April2024