这张9月26日的卫星照片显示的是，丹麦附近海域的“北溪”天然气管道泄漏点。

水下爆炸、管道漏气……

“北溪”遭破坏 谁干的？

水下爆炸、管道漏气……俄罗斯通往欧洲的“北溪”两大天然气输送管道9月26日遭遇“蓄意破坏”，令欧洲和美国震惊。欧盟方面已呼吁就此展开调查。目前还没有信息表明，谁可能是幕后黑手。

过去几年，美国一直施压德国等欧洲国家停止“北溪-2”管道建设，同时向欧洲兜售成本较高的美国液化天然气。乌克兰局势升级后，德国等欧盟国家寻求降低对俄能源依赖，但短期内难以实现这一目标。

“极其罕见”

据丹麦和瑞典官方通报，“北溪-1”管道有两处泄漏点，位于丹麦博恩霍尔姆岛东北方向，分属于丹麦和瑞典海上专属经济区；“北溪-2”管道泄漏点在丹麦杜厄角以南。

丹麦能源署署长在新闻公报中说，天然气管道出现泄漏是极其罕见的。俄新社援引瑞典电视台消息还称，当天，“北溪”天然气管道气体泄漏的区域发生了两次水下爆炸。

英国《卫报》称，丹麦通过军事飞行拍下了泄漏处的现场图像，其中一张显示海面上出现了一片类似气体冒泡区域。

受泄漏事件影响，欧洲天然气价格27日上涨。路透社报道，当前天然气价格仍低于今年最高纪录，但相比去年同期已经翻了一倍。

谁是幕后黑手？

欧盟委员会主席冯德莱恩表示，泄漏是由于“破坏”，并称要对任何故意破坏欧洲能源基础设施的行为做出“最强烈的反应”。她敦促进行调查，以充分了解“事件及其原因”，但现阶段猜测漏气原因为时过早。

丹麦首相弗雷泽里克森27日晚说，根据丹麦相关机构的综合评估，“北溪”天然气管道泄漏是“蓄意行为”造成的，不可能是意外事故的结果。目前还没有信息表明谁可能是幕后黑手。

瑞典政府官员表示，有信息表明“北溪”天然气管道泄漏事件可能是“蓄意破坏”，但这并不是针对瑞典的袭击，瑞典政府正与北约等合作伙伴以及丹麦德国等保持密切联系。

德国经济部长哈贝克表示，泄漏是对基础设施的有针对性的攻击造成的，德方认为“泄漏不是由自然事件或物质疲劳引起的”。

路透社援引一名关注欧洲安全事务人士的话报道，要追查“北溪”管道泄漏原因，需要问“谁将因此获益”。

“对任何人都没好处”

对此，美国国务卿布林肯27日表示，初步报告表明，“北溪”天然气管道泄漏可能是袭击或某种破坏的结果，“但这都是初步报告，我们还没有证实，但若得到证实，那显然对任何人都没有好处。”

布林肯还称，在他看来，泄漏不会对欧洲能源供给产生重大影响，并重申美方正在努力解决欧洲短期和长期的能源安全问题。

波兰前外长西科尔斯基的态度则十分微妙。他在社交媒体上仅发了一张“北溪”管道所在水域发生水下爆炸后的海面图，并配文称“谢谢你，美国。”

波兰总理莫拉维茨基则表示，泄漏事件是一种“破坏行为”，“可能标志着乌克兰局势的升级”。

“对手失去理智了？”

俄罗斯总统新闻秘书佩斯科夫27日对媒体表示，“北溪”项目的紧急状态事关整个欧洲大陆的能源安全，俄方对此极为关切。“不排除管道事故是破坏活动所致。”

俄罗斯“北溪-1”项目运营方北溪天然气管道公司27日发布声明说，目前尚无法评估维修时间。

据俄罗斯卫星网报道，俄罗斯联邦委员会国际事务委员会第一副主席贾巴罗夫称，如果“北溪”管道的事故调查证实美国参与了爆炸，那“局势将从根本上发生变化”。“难道我们的对手完全失去理智了吗？”

俄罗斯国家能源安全基金副主任阿列克谢·格里瓦奇接受俄罗斯卫星通讯社记者采访时说：“谁在打击俄罗斯天然气在欧洲（的地位），这一点并没有被特别掩盖。”美国政治风险咨询公司欧亚集团说，不论乌克兰局势如何变化，泄漏事件意味着俄罗斯今年冬季无法经由“北溪”管道向欧洲供气。

“北溪-1”管道2011年建成，东起俄罗斯维堡，经由波罗的海海底通往德国。俄罗斯天然气工业股份公司9月2日说，由于发现多处设备故障，“北溪-1”将完全停止输气，直至故障排除。“北溪-2”管道去年建成，与“北溪-1”基本平行，但尚未投入使用。

德国《明镜》周刊27日报道，据不愿公开姓名的消息人士透露，美国中央情报局今夏曾提醒德国政府，“北溪-1”和“北溪-2”管道可能会遭到袭击。《明镜》就此向德国政府求证，一名政府发言人拒绝置评。

本报综合

偷刷“脸”卡 美国安局这样网攻西工大

美国国家安全局（NSA）对我国西北工业大学发起网络攻击事件，又有新的细节公开。

今年6月22日，西北工业大学发布公开声明称，该校遭受境外网络攻击，随后西安警方对此正式立案调查。中国国家计算机病毒应急处理中心和360公司联合组成技术团队全程参与了此案技术分析工作，并于9月5日发布了第一份西北工业大学遭受NSA网络攻击调查报告，调查报告指出此次网络攻击源头系NSA下属的特定入侵行动办公室（TAO）。

9月27日，技术团队再次发布相关网络攻击的调查报告。报告披露，TAO在对西北工业大学发起网络攻击过程中构建了对我国基础设施运营商核心数据网络远程访问的“合法”通道，实现了对我国基础设施的渗透控制。

怎么攻击？

单点突破逐步渗透长期窃密 TAO控制西工大多台服务器

此次调查报告显示，TAO对他国发起的网络攻击技战术针对性强，采取半自动化攻击流程，单点突破、逐步渗透、长期窃密。

360公司网络安全专家边亮说：“通过漏洞的方式批量对网络中的设备或者一段IP进行投漏洞、投病毒，从而获取相关的权限，这可以做到自动化。后续需要进行潜伏，进行长期控制，并且需要有针对性地去窃取相关文件。这个过程背后需要有人来操作，来指定到底去窃取什么、去做什么以及最后在撤退的时候需要销毁什么，属于半自动化。”

技术团队发现，TAO经过长期的精心准备，使用“酸狐狸”平台对西北工业大学内部主机和服务器实施中间人劫持攻击，部署“怒火喷射”远程控制武器，控制多台关键服务器。

国家计算机病毒应急处理中心高级工程师杜振华说：“进入到这些服务器后，它会对网络流量进行劫持，采用这种中间人攻击的方式，把其他的武器投送到西北工业大学内网的主机或者服务器上，投送成功之后，尤其是投送持久控制类武器之后，可以说获得了西北工业大学内网的访问权。在这个基础上，会对内网进行探测，去寻找高价值的服务器、高价值的主机，然后再向这些服务器和主机进行横向移动，成功进入之后，可以去部署嗅探窃密类武器。”

窃取什么？

TAO偷刷西工大的“脸” 渗透控制中国基础设施

报告显示，TAO通过窃取西北工业大学运维和技术人员远程业务管理的账号口令、操作记录以及系统日志等关键敏感数据，掌握了一批网络边界设备账号口令、业务设备访问权限、路由器等设备配置信息、FTP服务器文档资料信息。

360公司网络安全专家边亮说：“它控制了西北工大（相关设备）后，相当于利用西北工大再去对其他单位进行攻击，这个过程是一个打引号的合法。相当于我们数据库当中有类似于人脸识别这么一个防护机制。比如美国人来的话，直接给他拦住了，不让他进去，但是他刷了西工大的‘脸’，会认为他是一个正常的用户，那么，在网络数据中就对他放行了。但实际上西工大的相关服务器是被美国（TAO）所控制的，TAO随后进一步对其他单位进行攻击。”

技术团队根据TAO攻击链路、渗透方式、木马样本等特征，关联发现其非法攻击渗透中国境内的基础设施运营商，构建了对基础设施运营商核心数据网络远程访问的“合法”通道，实现了对中国基础设施的渗透控制。

报告显示，TAO通过掌握的中国基础设施运营商的思科PIX防火墙、天融信防火墙等设备的账号口令，以“合法”身份进入运营商网络，随后实施内网渗透拓展，分别控制相关运营商的服务质量监控系统和短信网关服务器，利用“魔法学校”等专门针对运营商设备的武器工具，查询了一批中国境内敏感身份人员，并将用户信息打包加密后经多级跳板回传至NSA总部。

据央视新闻

今日16版　地址：山东省淄博市柳泉路280号　邮编：255000　广告许可证：鲁工商广字3700004000144　零售每份1.00元
新闻热线及投诉电话：0533-3585000　发行征订电话：0533-3595671　广告订版电话：0533-2270969　鲁中晨报印务有限公司电话：0533-8409106