主动应对气候风险,加快提升能源企业气候韧性

■刘敏 朱沛青

极端天气频发与气候变暖趋势对全球经济社会发展产生系统性深刻影响,气候变化议题下的巨大不确定性,尤其是极端天气事件成为未来十年内全球发展面临的首要风险。能源企业具有投资规模大、自然资源依赖性高等特点,气候风险将显著影响其供给端与需求端状况,改变企业在投融资、研发、生产、销售等方面的决策与行动。为此,能源企业应积极构建气候风险管理体系,通过有效治理、科学分析、灵活应对、持续沟通等途径,主动采取行动适应和减缓气候变化,实现具备气候韧性的可持续发展。

■■我国气候新规密集出台,转型步伐加快

气候风险在企业生存发展中的重要地位已成为共识。近年来,国际监管围绕企业可持续信息披露、国际标准等方面推进全球气候治理进程。我国高度重视企业气候风险管理,相关政策密集出台。2024年4月,在证监会部署指导下,上交所、深交所和北交所发布《上市公司可持续发展报告指引》(以下简称《指引》),2024年11月,三大交易所又发布《上市公司可持续发展报告编制指南(征求意见稿)》,细化了《指引》的相关规定,分为"总体要求与披露框架"和"应对气候变化议题"两项首批指南,其中与气候议题相关的核心要求见表1。同月,财政部会同外交部等九部门制定印发《企业可持续披露准则——基本准则(试行)》(以下简称《可持续披露基本准则》),对包括非上市公司在内的企业的可持续信息披露提出一般要求。至此,我国初步建立起从上市公司向非上市公司拓展、从定性要求向定量要求扩展、从自愿披露向强制披露扩展的可持续发展信息披露制度体系,对我国企业提出了本土化的披露规范要求。2024年12月,中国气象局、财政部等部门联合印发《关于加强金融气象协同联动 服务经济社会高质量发展的指导意见》,强化金融气象协同机制建设和政策指导,旨在发挥"气象×金融"乘数效应,提高全社会的气象风险管理能力。2025年4月,财政部与生态环境部联合发布《企业可持续披露准则第1号—气候(试行)(征求意见稿)》(以下简称《气候准则(征求意见稿)》),是《可持续披露基本准则》发布后的首部具体准则,体现了气候议题较其他诸多议题的重要性与紧迫性。

表1 《气候准则(征求意见稿)》要求披露的气候议题核心内容

序号	维度	对企业的要求
1	气候相关治理	企业应披露管理和监督气候相关风险和机遇所采用的治理架构、控制措施和程序,包括治理机构或人员情况、管理层职责作用等。
2	气候相关战略	企业应披露管理气候相关风险和机遇所制定的战略和可能结果,并对当期和预期财务影响进行分析评估。
3	气候相关风险和机遇管理	企业应披露识别、评估、排序和监控气候相关风险和机遇的流程,以及其如何融入企业的整体风险管理流程。
4	气候相关指标和目标	企业应披露在气候相关风险和机遇方面的绩效,包括企业自身设定的目标的进展和国家法律法规、战略规划要求企业实现的目标的进展。

■■能源企业应对气候风险存在的问题

能源行业是受气候变化风险影响最大的行业之一。一方面,能源企业的生产经营过程对气候条件依赖程度较高,且有大量、高价值固定资产暴露于气候风险之下,例如光照、降水异常会使发电企业的电力生产出现超出预期的波动,台风、暴雪频发会导致设备等资产老化、损毁的风险激增等。另一方面,气候异常变化也会打乱能源供给与需求的时空平衡,为应对热浪、极寒等极端天气,能源企业需要额外增加能源储备和调配支撑。为此,能源企业亟需主动采取行动适应和减缓气候变化,提高对于气候不确定性的应对能力。然而,现阶段我国能源企业在气候风险管理上仍存在诸多不足与挑战。

其一,在理念认知方面,对气候风险及其影响识别不完全、不清晰,对风险影响的性质和程度也判断不明。中国企业关注气候变化问题较晚,而且一些中国企业更关注的是与此相关的企业形象而非企业发展战略。

其二,在管理机制方面,不少能源企业可持续发展治理架构尚不完善,对相关机构和人员的职责定位不够清晰,气候风险管理活动的业务流程有待理顺,同时也缺少信息报告与监督机制等反馈途径。

其三,在技术方法方面,由于目前气候风险评估模型不成熟、气候相关信息数据可得性较低、企业自身缺乏技能和资源,以及缺少应用压力测试、情景分析等方法的实践经验与数据基础,难以科学合理地识别、评估气候风险影响程度。

其四,在信息披露方面,能源企业对气候变化议题的披露目前主要集中在社会责任报告、环境社会及治理报告(ESG报告)的绿色发展或环境保护章节,在披露内容与报告格式上以个性化披露为主、标准化程度较低,以定性分析或举例说明为主、定量分析较少。根据气候相关财务信息披露工作组(TCFD)的调查统计,企业在财务文件中披露气候相关财务信息仍然有限,大多数公司选择在可持续发展报告和年度报告中披露,而非在财务文件中披露。

■■能源企业应对气候风险的策略与行动建议

第一,全面提升对气候变化议题的认识。

一要识别具有实质性影响的气候风险。能源企业应通过绘制风险地图、更新风险库等方法,在急性气候事件、长期气候模式转变等物理风险与社会低碳转型时政策、技术、市场、声誉等转型风险中,重点关注与能源电力企业相关的实质性风险,例如,减弱电力设施生产力的极端高温天气,电力用户对绿色电力消费偏好的改变,影响实物资产投资的技术更迭,威胁电力设施安全的洪灾、暴雪等。

二要在战略制定和调整中考虑气候因素。能源企业应当筛选和排序对商业模式、业务运营、发展战略、财务状况、现金流、融资方式及成本、价值链等可能产生重大影响的气候相关问题,考虑它们对运营成本和收入、资本支出和配置等方面的影响,评价战略在不同气候情景下的适应力,并积极做出战略应对。

第二,建立健全气候风险治理架构。

一要加强董事会对气候议题的监督管理。在监督职责方面,明确气候风险管理部门、风险责任人并逐级划分气候风险管理责任及工作任务,定期及时向董事会(或专门委员会)报告相关目标设定、战略执行、目标实现的情况等。在能力配备方面,应关注董事会成员中是否具有气候议题处理的知识技能或经验背景,以促进董事会就气候相关风险和机遇进行高效讨论与理性决策。在风险文化方面,基于董事会的参与和支持,清晰界定自身风险偏好,营造气候议题讨论的有利文化基础,推动员工参与、配合企业在应对气候变化方面的变革行动。

二要把气候目标融入绩效评价与薪酬激励。治理架构的有效运转需建立科学合理的评价与激励机制,权责利相统一有助于推动管理者和员工采取行动、系统开展气候风险管理工作。具体而言,能源企业可梳理相关岗位工作职责、设定气候风险管理指标和目标,提供实施薪酬激励机制的基本条件;通过设计长期激励计划,把气候因素融入现有人力资源管理体系。例如,意大利电力公司持续提高气候相关绩效指标的激励强度,2022年部分高级管理人员长期可变薪酬的10%依赖于三年内企业减碳效果,到2023年,这一数字变为15%。

第三,应用气候情景分析等方法评估气候风险。

我国可持续发展报告编制指南和国际主要气候信息披露准则均要求或建议企业通过情景分析量化气候变化影响。能源企业应基于历史气候数据与经济数据提出关键假设,考虑自身经营活动和上下游价值链活动的气候相关风险和机遇,涵盖未来不同时期所有主要风险敞口,详细描述风险传导路径,评估资产和业务活动对这些气候相关事件的风险暴露和敏感性。例如,2023年法国电力参考四年前发生在法国的飓风、暴雨等一系列极端天气的经济影响,预计未来有一定可能发生类似天气事件,估计造成设备成本、人力成本等总计0.6亿欧元额外成本,用来提供应急电源支持、更换损毁设备等。

第四,加强气候变化议题的披露与沟通。

一要提高气候议题信息披露质量。2024年11月三大交易所发布的《上市公司可持续发展报告编制指南》中专门设置了第二号议题或第二章,来规范气候相关议题内容的编制。无论属于强制披露主体或自愿披露主体,能源企业均可把该指南作为参考性规范和典型实践推荐,以清晰、客观、一致的方式向所有利益相关者披露气候风险及其管理情况,接受评价和监督。随着可持续发展管理领域的经验积累,能源企业应逐步增加对气候风险预期影响的量化评估,提供更多可靠、可比的信息披露。

二要加强与利益相关方的沟通合作。除了治理层与管理层对气候议题的投入,利益相关者的支持和参与也是能源企业应对气候风险必不可少的力量。通过多渠道定期发布报告、组织员工培训、开展客户满意度调查、参与行业论坛交流等各种丰富形式,能源企业与投资者、员工、客户、合作伙伴等利益相关方保持关于气候议题的交流和对话,尝试开展广泛而深入的合作,推动在应对气候变化领域的共同行动。

(作者均供职于南方电网能源发展研究院投资与财务研究所)

电力行业网络安全态势分析

■张浩 胡俊 王宣元 李远卓 张昊

据媒体报道,5月10日,巴基斯坦启动"铜墙铁壁"军事行动,对印度实施网络攻击,导致印70%电网瘫痪。虽然该事件的真实性尚未得到证实,但是网络攻击的技战术可能带来的巨大影响不容忽视。历史案例显示,电力系统遭受网络攻击较为普遍:2019年委内瑞拉全国大停电影响90%人口,2015年乌克兰140万用户断电。电力等关键信息基础设施安全已上升至国家安全战略高度,电网瘫痪将引发医院停运、供水中断乃至社会动荡等连锁反应。全球关键设施网络攻击近五年来激增300%,电力系统因行业关联性成为主要目标。数字化转型虽提升效率,却使变电站控制、智能电表等物联网设备成为新型攻击入口,可能引发链式攻击。《中华人民共和国网络安全法》《电力监控系统安全防护规定》等法规对防护提出更高要求,构建新型防护体系已成国家安全战略亟需。

■■传统网络安全风险态势仍存

第一,能源行业面临传统漏洞的长尾安全风险,工控系统成为重灾区。监测数据显示,2023年全球能源行业暴露网络安全漏洞4500个,其中42%为高危级别,35%集中于工控系统(ICS),68%的ICS高危漏洞直接威胁电力基础设施。漏洞修复周期持续延展,传统系统平均需98天,工控设备突破150天,造成长期渗透窗口。攻击者重点利用供应链(27%)、勒索软件(35%)及APT攻击(18%)三类路径,典型案例包括LockBit 3.0通过美国天然气管道漏洞实施定向打击。值得注意的是,历史漏洞(如Log4j、ProxyShell)与弱密码、默认配置等基础安全问题仍被APT组织持续利用,暴露企业安全基线管理的系统性缺陷。

第二,电力行业勒索攻击呈现产业化升级态势。2023年全球电力系统勒索攻击量同比激增35%,中小型配电企业与新能源运营商受攻击占比达60%,单次事件平均赎金飙升至570万美元,叠加业务中断与修复成本,总损失达1200万—2500万美元。攻击模式主要呈现三重特征:一是供应链渗透,如SolarWinds式攻击;二是利用Citrix、VPN等系统漏洞实施网络穿透,如LockBit 4.0入侵南美电网事件;三是采用"数据窃取+系统加密"的复合型勒索策略,如Conti组织加密台湾电力客户系统勒索2000万美元。

第三,DDoS攻击向电力关键业务系统定向演进。2023年全球电力行业DDoS攻击量同比上升28%,65%集中于客户服务门户与智能电表管理平台。典型攻击呈现三重技术特征:一是僵尸网络驱动的大流量冲击,如2.3 Tbps攻击致巴西电力缴费系统瘫痪;二是针对工控协议端口(Modbus TCP 502)的协议层泛洪攻击(占30%);三是瞄准API接口的应用层精密打击,如德国50万智能电表通信中断事件。随着能源物联网设备激增,部分充电桩等边缘设备沦为新型僵尸节点。

第四,电力数据资产面临立体化泄露威胁。2023年全球电力行业数据泄露成本达530万美元,超行业均值29%,核心风险聚焦三类场景:供应链漏洞(47%)致印度火电公司10TB工控参数外泄,内部威胁(32%)引发美国电网SCADA日志暗网曝光,云配置错误(21%)暴露亿级用户用电行为数据。

第五,钓鱼邮件攻击精准化重构电力系统渗透路径。2023年全球电力行业钓鱼邮件攻击量同比激增42%,75%锁定员工账户与供应链厂商,成为突破关键系统的核心入口。攻击技术呈现三阶定向特征:一是深度伪造高管邮件(占62%),如仿冒西门子等供应商实施品牌钓鱼;二是载荷隐蔽化,38%采用ISO镜像或PDF工单绕过传统邮件网关;三是窃取凭证层级上移,45%针对VPN登录权限、30%直指工控远程密钥,如美国西南电力公司SCADA系统沦陷事件。

第六,电力物联网设备暴露全链路攻击面。监测显示,全球30%的电力IoT设备暴露互联网接口,65%因固件未签名存在远程代码执行风险,如CVE-2024-3350漏洞,48%仍使用默认密码。攻击者通过两类路径突破:僵尸网络利用Telnet漏洞劫持50万智能电表组建DDoS攻击集群(峰值1.8 Tbps);APT组织操控LoRaWAN协议篡改风电场传感器数据,如Sandworm引发电网频率震荡。

第七,供应链攻击纵向穿透能源行业防御体系。全球电力行业39%的网络攻击源自供应链环节,单次事件修复成本超850万美元,形成软件(58%)、硬件(23%)、服务(19%)三维渗透模式。典型案例揭示攻击演进路径:俄罗斯APT组织劫持OSIsoft PI软件更新窃取SCADA配置,欧洲供应商篡改IEC 61850协议引发德国变电站宕机。

■■新型网络安全风险态势显现

第一,APT攻击。2024年,全球电力行业记录在案的APT攻击事件达127起,同比增长24%。平均每次攻击导致电力企业直接损失2200万美元,约41%的攻击成功渗透至电力企业核心网络,如SCADA和EMS系统。

APT攻击分为三类:国家级破坏型APT(占比45%)、数据窃取型APT(占比35%)和勒索驱动型APT(占比20%)。国家级破坏型APT主要由Sandworm等组织实施,利用零日漏洞和供应链攻击等手段;数据窃取型APT主要由Fancy Bear和Lazarus等组织实施,利用云存储配置错误和钓鱼邮件等手段;勒索驱动型APT主要由LockBit 4.0和BlackCat(ALPHV)等组织实施,利用双重勒索和快速横向移动等手段。

第二,AI驱动的自动化攻击正在全面升级,呈现出显著的智能化趋势。攻击者利用生成式AI技术,例如ChatGPT的变种,大规模生成高度个性化钓鱼邮件和虚假客服对话,甚至模拟目标用户的行为模式,从而绕过传统检测机制。同时,自适应攻击工具,如基于AutoGPT的自动化渗透测试框架,能够实时分析目标的漏洞并动态调整攻击策略,大大缩短攻击周期。2024年出现的"DeepPhish"攻击,就是利用AI生成虚假的视频会议链接,成功诱骗企业员工授权访问内部系统,展现出AI驱动攻击的强大威力和隐蔽性。

第三,深度伪造技术为重要单位防范社会工程学攻击带来颠覆性挑战。2023年香港某企业因伪造CFO视频通话被骗2亿港元的事件,预示着多模态伪造攻击逐步成为新的威胁形式。攻击者通过AI技术融合深度伪造语音与视频,冒充企业高管实施精准欺诈,同时利用公开数据训练模型构建高价值目标的社交图谱,这种融合生物特征模仿与行为预测的复合攻击模式,正在重塑网络犯罪的渗透路径。随着生成式AI工具的普及,此类利用跨模态伪造突破人类感知阈值的攻击手法,预计将很快进入爆发期。

■■我国关键信息基础设施安全保护力度持续加强

2024年,面对全球网络攻击规模激增、国家级APT组织活动加剧的严峻形势,我国关键信息基础设施(CII)安全保护工作以"实战化、体系化、法治化"为主线,在政策落地、技术攻坚、行业协同等领域持续发力,取得显著成效。

政策法规体系方面,《中华人民共和国关键信息基础设施安全保护条例》明确关基信息基础设施的定义、安全保护的责任主体、安全保护措施和监督管理等。行业配套细则方面,国家发改委、国家能源局发布《电力监控系统安全防护规定》,细化和提高了电力监控系统的防护措施要求;工信部等十二部门联合印发《工业互联网标识解析体系"贯通"行动计划(2014—2026年)》。在技术防御方面,国产化替代进程显著加速。

2025年3月,中央网信办公开征求《中华人民共和国网络安全法(修正草案)》意见,提出造成大量数据泄露、关键信息基础设施丧失局部功能等严重后果的行为处罚措施。这表明,我国正在进一步完善网络安全法律体系,加强对关键信息基础设施安全的保护力度。

■■需构建多层次立体化防御体系

我国电力行业网络安全历经二十余年发展,已构建起"安全分区、网络专用、横向隔离、纵向认证"的栅格化防护体系,并取得显著成效。当前新型电力系统转型面临新挑战,分布式电源、储能设备大规模接入,叠加电动汽车充电网络、虚拟电厂等新兴业态扩张,致使安全防御节点激增。能源聚合商等多元市场主体的防护能力差异形成安全洼地,攻击者可借此跳板渗透核心控制区,导致网络空间安全边界向产业链动态延伸,防护难度与风险同步攀升。在此背景下,未来需构建多层次、立体化的防御体系。

随着新型电力系统的快速建设,电力系统正面临前所未有的网络安全挑战。一方面,融合终端等边缘设备的大规模部署扩大了攻击面,攻击者可利用设备漏洞发起攻击或伪造数据干扰业务运行;另一方面,AI算法在多场景的应用也面临对抗性样本欺骗风险,可能导致决策失误。此外,全球化供应链中的软硬件后门、跨域协同中的漏洞连锁反应(如充电桩攻击电网)、量子计算对传统加密体系的潜在威胁,以及地缘政治驱动的APT攻击等,均构成系统性风险。这些威胁不仅可能破坏核心控制系统,更可能引发电力供应中断,亟需构建全链条防御体系以保障电力系统的安全稳定运行。

针对日益严峻的网络安全威胁,未来需构建多层次、立体化防御体系。技术层面应重点推进零信任架构与网络隔离,通过动态权限管理和白名单机制防范内部渗透;同时,强化AI安全能力,提升系统鲁棒性。供应链安全方面,需建立可信供应商认证体系与SBOM管理,确保软硬件全生命周期的可追溯性。此外,应加快密码学升级,部署后量子加密与量子密钥分发技术抵御未来风险。跨行业协同防御同样关键,通过威胁情报共享与红蓝对抗演练提升响应能力。管理层面则需推动法规政策落地,着力培养既懂电力又通网络的复合型人才,弥合传统OT人员的安全能力缺口。

(张浩、王宣元、李远卓、张昊供职于国网冀北电力有限公司;胡俊供职于国家计算机网络应急技术处理协调中心)