“新基建”时代的网络安全与 APT 攻击

360 企业安全集团

2020 年 3 月

摘　要

“新基建”热潮持续升温已成为各界关注焦点，对于目前深受疫情影响的中国来说，“新基建”是应对疫情和经济下行最简单且最有效的手段，兼顾供给和需求。但是在我们大力投身“新基建”建设和发展的同时，也不能忽视因此而产生的更加复杂的网络安全挑战，特别是 APT 攻击。

- “新基建”是“新型基础设施建设”的简称，具体范围包括了 7 大领域，分别是：5G 基建、特高压、城际高速铁路和城市轨道交通、新能源汽车充电桩、大数据中心、人工智能和工业互联网；
- “新基建”对于国民产生的影响主要可以分为以 5G 为代表进行科技创新、产业升级为核心领域的配套基础设施建设和以旧基建为基础的“补短板”建设两个方面；
- “新基建”进程的突然提速同时伴随着机遇与挑战，发展和安全是一体两翼。随着新型基础设施建设和应用的开展，相关业务安全风险、应用场景安全风险和关键技术安全风险也正逐渐浮出水面。
- 回顾整个 2019 年，无论是 APT 组织数量，还是 APT 攻击频率，相比往年都有较大的增长，APT 攻击正逐渐呈现出常态化、高频率的特性。
- 目前网络空间已成为国家安全角力的主战场。“新基建”时代不仅给信息安全带来了安全的问题，也为信息安全技术的发展提供了新的发展机遇。未来，“360 安全大脑”将持续致力于防护针对“新基建”的 APT 攻击，为“新基建”的安全建设保驾护航。

目　录

前言

2020 年 1 月突如其来的新冠肺炎席卷了神州大地，我国大部分行业均受到了不同程度的影响。疫情的冲击叠加上经济下行压力的持续增加让我国的宏观政策更加趋向于“稳增长”的发展方向。

一般来说，如果想要对冲疫情影响、努力实现经济发展的预期目标，就离不开基建的托底和拉动作用。特殊时期在基建方面进行发力，既是国内外行之有效的经济实践，也符合经济运行的客观规律。

近日来“新基建”一词横空而出，受到了各大专家的关注和认可，升温的速度超乎想象。从时间节点来看，在 20 天的时间内中央级别的政府会议 4 次直接或间接提及“新基建”，频率可谓史无前例。

表 1 “新基建”概念会议提及梳理

3 月 4 日	• 中央政治局常务委员会会议：要加大公共卫生服务、应急物资保障领域投入，加快 5G 网络、数据中心等新型基础设施建设进度。要注重调动民间投资积极性。
2 月 23 日	• 中央统筹推进新冠肺炎疫情防控和经济社会发展工作部署会议：一些传统行业受冲击较大，而智能制造、无人配送、在线消费、医疗健康等新兴产业展现出强大成长潜力。要以此为契机，改造提升传统产业，培育壮大新兴产业。
2 月 21 日	• 中央政治局会议：加大试剂、药品、疫苗研发支持力度，推动生物医药、医疗设备、5G 网络、工业互联网等加快发展。
2 月 14 日	• 中央全面深化改革委员会第十二次会议：基础设施是经济社会发展的重要支撑，要以整体优化、协同融合为导向，打造集约高效、经济适用、智能绿色、安全可靠的现代化基础设施体系。

那么受到大家如此热捧的“新基建”到底是什么，将带来什么影响，与的“旧基建”又有何区别，“新基建”时代下的网络安全面临的最大挑战是什么？下文将详细论述。

“新基建”是什么?

所谓的“新基建”是“新型基础设施建设”的简称，早在 2018 年 12 月的中央经济工作会议中就已经被首次提出。会议中强调要加快 5G 商用步伐、推动发展人工智能、工业互联网、物联网等；2019 年 3 月政府工作报告又进一步指出“应加强新一代信息基础设施建设”，年末的中央经济工作会议也强调要“稳步推进通信网络建设”。

随着数字技术与网络技术的深入融合，以大数据、人工智能、物联网等新一代信息技术产业化应用为标志的数字经济，迫切需要一套完整的数字化基础设施作为支撑。相较于传统基建，聚焦于高质量发展的新型基础设施建设无疑更加适用于先进的科技脚步。

与俗称“铁公基”的铁路、公路、机场等传统基础设施建设相比，“新基建”主要指以 5G、人工智能、工业互联网、物联网为代表的新型基础设施建设，其本质是信息数字化的基础设施建设，具体范围主要包括了 7 大领域，分别是：5G 基建、特高压、城际高速铁路和城市轨道交通、新能源汽车充电桩、大数据中心、人工智能和工业互联网。

表 2 “新基建”7 大细分领域及其应用[①]

	领域	应用
“新基建”	5G 基建	车联网、物联网、工业互联网、企业上云、人工智能、远程医疗等
	特高压	电力等能源行业
	城际高速铁路和城市轨道交通	交通行业
	新能源汽车充电桩	新能源汽车
	大数据中心	金融领域、安防领域、能源领域、业务领域、以及个人生活等方面

[①]彭昭 物联网智库.深度分析““新基建””，5G、工业互联网 IIoT、物联网 IoT 发展逻辑梳理[EB/OL].https://mp.weixin.qq.com/s/qz_BUSSrwdQJRBWUODbzQQ,2020-3-8.

	人工智能	智能家居、服务机器人、移动设备、自动驾驶、其他行业应用
	工业互联网	企业内的智能化生产，企业和企业之间的网络化协同，企业和用户的个性化定制，企业与产品的服务化延伸

从细分领域来看，领域分处于不同的层次。进一步拆解后可划分为以下几个层面[②]：

1. 最内核是为数字、信息经济支柱提供基础设施：即 5G、大数据、人工智能、云计算、物联网、区块链等，如 5G 基站、IDC 数据中心等;
2. 第二层次是电子化、智能化改造现有城市的传统基建设施，如智慧城市、智慧交通等项目;
3. 第三层次是在城市中发展新能源、新材料的配套应用设施，例如为新能源产业提供支持的充电桩、光伏、垃圾发电等;
4. 第四层次也是最外层，属于补短板基建，如科技园区开发、连接城市群内部的城际高速铁、轻轨等。

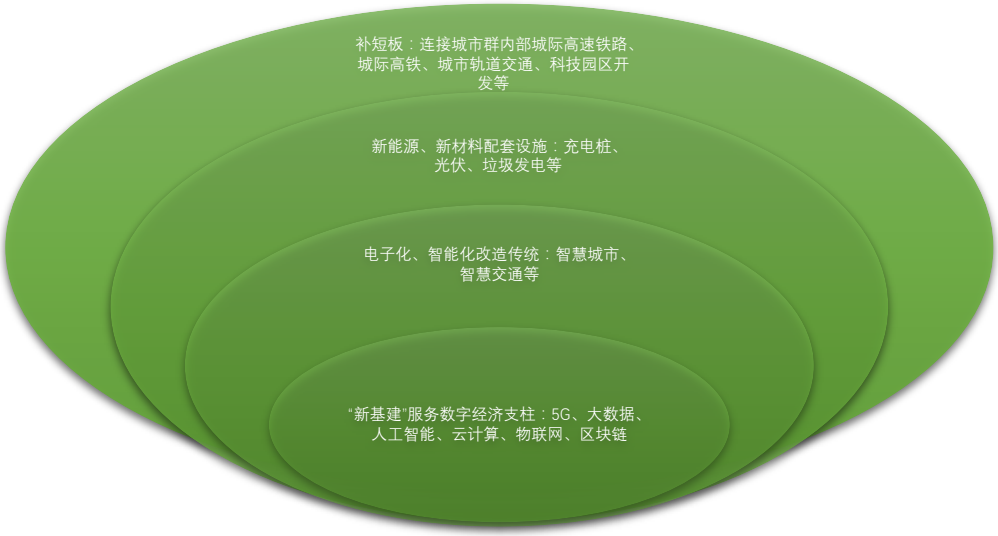

图 1 “新基建”领域层次细分

整体来说，“新基建”可以理解为对传统基建的扩展，兼顾了稳增长和促创新的双重任务。随着政府的

② 花长春,张捷.新版“4 万亿”?”新基建”?29 省(市)两会的线索 —— 全国“两会”前瞻系列(一)[R].北京:国泰君安证券,2020.

愈加重视，人工智能、工业互联网、物联网等新型基础设施建设将带动通讯、计算机和电子等相关行业的产品需求。新型基础设施不仅是制造业转型升级的关键也必将能激发更多的新增需求。

“新基建”对我们有何影响?

随着疫情的爆发以及“新基建”的持续升温势必会对目前的生活模式产生极大的影响，线上需求集中释放，受人员隔离影响，疫情期间居民线上娱乐、远程办公、在线教育等流量行业快速发展，无人配送等新型行业的需求也在逐步释放，同时在疫情发酵的背景下，互联网公司的大数据技术也得以在“数字防控”中大施拳脚。考虑到上述行业均离不开云计算、大数据的支持，对于以信息化、智能化为导向的“新基建”而言，当前的环境为其提供了良好的发展窗口；同时“新基建”的快速发展也将进一步促进科技水平的进步以及商业模式和消费习惯的转变，并形成“基建——产业”的良性互动。

从目前的发展来看，“新基建”对于国民产生的影响主要可以分为以下两个方面：

一是以 5G 为代表的，以科技创新、产业升级为核心领域的配套基础设施建设，总体上涵盖了 5G 基站建设、云计算、工业互联网、大数据、互联网数据中心、物联网等几大门类。其中 5G 毫无疑问成为了“新基建”的重要抓手。未来 7 年间我国拟建设 600 万个 5G 基站，并在此基础上加快 5G 商用步伐，特别是独立组网建设步伐，推动 5G+工业互联网融合应用，深化 5G 与工业、医疗、教育、车联网等垂直行业的融合发展。

二是所谓的“补短板”领域，与传统基建相似，基建补短板也将会对轨道交通、教育医疗、金融、公共设施等行业产生直接拉动作用，并间接促进工程机械、水泥建材等行业。由于“新基建”也包括补齐交通运输、农村基础设施和公共服务设施建设等短板，因此随着“新基建”的持续开展，轨道交通（主要以城际、高铁为主）、医疗养老（医院、养老院、福利院等医养结合项目）、旧改、文体（文旅产业、小区体育场）等行业也将迎来一定的发展机会，同时伴随着产业链的传导，建筑业、工程机械、水泥建材等上游行业也将迎来新一波发展机遇。

以 5G 为代表的“促创新”

5G、大数据、人工智能、工业互联网等狭义“新基建”将直接促进相关行业的发展，同时电子信息设备制造业、信息传输服务业、软件信息技术服务业等行业也将有所受益。与传统基建不同的是，狭义“新基建”的关键在于促进传统产业向数字化、网络化、智能化转型，因此“新基建”一方面将带动基建自身的几大领域（如 5G、特高压、大数据、人工只能、工业互联网），同时也会带动产业链上下游以及各行业的投资应用，如电子信息设备制造业、信息传输服务业、软件信息技术服务业等行业均有望获益。此外，随着工业互联网的持续推进，工业企业内部也有望迎来网络化、信息化改造，后续工业企业的生产效率也将迎来进一步提高。

1、5G 基建进入快进模式

2020 年是我国进入 5G 规模商用的重要时期，“新基建”政策的发布将加快我国 5G 建设的步伐，加速 5G 普及。中国联通网络技术研究院首席科学家唐雄燕认为，5G 建设将是“新基建”最重要的任务，也是我国信息通信业创新发展的战略支点。5G“新基建”对于推动产业升级至关重要，未来 5G 建设规模有望加速扩张，对产业链发展有积极促进作用，将利好 5G 基站、5G 传输、5G 核心网、5G 芯片等生产制造环境。中国信通院辛勇飞表示，预计 2020-2025 年，5G 可直接拉动电信运营商网络投资 1.1 万亿元，拉动垂直行业网络和设备投资 0.47 万亿元。另一方面，“新基建”有助于扩大和升级信息消费。预计 2020-2025 年，5G 商用将带动 1.8 万亿元的移动数据流量消费、2 万亿的信息服务消费和 4.3 万亿元的终端消费[3]。

2、云数据中心将加速增长

“新基建”政策的实施对于数据中心的发展也起到了明显的推动作用。国家的“新基建”政策将带动数据中心基础设施的进一步投资和发展，服务器、存储等计算设备以及云计算软件等平台软件的投入有望加

[3] 卓源科技. “新基建”风口已来：5G、AI、大数据发展升级？[EB/OL]. https://baijiahao.baidu.com/s?id=1660760150497875893&wfr=spider&for=pc,2020-3-10.

大，对于整个产业都是一个重大的利好消息。

从目前数据来看，截止 2019 年三季度，全球共有 504 个超大规模数据中心，这些数据中心按照最保守估计——每个容纳 5 万台服务器计算，整体可容纳服务器超过 2500 万台，而全球服务器年销量不足 1300 万台，另外还有 151 个超大规模数据中心在计划或者建设中，也就说未来市场销售的大部分服务器将会被部署在超大规模数据中心。根据 IDC 数据显示，在 2019 年全球企业和政府用于云基础架构的投资正式超过传统的非云 IT 基础架构的支出，过去几年全球 IT 基础市场的增长主要来自创新应用。

未来国家的“新基建”投资也将保持这一特点，主要集中于云服务器等创新产品的采购，加快服务器等 IT 基础设施市场结构的调整，实现产业的升级换代。

3、人工智能突破发展瓶颈

从国务院正式印发人工智能发展规划以来，已有接近 30 个地方政府发布各自的人工智能规划，并逐渐推动公共安全与服务领域率先落地。从企业层面来看，国内外已有包括谷歌、微软、阿里、百度、腾讯、浪潮等在内的众多科技巨头宣布将人工智能提升至战略高度。随着算力、算法和数据发展的不断成熟，将助力人工智能突破发展瓶颈。

从人工智能的产业发展角度看：芯片、服务器、云计算等人工智能基础设施已经初具规模；机器学习、计算机视觉、语音及自然语言处理等人工智能算法迭代优化正在不断加快；人工智能的场景化、产业化应用，与实体经济的融合将成为下一阶段发展的重点。

“新基建”的提出无疑给产业 AI 化的发展注入了“催化剂”，将极大促进人工智能基础设施、算法、产业应用的协同发展。虽然此次疫情对经济产生了一定程度的冲击，但数字经济的损失在相比之下就显得有些微不足道。很多此前在数据中心、人工智能计算力方面投资的企业已经获得红利。在线教育、在线办公、互联网电商等领域的很多业务也获得了十几倍甚至几十倍的增长。人工智能在此次疫情防控中发挥了极大的应用价值，数据中心、人工智能等“新基建”在现实中已经显现出了巨大的价值。

未来，人工智能将在此基础上努力打造良性的 AI 产业生态链，并有望在自动驾驶、AI 教育、AI 医疗等

方向的发展中进行持续创新。

以旧基建为基础的“补短板”

1、稳增长逻辑下，城际高铁、城际轨道有望“公交化”

从 2008 年京津城际铁路开通以来，我国城际高铁、城际轨道交通建设遍地开花，这背后显示出了我国城市群布局和架构的日益完善。目前，全国已经形成包括京津冀、珠三角、长三角在内的 20 多个城市群。城际轨道交通的出现把城市和城市群之间进行了连接，起到了通勤、公交化运营的作用。目前国家大力发展城市群的概念，强化都市圈层面的一小时通勤，在此背景下城际轨道交通和城际铁路也就成为了一个重要的组成单元。

目前城市轨道交通已成为我国基建重点。截至 2018 年底，我国（不含港澳台）共有 35 个城市开通城市轨道交通运营线路 185 条，运营线路总长度 5761.4 公里，可研批复投资额累计 42688.5 亿元。此外，截至 2018 年底共有 63 个城市的城轨交通线网规划获批（含地方政府批复的 19 个城市）。其中城轨交通线网建设规划在实施的城市共计 61 个，在实施的建设规划线路总长 7611 公里（不含已开通运营线路），规划、在建线路规模稳步增长[4]。

从长远来看，城际铁路建成后，将成为城市圈的血脉，各种要素通过它自由流动，效率远高于其它交通方式，这对城市群发展意义重大，尤其产业向高级化发展之后，生产性服务业等需要靠知识创新进行发展的产业，比如科技研发、商业服务等更加需要人员之间的交流。而人员之间的交流也会因为城际交通时间的缩短而变得更加便捷。

2、疫情促进教育、医疗行业转型升级

疫情爆发是史无前例的全民健康教育，未来国家会把疾病预防放在更加重要的位置上，国民健康消费

[4] 丁静 中国证券报. 我国 35 个城市开通轨道交通[EB/OL]. http://www.cs.com.cn/gppd/tzzx/201904/t20190403_5936067.html,2019-4-03.

支出有望持续增加，这也使得医疗健康行业的发展前景和投资价值更为凸显。2020 年资本市场投融资普遍收紧的趋势已经可以预见，但医疗健康行业的投融资却有望逆势而上。从社会发展来看，补足民生短板、加快智慧城市建设成为“新基建”重要内容。此次新冠肺炎疫情的暴发暴露出我国城市管理能力，特别是应对公共卫生危机能力薄弱，提升我国城市管理水平，加强包括医疗卫生、公共防疫、应急管理能力在内的公共卫生安全体系建设，加快智慧城市的建设成为刚需，在这些方面都需要更多的基础设施建设投资。

从教育行业来看，新冠肺炎的出现让在线教育、云教育的需求大量增加。自 2015 年以来，国务院、工信部就出台了多项文件支持在线教育的发展，随着 5G+工业互联网的融合应用，5G 与教育等垂直行业势必将进行融合发展，行业有望迎来转型。

3、金融云快速发展助力金融基础架构转变

金融基础设施是金融市场稳健高效运行的基础性保障，是加快现代金融建设和强化风险防控的重要抓手，伴随着人工智能（AI）、云计算、大数据和物联网等数字化技术的发展，金融行业的数字化转型进程也在不断加速。

一般来说，金融机构的传统 IT 架构采用的是集中式架构，核心业务系统运行在小型机上，性能可靠是重要标准。近年来随着国家信创政策的实施，移动互联网金融业务的兴起，普惠金融业务量的迅速提升，以及利率市场化导致收入受限，金融信息系统采用分布式架构已成大势所趋。通过实施分布式架构改造，可以构建起高可用、易扩展、低成本的现代金融信息体系。

另一方面，自 2019 年以来金融 IT 信息创新受到政策密集支持，金融业自主创新主要集中在银行业，从最初将 IBM 大型机小型机更换为 X86/ARM 架构服务器，到现在自主创新逻辑进一步深化，持续在底层芯片、操作系统、数据库、办公软件等基础软硬件上发力，逐步迁移至自主创新云平台的架构，金融基础架构转变已进入快速发展阶段。

“新基建”时代网络安全和 APT 攻击

“新基建”进程的突然提速必然同时伴随着机遇与挑战。通过“新基建”建设，能够帮助城市安全业务打下一个好的技术基础，为未来提供更多的技术可能性。并且“新基建”的兴起也能够从基础设施层面促进相关产业发展，提升竞争实力，促进相关上下游产业快速发展。但是所有的发展势必会涉及到新的问题，发展和安全是一体两翼。随着新型基础设施建设和应用的开展，相关业务安全风险、应用场景安全风险和关键技术安全风险也正逐渐浮出水面。

“新基建”时代下网络安全面临的挑战会愈加多样化，具体可表现为以下几个方面[5]：

1、从外部防御到内部对抗，由外到内

首先随着 5G 网络、物联网、大数据中心等数字基建的开展，未来数字化系统和服务的部署和运营模式将更加开放、互通和生态化，导致边界更加模糊化和攻击面扩大化，将带来新的安全威胁和风险，对数据保护、安全防护和运营部署等方面提出了更高要求。尤其是网络攻击将从内部发起的可能性大幅度增加，防御者将很难发现威胁，更难于判断攻击来自哪里，攻击目标是什么，攻击方式是什么以及什么时候发生。同时，为了保障数字经济的可持续性发展，将对安全防护能力提出更高要求，需要在复杂网络威胁形势下有效保障数字化业务的可用性、可生存性和可恢复性。

2、从关键基础设施保护到数字基础设施保护，由点及面

其次，由于最初的关键基础设施保护（CIP）大多是围绕重点行业开展，这些行业一般都有充足的资金建设严密的安全防护体系，但是随着数字基建的开展需要重点保护的基础设施将大规模增加。同时，由于数字基建相关软硬件产品的漏洞、数字基础设施对于 APT 威胁的高价值吸引、数字基础设施间具备多种网络互连等因素，防控网络安全风险将是数字基建的长期主线。需要更多的资金用于配置相应的安全设备、安全

[5] 360 未来研究院智库安全研究员高昕 证券市场红周刊. 360 深度解析：数字基建时代的四大安全挑战[EB/OL]. http://static.hongzhoukan.com/2020/03/14/wap_595810.html?from=groupmessage&isappinstalled=0,2020-3-14.

系统、安全服务和团队，以支撑对数字基础设施的全面安全防护。

3、从网络空间到现实空间，虚实结合

另外，由于大量业务伴随数字化迁移到数字基础设施以及物联网的广泛应用，例如智能交通运输、智能家居、智慧城市和智能制造等，网络攻击不但会影响虚拟空间的数据隐私和系统/服务的正常运行，还会逆向影响人们所处的办公环境、家居环境、出行环境等生活的方方面面，从而造成现实中的财产安全和生命安全等物理空间安全问题。此类网络安全问题也会影响到整个数字经济的正常运行，波及到政府、企业和个人。其中，随着零售、金融、企业合作等传统业务的数字化，网络犯罪活动将围绕数字基建和其上承载的业务快速增加，造成更加严重的问题。企业业务的数字化，阻断式网络攻击将会影响企业经济活动的正常开展，渗透式网络攻击将对企业开展窃密行为，都将有可能给企业造成严重的损失。对于政府业务的数字化，网络威胁也将影响社会管理工作的正常开展，影响政府的公信力和形象。并且随着民众对在线购物、交通、医疗、办公等生活模式的依赖，网络威胁同时将会严重干扰人们的日常生活。

4、从网络空间攻防到数字经济博弈，综合实力比拼

未来，伴随着国家经济活动进一步向虚拟空间转变，作为承载数字经济的数字基础设施也将成为从网络安全攻击方（捣蛋小子、犯罪团伙、恐怖组织、国家力量）到商业竞争者的重要博弈平台。在经济利益驱使下，将会产生更加激烈的网络空间对抗，远远超出单个企业和组织的能力范围。因此，需要汇聚数字基础设施运营者、数字经济产业、安全行业和国家监管机构等多方力量，共同应对。

近些年来，国际格局日趋复杂，中国与国际的技术交流、技术合作及技术供应链有被阻断风险，如果在“新基建”过程中没有考虑到网络安全，那么可能造成的后果将是不可预计的。“新基建”时代下的网络攻击将不会仅仅是传统的网络攻击，而是将从数字空间延伸到物理空间，造成非常严重的后果，在此背景下我们就更需要注重网络安全的重要，尤其是要时刻警惕 APT 攻击的发生。

5、面临巨大的 APT（Advanced Persistent Threat）攻击威胁

回顾整个 2019 年，虽然并没有发生过于轰动的 APT 攻击事件，但是攻击的事件数量却有增无减，无

论是 APT 组织数量，还是 APT 攻击频率，相比往年都有较大的增长。这一现象在某种程度上也显示出了 APT 攻击正逐渐呈现出常态化、高频率的特性。

一般来说，大部分 APT 组织背后都有着深厚的政府背景，他们不惧法律，也不会因为安全厂商的披露而停止攻击活动，大部分攻击者会在攻击活动暴露后改头换面、更新武器库并重新发起新一轮攻击，更有部分组织对安全厂商的曝光毫不在意，不但毫不收敛甚至变本加厉继续对目标发起攻击，据不完全统计，在 2019 年全球各大安全厂商披露的 APT 攻击事件中，新组织所占的比例不足 2 成，绝大部分是老组织进行新的攻击活动，这也直接印证了攻击不会因为曝光而停止的特性，APT 与反 APT 的对抗是长期战斗。

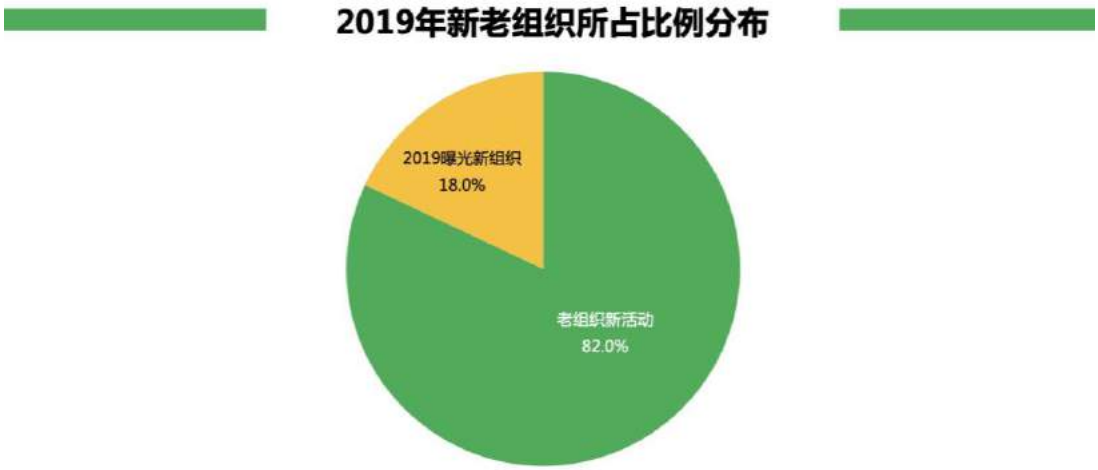

图 2 2019 年新老组织所占比例分布

从受害者的性质来看，政府、央企国企、科研单位和高校依然是 APT 攻击的重灾区，尤其是涉及对外进出口、国防军工、外交等重点单位。从行业分布上看，APT 组织的主要攻击目标包括政府、军队、外交、国防，科研、能源以及其他一些具有关键信息基础设施性质的行业和产业。

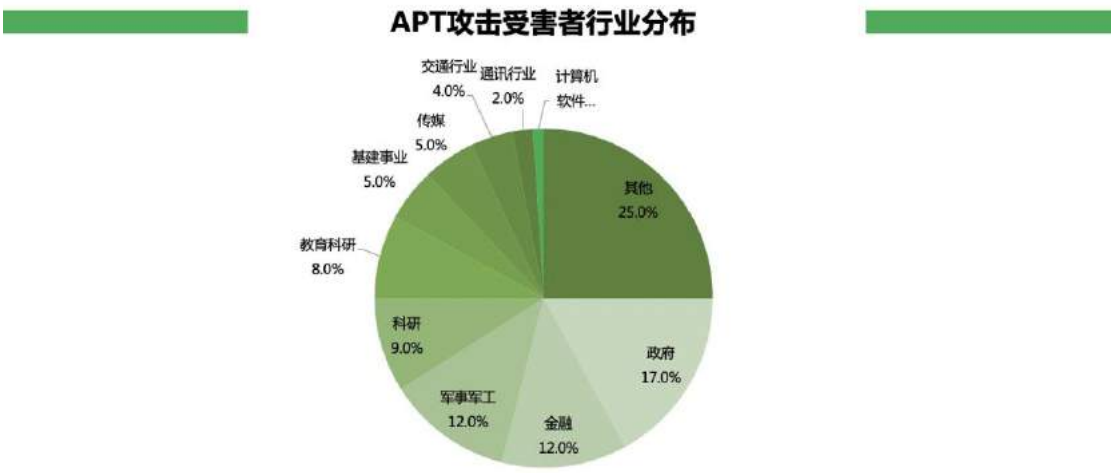

图 3 APT 攻击受害者行业分布

中国历来都是 APT 攻击的主要受害国，随着中国经济的快速发展，以及国际地位的不断攀升，中国面临的外部威胁形势更加严峻，从目前情况开看针对我国进行 APT 攻击的组织主要有以下几个：

海莲花（APT-C-00）

“海莲花”APT 组织是一个长期针对我国政府、科研院所、海事机构、海域建设、航运企业等领域的 APT 攻击组织，是近年来针对中国大陆攻击最频繁的组织之一。该组织在过去不仅频繁对我国境内实施 APT 攻击，也针对东南亚周边国家实施攻击，包括柬埔寨，越南等。

表 3 海莲花组织的攻击过程

攻击阶段	使用技术
攻击入口	利用鱼叉邮件投递漏洞文档，如 CVE-2017-11882 漏洞文档
初始控制	远程下载伪装成图片的 PowerShell 脚本载荷 利用白利用技术执行核心 dll 载荷
横向移动	主要利用系统命令实现横向移动： 使用 nbt.exe 进行扫描 net.exe 实现 IPC 用户添加 MsBuild.exe 在内网机器上编译生成恶意 dll 模块并执行

“海莲花”攻击目标众多且广泛，包括政府部门、大型国企、金融机构、科研机构以及部分重要的私营企业等。该组织攻击人员对我国的时事、新闻热点、政府结构等都非常熟悉。据 360 威胁情报中心监测，该组织在 2017 年疑似利用永恒之蓝针对国内高校的攻击测试活动。并且在 2018 年对该组织的持续跟踪过程中还发现海莲花组织针对柬埔寨和菲律宾的新的攻击活动，并且疑似利用了路由器的漏洞实施远程渗透[6]。

毒云藤（APT-C-01）

毒云藤（APT-C-01）也被国内其他安全厂商称为穷奇、绿斑。该组织从 2007 年开始至今，对中国国防、政府、科技、教育以及海事机构等重点单位和部门进行了长达 11 年的网络间谍活动。主要关注目标包括军工、中美关系、两岸关系和海洋相关领域，是专门针对中国大陆而生的黑客组织。该组织近年来的攻击活动虽然有所收敛，攻击事件大大减少，但是攻击活动却从未停止过，攻击手段和攻击技术也在不断的提升中。

图 4 360 截获的该组织鱼叉邮件内容

在 2019 年，该组织主要进行的攻击种类为钓鱼攻击，通过仿造 QQ 邮箱中转站和网易邮箱超大附件

[6] https://ti.360.net/blog/articles/oceanlotus-targets-chinese-university/

下载的页面，诱骗被攻击者输入账号密码的方式，来达到窃取邮箱账户和密码的目的，从而进行下一阶段的攻击。

蓝宝菇（APT-C-12）

蓝宝菇（APT-C-12）组织的活动最早起源于 2011 年，并从开始一直持续至今，对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息，攻击目标主要集中在中国大陆境内。

蓝宝菇大多使用鱼叉邮件实施攻击，投放的文件主要为 RLO 伪装成文档的可执行文件或 LNK 格式文件。从攻击来源来看，蓝宝菇和毒云藤两个组织属于同一地域，但使用的 TTP 却存在一些差异。

表 4 毒云藤和蓝宝菇 TTP 对比

组织名称	毒云藤	蓝宝菇
最早活动	2007 年	2011 年
攻击目标	国防、政府、科技、教育、海事	政府、军工、科研、金融
攻击入口	鱼叉攻击	鱼叉攻击
初始载荷	漏洞文档或二进制可执行文件	RLO 伪装成文档的可执行文件或 LNK 格式文件
恶意代码	Poison Ivy，ZxShell，XRAT	Poison Ivy、Bfnet PowerShell 实现的后门
控制回传	动态域名，云盘，第三方博客	动态域名或 IDC IP AWS S3、新浪云等云服务

除去上述提到的几个组织，还有包括摩诃草、蔓灵花、Darkhotel，Group 123 等一系列 APT 组织持续对中国进行攻击，中国的网络安全正面临着严峻的挑战。

“新基建”时代的网络安全，360 做了什么?

通过对行业趋势以及攻击形式变化情况来看，APT 组织在攻击中正变得愈加谨慎，随着“新基建”时代我国信息基础设施快速发展的同时，APT 攻击也将伴随着着 5G 和物联网技术的发展具备更强大的攻击能力，可以预见未来网络攻击破坏活动势必会更加复杂且频繁。

境外针对中国境内目标的攻击最早可以追溯到 2007 年，对中国境内超过万台的电脑产生了影响，攻击范围遍布国内 31 个省级行政区。从 2014 年开始，“360 安全大脑”通过整合海量安全大数据，实现了 APT 威胁情报的快速关联溯源，独家发现并追踪了四十个 APT 组织及黑客团伙，独立发现了多起境外 APT 组织使用“在野”0day 漏洞针对我国境内目标发起的 APT 攻击，大大拓宽了国内关于 APT 攻击的研究视野和研究深度，填补了国内 APT 研究的空白。

可以说攻防能力是一直是 360 的核心安全能力之一。公司通过数十年在安全领域的数据积累，在全网安全大数据、态势感知和分析、漏洞挖掘能力、APT 攻击的发现等方面的能力均处于全球领先位置。拥有最大的程序文件样本库，总样本数 180 亿+；最全的程序行为日志库，总日志数 22 万亿条；最大的存活网址库，每天 800 亿活跃网址访问记录；最全的全球域名信息库，全球 80 亿域名信息。通过“360 安全大脑”发现的 APT 攻击和部分国外安全厂商机构发现的 APT 攻击事件都可以直接证明中国是 APT 攻击中的主要受害国。

一直以来公司为十余个国家部委、监管机构及央企国企等提供网络攻防实战演练服务，演练规模空前。通过演练使国家重点单位及机构能够切实了解网络攻击对核心业务和数据的实际影响，锁定其防守的薄弱环节，从而向可防御有组织进攻的能力迈进。借助大数据分析、人工智能和强大的专家系统能力，“360 安全大脑”在监测和应对国际网络威胁方面成功溯源和发现多个境外高级持续性威胁攻击(APT)组织。

在发现未知威胁方面，360 团队已做出多项领先成绩。2019 年，360 威胁情报中心全球独家捕获了一起一直活跃在中亚地区，从未被外界知晓的 APT 组织，并将其命名为黄金雕(APT-C-34)。2019 年 10 月 20 日，360 发布了 360 全视之眼，能够捕获 0day 漏洞攻击，防范网络攻击于未然。

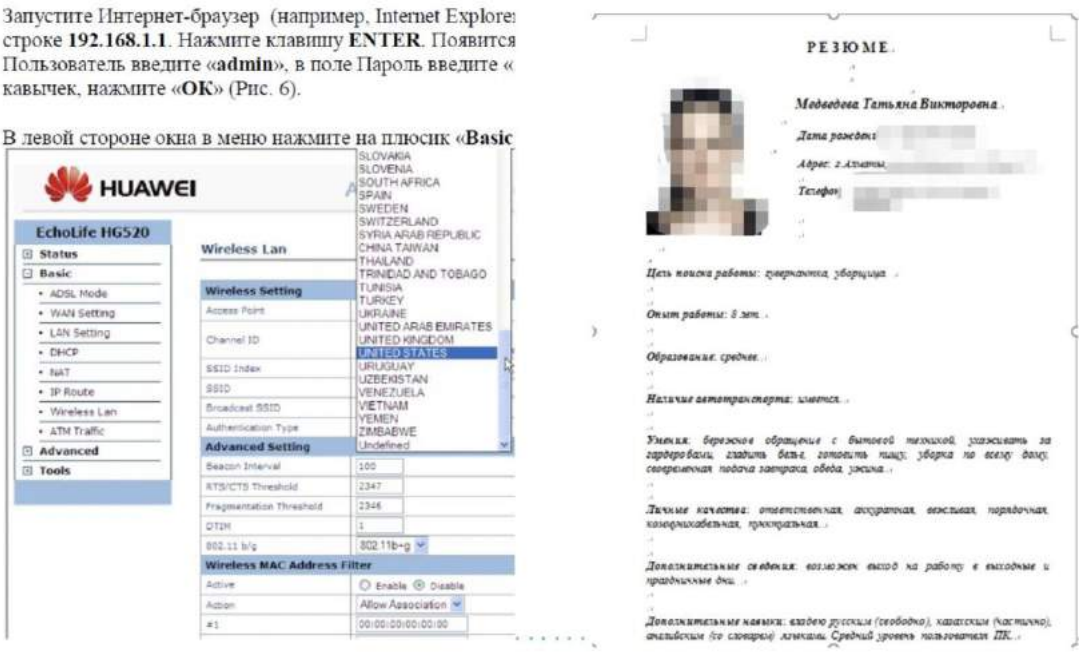

图 5 360 截获的诱饵文档（包括华为路由器说明书、伪造的简历等）

在今年 3 月初，“360 安全大脑”更是通过对泄漏的“Vault7（穹窿 7）”网络武器资料的研究，对其展开深入分析和溯源，于全球首次发现捕获了美国中央情报局 CIA 攻击组织（APT-C-39）对我国进行的长达十一年的网络攻击渗透。

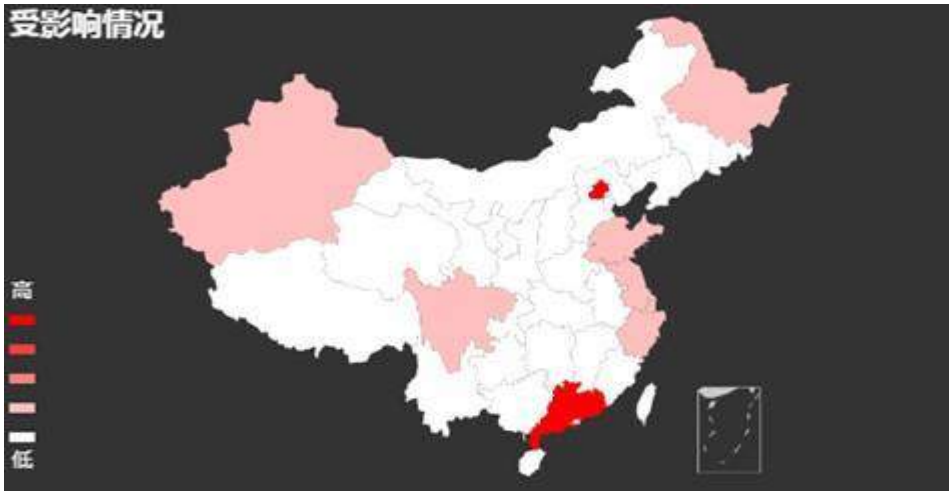

图 6 （APT-C-39）攻击影响地区

其中 CIA 在针对我国航空航天与科研机构的攻击主要是围绕机构的系统开发人员来进行定向打击。在此期间，我国航空航天、科研机构、石油行业、大型互联网公司以及政府机构等多个单位均遭到不同程度的攻击。在调查分析过程中，“360 安全大脑”通过资料比对列举出了五大关联证据，石锤证明该组织与美国 CIA 的关联。种种证据也表明，美国已打造了全球最大的网络武器库，这不仅给全球网络安全带来了严重威胁，更是展示出该 APT 组织高超的技术能力和专业化水准。

可以说当今时代，网络空间已成为国家安全角力的主渠道、主战场、最前沿。网络控制、诸多病毒感染、网络犯罪等威胁频频发生。APT 攻击愈演愈烈的背后，是国家间网络安全对抗战日趋紧张的表现，可以说只要存在政治目的和经济利益，APT 组织的攻击就不会停止，我们必须时刻以最高的安全意识来应对各种不同的网络风险和攻击。“新基建”时代不仅给信息安全带来了安全的问题，也为信息安全技术的发展提供了新的发展机遇，它就像是一把双刃剑，既可以利用新兴技术提升防控，也可以为安全分析提供新的可能。未来，“360 安全大脑”也将继续致力于防护针对“新基建”的 APT 攻击，为“新基建”的安全建设保驾护航。