全球新冠疫苗接种总量超15亿剂

新华社华盛顿5月18日电美国约翰斯·霍普金斯大学统计数据显示，截至18日全球新冠疫苗接种总量已超过15亿剂。从接种人口比例来看，塞舌尔是全球新冠疫苗接种率最高的国家，全国63.13%的人口已完成接种。

其他已完成接种人口比例较高的国家包括以色列、圣马力诺、智利、阿拉伯联合酋长国、巴林等。

该校最新疫情统计数据显示，截至18日全球累计确诊163952478例，累计死亡3399194例。美国仍是全球累计确诊和死亡病例最多的国家，分别为32996675例和587198例。

另据法新社使用各国官方数据进行的统计显示，截至北京时间18日23时30分，全球210个国家或地区总计接种1500017337剂新冠疫苗。接种剂量居前三位的国家分别为中国、美国和印度，三国接种总剂数约占全球接种总量的近60%。欧盟27个成员国接种总量超过2亿剂，已接种至少一剂的人口比例约32%。

据法新社统计，自去年12月一些国家陆续启动新冠疫苗接种以来，全球疫苗接种呈加速态势：全球接种总剂数超过5亿剂历时约4个月，从5亿剂增至10亿剂历时不到一个月，从10亿剂增至15亿剂历时仅3个星期。

印度单日新冠死亡病例超4500例

创全球新高

据新华社新德里5月19日电（记者赵旭）印度卫生部19日公布的数据显示，过去24小时该国新增新冠确诊病例267334例，累计确诊25496330例；新增死亡病例4529例，创该国疫情暴发以来单日死亡病例数新高，这也是目前全球范围内单日死亡病例数最高纪录，累计死亡283248例。

近日印度疫情数字呈现分化趋势。自17日开始，印度单日新增确诊病例连续3天降至30万例以下，但单日死亡病例数却不断升高，3天内连续突破4100例、4300例和4500例。

《印度斯坦时报》在19日的报道中指出，过去24小时印度单日死亡病例数超过了今年1月20日美国创下的4400例的全球纪录。《印度时报》当天还援引印度官方数据称，过去一周里该国仅15日报告的死亡病例数低于4000例。

勒索软件攻击频发

网络空间治理亟须合作

美国科洛尼尔管道运输公司遭网络勒索，一条输油干线被迫关停。爱尔兰卫生服务执行局网络遭“重大勒索软件攻击”，全国多家医院的电子系统和存储信息无法进入……近日，全球接连发生多起勒索软件攻击案件。

专家认为，随着关键基础设施的数字化程度不断提高，针对关键基础设施的勒索攻击不断增多，攻击模式也发展出一些新特点。网络安全是全球性挑战，没有哪个国家能置身事外，维护网络安全也是国际社会的共同责任。各国需就打击网络犯罪增加互信，加强应急响应协作，共同维护安全、清朗的网络空间。

A 网络勒索快速增长

勒索软件是一类木马病毒，常见的有Maze、WannaCry、Ryuk等，一般伪装成普通应用软件、程序更新补丁或电子邮件附带的文件、链接等。这些向受害者发送的恶意程序或链接一旦被打开，黑客就可以将勒索软件植入计算机系统，通过骚扰、恐吓甚至绑架用户文件等方式，使受害者的数据资产或计算资源无法正常使用，并以此勒索赎金。

据美国媒体报道，本月6日的攻击中，黑客采取了“双重勒索”策略，在2小时内从科洛尼尔管道运输公司计算机网络中窃取了近100千兆字节数据并将其加密，要解锁被窃信息就必须付赎金，如不接受勒索，黑客还威胁在网上公布这些信息。美国联邦调查局称，一个名为“黑暗面”的网络犯罪团伙是幕后黑手。

爱尔兰公共支出与改革部负责政府电子政务的国务部长奥西安·史密斯14日对媒体表示，当天对爱尔兰卫生服务执行局网络系统的攻击也许是该国遭受的迄今最严重的网络攻击。攻击者来自国外网络犯罪团伙，其目的也是为了钱。

这两起网络勒索的共同点是面向关键基础设施，严重威胁社会秩序。根据美国网络安全与基础设施安全局定义，关键基础设施指对经济运行、公共卫生和国家安全至关重要的资产、系统和网络，包括能源、金融服务、食品和农业等十多个领域。

美国坦普尔大学发起的“关键基础设施勒索软件攻击”数据库追踪项目显示，最近几年全球针对关键基础设施的网络勒索呈快速增长态势。该数据库分析结果显示，2019年至2020年针对关键基础设施的网络勒索大幅增长，占过去7年多此类案件报告总数的一半以上，其中政府设施、医疗设施和教育部门遭网络勒索的频次排前三位。

对这一现象背后的成因，美国“一号哨兵”网络安全公司发文认为，关键基础设施领域的许多组织是公共投资，往往缺乏大型私营企业的预算和专业资源，使其面对网络勒索时更加脆弱。

中国全国政协委员、安天科技集团首席技术架构师肖新光对新华社记者表示，基础设施的信息化水平不断提升，可攻击面持续扩大，对应的数字资产的价值也同步提升，对攻击者的诱惑力增强，这些因素都增加了被攻击风险。他还指出，要特别警惕黑客将对基础设施的破坏性攻击隐藏在网络勒索中的情况。一个典型案例是，2017年乌克兰遭遇伪装成网络勒索的破坏性攻击，其真实目的是破坏乌克兰信息系统运行。

B 防范威胁亟须合作

多家媒体报道，攻击科洛尼尔管道运输公司的“黑暗面”主要采取被称为“勒索软件即服务”的作案模式：它向其附属组织提供勒索软件和相关设施，并从附属组织获得的赎金中抽成。

肖新光介绍，勒索软件也在演化。较早的主流勒索软件是非定向传播的，带有数据加密和删除功能的蠕虫病毒依靠网络或U盘大面积感染计算机，但勒索赎金额度较低。此后勒索攻击与高级持续性威胁攻击相结合，演化出针对高价值目标的定向勒索，并形成勒索“产业链”，上游团伙编写勒索软件并提供设施，下游团伙则负责攻击投放，上下游收益分成。

由于网络勒索多为跨国、跨境作案并具有在网络空间难以追踪等特性，取证和执法面临诸多障碍。这凸显了构建网络空间治理体系、健全打击网络犯罪司法协助机制的必要性。

美国约翰斯·霍普金斯大学兼职网络安全讲师特里·汤普森近日在“对话”网站发表观点文章说，美国国家网络防御是一个没有明确解决方案或成功衡量标准的政策问题，难点包括脆弱的软件供应链存在安全隐患、政府部门在网络安全领域权力分散、有组织网络犯罪和情报活动之间界限模糊以及政府在软件和网络安全技能方面存在不足等。

欧洲刑警组织每年发布的“互联网有组织犯罪威胁评估”报告就最新网络犯罪形势提出应对措施。去年10月发布的新版报告指出，为了更有效应对网络犯罪挑战，应通过公共部门和私人伙伴之间的协调与合作加强信息共享，增强防范意识和防御能力建设，同时让欧洲刑警组织网络犯罪联合行动特别小组等多边协作机制继续在当前网络犯罪领域发挥关键作用等。

肖新光认为，应对勒索软件威胁的关键是做好事前防御，政府应引导关键基础设施运营方进行有效防御能力建设。在国际层面，各国应就打击国际化网络犯罪增强互信，加强应急响应协作和信息共享。

（据新华社北京5月18日电）