我国金融网络安全韧性监管研究：现实困境、英国经验及制度构建*

宋心然 李鹏飞 张丽迎

（首都经济贸易大学城市经济与公共管理学院 北京 100070）

摘 要：[**研究目的**]新技术与金融行业的结合不仅催生出新的金融产品，也不可避免地带来了新的金融网络安全问题。如何在鼓励金融从业机构创新发展的同时，防控金融网络风险，完善金融网络安全监管，就成为各国金融监管部门面临的重要问题。英国的“渗透性韧性测试”是兼顾金融从业机构创新与金融网络安全的有效机制，研究其运作特点可为我国金融网络安全监管提供有益思路。[**研究方法**]通过分析我国金融网络安全监管面临的困境，着重研究英国“渗透性韧性测试”机制的建设历程、具体运作模式与本质特征，分析我国在金融网络监管层面引入渗透性韧性测试的可行性。[**研究结论**]对英国金融网络安全韧性监管的模式进行本土化借鉴，即加强金融网络安全监管的合作治理，在重构监管组织体系的基础上，完善相关激励机制，提高各参与主体抵御风险的专业能力，推进传统金融网络安全监管向金融网络安全韧性监管防控体系方向嬗变。

关键词：网络安全；金融监管；韧性监管；金融科技；渗透性韧性测试；英国

中图分类号：G351.3；TP393.08 **文献标识码**：A **文章编号**：1002-1965(2022)03-0080-07

引用格式：宋心然，李鹏飞，张丽迎. 我国金融网络安全韧性监管研究：现实困境、英国经验及制度构建[J]. 情报杂志，2022，41(3)：80-86，94.

Research on Financial Network Security Resilience Regulation in China: Practical Dilemma, British Experience and Institutional Construction

Song Xinran Li Pengfei Zhang Liying

(College of Urban Economics and Public Administration, Capital University of Economics and Business, Beijing 100070)

Abstract: [**Research purpose**] The combination of new technology and financial industry not only gives birth to new financial products, but also inevitably brings about new financial network security problems. How to prevent and control financial network risks and improve financial network security supervision while encouraging innovation and development of financial institutions has become an important issue that financial supervision departments in each country will be confronted with. The CBEST in Britain is a useful way to assure the innovation of financial institutions and the security of financial networks. [**Research method**] We have researched on its construction process, specific operation model, and substantive characteristics, and illustrated the feasibility to introduce CBEST into our country in the aspect of financial network regulation. [**Research conclusion**] The author carries out localized reference to this model, it should strengthen the cooperative governance of financial network security supervision, based on the reconstruction of the regulatory organization system, perfect the related incentive mechanism, improve the professional ability of each participant to resist risks, and promote the transformation of traditional financial network regulation to financial resilience regulation of the prevention and control system.

Key words: network security; financial regulation; resilience regulation; financial technology; CBEST; Britain

收稿日期：2021-09-07 修回日期：2021-10-18

基金项目：北京市2018年社会科学基金青年项目“北京市共享经济监管困境及其治理创新研究”(编号：18ZGC011)研究成果之一；首都经济贸易大学研究生科技创新资助项目“我国金融网络安全韧性监管研究：现实困境、英国经验及制度构建”最终成果。

作者简介：**宋心然**，女，1982年生，博士，副教授，研究方向：共享经济及新兴行业监管；**李鹏飞**，男，1994年生，硕士研究生，研究方向：金融监管、信息安全；**张丽迎**，女，1997年生，硕士研究生，研究方向：市场监管。

在网络冲击难以预测的环境下,网络安全是近年理论界与实务界广泛关注的焦点性议题。而金融作为一国经济的风向标,是最易受到网络围攻的行业。无论是风险管理、记账清算,还是资产定价、数字货币,金融行业的网络化建设都已走在各行业前列。2017 年 6 月 1 日,《中华人民共和国网络安全法》明确将金融列入重点保护的行业及领域,在顶层统筹方面反映了网络安全对于金融安全至关重要。为进一步完善金融行业的网络安全建设,中国人民银行于 2020 年 11 月相继出台《金融行业网络安全等级保护实施指引》《金融行业网络安全等级保护测评指南》以及《个人金融信息保护技术规范》(JR/T0171-2020)等文件。2021 年 9 月 1 日,国务院在《关键信息基础设施安全保护条例》中正式将"关键基础设施运营者责任义务"作为网络安全的重点予以推进,更凸显了国家对网络安全的关注,但国家网信部门和行业主管部门、监管部门之间如何协调配合,如何共同构建金融网络安全的防御机制,如何"构建风险识别、风险评估、风险监测、风险控制、风险处置的全流程风险防控体系"[1],尚待进一步研究完善。

鉴于此,本文在分析我国现阶段金融网络安全监管发展面临的现实困境的基础上,深入研究英国渗透性韧性测试的成功经验,重点总结、提炼其运作模式,并阐述该机制在我国落地的可行性,建构我国的金融网络安全韧性监管制度,为创新金融网络安全监管、提高监管效能提供参考。

1　现阶段我国金融网络安全监管发展面临的现实困境

金融行业由于网络技术路径突破了传统金融业瓶颈,催生了新的金融产品,但也给金融网络安全监管带来巨大挑战。目前的金融从业机构由于诸如分布式记账技术(distributed ledger technology,DLT,一种网络成员之间共享、复制和同步数据库,而且每个节点都进行独立更新的技术)、加密技术等新一代网络算法的加持,重塑了全新的金融交易方式,亦使互联网金融、大数据征信、智能投顾、虚拟货币等新金融业态深度嵌入了个体生活。而在金融领域衍生出来的网络风险包含移动 app 敲诈、信用卡欺诈与网络钓鱼等方面,也包括分布式拒绝服务(Distributed Denial of Service,DDoS,多个攻击者利用网络的缺陷入侵目标主机的同时,隐蔽性工作做的很好的一种攻击方式)、ATM 与 POS 机攻击、加密勒索等。据《金融行业网络安全白皮书 2020 年》记录,近几年"区块链技术+金融"等新型攻击手段引发的安全事故损失高达上百亿美元[2]。由此可见,在新技术背景下金融行业暴露出大量网络安全问题,对金融系统安全带来重大威胁,产生了严重损失。如何在鼓励金融创新发展的同时,防控金融网络风险,完善金融网络安全监管,就成为我们需要研究的重要课题。那么,中国现行金融网络安全监管体制面临怎样的困境呢?

1.1　整体性监管机制的缺失难以抵御系统性金融风险　现有金融业的分业监管体制虽有简单明晰的优点,但在金融网络安全监管的协作治理方面存在不足,恐难以应对系统性金融网络风险。当前我国金融行业网络安全管理以行业监管部门为主、国家相关部门为辅,坚持分业监管为主的架构。这种微观管理体制与金融科技综合化的发展趋向不符。新技术与金融产品的结合,导致金融科技从业机构成为跨行业、跨市场、跨地域的一种新型的混合业态,大大加强了系统的关联性和开放性,同时亦加剧了系统性金融风险爆发的可能。面对具有混合属性的金融科技从业机构,监管部门仅针对本行业领域内的金融科技风险制定监管细则,且内容多以准入资格审批与行为合规审查为主,没有统一的网络安全监管标准,亦未涉及对金融科技行业的宏观风险监测,在金融科技监管数据共享、风险预警、联动执法等方面缺乏相应的协调机制。囿于整体性监管的缺失,导致我国各行业监管部门之间的协调配合存在明显不足,欠缺应对混业经营的有效规制。

1.2　静态监管模式难以及时获取真实全面的网络安全信息　金融网络安全监管的风险评测有赖于金融从业机构定期披露的相关信息,因此信息的及时性和准确性会极大制约监管的效力。而我国现行金融监管模式为"命令—控制"型的静态监管模式,很难在第一时间获得真实有效的网络安全信息。一方面,随着人工智能、区块链等新技术赋能金融行业,金融产品更新换代的速度加快,网络安全风险也成几何倍数增加。在传统的自上而下的监管模式下,监管主体很难自主地及时察觉潜在风险,往往会在问题暴露并产生一定影响之后,才会对其加以监管。因此,新技术在金融产品中的应用,更加放大了静态监管体制的监管滞后的弊端。

另一方面,由于金融从业机构在监管的过程中往往处于"被动服从"的地位,缺乏向上级监管部门报送真实全面信息的动力。一是为规避监管,金融从业机构可能就现有的金融业务与现行的法律法规、政策进行合规性的自我审查与评估后,选择上报对己方有利的信息;二是金融从业机构出于市场竞争的考虑,为维护自身的优势地位,更愿意独占自己采集、存储和分析的相关信息,而不愿与监管部门或其他企业共享。此时,监管部门的风险评测在缺乏真实全面的信息为基础的情况下,无以窥风险全貌,实现监管效能。

1.3 **传统监管体制难以应对监管对象的日趋复杂化** 新技术和金融产品的结合,使金融网络引入了第三方科技机构。我国金融科技从业机构的存在形式主要有三种:一是“互联网系”大型科技从业机构,包括但不限于中国的 BAT(百度、阿里巴巴、腾讯),二是“金融系”金融科技从业机构,如上市银行设立的金融科技子公司或者子部门,三是中小型金融科技从业机构。具体而言,大型科技机构凭借着巨大的用户流量、用户口碑而进入金融领域,容易抵达长尾用户的需求端,实现支付清算、客户画像等金融功能,据了解蚂蚁服务生态系统中合作的金融从业机构超过 2000 家,其中包括 100 多家银行、90 多家保险机构以及 170 多家资管机构[3];商业银行为了抵御大型科技机构所带来的竞争,也纷纷开始科技转型,打造自己的金融科技从业机构,据统计 36 家上市银行已有 12 家单独成立金融科技从业机构[4];中小型金融科技从业机构利用企业科技的优势,整理金融机构资源,搭建金融信息服务平台。

金融科技从业机构由于缺乏完善的金融网络安全防护技术规范和相应的技术管理人员,成为网络安全防护新的风险点。传统的金融监管对象主要为银行、证券、保险等金融从业机构,有着严格的防范标准和准入标准。金融科技从业机构虽然通过资格审查暂时获得金融业务牌照,但是由于缺乏明确的监管规则,它们不仅在金融产品、运营、防护技术方面与金融从业机构的信息安全标准存在管理差异,而且自身防范风险能力也参差不齐,由此产生的网络风险尚不能被监管机构精准识别与界定,存在较大的安全隐患。

2 英国金融网络监管实践:“渗透性韧性测试”机制

2.1 **英国“渗透性韧性测试”机制概述** 为大力支持金融科技创新的同时,保证金融稳定、防御系统性风险,英国政府在近十年间进行了监管制度的创新,并探索出一些较为成熟的经验和成果。其中,渗透性韧性测试机制就是防范金融网络风险的一种行之有效的网络安全监管合作机制,值得我国借鉴和研究。

何为“渗透测试”?相关研究对渗透测试进行了六大阶段划分,分别为明确渗透目标、资料收集、假设目标漏洞、确认目标漏洞、扩展目标漏洞和消除目标漏洞[5]。亦即,学者认为渗透方法虽拥有不同的步骤,但一般为信息侦查、漏洞与端口扫描、漏洞利用和维持访问[6]。当然,还有学者认为渗透测试就是通过模拟所有可能的恶意攻击,发现现有的网络系统漏洞,以此来评估和修复网络防御系统的一种方式[7]。可以说,渗透测试以状态管道连接性、行为特定性、过程动态性、资源约束性、路径最优性为特点,攻击路径为核心,发现漏洞序列并修复脆弱的环节[8]。鉴此,笔者认为,渗透性韧性测试中的“渗透测试”是指以测试人员掌握的金融从业机构信息为基础,模拟现实环境中的恶意攻击,以此来提前发现、修补与规避金融机构的不确定性风险。

“韧性”一词最初是一个生态领域的概念,是一种常见的生态表达形式和重要概念。美国生态研究者霍林首次从韧性视角出发探讨生态韧性的结构规律,即生态系统受到外部干扰时为维持内部均衡状况所表现出能动的吸收力与适应力,以此开创了韧性主义先河[9]。学者在霍林实验的基础上首次将韧性模型用于日本私营部门经济行为的决策,为生物韧性决策模型提供了新的假设范式——预测力和复原力的增强可以在不断变化的环境中做出高效率的决策和回应,并降低整个系统的风险脆弱性[10]。此后,“韧性”理论以生态科学为基础,多元主体协调合作的韧性方式为特征,探讨区域事物发展逻辑的研究进路在人文、社会科学、制度与组织安排中得到了越来越广泛的测试与应用[11]。同时,以韧性视角为基础的研究范式逐渐进入经济领域研究视野,学者将经济韧性解读为二种:静态经济韧性是指系统在受到外部扰动时依旧能保障功能的正常运作;动态经济韧性是指系统迎接冲击后在底端恢复和重建之前均衡状态的速度[12]。学者将韧性理念引入到当前网络时代,网络韧性被表示为系统在受到冲击时所表现出来的集预测力、识别力、保护力、检测力、响应力和复原力于一体的稳定态势,这六种能力组合在一起可以抵御网络威胁,从而保护社会的网络安全[13]。由此可见,“韧性”理论更强调复杂系统或组织之间的相互运作以及风险调适能力,以实现各类主体的可持续发展。

英国的渗透性韧性测试就是这样一种通过渗透测试的方法,提高金融网络安全预测力、适应力、抵御力与发展力的非线性的协同与自我纠错的机制。具体而言,它以英国政府通讯总部为主导机构,允许金融从业机构在自愿的前提下提供自身真实情报,并批准测试服务提供商通过真实情报模仿网络攻击者意图进行测试推演,于 6 ~ 7 个月测试期限内,测试并提前修复其具有风险性的金融产品和金融系统的一种以情报为主的金融网络监管机制。该机制为金融网络安全监管提供了集预测、适应、抵御和发展于一体的韧性发展路径,在一定程度上缓解其面临网络攻击或者突发事件应对的压力,同时与监管沙盒体制形成完美闭环。因此,监管机构可以据此构建一个全程参与与掌握现有金融网络安全信息的反馈路径,有效管理金融网络化发展过程中存在的必然风险,从而一定程度上降低系统性金融风险的集中与爆发。

2.2　**英国“渗透性韧性测试”机制建设历程**　英国的渗透性韧性测试是 2013 年 6 月英国财政部、英格兰银行、金融行为监管局与金融从业机构协商的结果,其目的是在确保金融从业机构的关键资产不受损害的基础上,利用网络威胁情报对其进行真实的渗透测试[14]。2016 年 12 月,英格兰银行在以往基础上对渗透性韧性测试的基本框架进行更新,使得测试中的威胁情报更加成熟化和智能化[15],从而进一步巩固了英国作为欧盟地区领先的金融中心和网络空间的地位。

2.3　**英国“渗透性韧性测试”机制运作模式**　英国的渗透性韧性测试在运作模式中涉及六方主体,即统筹者、运筹者、监管者、威胁者、渗透者和被测试者。其中,统筹者由政府通讯总部担任,在整个测试机制中起主导作用;运筹者由英格兰银行网络部门小组担任,推进与评估整个测试机制的运作;监管者有英格兰银行审慎监管局、金融行为监管局和金融市场基础设施理事会,具体的监管者会根据被测试者(测试客体)的不同产生相应的变化(被测试者如果是保险投资类的金融从业机构,则需要审慎监管局和金融行为监管局联合监管;被测试者如果是金融市场基础设施,则需要金融市场基础设施理事会监管);威胁者包括威胁情报服务商和管理者;渗透者包含渗透测试服务商和管理者;被测试者可以是金融从业机构,也可以是金融市场基础设施。

上述主体贯穿于渗透性韧性测试的整个运作模式中。整个运作过程可以分为四个阶段:启动阶段、威胁情报阶段、渗透测试阶段和项目评估阶段。在这四个阶段中,英格兰银行网络部门小组为金融从业机构或者金融市场基础设施提供监管解读、服务范围审定以及评估反馈等支持,英国渗透性韧性测试机制的具体运作模式见图 1(资料来源于英格兰银行官网)。

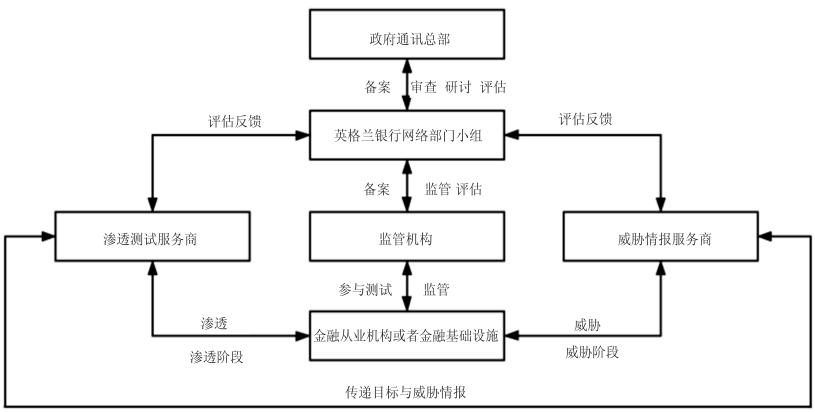

图 1　英国渗透性韧性测试机制运作模式

2.3.1　启动阶段　通常而言,在申请启动阶段,被测试者大约需要花费 4 ~ 6 周的时间,启动阶段分为四步:第一,在渗透性韧性测试过程开始之前,英格兰银行网络部门小组向相应的监管机构简要介绍渗透性韧性测试过程和各自的职责;第二,在参与过程中,英格兰银行网络部门小组和监管机构要同被测试者会面,共同协商测试时间与安全合同协议;第三,在渗透性韧性测试服务范围界定期间,英格兰银行网络部门小组规范了该机制测试的范围,特别是所涉及的关键“职能”,即提供核心服务所需的人员、过程和技术。在以上基础上,英格兰银行网络部门小组、监管机构与被测试者这三方主体共同讨论具体的服务范围。最终,渗透性韧性测试服务范围草案、被测试者的项目启动文件草案和互联网资产登记表,这三份文件将一同交付给监管机构、英格兰银行网络部门小组与政府通讯总部。如果启动阶段提前中断,可能会对金融从业机构的安全,包括客户群及金融稳定产生不利的影响;第四,被测试者需要在渗透测试资格认证组织采购威胁情报服务商和渗透测试服务商,以确保测试的正常运行(渗透测试资格认证组织是一个专门进行渗透测试专业级别认证的国际性非营利组织,且与英格兰银行网络部门小组合作开发了威胁情报经理资格、渗透测试经理资格,所有的威胁情报服务商和渗透测试服务商都必须取得相应的专业资格)。

2.3.2　威胁情报阶段　在威胁情报阶段中,被测试者大约需要花费十周的时间。此阶段分为四步:第一,被测试者向威胁情报服务商提供测试服务范围,其中需要包括被测试者的每个关键“职能”;第二,威胁情报服务商收集与分析当前的威胁评估与网络攻击事项,这些情报使得威胁情报服务商尽快地锁定攻击者的目标,其目标可能是客户资料或者是数据资源等;第三,基于这种“灰盒测试”(一种介于白盒测试与黑盒测试的方式,关注输出对输入的正确性,既不同于了解产品内部工作流程的白盒测试,也不同于从程序外部结构应用穷举法进行测试,是在部分了解目标系统主机的信息条件下,通过信息收集与利用等行为来评估目标网络系统安全性的过程),威胁情报服务商根据攻击者的动机和方法构建高概率的真实威胁场景,最终形成一份威胁情报报告。这份报告需要交付给被测试者、英格兰银行网络部门小组、监管机构与渗透测试服务商。随后,威胁情报服务商、被测试者与渗透测试服务商一起举行研讨会,讨论威胁情报报告草稿,并获得多方反馈;第四,政府通讯总部审查该草稿,通常需要花费三个星期,并且审查的目的是确保威胁情报的可用性与合理性;第五,在进入威胁情报的评估阶段需要形成两项评估报告,分别是:威胁情报服务商

评估被测试者的内部威胁情报能力、英格兰银行网络部门小组评估威胁情报服务商的能力，这两项评估将使被测试者更深刻地理解内部网络安全，同时也使监管机构了解市场上的金融网络安全。

2.3.3 渗透测试阶段 在渗透测试阶段中，被测试者大约需要花费十周的时间，在威胁情报阶段完成之后，渗透测试服务商基于威胁情报策划一份量身定做且行之有效的渗透测试计划；其次，根据威胁情报构建真实场景，渗透测试服务商模拟攻击路径，并渗透服务范围内的每个关键“职能”；再者，渗透测试服务商需形成一份渗透测试报告，其中包含目前关键“职能”性能问题、漏洞问题和其他补救成功的商业案例等；同时，被测试者需要根据渗透测试发现的漏洞，及时作出补救计划，并且英格兰银行网络部门小组对渗透测试报告和补救计划一同进行审查；最终，在渗透测试的评估阶段需要形成两项评估，即：渗透测试服务商评估被测试者的攻击响应能力、英格兰银行网络部门小组根据服务协议评估渗透测试服务商的能力，这两项评估旨在作为最终网络安全评估的一部分。

2.3.4 项目评估阶段 在项目评估阶段的工作中，英格兰银行网络部门小组大约需要花费为期四周的时间。英格兰银行网络部门小组评估威胁情报服务商与渗透测试服务商提交的威胁情报、渗透测试报告，并协同多方利益主体一起审查评估的结果，最终被测试者完成漏洞的补救计划。在补救过程中，监管机构全程监督补救计划的执行，直至被测试者完成补救任务。

英国渗透性韧性测试机制更注重事后评估，英格兰银行网络部门小组要求服务提供商在测试期结束后向其提供反馈报告。报告中应详细列出以下信息：一是测试期间哪些活动进展良好；二是测试期间哪些活动可以得到改进；三是其他多方利益主体的反馈。服务提供商所提供的资料与信息将会协助英格兰银行网络部门小组反思与改进渗透性韧性测试机制的运作和成效，以及及时识别该机制面临的主要问题和风险。

2.4 **“渗透性韧性测试”机制本质特征** 由此可见，英国渗透性韧性测试机制的运行过程处处渗透出通过协同共治、提前防范，实现对金融从业机构资产安全的保护，减少了监管的沉默成本，是金融科技背景下抵御网络安全风险的良好范例，有必要对其特征进行深入分析和总结。

2.4.1 参与主体的协同性 渗透性韧性测试中的各方参与主体在政府通讯总部的主导下，分工明确、协调配合，共同为防御网络安全风险发挥了作用。不同与以往的微观管理，该机制将与网络安全相关的各类公私部门都统筹在一起，如英格兰银行网络部门小组、审慎监管局、金融行为监管局、金融市场基础设施理事会、威胁情报服务商、渗透测试服务商等，形成一种多元主体协同共治的情形。英国政府通讯总部作为政府重要的情报部门，通过备案审查、研讨评估，确保渗透测试整个过程的有效性和安全性，并统筹协调测试中的各个参与主体，使各方职责都得到相应地把控和划分；英格兰银行网络部门小组作为金融行业的专门负责网络安全的技术部门，负责整个测试过程的推进和运作，在事前备案、事中监管和事后评估中不断完善该测试；威胁情报服务商和渗透测试服务商作为技术服务商，分别提供威胁情报和渗透测试的技术服务；金融从业机构负责提供当前的威胁评估与网络攻击事项；审慎监管局、金融行为监管局和金融市场基础设施理事会作为监管部门，会根据具体监管对象的不同，分别从各自的专业领域提供指导和监督……这种多元协同机制在后期指导金融从业机构的补救计划、制定针对性的金融网络监管规则指南意义重大。

2.4.2 测试客体的自主性 在渗透性韧性测试的测试客体上，监管机构并不强制金融从业机构参与测试，而是金融从业机构认识到自身存在网络风险之后主动要求进行测试与评估。这与传统监管模式中，金融从业机构被动披露信息不同。这些金融从业机构具有较强的风险意识，认为通过与监管机构合作，可以有效降低网络安全风险。因此，它们愿意积极地向威胁情报服务商告知其关键“职能”以及网络攻击等情报，从而使威胁情报服务商极大概率地分析出关键“职能”的脆弱性领域和构建真实的威胁场景。这就极大地解决了在监管中存在的信息不对称问题，让监管部门可以尽快获得真实有效的数据，对可能出现的相应风险进行更为精准地识别、测试与评估，从而及时制定相应的策略。

2.4.3 监管模式的抗逆性 英国渗透性韧性测试的显著优势在于，它可以在较大程度上对未来的风险进行预测和防范，从而尽可能降低监管滞后带来的损失。该机制通过对既有网络安全情报进行汇总收集，模拟攻击，并及时弥补漏洞，对关键“职能”脆弱性领域进行补救和升级，以真正防范风险，确保网络安全。这一过程的不断循环往复，在一定程度上就实现了实时动态监管，可以对新技术带来的新增风险点做出较快反应，制定相应预防措施，从而避免事后监管滞后的弊端，做到防患于未然。

3 我国引入“渗透性韧性测试”机制的可行性分析

很多欧盟国家均对渗透性韧性测试的英国蓝本进行了关注和本土化适用，我国能否具备实行渗透性韧性测试的条件？以下将从治理目标、监管逻辑与政策

路径三个方面进行叙述。

3.1　**“渗透性韧性测试”机制与构建网络空间命运共同体的治理目标相契合**　金融网络治理强调依法治网和合作治网,属于多元参与和立体协同的治理模式,无论在内涵外延还是实践意义上,都是网络空间命运共同体治理的根本遵循,能够保证网络空间创新发展与安全有序。渗透性韧性测试正是建设网络空间命运共同体的突出表现,能够契合网络空间命运共同体的构建需求。渗透性韧性测试为金融从业机构提供真实的渗透环境,使得金融网络风险提前暴露出来,有助于监管机构提前根据金融系统的运作情况进行动态调整,进一步夯实金融行业的共同安全,并藉此实现网络空间命运共同体的现实目标。

3.2　**“渗透性韧性测试”机制与我国金融网络监管的逻辑趋同**　我国金融网络监管以安全和发展两者兼顾为目标。中国人民银行于 2019 年下半年组建金融业态度感知与信息共享平台项目,金融从业机构已基本全部参与进来。这些动向与措施都体现了监管机构面对金融网络呈现出明显的风险态势意识,其逻辑在于不断平衡金融创新与金融网络安全之间的关系,即一方面鼓励金融科技创新,提高金融资源传输效率,另一方面巩固金融网络安全,守住不发生系统性金融风险的底线要求。渗透性韧性测试与我国金融网络监管的逻辑趋同。它没有为了规避风险,而完全禁止新科技在金融产品中的应用,而是在不抑制金融创新的同时,尽最大可能及时识别风险、实施动态监测,通过评估和反馈,制定防范和预防措施,从而实现金融创新和安全之间的平衡。

3.3　**“渗透性韧性测试”机制与我国金融政策试点实施路径吻合**　我国的政策试点形式是以“干中学”的方法来探寻未知问题领域的政策备选方案,获取回归反馈信息,反复修复政策信息,以此摸索出适合推向市场的正确解决方案[16]。而由新科技衍生出的金融产品潜在的网络安全风险,对于监管者而言,同样是未知领域,需要“摸着石头过河”,以局部实验的形式逐步推究适当的监管方式。“渗透性韧性测试”本质亦属于局部试点,通过实践中的威胁情报模拟攻击,不断评估、调整防御方案,逐渐实现金融网络安全系统的优化。这种“点-面-点”的递归迭代循环治理路径符合我国金融政策试点的实施路径理念,在实践中具有可行性。

4　我国金融网络安全韧性监管的制度构建

渗透性韧性测试的英国发展经验对于我国走出金融网络监管困境具有一定的启发,同时也符合我国先行先试的监管理念,我国可以从该机制汲取成功经验,寻绎一条符合我国国情的切实可行的制度路径。渗透性韧性测试机制是以各专业组织的协调配合为基础,发挥合力并共同形成较强的风险调适能力,完成对网络安全风险的高效预测和处置。因此,金融网络安全韧性监管制度的构建,需要从组织机构设置、激励机制、能力提升等方面,研究如何让多元主体参与到治理中来,并自主自愿地协调配合,不断完善提高自身能力,从而共同实现金融网络安全治理体系和能力现代化。

4.1　**重构我国金融网络渗透性韧性监管体系**　英国渗透性韧性测试机制是在政府通讯总部的领导下运作的。而该机构并非金融领导部门,而是国家安全部门,且不隶属于外交部,而直接向英国外交大臣负责。该架构可以将与网络安全有关的所有部门,包括金融从业机构,又不限于金融监管部门组织起来,共同为金融网络安全监管服务。这就弥补了新技术背景下金融混业经营状态下分业监管的不足,更有利于抵御系统性风险。因此,在网络安全监管的组织架构上,应当突破金融行业微观管理的壁垒,以维护国家安全为目标,建设整体性的金融网络安全监管体制。具体而言,在组织体系上,其一,当以国家互联网信息办公室担当统帅,突出“总司令”职责。其二,当以国务院公安部门作为运筹者用于衔接国家互联网信息办公室、一行两会以及模拟服务商,在此充当英格兰银行网络部门小组的角色与职责。其三,一行两会应当作为监管机构全程参与被测试者的测试过程,突出“监管”职责。其四,中国互联网络信息中心应当以威胁情报服务商的身份承担收集情报的职责,突出“灰盒”测试的涵义。其五,渗透测试服务商当以中国信息安全测评中心担当渗透者角色,承担“真实”测试的职责。金融网络渗透性韧性监管体系的重构在一定程度上契合金融微观审慎监管理念,加强各监管机构统筹协调性,降低金融网络体系的风险传染性,从而有助于正处在风口浪尖的金融从业机构及时发现风险与管控风险。

4.2　**完善企业主动披露信息的激励机制**　渗透性韧性测试的作用机理是“报告-诊断-预测-操作-激活”[17],其实现是建立在金融从业机构能够主动提供真实准确信息的基础之上。金融从业机构之所以愿意主动披露内部信息,主要原因在于英国能提供较完善的制度保障:一是 2016 年英国出台的《国家网络安全战略》、欧盟实施的《关键信息基础设施保护》以及《信息共享最佳实践指南》这三部法律更加强调在网络风险下公私合作伙伴以及信息共享建设的重要性,夯实了英国的金融从业机构自愿披露信息的基础;二是英国实施的《通用数据保护条例》和《数据保护法》不仅扩大了个人数据主体的权利,更细化了数据保护的规

则,从而奠定了渗透性韧性测试的数据法律基础;三是英格兰银行把网络风险补充到操作风险管理规范之中,并且网络情报一直在更新,以确保测试的安全性。这些法律法规既加大了企业的违法成本,迫使其主动披露数据;又加强了对企业在渗透测试中的安全防护,免除其后顾之忧。

因此,建议我国应首先制定更完善的金融数据分类标准和监管办法。中国人民银行制定并发布的《个人金融信息保护技术规范》《金融数据安全数据生命周期安全规范》等行业标准,对金融信息保护提供了规范性要求,但没能根据金融从业机构的敏感程度进行分类。由于"金融机构的性质不同,风险累积也各异"[18],建议在充分研究的基础上,根据金融从业机构的性质与规模大小,区分敏感程度,对敏感度较高的企业进行重点监管,对敏感度低的企业则适度监管。第二,明确企业在金融数据泄漏和网络安全事故中的责任,完善金融消费者的个人信息保护制度。完善的金融消费者个人信息保护制度是倒逼金融从业机构披露数据的重要抓手。正是由于金融从业机构不主动披露真实数据可能承担更大的经济和声誉损失风险,才使得这些机构愿意积极投身网络安全的共同建设之中,将自己掌握的金融网络安全数据与政府和其他组织共享。值得一提的是,即将正式实施的《中华人民共和国个人信息保护法》已经规定了金融从业机构对个人信息保护应尽的义务和责任,下一步有必要对金融信息保护制定更高等级的专门立法,加大对企业泄漏金融数据的惩处力度。第三,完善测试客体的外在保障机制。在测试中,我国可考虑明确测试者访问范围的若干限制性规定,并完善金融从业机构的财产安全权,以及发生网络风险事件时及时告知金融从业机构可采取的司法救济途径。

4.3 加快学习型与考核型金融网络安全治理主体建设 在合作治理网络中,各参与主体自身的专业能力提高是组织之间协调合作的充分条件,亦是制约韧性监管发挥实效的瓶颈。在复杂且以技术为依托的金融网络环境下,渗透性韧性测试能否实现真实且安全的网络威胁场景建构,对现实风险进行预测和抵御,在一定程度上有赖于服务提供商的专业化程度、金融从业机构网络风险的响应能力和监管机构的判断能力。在英国的渗透性韧性测试中,英格兰银行网络部门小组与渗透测试资格认证组织举行渗透测试考试,制定认证标准,目的是筛选出专业级别的威胁情报服务商和渗透测试服务商。基于此,本土化渗透性韧性测试机制应当加快服务提供商的学习型与考核型建设,这样可以提升渗透性韧性测试机制作用于金融从业机构的规范、目标导向型监管效用,使得服务提供商可以及时为金融从业机构识别金融网络风险、构建高概率威胁场景、依托威胁情报实现全方面渗透、完成渗透评估报告,以对接信息化驱动精准监管的未来。同时,加强金融从业机构和监管部门在网络安全方面的专业人才、设备和制度等多方面建设,发挥网络安全协会在相应的考核干预中的作用,全面提升风险识别和监测能力,满足新时期金融网络安全建设的需要。

5 结 语

金融网络安全的健康发展离不开完善的制度庇护,加快弥补金融网络方面的监管空白是当务之急。渗透性韧性测试机制作为监管机构、金融从业机构等多方参与主体与新技术相结合的产物,依托渗透性韧性机制所开展的金融网络监管具有协同性、自主性与抗逆性特征,可以内外联动应对金融网络本身发展所带来的风险,尤其是金融网络这个轮廓尚不鲜明、规则尚待生成的领域,更好地平衡金融从业机构风险与监管之间的关系,着眼于在监管机构与金融从业机构之间建立良好的风险防控体系,立足于金融网络风险被早识别、早预警、早发现、早处置,致力于日臻提高我国金融网络安全能力建设,一起合力促进防范系统性金融风险这一目的的实现,打造"金融安全 3.0"时代的安全生态圈(金融安全 3.0 是以金融信息基础设施为底层建设,金融业务为导向,共同支撑金融科技的安全,其中包括网络安全、云计算安全、风险控制等)。

参 考 文 献

[1] 陈启清. 以系统性策略防范系统性金融风险[N]. 经济日报,2019-04-30(012).

[2] 中国银保传媒股份有限公司,亚信网络安全产业技术研究院. 2020 金融行业网络安全白皮书[EB/OL]. [2021-10-10]. https://www.sohu.com/a/439502345_653604.

[3] 金融网科技. 蚂蚁数金科技平台曝光:合作金融机构超 2000 家收入源于技术服务[EB/OL]. [2021-10-10]. https://baijiahao.baidu.com/s?id=1675998358373871813&wfr=spider&for=pc.

[4] 消金界. 2020 年度金融科技报告:行业再出发——金融的归金融,科技的归科技[EB/OL]. [2021-10-10]. https://www.sohu.com/a/446096261_116132.

[5] McDermott J P. Attack net penetration testing[C]//Ballycotto, Proc of the 2000 workshop on New security paradigms. New York:ACM,2001:15-21.

[6] Patrick Engebretson. 渗透测试实践指南:必知必会的工具与方法[M]. 北京:机械工业出版社,2012:11-12.

[7] Ghanem M C, Chen T M. Reinforcement learning for efficient network penetration testing[J]. Information, 2019, 11(1):1-2.

[8] 臧艺超,周天阳,朱俊虎,等. 领域独立智能规划技术及其面向自动化渗透测试的攻击路径发现研究进展[J]. 电子与信息学

(下转第 94 页)

(上接第 86 页)

报,2020,42(9):2095-2107.

[9] Holling C S. Resilience and stability of ecological systems[J]. Annual Review of Ecology and Systematics, 1973(4):1-23.

[10] IVertinsky I. An ecological model of resilient decision making: An application to the study of public and private sector decision making in Japan - ScienceDirect[J]. Ecological Modelling, 1987, 38(1/2):141-158.

[11] Lebel L . Governance and the capacity to manage resilience in regional social - ecological systems[J]. Ecology & Society, 2006, 11(1):230-250.

[12] Rose A, Krausmann E. An economic framework for the development of a resilience index for business recovery[J]. International of Disaster Risk Reduction,2013(5):73-83.

[13] Paul, Theron. Through-life cyber resilience in future smart manufacturing environments: A research programme[J]. Procedia Manufacturing, 2018,16:193-207.

[14] Bank of England. An introduction to CBEST [EB/OL]. [2020-10-10]. https://www. bankofengland. co. uk/financial-stability/financial-sector-continuity.

[15] Bank of England. CBEST intelligence-led testing implementation guide version 2. 0[EB/OL]. [2021-10-10]. https://www. bankofengland. co. uk/financial-stability/financial-sector-continuity.

[16] 周　望. 中国"政策试点"研究[M]. 天津:天津人民出版社, 2013:127-177.

[17] 王向楠,吴　婷. 互联网韧性监管动态及借鉴意义——以金融业为例[J]. 电子政务,2020(1):51-63.

[18] 李　政,鲁晏辰,刘　淇. 尾部风险网络、系统性风险贡献与我国金融业监管[J]. 经济学动态,2019(7):65-79.

(责编:刘影梅;校对:王育英)