外交部回应七国集团峰会涉港声明：

莫再居心叵测多管闲事图谋不轨

□据新华社报道

外交部发言人耿爽昨天在谈到七国集团峰会涉港声明时说，香港事务纯属中国内政，任何外国政府、组织和个人都无权干预。七国集团成员不要再居心叵测、多管闲事、图谋不轨。

当日例行记者会上，有记者问：据报道，七国集团峰会发表领导人声明，其中重申《中英联合声明》的存续性和重要性，呼吁避免暴力。中方对此有何评论？

“我们对七国集团峰会领导人声明对香港事务说三道四、指手画脚表示强烈不满和坚决反对。”耿爽说，“我们多次强调，香港事务纯属中国内政，任何外国政府、组织和个人都无权干预。”

耿爽说，发生在香港的游行示威和暴力活动已经持续了两个多月，香港的法治、社会秩序、经济民生和国际形象受到了严重冲击。没有人比包括香港市民在内的中国人民更关心香港的繁荣稳定。

“我们自己的事情，我们会处理好。请七国集团成员不要再居心叵测、多管闲事、图谋不轨。”他说。

耿爽指出，《中英联合声明》的终极目的和核心内容是确定中国收回香港，对香港恢复行使主权。随着香港回归祖国，中国政府依照宪法和基本法对香港实行管治。根据国际法和国际关系基本准则，任何国家和组织无权假借《中英联合声明》干涉香港事务。

针对持续多日暴力和混乱，香港法律专家指出——

特区政府有多项法律手段止暴制乱 应加快检控

□据新华社报道

针对香港持续多日的暴力和混乱局面，多名法律专家表示，香港现有法律赋予特区政府诸多可有效止暴制乱的法律手段，希望相关机构严格依法行使职权并加快对涉事者的检控，真正彰显法治。

香港城市大学法律系副教授、特区立法会议员梁美芬介绍，香港特区的《公安条例》《警队条例》等法律，实际上都赋予特区政府有效制止乱局的法律手段。

《公安条例》在对集会、游行及聚集的管制，非法集结、暴动及相类罪行，虚假消息及炸弹吓诈行为，对场所、船只、攻击性武器等的管制等方面均有详细规定。梁美芬说，参照《公安条例》规定，一些暴力和破坏行为已牵涉非法集结、暴动及相关罪行，如拆卸或破坏建筑物、阻止铁路列车开行、强行进入、强占处所、在公众地方打斗、在公众聚集中倡议使用暴力等。

她强调，香港是个法治社会，香港的法律对哪些行为属于违法行为，有明确细致的规定。“实际上，根据香港的法律，任何人未经批准在行车马路上行走就已经犯法。”她说，在最近一些未经批准的游行示威中，有人霸占马路、阻塞隧道，甚至破坏公共设施、威胁他人安全，均已触犯相关罪刑。

就执法而言，《警队条例》对警务人员在执法过程中的权力有明确规定。梁美芬说，参照这些规定可见，私人屋邨、地铁站、商场等场所拒绝警方进入、阻碍警方抓捕暴力破坏者的做法，并不合理合法。

梁美芬强调，香港有足够的法律，应该严格执行这些法律，不能纵容违法者。

她说，警务人员在近期持续的乱局中承受巨大压力。必要时可根据《警队条例》相关规定雇用临时警务人员，增加执法人手。

港区全国人大代表、香港中小型律师行协会创会会长陈曼琪表示，要阻止公众集会和游行期间的暴力行为，警方可根据《公安条例》第 17 条对集会和游行等活动加强规管。

她说：“警方如果认为一些示威集会会危害公共安全和社会安宁，可以立即停止这些示威集会。这是警方的权力，合适的情况下就要无畏无惧地使用。”

多名法律专家建议，过去一段时间机场、地铁、过海隧道等地都有违法暴力行为发生，危害公共交通。类似情况下，政府可以考虑需要时主动采取措施，申请临时禁制令。

香港的法律也赋予特区行政长官有效处理紧急情况的权力。行政长官会同行政会议有权根据《公安条例》第 17E 条禁止在某些地方公众聚集。行政长官还可根据《公安条例》第 31 条发出宵禁令，或根据第 36 条宣布某些地区或地方为禁区。

此外，《紧急情况规例条例》授予行政长官会同行政会议在紧急或危害公安的情况时订立规例的权力。

多名法律专家指出，面对眼下乱局，特区政府应该有全盘计划，把所有可行的法律手段都放在考虑范围之内，当然考虑到宵禁令、设立禁区等措施均属比较强烈的措施，应谨慎使用。

香港城市大学法律学院前副院长顾敏康表示，实施宵禁、戒严等措施在香港有法律依据，也并非没有先例，但这些措施对香港的营商环境和国际形象有很大影响。现阶段而言，止暴制乱关键在于严格执行现有法律，尽快拘捕违法者，并及时起诉。

陈曼琪表示，要尽快制止暴力破坏行径，首先要加快拘捕及起诉涉事者，“如果只抓不起诉的话，别有用心的人会继续煽动别人违法”。此外，不能只抓捕被煽动的年轻人，更要惩处背后的头目。“如果只抓‘小鱼’不抓头目，这些有计划的暴力行径也不会停止。”

梁美芬指出，近期违法者众多，检控工作面临繁重压力。在这种情况下，香港可参照其他地方设立“特别法庭”的做法，由熟悉此类案件的法官专职处理，加快检控进程。

她表示，面对暴力乱局，特区政府有多项法律手段可用。而除了使用法律手段外，还需要做大量沟通工作，在不同背景和立场的人士之间寻求共识，共同恢复社会秩序。

公安部发布 A 级通缉令

公开通缉第二批 50 名重大在逃人员

□据新华社报道

公安部昨天发布 A 级通缉令，公开通缉第二批 50 名重大在逃人员。该 50 名重大在逃人员主要涉嫌故意杀人、绑架、非法制造爆炸物、电信网络诈骗、非法吸收公众存款和组织、领导、参加黑社会性质组织等犯罪。

据了解，自 6 月 13 日全国公安机关“云剑”行动开展以来，全国共抓获在逃人员 10.8 万余名，比去年同期增长 40%。特别是公安部 7 月 24 日召开新闻发布会，发布 A 级通缉令公开通缉 50 名重大在逃人员，并公布“两高一部”关于敦促在逃人员投案自首的通告后，全国公安机关严密查缉布控，全力侦查抓捕，社会各界广泛参与，迅速形成了全警追逃、全民追逃的强大声势和浓厚氛围，取得显著成效。截至目前，第一批公开通缉的 50 名重大在逃人员已到案 28 名，其中根据群众举报抓获 3 名，主动投案 8 名，公安机关组织侦查抓获 17 名。

公安部有关负责人表示，下一步，公安机关将不断加大追逃力度，力争尽快将通缉的在逃人员全部抓获归案。公安机关希望社会各界和广大群众继续支持追逃工作，积极举报线索，协助抓捕犯罪嫌疑人。对提供有效线索，为抓捕工作发挥关键作用的人员，每抓获其中 1 人，公安部将给予人民币 10 万元奖励。公安机关承诺，对举报人信息严格保密。同时，公安机关再次敦促在逃人员抓住机会，主动投案自首。对主动投案，如实供述自己罪行的，公安机关将会同检察机关、审判机关严格落实“两高一部”关于敦促在逃人员投案自首的通告，依法予以从宽处理；对执迷不悟、顽抗到底的，将坚决依法严惩。

对个人隐私不敏感？越来越多机构和企业说不！

□据新华社“新华视点”报道

曾引起广泛关注的“隐私与效率”之争，正逐渐形成共识：越来越多的机构与企业对公民隐私保护更加重视。

8 月 21 日至 23 日召开的 2019 北京互联网安全大会公布的一组数据显示，网络安全产业规模迅速扩大，企业级终端安全软件装机量破亿；过去一年间，网络安全人才的需求猛增 3 倍。

政企安全防护升级 人才需求一年增长 3 倍

与会的赛迪智库网络安全研究所所长刘权指出，近年来，各行业更加重视网络安全和信息保护，网络安全产业得到前所未有的发展。

在政府层面，越来越多的政府使用了网络安全运营平台。大会发布的《2019 大中型政企机构网络安全建设发展趋势研究报告》显示，48.5%的部委机关和 56.3%的中央企业已经部署使用了安全运营中心。安全事件的平均响应时间从 3 年前的平均 3 天左右，降低到现在 1 小时以内。

在企业层面，普遍加强了防火墙建设。上述报告显示，企业级终端安全软件装机量快速增长。2019 年上半年，装机量已达 1.05 亿台，远远高于 2016 年的 6189 万台。越来越多的企业引入源代码安全审计，这一工作可节约 5%至 20%的后期安全维护费用，减少 10%至 50%的系统安全漏洞，大大降低了隐私泄露风险。

与此同时，网络威胁情报逐步成为企业安全防御标配。报告指出，超过 80%的受访者认为威胁情报提升了安全能力。

在政府和企业的共同努力下，网络安全建设成效明显。系统安全漏洞修复平均周期已从 2016 年的 35 天下降到现在的 16 天。

人才需求猛增，印证了网络安全产业发展之快。根据大会上智联招聘的网络安全人才大数据显示，2019 年 6 月网络安全人才市场需求的规模达到 2016 年 1 月需求的 24.6 倍，相比 2018 年 7 月增长了 3 倍。

个人信息买卖异常猖獗 警惕隐私数据泄露三大渠道

隐私数据是通过哪些渠道泄露的？与会的网络安全专家、中国工程院院士邬贺铨表示，一方面，一些互联网公司的 App 越权收集用户信息，侵犯了个人隐私权；另一方面，一些合法利用用户个人信息的公司，没有做好信息保护工作，导致个人信息大量泄露。

个人隐私泄露究竟有多猖獗？记者做了一个小测试。在搜索引擎键入“个人信息买卖”“私家侦探”等关键词，就能看到不少关于信息贩卖的内容。记者找到一家私家侦探公司，客服人员表示，只要记者给出手机号和身份证号，他可以在 5 天内查到该号码的通话记录和 2 年内开房记录，开房记录查询价为 4200 元。

这只是公民信息泄露乱象的冰山一角。参加大会的奇安信行业安全研究中心主任裴智勇表示，除了部分网络公司越权收集用户数据，网络攻击、内鬼窃取、工作人员操作失误是个人信息泄露最主要的三大原因。

首先，网络漏洞被黑客攻击，隐私信息批量流出。去年 6 月，视频播放网站 A 站自曝遭遇黑客攻击，数据库近千万条用户数据泄露。

国家互联网应急中心近日公布的《2019 年上半年我国互联网网络安全态势》显示，今年初，在我国境内大量使用的 MongoDB、Elasticsearch 数据库存在严重安全漏洞，访问者无需权限验证即可通过默认端口本地或远程访问数据库并进行任意增、删、改、查等操作，信息泄露风险严峻。

其次，在高额利益引诱下，部分机构内部人员非法获取公司数据贩卖。2017 年，四川警方侦破一起新生婴儿信息倒卖案，发现是某社区卫生服务中心工作人员徐某利用职务之便，掌握该市妇幼信息管理系统市级权限账号密码，非法下载新生婴儿数据 50 余万条，贩卖数万条。

第三，由于企业工作人员缺乏安全和风险评估能力，导致错误操作引起信息泄露。

误发送邮件、权限设置错误和服务器配置不当等误操作都可能导致数据泄露。奇安信针对 2018 年全球重大数据泄露事件进行统计分析后发现，11.1%的事件是由于配置错误或操作不当导致的。奇安信就曾发现某健康 App 的服务器没有设置密码，任何人都能够查看登录者状况和发送的消息内容。

严厉打击数据黑产 夯实数据管理法律基础

公民隐私被严重侵犯以及多行业个人信息数据非法暴露在互联网中，反映了我国数据安全管理仍存在薄弱环节。业内人士表示，打击数据黑产，重在企业自身“强身健体”，同时还要健全法制保障，并建立各部门协同治理的机制。

政企机构应进一步加强网络安全防护能力。邬贺铨表示，仍有大量企业缺乏安全观念，内外网不隔离、员工私自登录高危网站、忽视漏洞检测与修复等，将机构暴露在黑客攻击目标之中。“黑客容易上手，很大程度上是由于企业安全意识不强导致的安全能力欠缺。”邬贺铨说。

其次，应加强源头端数据权限管理。针对学校、政府机关、快递公司、电商等信息泄露高发领域，应建立有效的数据管理机制，将系统权限和数据获取记录集中管理，并增加预警。

思科安全业务集团首席技术官表示，网络服务牵涉太多环节，包括云服务、应用、数据库等，必须建立有协同的架构体系才能提升网络安全，应对充满不确定性的威胁。

此外，尽快夯实数据管理的法律基础。与会的中国通信学会网络空间安全战略与法律委员会副主任敬云川表示，值得期待的是，个人信息保护法和数据安全法都已列入立法规划。他建议，未来法律对数据的属性、数据持有者的权利、义务应作出进一步详细规定，并平衡市场发展与个人信息保护的关系。