军事紧张事态一触即发

朝鲜8个炮兵旅团“射击待命”

央视总台记者当地时间13日获悉，朝鲜国防省发言人说，朝鲜人民军总参谋部已指示朝韩边境的部队进入射击准备态势。

朝鲜人民军总参下达作战预备指示

据CCTV国际时讯最新消息：朝鲜国防省发言人10月13日表示，“由于韩国对朝鲜首都平壤的挑衅行为，军事紧张事态一触即发。朝鲜人民军总参谋部已于10月12日发出作战预备指示，要求前线朝鲜人民军炮兵联合部队和承担重要火力任务的部队做好全面射击准备。如果确认韩方再次挑衅，必须立即对其予以打击，这可能会导致武装冲突扩大，各级单位必须做好充分准备，应对不同事态发展。”

朝鲜人民军总参谋部的作战预备指示指出，按照战时定员编制，将8个全副武装的炮兵旅团在当地时间10月13日20时之前转为“射击待命状态”，完成各项作战保障工作。总参谋部指示各级部队、区分队加强监视警戒，首都平壤市加强防空监视戒备。

朝鲜谴责韩国使用无人机渗透至平壤

朝鲜外务省10月11日晚发表声明，谴责载有反朝传单的韩国无人机侵犯朝鲜首都平壤领空，称此系严重犯罪行为。韩国国防部方面随即表示，韩军方没有向朝鲜发射无人机。韩国联合参谋本部相关人士表态称，需要确认无人机是否为韩国民间团体发射。

朝鲜劳动党中央委员会副部长金与正10月12日就此发表谈话，认为“韩国军方难以推卸作为重大主权侵害挑衅主犯或共犯的责任”。谈话说，“在他国首都空投传单本身就会被视为严重的政治挑衅和主权侵害，且运载传单的是无人机，这是此次事件严重性的核心所在。一国国民利用无人机做出侵害他国主权的行为，由此可能引发武装冲突危机，军方却对此袖手旁观，无异于有意默认和共谋行为。”谈话警告说，如果有韩国无人机运载反朝传单再次侵犯朝鲜领空，朝方将采取“强有力的报复应对行动”。

韩方回应朝鲜警告若构成威胁，朝鲜政权将终结

当地时间13日，针对朝鲜劳动党中央委员会副部长金与正做出的“如果在平壤上空再次发现韩国无人机，将发生惨痛的悲剧”的发言，韩国国防部表示，若对韩国国民安全造成危害，朝鲜政权将终结。

韩国国防部称，“最近一直在向韩国进行垃圾气球挑衅的朝鲜，企图恐吓韩国国民，是贼喊捉贼的行为”。

韩国国防部表示，“朝鲜至今已经侵犯过韩国领空10余次”。朝鲜无人机分别在2015年8月、2016年1月、2017年6月、2022年12月进入韩国领空。其中在2022年12月，一架朝鲜无人机还进入首尔龙山总统府一带的禁飞区。

据央视新闻

最新曝光的美网络武器设置了“嫁祸”功能

继4月15日和7月8日之后，国家计算机病毒应急处理中心等部门14日再度发布“伏特台风”调查报告，持续揭露美国政府机构实施的网络间谍和虚假信息行动，最新曝光的美网络武器设置了“嫁祸”功能。此次报告首次以中英法德日文多种语言发布。

国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室14日发布《伏特台风Ⅲ——揭秘美国政府机构实施的网络间谍和虚假信息行动》（以下简称“伏特台风”调查报告），进一步公开美国联邦政府、情报机构和“五眼联盟”国家针对中国和德国等其他国家及全球互联网用户联合实施网络间谍窃听窃密活动。

“今年4月和7月，我们连续两次发布‘伏特台风’调查报告后，先后有来自美国、欧洲、亚洲等国家和地区的50余位网络安全专家通过各种方式与我中心联系，认为美国和微软公司将‘伏特台风’与中国政府关联，缺乏有效证据，同时表达了对美国操弄‘伏特台风’虚假叙事的关切。”国家计算机病毒应急处理中心相关研究人员14日对《环球时报》记者表示。

美情报机构打造严禁透露给盟友的“秘密武器”

最新发布的报告公布了美国情报机构研发的网络武器——隐身“工具包”，代号“大理石”（Marble）。此前，中国国家计算机病毒应急处理中心已经连续公开披露了多款美国国家安全局（NSA）、中央情报局（CIA）开发的网络武器。

作为全球最大的军火供应商，美国拥有规模庞大的军事工业体系，由此形成的美国网络武器库不仅规模庞大、形式多样，而且功能复杂、产品丰富。最新披露的“大理石”工具包是一个工具框架，可以与其它网络武器开发项目集成，辅助网络武器开发者对程序代码中各种可识别特征进行“混淆”，有效“擦除”网络武器开发者的“指纹”，类似于改变了“枪械”武器的“膛线”，转移武器的指向，使调查人员无法从技术角度追溯武器的真实来源。

“长期以来，美国在网络空间积极推行‘防御前置’战略并实施‘前出狩猎’战术行动，也就是在对手国家周边地区部署网络战部队，对这些国家的网上目标进行抵近侦察和网络渗透。为适应这种战术需要，掩盖自身恶意网络攻击行为、嫁祸他国并误导溯源归因分析，美国情报机构专门研发了‘大理石’工具包。”上文中的研究人员表示。据介绍，该框架还设置了“嫁祸”功能，可以随意插入中文、俄文、朝鲜文、波斯文、阿拉伯文等六种外语字符串，其目的旨在误导调查人员，以此栽赃陷害中国、俄罗斯、朝鲜、伊朗以及众多阿拉伯国家。

美国国家安全局（NSA）建立运营的海底光缆监听站

研究人员依据“大理石”工具框架源代码及其注释分析发现，其被确定为一个机密级（且不可向国外透露）的武器研发计划，起始时间不晚于2015年。因此该计划是美国情报机构为自身量身打造的“秘密武器”，甚至严禁透露给所谓的“盟友”国家。

美在海底光缆建立监听站

报告依据美国国家安全局（NSA）的内部绝密级资料称，美国依托其在互联网布局建设中先天掌握的技术优势和地理位置优势，把持全球最重要的大西洋海底光缆和太平洋海底光缆等互联网“咽喉要道”，先后建立了7个国家级的全流量监听站，与美国联邦调查局（FBI）和英国国家网络安全中心（NCSC）紧密合作，对光缆中传输的全量数据深度开展协议解析和数据窃取，实现对全球互联网用户的无差别监听。

美国国家安全局并不满足于仅仅停留在海底光缆所覆盖的特定区域，而且这些监听系统所窃取的数据也远远不能满足其情报工作需要。因此，美国国家安全局对位于监听系统“盲区”的特定目标实施了网络秘密入侵行动（CNE）。

从美国国家安全局的绝密文件中可以看到，隶属于美国国家安全局的“特定入侵行动办公室”（TAO）在全球范围内发动无差别的网络秘密入侵行动，并植入了超过5万个间谍程序（Implants），受害目标主要集中在亚洲地区、东欧地区、非洲地区、中东地区和南美地区。“从美国国家安全局的内部文件中可以清楚看到，中国境内的主要城市几乎都在其网络秘密入侵行动范围内，大量的互联网资产已经遭到入侵。”报告披露称。

美国同盟国也摆脱不了被监听的命运

最新公开的报告还例举了美国情报机构对法国、德国、日本等国家实施的监听行为。

研究人员介绍称，为了建立了规模庞大的全球化互联网监听网络，向美国政府机构提供了大量高价值情报，使美国政府屡屡在外交、军事、经济、科技等领域占得先机，任何目标都有可能被列入“重点监控名单”。

在2004年至2012年期间，美国对法国实施了长期的间谍行动，监听对象包括前法国总统、法国财政部长、法国外交部长、法国参议员、法国财政和经济政策局官员、法国驻美国大使，以及直接负责欧盟贸易政策的官员等。监听内容涉及法国政府政策、外交、金融、国际交流、基础设施建设、商业和贸易活动等，其中一些重要情报被美国授权与“五眼联盟”伙伴国家共享，揭示了“五眼联盟”国家亦为美国间谍行动的获益者。

此外，美国把德国排除在“五眼联盟”之外，并划为第三等级的伙伴，既是利益伙伴，也是监视目标，充满了不信任。美国国家安全局长期对德国总理、外交部长、驻外大使和总领事等政府高级官员的通信内容进行监听，监听内容广泛，包括德国政府对国际形势和突发事件的看法，以及德国官员参与对美国际交流后的私下讨论，涉及政治、军事、经济、外交、政策、民族、安全、资源等重要领域。值得一提的是，美国情报部门对欧盟国家的内部考虑，特别是对防范金融风险的解决方案有着浓厚兴趣。

美打造“伏特台风”计划

报告认为，美国的全球互联网监听计划及其所建立的监听站就如同网络空间中无处不在的“窥探者”，实时监听窃取全球互联网的用户数据，这种监听能力也成为美国构建“黑客帝国”和“窃密帝国”不可或缺的基石。而要维持这样庞大的监听计划，每年需要的经费预算相当惊人，随着互联网数据的爆炸式增长，美国全球网络监听计划对经费的需求也必然是“水涨船高”。这就是美国联邦政府及其情报机构合谋策划、推动“伏特台风”计划的主要动力。

多年来，美国联邦政府机构出于一己私利，不断将网络攻击溯源问题政治化。此外，微软和CrowdStrike等公司为了迎合美国政客、政府机构和情报机构，出于提高自身商业利益的考虑，在缺乏足够证据和严谨技术分析的情况下，热衷于用各种各样稀奇古怪且带有明显地缘政治色彩的名字对黑客组织进行命名，如“台风”“熊猫”和“龙”等嫁祸中国。

报告呼吁，在地缘政治冲突不断加剧的今天，国际间正常的交流恰恰是网络安全行业最需要的，网络安全需要广泛的国际协作，广大网络安全企业和研究机构也应该专注于对网络安全威胁对抗技术的研究以及如何为用户提供更高质量的产品和服务，使互联网在促进人类社会共同发展进步中行稳致远。

据环球时报

传真：0551-65179655 办公室：0551-65179710 总编办：0551-65179615 融媒体新闻中心：0551-65179651
广告中心：0551-65179727 发行部：0551-65179700
国内统一刊号 CN34-0044 邮发代号 25-47 广告经营许可证：皖工商广字 014 号
社址：合肥市潜山路1469号 邮编：230071 印刷：新安传媒有限公司印务公司承印 今日印完时间 4:30