委内瑞拉大规模停电事件的初步分析与思考启示

摘要：安天研究院与广东省电力系统网络安全企业重点实验室对委内瑞拉大规模停电事件进行了联合分析研判。

转发语：

安天研究院
广东省电力系统网络安全企业重点实验室

联合分析发布

说明：2019 年 3 月 7 日，委内瑞拉发生大规模停电事件。安天科技集团组织研究院、安天 CERT 等内部力量进行跟踪研判，并于 3 月 9 日、3 月 10 日，向国家相关主管、职能部门报送了两期研判简报；广东省电力系统网络安全企业重点实验室积极跟进分析研判，于第一时间向主管部门报送了《委内瑞拉停电事件分析》，并于 3 月 12 日通过“南方电网技术情报中心”公众号发布《“3·7”委内瑞拉大停电事件快报》。为进一步加强分析研判力量，双方决定成立联合分析研判组，继续推动该事件的持续跟进分析。基于双方已调研了解的情况和初步判断整合形成此份初步分析。

【事件概述】

（一）事件发生及进展

2019 年 3 月 7 日傍晚（当地时间）开始，委内瑞拉国内包括首都加拉加斯在内的大部分地区停电超过 24 小时[1]，在委内瑞拉 23 个州中，一度有 20 个州全面停电，停电导致加拉加斯地铁无法运行，造成大规模交通拥堵，学校、医院、工厂、机场等都受到严重影响，手机和网络也无法正常使用。8 日凌晨，加拉加斯部分地区开始恢复供电，随后其他地区电力供应也逐步恢复，但是 9 日中午、10 日的再次停电，给人们带来巨大恐慌。长时间大范围的电力故障给委内瑞拉造成严重损失，包括连续多日停工停学，部分网站无法访问，甚至部分地区出现严重的哄抢商场超市情况[错误!未找到引用源。]。此次停电是委内瑞拉自 2012 年以来时间最长、影响地区最广的停电。

据媒体报道，初次停电是因为南部玻利瓦尔州的一座主要水电站发生故障，这个水电站属于古里（Embalse de Guri）水电站[3]。古里水电站位于奥里诺科河卡罗尼河口上游约 100 公里的 Necuima 峡谷处，

一期建设于 1963 年，二期建设于 1976 年。水电站大坝高约 162 米，长度为 7426 米，总蓄水容量达 1350 亿立方米。水电站共计装设 21 台水轮机组共计 10235MW，分别为：10×730MW，4×180MW，3×400MW，3×225MW，年发电量约为 47,000GWh,约占委内瑞拉用电量的近四成。古里水电站外观及地理位置如图 1 所示。

图 1 古里水电站外观及地理位置

（二）委内瑞拉政府反应

事件发生后，委内瑞拉政府立刻组织人力调拨资源全力恢复，与此同时，总统马杜罗指出，大规模停电“是美国方面的攻击行为造成的”。3 月 11 日晚，马杜罗表示，对该国电力系统发起的攻击分为三个阶段，包括网络攻击、电磁攻击、燃烧爆炸。3 月 12 日，马杜罗在一次电视直播的活动中再次透露[4]，攻击是在五角大楼的命令下由美军南方司令部直接执行的。同时，马杜罗请求俄罗斯、中国、伊朗和古巴协助调查。

较早前，委内瑞拉新闻通讯部长罗德里格斯曾表示，马杜罗政府计划将证据提交给联合国人权事务高级专员。委国防部长称，军方已在该国的电力线上引入了空中监视系统。委军方还计划进行旨在保护电力系统的军事演习[5]。

【委内瑞拉电力系统相关情况】

（一）委内瑞拉电力系统现状

委内瑞拉全国发电量约为 117,000GWh，其中水电占 64%，天然气发电占 19%，石油发电占 17%[6]。水力发电集中在瓜亚纳地区的卡罗尼河上，位于该国东部，共有 4 座水电站，其余分别是古里（Embalse de Guri）水电站、卡鲁阿奇（Caruachi）水电站、马卡瓜（Macagua）水电站、卡罗尼（Caroní）水电站。其中，最大的古里水电站位列世界第四大水电站[7]。因水力发电厂所发出的电力电压较低，要输送给距离较远的用户，就必须将电压经过变压器增高，再由空架输电线路输送到用户集中区的变电所，最后降低为适合家庭用户、工厂用电设备的电压，并由配电线输送到各个工厂及家庭。EDELCA 公司是委内瑞拉国内最大的一家电力公司，公司目前拥有两个已投产水电厂，即古里电厂和马卡瓜电厂，EDELCA 公司两厂各机组电力外

送示意图如图 3 所示。

Rank	Name	Country	River	Years of completion	Installed capacity (MW)	Annual production (TW-hour)[6]	Area flooded (km²)
1	Three Gorges Dam	China	Yangtze	2008/2012	22,500	98.8[7]	1,084
2	Itaipu Dam	Brazil Paraguay	Paraná	1984/1991, 2003[8]	14,000	103.1 [1]	1,350
3	Xiluodu	China	Jinsha	2014[9]	13,860[10]	55.2	
4	Guri	Venezuela	Caroní	1978, 1986	10,235	53.41	4,250
5	Tucuruí	Brazil	Tocantins	1984, 2007	8,370	41.43	3,014
6	Grand Coulee	United States	Columbia	1942/1950, 1973, 1975/1980, 1983/1984, 1991[11]	6,809	20[12]	324

图 2 古里水电站安装容量排名

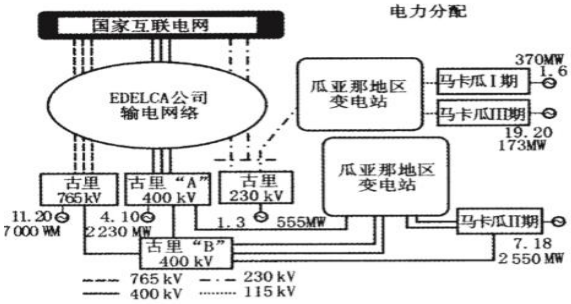

图 3 EDELCA 公司两厂和各机组外送示意图

委内瑞拉自主工业体系相对薄弱，在发电机组、高压输变电等设备上基本依赖进口，在较长一段历史时期，其供应商和承包商均为欧美电器巨头。如委内瑞拉中央电厂共有 6 个机组，1、2 号机组建成于上世纪 70 年代，均为 40 万千瓦，是引进意大利与德国的设备；3、4、5 号机组建于上世纪 80 年代初，是德国与日本的设备,彼时单体 40 万千瓦的装机容量均属世界领先技术。但随着设备的老化，目前这 5 个发电机组均已退役。近几年，中国公司开始参与到委内瑞拉重要电力基础设施的建设工作中，包括发电厂的升级改造、新建大型水利和火力发电厂，承担输变电工程建设等。委内瑞拉中央电厂 6 号机组发电项目，由中国机械设备工程股份有限公司（CMEC）于 2016 年完成，装机容量 60 万千瓦，能为委内瑞拉全国电网提供约 3%的发电量[9]。

由于主力发电能力分布在东部地区，委内瑞拉主网电力流呈现“东电西送”格局。从图 4 委内瑞拉主网架结构可以看出，委内瑞拉输电网由 765kV、400kV、230kV 三个电压等级构成，其中古里水电站输送给负荷中心的电力是通过 765kV 和 400kV 输送的。

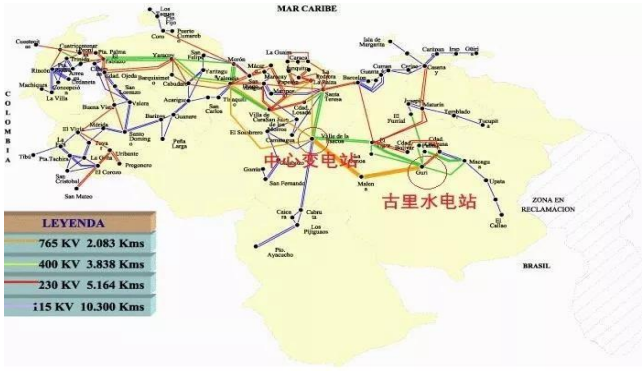

图 4 委内瑞拉电力系统主网架结构

（二）委内瑞拉的电力安全运维能力

关于委内瑞拉在电力系统安全运维能力上缺少足够的资料分析。从目前了解的有限信息来看，其运维能力和人员水平和我国相比，相对偏弱。但从少量公开资料来看，委内瑞拉电力相关产品选型和工程实施的标准起点，基本向欧美标准靠拢，其起点并不低，部分要求甚至高于我国。表 1 是委内瑞拉变电站系统相关建设要求与我国的对比。不过需要指出的是，绝大多数国家电力安全运维的措施，都是从应对事故的角度所建立，而这些措施对于应对物理攻击和破坏是远远不够的。

表 1 委内瑞拉变电站系统相关建设要求及与中国的对比

		中国	委内瑞拉
控制系统	测控装置	每台断路器配备一套测控装置	每台断路器配备一用一备两套测控装置，可靠性增加，但成本翻倍
	断路器重合闸配置	配置在保护装置中	配置在 I/O 测控单元中
保护装置	母线差动保护	集中式配置	分布式配置（主单元+子单元），成本较高
	变压器保护	双套保护（为 2 套完整独立的主后备一体化保护装置，测量电流回路一般从断路器 CT 引接，无独立的方向过流保护装置做后备）	双套保护（需要按 3 个保护装置配置，置一套采用套管 CT 做小差动，一套采用串内断路器的 CT 做大差动，并另配置一个方向过流保护装置做后备保护），成本较高
	230kV、138kV 线路保护	专用芯或通道复用接口装置	光纤电流差动保护和一套光纤纵联距离保护。光纤差动保护通信接口为专用芯，而光纤纵联距离保护通信节点为干节点，与对侧变电站的通信必须通过专用的通信转换装置完成
	24kV 开关柜弧光保护	默认不配置弧光保护（因该保护机制易误动）	必须配置弧光保护
	安稳装置	并非标配，默认配置单相电压互感器即可	三相母线均配置电压互感器
	故障录波系统	用变电站内的统一对时	求每台故障录波器配置独立的 GPS 天线和对时系统
系统通信	变电站通信	在变电站主控室配置一套光传输设备，各就地继电器室是不配置光传输设备的，保护室的信息均由控制、保护设备汇总后在主控制室内与光传输设备进行接口，从而上传调度	主控室配置一套光传输设备之外，在每个就地继电器室里也均配置了一套光传输设备，并要求要求在变电站内形成一个简单的通信网络

注：表格内容系分析人员从公开文献《委内瑞拉变电站控制和保护设计研究》[10]一文中提炼整理。

【各方对停电事件的原因表态和相关信息】

（一）委内瑞拉政府方面宣布遭遇三个阶段攻击

3 月 11 日晚，马杜罗表示电力系统遭遇了三阶段攻击。第一阶段是发动网络攻击，主要针对西蒙·玻利瓦尔水电站，即国家电力公司（CORPOELEC）位于玻利瓦尔州（南部）古里水电站的计算机系统中枢，以及连接到加拉加斯（首都）控制中枢发动网络攻击。第二阶段是发动电磁攻击，“通过移动设备中断和逆转恢复过程”。第三阶段是“通过燃烧和爆炸”对 Alto Prado 变电站（米兰达州）进行破坏，进一步瘫痪了加拉加斯的所有电力。随后，马杜罗 3 月 12 日在一次电视直播的活动中再次透露，攻击来自休斯顿和芝加哥，是在五角大楼的命令下由美军南方司令部直接执行。马杜罗没有公布上述指控的证据，称已下令设立了一个总统特别调查委员会对网络攻击事件展开调查，并请求俄罗斯、中国、伊朗和古巴协助调查。较早前委内瑞拉新闻通讯部长罗德里格斯曾表示，马杜罗政府计划将“美国参与停电”的证据提交给 12 日到访的联合国人权事务高级专员米歇尔·巴切莱特。

同时在 3 月 11 日，委内瑞拉方面宣布，已经逮捕两名纵火破坏电力系统嫌疑人。

图 5 委内瑞拉南方电视台报道马杜罗就电力系统遭受三阶段攻击发表讲话所配示意图

（二）反对派声称火灾导致停电

委内瑞拉反对派领导人胡安·瓜伊多表示，根据委内瑞拉 Corpoelec 输电公司内部人员透露，当地时间 7 日 16：42 分左右，古里水电站送出线路路径发生火灾，导致联络 Guri~Malena~SanGerónimoB 变电站三回 765kV 线路跳闸。值得注意的是，委内瑞拉 765kV 的线路是国家输电主干线，负责该国 85%的电力传输。由于三回 765kV 跳闸，SanGerónimoB 国家中心失去电源，该站全站失电导致送入国家负荷中心的主干线也全部失电。该中心站系统接线图如图 6 所示[11]。

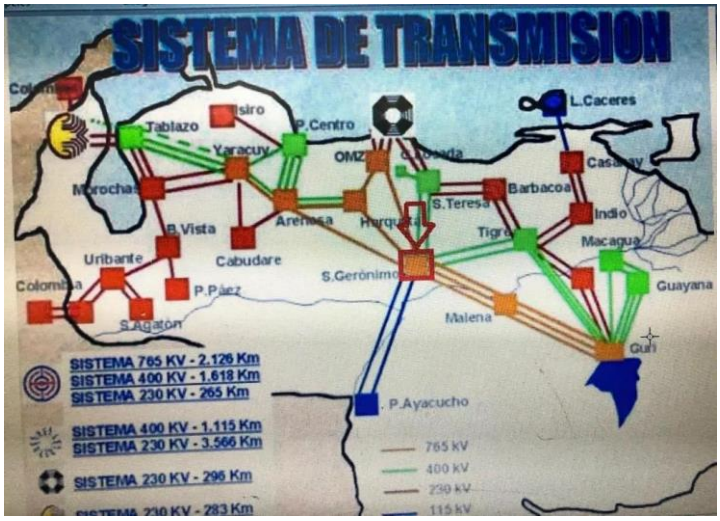

图 6 SanGerónimoB 系统接线示意图

（三）技术人员分析恢复系统困难重重

本次大停电事故发展演化过程暂不明确。但是，据后续媒体报道，由于送出线路跳闸，送端古里水电站 15、17、19 三台机组被切除，水电站 12 号机组因系统频率超过 62Hz 被切除。随后，周边卡鲁阿奇水电站 1 号、4 号机组，以及马卡瓜水电站全部机组也受到影响，陆续被切机。

委内瑞拉工程师 MiguelLara 解释长时间停电原因时称，恢复古里电力系统的操作很复杂，为了投入使用 Guri~ Malena~SanGerónimo 三回 765kV 线路，要求三座变电站具备合格的操作人员，但是该国电力系统发展滞后十年，并未有过预案处理经验，缺乏合格的操作人员，使得很难在 48 小时内解决复电问题。据报道，该国试图通过 400kV 网架重新构建电力系统，但是也失败了，导致 3 月 9 日第二次全国范围内大停电。该国输电专家米格尔拉拉说：大停电最大的问题是电力传输，即使他们在古里水电站发出电力，如果没有 765kV 系统，他们也无法把它送出，该国负荷中心 85%的电力依靠这条输电线路。

【综合研判】

联合研判组在事件跟进分析中，整合和事件相关的所有信息，并尝试与多方取得联系，但均未获得进一步更直接的信息。

委内瑞拉停电事件很容易被与“震网事件”[12]和“乌克兰电网遭遇攻击停电事件”[13]对比看待，而后两者都是已经被多方详细分析，并充分论证为网空攻击行动。安天此前对这两起事件都发布了详细的分析报告，但这些分析工作都是在能够部分获取到攻击载荷的情况下，基于深入的样本分析支撑攻击过程复盘的结果。“震网”攻击成功后，可能出于掩盖攻击意图或其他考虑，攻击方一度激活 USB 传播开关，使病毒样本出现一条从中东到东南亚的传播感染带，但也使攻击载荷相对容易被获取到；乌克兰停电事件则是基于长期建立的僵尸网络进行活动，加之使用了易于留下痕迹的邮件投放等手段，其在最终目标机的自毁也并不彻底，使之较为容易找到可供分析的对象与资源。

在是否存在高级网空攻击活动的分析中，依赖于采集面、环境勘察与提取、人员访谈、及第三方威胁情报导入作为输入，以驱动分析团队依托分析工具、威胁大数据平台进行基础分析，形成研判。对高度定向化的攻击，尤其依赖于被攻击目标防御体系的纵深性和能力留下有价值的痕迹，以及深入的环境提取。

而本事件基于目前事件特殊地缘特点限制，难以进行深入场景的提取分析，也无间接的样本、日志、系统环境镜像和其他数据资源情报，因此该事件尚不具备是否存在网空攻击层面的基础技术研判条件，目前仍只能从能力、动机等方面，基于相关消息进行研判。

联合研判组分析认为：

（一）基于委内瑞拉不稳定的社会局面，人为攻击破坏的可能性极大

鉴于委内瑞拉当前之局面，及相关国际形势，委内瑞拉基础设施崩溃及连带影响有比较明显的获益方，客观存在实施攻击获利的动机，因此有较大的人为破坏的可能性。但从目前线索来看，除纵火行为有更多相关信息外。关于网络攻击和电磁攻击尚无更多信息支撑。

在针对关键基础设施的攻击中，电力系统极易被当作首选目标，除了电力对现代社会运行起到关键支撑作用，被攻击可能引起连锁反映外。电力系统高度复杂，暴露面多也是一个原因。电站、输变电设备、线路层面均可能遭到物理、电磁和网空层面的攻击。而电力系统的空间特点则决定了，只有电厂和关键变电站能获得相对封闭的物理空间保障。大量无人变电站和线路均处在自然开放空间之中。而从电力系统的机理来看，局部的攻击很容易造成大面积影响。从委内瑞拉相关事件中，可以判断出发生了多次电网解列，电网解列的可能原因是关键节点注入功率不足，导致电网潮流异常或者过载，引发保护，局部停电到电网解列，最终就会引发大面积停电事件。

（二）美方有主导或参与的动机与可能性，但尚无技术层面的实证

威胁是能力和意图的乘积。从能力上看，美方具有全球最强的体系化网络攻击能力。在复杂的组织机构、庞大的人员规模和充沛的预算保障下，美方建设了一系列大型的信号情报获取和作业的工程系统、研发了制式化装备体系，建立支撑网空情报活动和攻击活动的框架，将情报获取、进攻作业、积极防御等网空能力整合成整体国家能力。可参见安天此前系列的相关分析【14-18】。

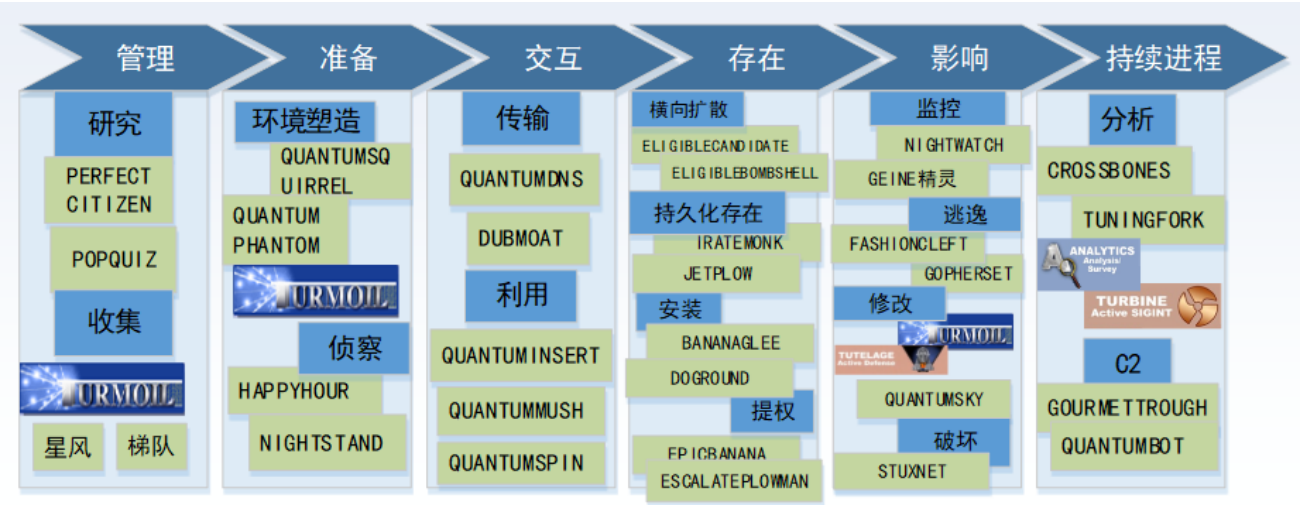

图 7 美方 NSA/CSS 网空威胁框架与其部分工程和装备体系的映射

从意图上看，美国一直背后支持委反对派反对马杜罗政府，此前还曾威胁直接军事干预。美国此前有利用“震网”攻击主权国家关键基础设施的先例。美方在攻击电力系统方面有长期的准备，早在 2007 年，美国爱达荷国家实验室就是实施了一项非机密的政府内部实验——即“极光漏洞”试验，针对一台 225 万瓦功率的柴油发电机，通过计算机程序以异常的方式反复高速关闭和重启此发电机，在短短的三分钟时间内，发电机被彻底摧毁，部分组件因为压力的反复变动导致炸裂，部分碎片被崩裂到 80 英尺之外。上述资料于 2014 年 7 月 3 日，被美国国土安全部根据信息公开法公布。根据《Division Cyber Operations》[0]等文献，美方已经将政治、军事、经济、社会、基础设施等宽频目标，纳入到目标打击规划工具的目标列表中，其中基础设施目标中就包括电力系统。美军目标打击规划工具（PMESII Crosswalk）考虑事项和可攻击侧面如图 8 所示。

PMESII Crosswalk考虑事项和可攻击侧面

政治	军事	经济	社会	信息	基础设施
舆论控制	A2AD环境	产品出口收入 (能源、自然资源)	舆论控制	互联网流量 状态监测	水处理和交通
政府合法性	Mil数据链路	工业控制	社交媒体		电力分布
流离失所者	精确的导航和时间	货币实力	流离失所者舆论	信息泄露控制	铁路管理
北约第5条	对太空资产的依赖	国家储备	非国家行为者	社交媒体	桥梁和公路
国际压力 (制裁、公民投票)	物流配送系统	市场实力	娱乐	MILDEC	天然气
	空降C2	石油精炼		互联网访问	水路管理
	地面系统的OR率	港口设施			

图 8 美方 PMESII 的可攻击面清单

从行为模式的角度来看，瓜伊多所声称如他上台执政就能马上恢复电力，而美方恰恰将“重建”作为网络武器参与的作战阶段之一，美国陆军参谋长前高级顾问 Maren Leed 曾在《Offensive Cyber Capabilities at the Operation Level》[0]一文中指出，“网络武器具有无与伦比的多功能性，它们可用于从参与到高端作战的所有军事行动。因为它们的影响是可逆的，所以非常适合于作战的所有阶段，包括环境塑造、高烈度对抗 以及目标重建”。

（三）委内瑞拉部分电力设施陈旧，在社会动荡背景下故障频发，亦不能排除自身发生故障所致

乔治华盛顿大学网络与国土安全中心高级研究员 Kalev Leetaru 认为[0]，“由于电网经年累月管理不善，停电在委内瑞拉已是司空见惯，不需要美国国家安全局的帮助”，“该国电网自己就可以引起下一次停电事件。大多数国家，包括美国，都对其老化和日益超载的公共基础设施感到担忧。因设备故障或输电线路过载而停工的发电厂更可能被归咎于投资不足，而非外国网络攻击。引起大规模山火的电力线故障很可能是预防维护工作不力导致，而非蓄意的外国破坏。”

2013 年 1 月至 6 月期间，委内瑞拉国家电力系统发生了 10,647 次失败事故；2013 年 9 月 3 日，19 个州和加拉加斯经历了由于输电线路故障导致的 4 小时停电，该国 70%的面积停电；2018 年 8 月 31 日，苏利亚州首府马拉开波的一个变电站发生爆炸，导致城市大片区域停电；2018 年 10 月 16 日，卡拉沃沃州 La Arenosa 发电站发生爆炸事故，导致本国西南部电力供应中断，12 个州出现电力短缺，至少 1000 万名用户可能受到停电的影响。当然也不能排除这些事件的背后同样可能存在人为因素的影响。

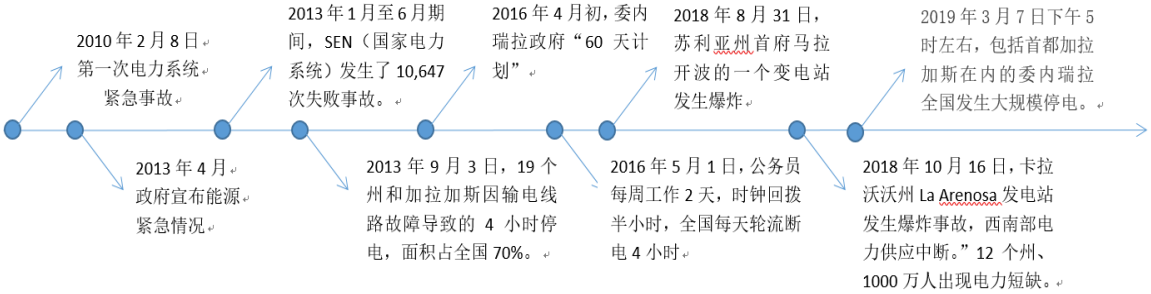

图 9 委内瑞拉电力系统历史事故图

（四）网络空间安全、关键基础设施安全需要相应的基础支撑条件

如果将“震网事件”和“乌克兰电网遭遇攻击停电事件”与委内瑞拉停电事件对比，前两起事件都是在被攻击设施拥有国社会基本稳定、主权与安全有基本自我保障的能力下所发生的，在基础设施的物理安全有一定的保障基础上，攻击方往往会优先选择采用网空攻击这种相对更隐蔽、具有穿透性手段进行攻击。以在达成攻击效果的同时，限定影响后果，同时其成本也比物理域军事打击更低廉。而物理手段和网络手段叠加往往能达成更大的攻击效果。在委内瑞拉社会动荡的背景下，内部破坏、里应外合等各种可能性都急剧增加，物理、电磁、网空多个领域风险相互叠加，而被削弱的社会应急能力、和基础设施运维水平，又增加了恢复难度和成本。国家的主权与安全是关键基础设施安全的基本屏障，社会治理能力是关键基础设施安全

的前提基础。当前委内瑞拉政府虽然能维持政府的基本运行，但在巨大的外部颠覆、干预压力以及内部反对派的干扰下，主权与安全遭到严峻挑战，治理能力就已经高度削弱。在这种情况下，如果遭遇入侵攻击，很大可能是带有网络空间和实体空间的复合性因素，而非单纯的网络攻击问题。而多起事件间，既有可能是强关联组合打击，也可能是弱关联的多源并发。

此次委内瑞拉政府多次发声中，包括 “电力系统已成为美国最新一轮网络攻击”、“国内渗透者从内部攻击了电力公司”、“抓获纵火破坏电力系统嫌疑人”等，同时网络上也出现了西部变电站发生爆炸的相关信息，如果这些都属实，这就是一个里应外合、多域交织的结果，是国家政权受到挑战的情况下集中爆发出的基础设施安全问题。而也正是由于政权管控能力下降，导致攻击事件发生后，政府没有足够资源和能力有效应对，进而接连受到的攻击令损失进一步扩大化。

【几点启示】

启示一：必须从总体国家安全观来统领关键基础设施安全防护工作。关键基础设施是各种威胁行为体所觊觎的目标，而其攻击往往是跨域组合的。因此不能简单的将基础设施防御视为技术对抗，而要视为综合对抗。

在常规防护中，要将物理安全、人员安全因素与技术安全因素都充分考虑在内，对可能发生的紧急情况，制定更为全面的预案。目前国内在网络空间安全领域，存在缺少总体国家安全视角，不以结果/后果角度分析威胁，而以攻击的“技术含量”高低看待威胁的倾向，认为“非技术层面的攻击，就不是事儿，不是‘高技术含量’的攻击，都不是大事儿”。但网络空间安全和关键基础设施安全都具有非对称性的特点，决定了攻击中是组合拳打击薄弱点的特点。并非只采用技术手段或高技术手段。威胁行为体在攻击中并不关心“技术含量”，而更多考虑目标价值、攻击成功率、攻击成本、攻击隐蔽性等“作战指标”。一些针对关键目标的简单技术或人为操作在与其相适应的时间点爆发，一样可以造成重大损害。

启示二：能力导向建设模式，提升关键信息基础设施安全防护能力。

当前，我国面临着复杂严峻的内外部形势，在众多的风险挑战中，“网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击”是一项突出的风险。防控能力建设及以国家大型工程为主干，也以各政企机构建设管理的每一个重要信息系统和信息基础设施的安全为基石。基石不稳，则大厦难安。重要信息系统和关键信息基础设施处于“低水平防护”，甚至“无效防护”的状态中，是国家安全与稳定的严重隐患，影响到国家的战略主动性。

目前政企网络安全防护中规划能力不够、预算保障不足、问责机制没有落地等问题十分明显，在安全规划建设工作中往往是在满足一般性合规要求的基础上，再简单堆砌部分产品应对各类单点威胁，未形成动态综合的网络安全防御体系，缺少实战化安全运行机制保障。面对既有安全环节单点失效、面临新的威胁类型，疲于应付，顾此失彼。对隐蔽性更强的高级网空威胁行为体的持续性威胁，缺少足够的发现和防御能力。在预算保障上，受经济下行压力影响，安全投入纷纷削减或延迟。

但越是在面临复杂严峻挑战下，越应优先建设安全支撑能力，建议主管部门通过系统规划指引、保障预算投入、加强问责落实，全面提升政府、央企网络安全防护水平。

政企机构、关键信息基础设施建设运维方，面对复杂的敌情，需要将“敌已在内，敌将在内”作为驱动防御的前提设定，并根据自身网络与信息系统的国家安全、社会安全和业务安全属性，客观判断必须能够有效对抗哪些层级的网络空间威胁行为体，并据此深入分析安全需求，建立安全规划，保障预算投入。

采用叠加演进能力导向的网络安全建设模式指引规划设计，科学合理地分阶段扎实开展网络安全建设实施工作，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的网络安全能力【22】，构建动态综合的网络安全防御体系。

针对电力等基础设施和工业系统，在落实能力导向建设模式构建动态综合防御体系的工作中，必须以保障业务运行的连续性和可靠性要求为基本前提，这就对基础结构安全能力、纵深防御层面安全能力的规划、建设和安全运行提出了更高的要求，对于现网系统，针对各种等可能对业务连续性产生潜在影响的安全动作，需要极为慎重，综合采用合理规划、分区分域、收窄暴露面等方式，有效布防，并通过完备的应急响应预案制定、演训式威胁评估等相关措施，最大限度避免或减少对业务系统可能产生的影响，确保系统业务的弹性恢复能力。

【调研分析参与方简介】

安天研究院简介

安天研究院是安天科技集团的下属研究机构，专注于网络安全威胁检测和知识工程方向的前沿探索，研发下一代威胁检测引擎，完善配套的知识工程体系；对认知能力、推理和本体模型、威胁知识图谱等领域进行研究探索；对智能终端、物联网、工业控制系统和各种新兴场景下的安全威胁进行分析和预判；对各种高级网空威胁行为体的工程体系、装备体系、作业框架等进行分析梳理。

安天研究院下设多个专家工作室。同时与多所高校进行合作，按照“优势互补、窄带聚焦、实战导向、追求领先”的原则，选择安天有工程能力和数据基础，高校有学术积累的窄带专业方向展开深入研究，助力高校形成具有前瞻性和实用前景的高水平学术成果，推动科研成果向有效的安全价值转化。

安天研究院积极跟进国际网络安全领域的前沿成果，发起成立了安天技术公益翻译组，累计翻译了超过1600 万字的文献资料。

广东省电力系统网络安全企业重点实验室简介

广东省电力系统网络安全企业重点实验室，依托于南方电网公司网络安全实验室建设，2018 年度获得广东省科技厅正式批复成立。同时，该实验室也是电力行业信息安全等级保护测评中心第五实验室、国家能源局南方能源监管信息安全技术支撑单位、广东省能源互联网网络安全工程技术研究中心、南方电网公司

电力监控系统安全防护实训基地，是南方电网公司网络安全领域的的科技研发中心、技术服务中心、测评认证中心和培训交流中心。

本实验室是南方电网公司海外高层次人才创新创业基地的重要组成部分。目前，已建成了一套科学、完善的质量管理体系，申请获取了 CNAS17020 检验机构、CNAS17025 检测校准实验室、国家注册信息安全等级保护测评机构、国家注册信息安全员培训机构等认可资质，申请获取了信息安全综合服务、风险评估、应急响应、工程集成等业务资质。实验室在等级保护测评、安全风险评估、软硬件测试、威胁信息通报、事件调查取证等方面有丰富的工作经验和丰硕的工作成果，为十八大、十九大、G20 峰会、博鳌亚洲论坛等国家重大活动提供了信息安全保障。

【参考资料】

[1] Telesur English：Venezuela Denounces US Participation in Electric Sabotage

https://www.telesurenglish.net/news/Venezuela-Denounces-US-Participation-in-Electric-Sabotage-20190308-0021.html

[2] Lapatilla.com：Fedecámaras Zulia ofrece balance de saqueos en la región por crisis eléctrica

https://www.lapatilla.com/2019/03/12/fedecamaras-zulia-ofrece-balance-de-saqueos-en-la-region-por-crisis-electrica/?tdsourcetag=s_pcqq_aiomsg

[3] Telesur English：Venezuelan Gov't Denounces Latest Attack on Electric System

https://www.telesurenglish.net/news/Venezuelan-Government-Denounce-New-Attack-On-Electric-System-20190307-0033.html

[4] https://www.voacna-help-investigate-alleged-us-cyber-attack-20190313/4826828.htmlhinese.com/a/venezuela-asks-chi

[5] Twitter：https://twitter.com/teleSURtv/status/1105964204023050241

[6] IEA：https://www.iea.org/countries/Venezuela/

[7] 维基百科：https://en.wikipedia.org/wiki/List_of_largest_power_stations_in_the_world

[8] 委内瑞拉 EDELCA 电力公司梯级与三峡-葛洲坝梯级 AGC 比较，李晖，《华中电力》，2003 年第 1 期

[9] 国机集团：http://www.cmec.com/xwzx/mtbd/201809/t20180903_192153.html

[10] 委内瑞拉变电站控制和保护设计研究，赵焱、张庆伟，《国际工程与劳务》 2015 年 01 期

[11] 北极星电力网：“3·7”委内瑞拉大停电事件快报

http://m.bjx.com.cn/mnews/20190312/968255.shtml

[12] 安天：对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告

https://www.antiy.com/response/stuxnet/Report_on_the_Worm_Stuxnet_Attack.html

[13] 安天：乌克兰电力系统遭受攻击事件综合分析报告

https://www.antiy.com/response/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage.html

[14] 安天：修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件

https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html

[15] 安天：方程式（EQUATION）部分组件中的加密技巧分析

https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html

[16] 安天：从“方程式”到“方程组”EQUATION 攻击组织高级恶意代码的全平台能力解析

https://www.antiy.com/response/EQUATIONS/EQUATIONS.html

[17] 安天：方程式组织 EQUATION DRUG 平台解析—方程式组织系列分析报告之四

https://www.antiy.com/response/EQUATION_DRUG/EQUATION_DRUG.html

[18] 美国网络空间攻击与主动防御能力解析（连载），网信军民融合杂志，安天研究院

[19]《Division Cyber Operations》

https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136080/division-cyber-operations/

[20]《Offensive Cyber Capabilities at the Operation Level》

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf

[21] Forbes：Could Venezuela's Power Outage Really Be A Cyber Attack?

https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/

[22] 网络安全滑动标尺模型—从架构安全到超越威胁情报的叠加演进（安天译本）

【委内瑞拉电力-能源危机与其国内局势历史时间记录表】

（截至 2019 年 3 月 12 日）

注释:黑色字体为能源危机，蓝色字体为局势动向

- 2010 年 2 月 8 日，委内瑞拉发生电力系统紧急事故。
- 2012 年 10 月，查韦斯再次赢得连任。
- 2013 年 1 月至 6 月期间，SEN（国家电力系统）发生了 10,647 次失败事故。
- **2013 年 3 月 5 日，查韦斯逝世。**
- 2013 年 4 月，政府宣布能源紧急情况。
- **2013 年 4 月 14 日，马杜罗成为委内瑞拉总统。**
- 2013 年 9 月 3 日,根据官方报告,19 个州和加拉加斯经历了由于输电线路故障导致的 4 小时停电。该国 70%的面积停电。
- 2016 年 4 月初，委内瑞拉政府“60 天计划”,“60 天计划”包括 4 月和 5 月的每个周五，委内瑞拉公共服务部门放假，学校停课，并且工作日也相应减少上班时间，目的是为了节约用电。
- 2016 年 5 月 1 日，委内瑞拉政府实施公务员每周工作 2 天，休息 5 天的临时措施，还将时钟回拨半小时以充分利用日间时光，全国每天轮流断电 4 小时，委内瑞拉所使用的时间称为“委内瑞拉标准时”。委内瑞拉标准时为 UTC-4:30，是唯一一个使用该时间的国家。
- **2017 年 7 月 31 日，美国财政部宣布对委内瑞拉总统马杜罗实施制裁。根据制裁措施，马杜罗在美国境内的资产将被冻结，同时美国人将被禁止与其进行交易往来。**
- **2018 年 5 月 20 日，委内瑞拉国家选举委员会宣布，现任总统马杜罗赢得本次总统选举。**
- 2018 年 8 月 31 日，苏利亚州首府马拉开波的一个变电站发生爆炸，导致城市大片区域停电。
- 2018 年 10 月 16 日，卡拉沃沃州 La Arenosa 发电站发生爆炸事故，导致本国西南部电力供应中断。”12 个州出现电力短缺。据消息，至少 1000 万名用户可能受到停电的影响。
- **2019 年 1 月 23 日，委内瑞拉议会主席、反对党人士瓜伊多在一场反对党支持者集会活动中自封为“临时总统”，要求重新举行总统大选，完成政府权力过渡。**
- **2019 年 1 月 23 日，委内瑞拉加拉加斯，委内瑞拉总统马杜罗对千名支持者说：“我已决定，将切断与美帝国主义政府的外交与政治关系。”**
- **2019 年 1 月 28 日，美国宣布对委内瑞拉国家石油公司——PDVSA 实施制裁，该公司无法出售石油至美国。**
- **2019 年 1 月 30 日，委内瑞拉最高法院 29 日宣布,决定对委议会主席、反对党人士瓜伊多采取限制措施。**
- 2019 年 3 月 7 日下午 5 时左右，包括首都加拉加斯在内的委内瑞拉全国发生大规模停电。多数地区的供水和通信网络受到影响。
- **2019 年 3 月 12 日，美国务卿蓬佩奥在社交网站“推特”上宣布，将从美国驻委内瑞拉使馆中撤出所有剩余美国外交人员。**