第 40 卷 第 7 期 2016 年 4 月 10 日
电力系统自动化
Automation of Electric Power Systems
Vol.40 No.7 Apr.10,2016
DOI：10.7500/AEPS20160202101

乌克兰停电事件引起的网络攻击与电网信息安全防范思考

童晓阳，王晓茹
（西南交通大学电气工程学院，四川省成都市 610031）

Inference and Countermeasure Presuppostion of Network Attack in Incident on Ukrainian Power Grid

TONG Xiaoyang，*WANG Xiaoru*
(School of Electrical Engineering，Southwest Jiaotong University，Chengdu 610031，China)

1 乌克兰停电事件网络攻击过程及电网薄弱环节分析

近两年来，中国提出了能源互联网的发展战略，已开展了许多相关基础性研究。能源互联网可认为是由传统电力系统（一次系统与二次系统）、分布式能源、通信网络等混合组成的具有互动性的电网物理信息系统，其中信息安全是保证能源互联网健康发展的重要基石。

2015 年 12 月 23 日，乌克兰电网遭受的停电事件展示了黑客攻击电网的实际威力。根据乌克兰国家安全局事后分析，它是由一起有组织的黑客攻击行为造成的。初步查明，黑客采用多种网络手段对乌克兰国家电网进行了攻击，如植入了被称为“BlackEnergy”的恶意软件，导致发电厂跳闸断电，并且，乌克兰地区多家电力公司同时遭受了拒绝式服务攻击，使各大电力公司的呼叫支持中心不堪重负，阻断电力运营商以远程控制方式对受感染系统实施的应急工作。国外信息安全专家 John Hultquist 称，BlackEnergy 之前先后曾攻陷过美国和欧洲的电力供应商，使这些欧美国家在攻击事件中受到了不同程度的损害。事实上，在这次乌克兰网络攻击停电事件之前，国外已有多起遭到恶意攻击的报道。

1.1 乌克兰停电事件中网络攻击过程

对于此次事件主要攻击手段，到目前为止的报道是，乌克兰计算机紧急响应小组（CERT-UA）已确认收到来自安全厂商 ESET 给出的报告，认定确实安装了名为 KillDisk（即 Disakil）的清除型恶意软件，其设计目标在于删除计算机中磁盘驱动器内的数据，并导致系统无法重启，但是乌克兰方面还无法解释受到 KillDisk 恶意软件攻击与发电站跳闸停电之间的直接关系。

中国金山安全反病毒实验室第一时间从各渠道采集到乌克兰停电事件中的 BlackEnergy 样本，并做了相应的分析报告（参见 http://www.admin5.com/article/20160114/642816.shtml）。该报告展示了 BlackEnergy 入侵目标主机的过程。首先黑客直接或通过傀儡机收集被攻击用户的邮箱，定向发送含恶意文件的邮件，无安全防范意识的用户打开了带宏病毒的文档，该文档伪装为微软 USB MDM Driver 驱动文件，但缺乏数字签名，用户运行了恶意安装程序，它释放和加载 Rootkit 内核驱动，Rootkit 使用某线程注入系统关键进程 svchost.exe，后者开启本地网络端口，以 HTTPS 协议主动连接外网的主控服务器，黑客在该连接成功后发指令下载黑客工具或插件，这样用户机器被渗透攻击成功，这个攻击过程见图 1 中的红线部分（攻击路径①）。然后黑客远程控制实施了后续具体攻击，通过网络传播病毒，删除计算机上的文件使其瘫痪，并通过网络穿透各种通信协议，从某台工控机向断路器发出了跳闸命令（如何做到这点尚无具体报道），并且黑客在攻击过程中清除了所经过计算机上的痕迹，使事后较难追踪到其攻击路线。

另一种黑客运用的攻击手段，可能是黑客事先在几个月前就通过某种方式在被攻击对象的局域网中植入了木马病毒，比如通过发送带有木马病毒的邮件，或者通过工程师的调试电脑把病毒下载到某台计算机上，时隔几个月后该病毒启动并与外界取得连接，实施后续攻击，见图 1 中攻击路线②。

相关报道中称乌克兰停电发生后，乌克兰多家

收稿日期：2016-02-02。
上网日期：2016-02-05。

电力公司同样遭受了拒绝式服务攻击，即图 1 中攻击路线③，导致这些电力公司的呼叫支持中心的网络流量激增，破坏了正常和应急通信，电力运营商不能以远程控制方式对受感染系统进行远程应急救援。

据国外相关报道，这次起主导攻击作用的 BlackEnergy 病毒，经过几年来的发展，逐渐加入了 Rootkit、插件、远程代码执行和数据采集等功能，可由黑客来选择特制插件进行攻击，能够提供支持代理服务器、绕过用户账户认证以及 64 位 Windows 操作系统的签名驱动等技术。

由以上攻击过程分析可见，它的确是一起有预谋有组织的网络攻击行为，并且其攻击者不仅仅包括那些黑客（电脑高手），可能还包括熟悉电力业务的人员，因为此次网络攻击成功地完成了跳闸断电，这个过程的成功实施需要相关电力知识、经验及技术。

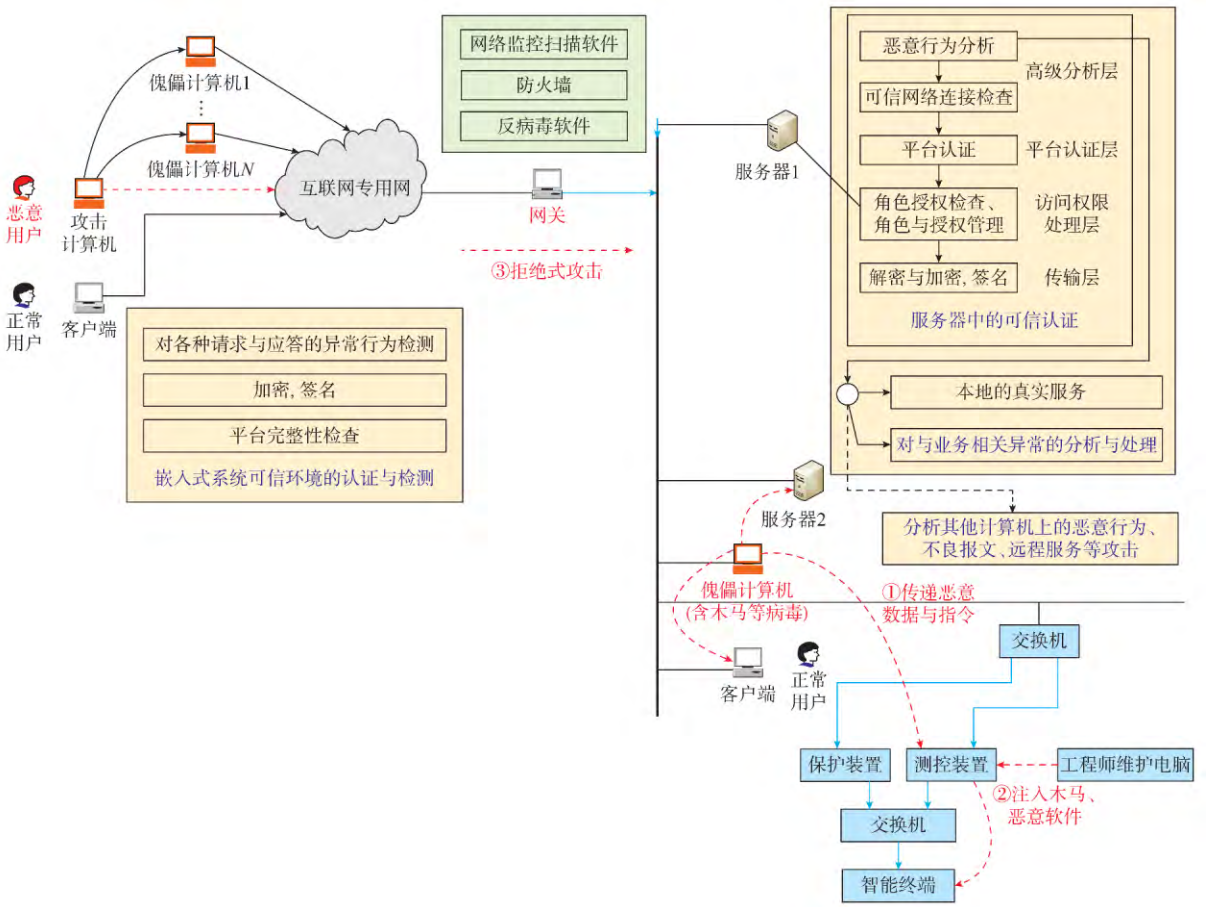

图 1　停电事件中网络攻击路径以及电力系统与信息系统的层次化防御体系预想

1.2　乌克兰电网存在的薄弱环节

这次停电事件暴露了乌克兰电网的一些薄弱环节。

1）首先是乌克兰电网信息安全防范体系不健全、发电厂安全技术手段不到位。尽管这次网络攻击的病毒入侵手段先进，但是乌克兰在几个月前曾经有过类似恶意网络攻击的预警，因为恶意软件 BlackEnergy 已经在欧洲某些国家的数据采集与监控（SCADA）和工业控制系统有所表现，乌克兰电力公司对此没有引起重视。同时没有建立起有效的层次化、网络化信息安全防御体系，没有通过技术手段去扫描、检查及发现其系统中潜在的病毒。

这次乌克兰停电事件发生发电厂跳闸，说明其发电厂自动化系统还没有采取有效的安全技术手段，导致未经授权或者非正常的跳闸指令，下达到相关控制单元，而且对于关键报文的通信加密技术没有做到位。

2）在遭受攻击过程中网络安全应对措施不力。当乌克兰发电厂受到攻击时，其电力监控系统并没有有效观察到攻击行为的发生、轨迹及动向，只能被动地遭受攻击直到其完成，更谈不上采取反击与反制措施。

3）信息安全制度不严密、人员安全防范意识薄弱。中国电力系统实现了严格的网络物理隔离措

施,即办公系统与生产系统严格分开,可杜绝此类通过邮件传播病毒的事件。而乌克兰发电厂显然没有或工作人员未遵循此规章制度,其安全意识单薄,通过邮件服务器自由收发来自外网的邮件,给病毒攻击提供了便利的渠道,这对电力系统敲响了警钟,信息安全制度和人员安全防范意识只能加强、不能放松。

2 网络攻击对中国电力信息安全防范对策的思考

2.1 先进国家信息安全应对策略的借鉴

美国作为世界上的信息技术强国,在电网安全方面投入了大量资源进行研究,开展了相关立法和战略。包括以下几点。①将能源系统列为国家关键性基础设施,对能源安全高度重视。2000 年 12 月提出美国的国家网络安全战略,对关键基础设施的保护一直处于核心地位。②提倡保护个人隐私前提下推进网络安全信息共享。2015 年 10 月,美国参议院通过《网络安全信息共享法案》,鼓励遭遇网络安全威胁与攻击的私营企业向政府共享信息,并将此信息分享给相关机构,建立网络安全共享系统以阻止网络攻击。③制定和指导能源行业的网络安全指南。2013 年,在 2009 年《美国网络空间政策评估报告》基础上修订《智能电网网络安全指南》,2015 年1 月发布《能源部门网络安全实施框架指南》。

2.2 电力与信息混合系统的信息安全防御思考

从乌克兰这次网络攻击行为看,它是针对电力系统的监控系统、运行装置及一次系统等实施的系统性攻击,即是对电力与信息混合系统的攻击。对于信息安全专家与电力科研人员来说,如何合作完成构建分布式层次化的信息安全防御系统,有许多问题值得研究。

1)电力与信息联合仿真平台的构建

电力与信息联合仿真平台研究工作最早得到人们的重视,它有助于帮助人们定量模拟和分析网络攻击对电网信息混合系统的破坏程度,尤其是对新型借助于广域通信网的广域控制系统等的影响。

国内外在建立电力与信息联合仿真平台方面已经做了大量工作,如 2003 年 Hopkinson K.M.博士、J.S.Thorp 教授和王晓茹博士联合研发了电力和通信同步仿真平台(EPOCHS),以电力系统分析及仿真软件 PSCAD,PSS/E,PSLF 等作为电力系统仿真工具,采用通信网络仿真软件 NS2 作为通信系统仿真工具。美国弗吉尼亚理工大学 Hua LIN 等人于 2011 年提出了全局事件驱动混合仿真方案(global event-driven co-simulation,GECO)等,其系统结构相似。近几年中国南瑞集团公司、华中科技大学、东南大学等单位开展了一些联合仿真平台的初步研究,搭建电力系统仿真软件和网络仿真技术软件包(OPNET)联合仿真平台。这些已有平台的共同特点是利用电力系统仿真软件模拟一次系统,采用通信系统仿真工具模拟通信延迟。弥补了电力二次系统的大量业务功能及其数据仅采用统计数据来模拟,与实际业务情况相距较远的不足。另一方面,与 ADPSS 和 RTDS 等全数字实时仿真系统进行联合也是个有意义的研究方向。

2)加强电力系统信息安全的防御体系

此次乌克兰停电事件,首先是信息安全事件,通过网络进行攻击是其主要手段,攻击的对象首先是信息系统,最终导致一次设备的跳闸。对于信息行业,信息安全是几十年来一直研究的问题,不断提出了许多算法和技术方案,对信息系统提出了机密性、完整性、可用性、可认证性、可识别性、可追溯性等一些重要的评估指标。

已有信息安全的威胁原因很多,包括恶意主机及其所控傀儡机的恶意攻击、软件设计漏洞(代码 bug、缓冲区溢出、解析错误等)、通信安全漏洞、远程调试后门、业务容错性处理不好、操作人员的不慎或恶意操作等。传统的密码学采用口令、加密、签名、公钥基础设施 PKI 等技术,信息安全专家提出了可疑代码与进程扫描、防火墙、虚拟专网、口令认证、反查毒软件(如图 1 中网关具有的功能)等方案,虽然它们极大地增加了恶意攻击的难度和代价,但仍不能完全防范病毒入侵。

近几年来信息行业可信计算组 TCG 提出了可信计算理论,认为“如果一个实体行为总是以预期方式达到预期目标则称其为可信的”。IBM 推出 4785 安全协处理器构造可信平台模块 TPM,提供平台完整性检查、公钥签名、身份认证、数字签名及加密等功能,将计算机和工控机置于可信的环境中运行,以减少不可信的恶意行为,应引起国内信息行业重视,尤其在打造电力可信运行平台及其环境方面。

国内的 360、金山等信息安全公司为各种个人计算机、手机研发的杀毒软件,通过查杀各种病毒与可疑代码来建立安全的计算机运行环境。对于 BlackEnergy 病毒攻击,金山网站给出了防范与拦截措施,具体如下。①用户对收到的邮件所包含的所有文件进行动态行为鉴定,如果具有恶意行为,则删除或隔离该文件。②对系统关键进程进行监控,一旦发现可疑操作,立即阻断其执行。③阻断恶意代码对外连接,设置一个 IP 黑白名单库,对系统外连的 IP 地址进行过滤,拦截与恶意服务器交互的所有网络数据包。能否在电力信息安全环境的搭建时

借鉴和运用当前先进的信息安全技术手段是一个研究方向。

国内外一些学者已认识到信息安全对于电力系统运行的重要性，但电力系统如调度中心、变电站等由于其业务安全方面有其一定的特点，如尚未建立专门统一的安全认证中心CA，变电站国际标准IEC 61850未涉及报文加密传输，各保护与测控装置均是嵌入式系统，在无认证中心CA认证下进行点对点通信。采用现有加密算法对变电站内各类报文加密，其防攻击的能力有待于验证，而面向通用对象的变电站事件（generic object oriented substation event，GOOSE）等快速报文的传输延时有专门要求（小于3 ms），研究轻量级且安全的加密算法迫在眉睫。每台装置缺乏平台完整性、身份认证、可疑进程与异常行为检测等可信运行环境的支持，而商用可信平台模块TPM也不能直接嵌入到其中。

3）电力业务的安全与容错处理的思考

对于潮流计算、状态估计、安全风险评估等电力高级功能，目前或以后都是在电力与通信混合的环境中运行，其数据大多要通过通信网络传输获得，在网络遭到攻击或者攻击者有意损坏数据、提供假数据、发出恶意指令等异常情况下，各类电力高级模块能否正常运行、受影响程度、灵敏度、波及范围等问题都值得研究。

电力工作者研究了对潮流计算、状态估计等模块在数据缺失情况下算法的容错性处理，也研究了保护与电气量报文部分缺失、通信部分失效等异常情况下，状态估计、广域控制系统等的受影响程度，还研究了在高度数、高介数、关键断面或线路等连续受攻击情况下，电力系统的安全风险指标及与耐受度之间的关系等。

假设网络攻击者包含一些电力专家，对当前被攻击电网具有同等的知识和相关分析工具，或凭借其经验与一些策略，在网络攻击过程中有针对性地对电网的关键点或薄弱环节进行攻击，运行中的电力系统是否有正确的应对、如何应对，也值得研究。

2.3　网络化分层协同信息安全防护体系

1）顶层设计

针对电力与信息混合系统及正在发展的能源互联系统，预想构建一个新型的电力网络化分层分布主动型安全防御体系。需要联合电力科研人员、信息安全专家、电力运行人员等，对该信息安全协同防范体系进行顶层设计，从异常检测与防御的网络化信息安全可信平台、电力业务模块对异常数据与行为的检测与容错算法、各装置的可信环境、传输加密算法及对异常代码与行为的抑制、电力人员安全防范意识和制度的检查落实等多个角度提高整体防御能力。

2）网络化安全防御系统的构建与技术研究

从信息安全角度出发，针对电力系统中每台运行的计算机及装置，运用反病毒技术手段，运用可信理论，建立信息安全可信防御平台，将各种应用置于可信的沙箱中运行，进行各类计算机的可信环境检测与认证，减少和尽量消除可疑进程的加载与运行。建立网络化信息检测系统，对网络上各类报文进行实时监控，实时扫描与检测异常报文、恶意行为等（如拒绝式服务等），甄别不可信的网络连接，追踪异常报文的规模、去向等，及时进行分析与报警，甚至予以拦截。针对智能变电站，研究变电站的新型数据安全传输加密、认证、角色授权管理与访问权限检查等算法与技术，加强二次设备，使其除了满足已有业务的运行要求，也能够抵御来自内网与外网的恶意指令、报文等的攻击（见图1中的绿色和橙色背景的模块）。

从电力业务的安全与容错处理角度出发，对于潮流计算、状态估计、安全风险评估等电力高级功能做进一步研究，在数据损失、坏数据、假数据、恶意指令、通信部分失效等异常情况下，提高各功能的运行性能、敏感性及生存能力，对异常数据的分析、检测及容错处理。研究在各种针对性连续攻击下电力监控系统的应对措施与预案等。

3）对各厂家装置的信息安全扫描、代码管理、异常线程行为检测及可信环境的搭建

各厂家装置是电力系统运行的基础和执行机构，而装置中各厂家程序首先要置于可信环境，针对嵌入式系统建立安全防御体系的研究未得到重视。各厂家程序的规范化管理也需要重视，对各程序进行统一有效的编码校验、注册登记及版本管理，离线和在线检测程序中异常模块，防止不合适的程序或恶意程序被装置加载运行，在遭到破坏时进行必要的重启或原始程序回滚。对各厂家的可能远程调试接口（调试后门）进行有效管理，防止恶意的远程攻击。

4）电力员工信息安全制度健全与意识的提升

乌克兰电力人员安全意识弱与防范制度不健全是这次网络攻击得逞的重要原因之一，因此中国电力人员在安全防范意识和制度检查落实上仍需加强，并加强电网监控与运行系统的日常巡检、运行监测、安全审计、漏洞检测及整改加固，强化风险辨识，做好安全风险和预警，严格落实网络信息安全制度。

2.4　遭受攻击后防范、补救及反击预案与预演

现在人们的研究方向主要集中在如何检测与防御网络攻击，还是有必要研究电网遭受攻击后，检测

与捕捉到恶意攻击行为与报文的轨迹的方法，在电力一次系统当时的拓扑结构下如何利用当下数据尽量保证业务模块的正常执行，在通信信道部分遭受破坏情况下，研究采用有效路由算法，仍能获取所需广域数据。甚至在发现与检测到内网与外网的攻击者，研究采取网络技术手段，隔离与阻断攻击者的行为，向攻击者发起反制攻击，阻止其进一步的攻击。

未雨绸缪进行信息安全攻击场景下预演，也许是今后需研究的一个新问题。如何模拟电网遭受网络攻击时的典型场景，让电力运行人员切身感受到网络攻击的手段、遇到的不利情景，积累经验，锻炼应对能力，也许以后需要投入相应的精力。

童晓阳(1970—)，男，通信作者，博士，副教授，主要研究方向：电网故障诊断、广域后备保护、智能变电站、信息技术及其在电力系统应用。E-mail：xytong@swjtu.cn

王晓茹(1962—)，女，教授，博士生导师，主要研究方向：电力系统保护和安全稳定控制。E-mail：xrwang@swjtu.cn

(编辑　王志鸿　许文杨)

(上接第 67 页　continued from page 67)

Enhanced Fault Ride-through Method for VSC-HVDC Supply of Passive Industrial Installations

BIAN Zhipeng, *XU Zheng*, *XUAN Yi*
(College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract: Since industrial installations are much more sensitive to voltage drops than frequency deviations, it is essential to guarantee the stability of voltage during severe faults. First, the main factor that affects the AC voltage in the passive system is analyzed. According to the analytical results, the control strategy is proposed to increase the AC voltage in transient conditions. The strategy consists of two parts, i.e., a modified current limit tactic and a frequency hysteresis control. The simulation tests uring metallic single-phase and three-phase faults are done via PSCAD/EMTDC to verify the validity of the control methods.

Key words: passive industrial installations; frequency hysteresis control; limit strategy; voltage sag; voltage source converter based high voltage direct current (VSC-HVDC▮

(上接第 143 页　continued from page 143)

An Overview of Robust Optimization Used for Power System Dispatch and Decision-making

YU Danwen, *YANG Ming*, *ZHAI Hefeng*, *HAN Xueshan*
(Key Laboratory of Power System Intelligent Dispatch and Control (Shandong University), Ministry of Education, Jinan 250061, China)

Abstract: Robust optimization, as one of the optimization methods utilizing disturbance molded by interval, is intended to find optimal decision under the worst disturbance conditions. It can be applied to power system dispatch and decision-making for its advantages, such as data availability, computing efficiency and applicability of large-scale systems, etc. First of all, on the basis of illustrating the characteristics of robust optimization itself, this paper introduces the application of robust optimization to unit commitment problems in power system, expounds the law of model-building under continuity and accidental disturbance, discusses the commonly used uncertainty sets and ways to limit the degree of conservatism. Secondly, this paper describes current researches on robust optimization in economic dispatch problems, presents the characteristics of three kinds of typical methods, including adaptive robust optimization, robust optimization considering affine policy and robust optimization with the objective to maximize the acceptable range of deviations. Finally, key problems and future direction in this field of research are discussed and analyzed.

This work is supported by National Basic Research Program of China (973 Program) (No. 2013CB228205), National Natural Science Foundation of China (No. 51007047), Shandong Provincial Natural Science Foundation of China (No. ZR2014EEM022), and Young Scholars Program of Shandong University (No. 2015WLJH43).

Key words: robust optimization; dispatching decision; unit commitment; economic dispatch