网络安全补漏：市场与监管

编者按：在互联网 + 和大数据飞速发展之际，网络安全受到了史无前例的关注。5 月，中国互联网企业的安全事件以连环撞车的形式接连发生：5 月 27 日支付宝瘫痪，5 月 28 日携程瘫痪、艺龙遭到 DDos 攻击，5 月 30 日招商证券等券商系统在 A 股大跌的大流量下发生故障，此外，Uber、网易等公司亦遭遇网络问题。尽管此后支付宝自称“电缆被挖断”，携程自称是员工误操作，但两者的解释并未能令公众信服。更多的质疑指向“互联网公司系统为何如此脆弱?”在对网络安全的一片质疑声中，“企业安全”成为互联网产业新的增长点。5 月 20 日，华为推出 APT 大数据安全解决方案；5 月 25 日，360 企业安全集团成立。在“携程瘫痪”事件中，腾讯云自称 14 分钟即完成了对艺龙遭遇攻击流量的清洗。

支付宝：“异地多活”

■ 韩玮 报道

5 月 27 日下午，拥有将近 3 亿活跃用户的支付宝突然出现大面积访问故障，这场大瘫痪持续了约两个半小时。就在同一天，阿里系蚂蚁金服为第一大股东的浙江网商银行终于拿到了开业牌照。

次日，中国电信杭州分公司出具的一份《关于阿里巴巴(以下简称“阿里”)故障说明的函》表示，由于杭州市政建设工程施工方野蛮顶管施工，导致电信管道内四条大对数光缆中断，从而影响了阿里的相关业务。

这番解释并没有阻止舆论对于支付宝灾备系统的质疑。紧接着的第二天，占据在线旅游 31.1%市场份额的携程旅行网宕机近 12 个小时。至此，中国互联网企业的灾备能力开始让很多人心忧，“互联网+”再牛也干不过挖掘机啊！

据记者了解，由于观念意识淡薄以及容灾系统成本高、又不能及时体现经济效益等原因，国内大多数互联网企业及中小银行的灾备能力偏弱。而且，国内提供容灾备份服务的企业少得可怜，与海外几百家公司分食这块蛋糕的“盛况”无法相比。

“异地多活”

这场由“挖掘机”引发的大瘫痪，让很多人开始知道一个叫做“异地多活”的词汇。疑问也随之而来：既然能够“异地多活”，2.5 小时的“空窗期”又如何解释?

“异地多活”的说法，首先出现在支付宝 5 月 27 日发表的声明中，这距离故障事件发生约半小时。声明提及，支付宝的异地多活系统架构在此次意外中发挥了巨大作用。一方面，没有因光缆被挖断而影响全部用户；另一方面，紧急将故障机房的流量切换到了其他机房。

所谓“异地多活”，是一种区别于传统的同城灾备、异地灾备等方式的做法，其特点是在不同地方设置多个数据中心，对数据进行活备份。

去年 8 月，阿里上线数据中心“异地双活”项目。主导该项目的阿里技术保障部研究员毕玄曾在接受采访时这样解释“异地双活”：以去年双十一为例，当时，淘宝在杭州有一个数据中心，在另外一座城市还有一个，一共两个，分别承担 50%的用户流量。

记者了解到，5 月 27 日，受到光缆事故影响的杭州机房实际上不仅支撑支付宝业务，同时也支持着淘宝业务。但目前，淘宝已完成“异地双活”的架构改造，并经受了去年双十一的考验。故而，在这次故障中，淘宝可以实时、平滑地将流量切换到另一个数据中心，做到用户无感知。

而支付宝的“异地双活”架构升级目前正在进行之中。5 月 30 日，有支付宝员工向记者透露称：“‘异地双活’正在做，但还没完成。”这一说法可以从阿里巴巴技术保障部的官方微博上得到印证。

5 月 27 日，该微博账号转发了一条蚂蚁金服工程师“半兽人 __ 李洪彬”的微博，内容是，支付宝今年双十一前就会完成“异地双活”架构升级。

既然如此，“黑暗 2.5 小时”里，支付宝是如何被恢复的呢？5 月 28 日，蚂蚁金服方面转给记者一篇知乎文章，并表示“赞同”文中的分析。

按照这则帖子的说法，鉴于国家对金融行业的诸多要求，尤其是对交易一致性、数据完整性等方面的要求，支付宝的“异地多活”还处于小范围试用阶段，没有全体上线。这次杭州机房瘫痪后，一部分流量跑到了支付宝的异地机房，因此，在支付宝整体恢复之前，并不是所有交易都停止了。

至于没有通过“异地多活”技术切换的交易流量，支付宝在进行完整的数据校验，保证所有客户的客户信息、账户信息、资金信息、交易信息都正确后，再“开门迎客”。这个过程耗时一个多小时。

而阿里技术保障部在支付宝瘫痪当天发布的致歉信中则提到，“完全实现‘异地双活’后，即使再次出现某地机房光纤被挖断的情况，都不会再对用户产生任何影响”。

数据管理乱象

公开资料显示，支付宝是全球最大的第三方支付机构。根据阿里此前的招股说明书，2014 财年支付宝的总支付金额达到 38720 亿元，日均支付量超过百亿，占中国第三方支付市场份额的 70%以上。

在互联网企业中，类似的“国民应用”突然宕机并非没有先例。2013 年 7 月和 8 月，由于市政道路建设导致网络光缆被挖断及机房网络设备故障，微信曾出现近 7 个小时和 3 个多小时的大面积瘫痪。

今年 5 月 11 日，因骨干网络遭受攻击，网易旗下游戏、有道云笔记、LOFTER 等服务无法正常使用，宕机时间长达 8 个小时。

而在美国，当地最大的在线支付 PayPal 也曾在 2009 年 8 月和 2010 年 10 月遭遇宕机故障，持续时间都超过 1 个小时。

据记者了解，我国监管部门对金融机构，尤其是银行，有着灾难备份机制的要求。目前，国有大型银行基本采用“两地三中心”的模式，即一主两备，除了主机房，同城和异地还各配备一个灾备中心。

“这种机制的好处在于，除非三个中心同时宕机，否则，当一个机房发生故障，在较短的时间里，另一个备用机房会马上重启、接管。”北京三一银通信息技术有限公司(以下简称“三一银通”)副总经理龚振夏告诉记者。三一银通主要是一家为中小银行和村镇银行提供 IT 一体化服务的公司，业务内容包括建立“云上”的灾备系统。

“目前，国内大多数银行都做不到‘两地三中心’，首先是因为成本太高。按照传统方式，中型银行建设一个容灾系统少则上千万，多达上亿；其次，银行系统太多太复杂，小银行几十套系统，大银行成百上千套，这导致多中心的数据一致性、完整性和实时性很难实现。”

龚振夏认为，国内一些大银行确有“两地三中心”的机制，但很难做到完整地保证数据的统一性、同步性和实时性；而且，很多大银行只对关键业务进行灾难备份，其他非致命性的系统考虑得较少。与此同时，容灾切换演练存在风险，既然连演练一次都那么费劲，那么，当故障真正发生，故障原因又不清楚时，很难做到无缝切换。

而在国内的互联网行业，目前大多数企业都无法达到“两地三中心”的要求。多备份联合创始人兼 CEO 胡茂华告诉记者，首先，“两地三中心”对技术的要求较高；其次，在两个异地机房复制与主服务器相同的环境，成本很高，因为这两个环境要好几年甚至更长的时间才可能会用到一次。故而，很多公司都选择在异地做缩略版的数据中心。在这种情况下，当意外发生，流量被切换到备用数据中心时，很容易发生雪崩效应，也就是用户越打不开网页，越要拼命刷新，从而产生比正常情况大得多的流量。

历任总监、CTO、技术副总裁等职位的胡茂华透露，在他工作过的几个大的互联网公司，包括腾讯、盛大和 1 号店，都做了数据管理流程和备份恢复服务，但这些安全业务比较边缘，在整个公司关注程度很低，因而没有落到实处。

“我有理由相信，所有的公司都有做数据管理和备份，但 99%的公司都没有做数据管理流程、备份和恢复的演练，恢复后的数据是否可用，如何快速恢复等操作演练。”胡茂华说。

蚂蚁金服灾备路径

在支付宝大瘫痪这天获得牌照的浙江网商银行，将是蚂蚁金服未来的旗舰业务。在这样的行业背景下，阿里系的蚂蚁金服又是如何进行灾备的呢?

按照阿里技术保障部研究员毕玄此前的介绍，为了应对灾难，阿里最初在杭州建设了多个数据中心；2009–2010 年，开始尝试在异地做灾备中心。

彼时，阿里做的是冷备份，技术人员很快发现了两个问题：第一，备份整个阿里巴巴网站，包括淘宝、天猫、聚划算等，成本很高；第二，冷备份意味着不是一直跑流量，那么，当灾难发生时，他们未必敢把流量真的切过去。

2013 年左右，阿里决定尝试“异地多活”项目，而当时，国内没有现成的案例可供参考、借鉴，只能依靠自我摸索。

有业内人士透露，支付宝之所以至今还没有完成“异地双活”，是因为没法很好处理异地核心交易库的强一致性问题；而淘宝的实时强一致性需求远远比不上支付宝，所以比较容易实现。不过，这一说法目前没有被阿里方面确认。

这一次，阿里技术保障部的工程师花了 2.5 小时恢复支付宝系统。

对于这个速度，支付宝在声明中表示“不满意”，并承诺将完善“异地双活”架构，未来做到让用户无感知。但声明没有披露更多恢复的细节。此后，支付宝被推向舆论的风口浪尖。

事实上，对照我国于 2007 年 11 月起实施的灾难备份与恢复行业首个国标《信息系统灾难恢复规范》，以 2.5 小时的 RTO(Recovery Time Objective，恢复时间标准，也可以不严谨地理解为停业时间)衡量，支付宝的灾难恢复能力等级为 4 级，而最高级是 6 级，RTO 为数分钟。

有国有大型银行内部人士在接受记者采访时更表示，如果银行支付系统发生大面积瘫痪超过 2 小时，属于重大安全事故，很可能要向国务院汇报备案。

不过，胡茂华认为，以支付宝目前的业务量，其能在 2 个多小时内恢复系统，这在业界已算是比较快的速度，同时也证明了阿里的技术能力。

更脆弱的是中小互联网企业

■ 刘巍 报道

在多备份联合创始人兼 CEO 胡茂华看来，资源优渥的互联网巨头 BAT 做异地容灾备份的能力很强，真正脆弱的其实是大量中小企业，不管是技术，还是资源，他们搭建容灾系统都存在难度。

“国内很多企业的灾备意识薄弱，由于人力成本低，企业可以通过人工解决问题，故而，丢失数据也不被视作多么重要的事情；但国外普遍重视数据，很多家庭甚至购买专业设备备份家庭数据。”胡茂华说。

他介绍，目前，海外专门做容灾备份的企业多达几百家，包括 IBM、HP、赛门铁克等十几家老牌上市公司以及很多新型的互联网创业公司，比如 Datto、code42、durva 等。而国内这个领域的企业少得可怜。

传统安全技术失灵

来自 Verizon 的报告显示，过去一年全球有近 8 万家公司被黑，其中 2122 家公司公开确认信息被窃取，全球 500 强企业大面积沦陷，且在大多数情况下，攻击者只需要短短数分钟内就可以入侵一家企业。银行、信用卡公司、医院、零售业、保险业、电商、娱乐等行业巨头们纷纷中招。

目前，网络攻击已成为企业竞争中商业情报窃取的重要方式。

在全球最大的漏洞响应平台补天上，已经搜集了 4 万多个有效漏洞，中国企业和机构的网站和信息系统中的漏洞数量和危害程度惊人。仅从高校一个领域来看，自 2014 年 4 月–2015 年 3 月的 12 个月间，补天平台上显示的有效高校网站漏洞多达 3495 个，涉及高校网站 1088 个。

数据泄露让企业蒙受的损失也越来越高。Ponemon 研究所发现，2014 年数据泄露事故的平均损失为 350 万美元，这比 2013 年增长了 15%。“传统的网络安全技术正在失灵。”这是 360 总裁齐向东在 2014 年 9 月的自陈。互联网正在与实体经济进行快速融合。“伴随着移动终端、物联网、车联网的快速普及，传统的网络边界正在消失。”齐向东认为，未来 5 年或 10 年里，网络安全问题会变得更加复杂，更加严峻。

据《福布斯》报道，2014 年美国企业砸下大约 710 亿美元，购买和部署安全解决方案。预计今年将增长 8%，达到 770 亿美元。

但目前，企业面临的安全威胁的形式、数量和攻击手段等都发生了巨大的变化，企业部署的防火墙、IPS 和各种网关等传统安全防护产品还停留在兵来将挡，水来土掩的签名防护思路，面对未知威胁束手无策。

企业投入不足

在 2014 年中国互联网安全大会上，360 董事长兼 CEO 周鸿祎就曾呼吁，当所有的企业都变成互联网企业后，“企业安全一定要提高到一个更重要的优先级上”。

这从另一个侧面说明，相较于产品和服务的快速互联网+，相较于国际知名公司，中国企业和机构对安全重视程度更低。来自 IDC 的数据显示，中国企业在网络安全上的投入只有美国企业的 1/10。

目前互联网公司多以“尽力而为”作为服务承诺和网络架构，而传统电信、IT 领域则被要求高达 99.999%的“5 个 9”安全级别。

在对包括支付宝等准金融机构和其他互联网公司的较低程度监管下，多数企业的投入相对较小。一名信息存储公司的管理层人士向记者表示，就中国企业而言，受到法律严格监管的金融机构、特别是国有银行在安全方面投入较多，体系建设也领先许多。而相较之下，互联网企业们追求低成本和易扩张，在处理同等数据方面的投入也许不到 1/10，“恐怕要差一个量级”。

国务院发展研究中心金融研究所副所长巴曙松曾表示，“目前我国对整个支付体系的监管制度建设相对滞后，今后应逐步向完善支付法规制度、提高支付监管效率方面倾斜”。

据了解，在美国，企业普遍会购买一些安全服务，因此也催生了企业安全行业里一些大公司，比如赛门铁克、迈卡菲、CheckPoint、火眼等。而且企业正越来越意识到威胁的严重性。Gartner 公司估计，去年全球信息安全支出增长 7.9%，达到总额 710 亿美元，预计今年将会增长 8.2%，达到 770 亿美元。

根据 2015 年证券公司 Piper Jaffray 首席信息官调查显示，安全是首席信息官在 2015 年的最高优先级开支，与去年一样。其中 75%的受访者预计会在今年增加安全开支，平均在年度 IT 预算增长 2%。

携程：“宕机”12 小时全记录

■ 施露 报道

12 个小时！携程在 5 月 28 日尴尬地创下了国内互联网公司系统瘫痪的新纪录。

当天上午 11:09，携程网站和 APP 全线瘫痪，多项功能无法使用，直至晚上 11 时，部分功能才得以修复。从瘫痪到修复，携程“宕机”近 12 小时。若按携程一季度营收 3.37 亿美元估算，“宕机”一小时的平均损失为 106.48 万美元，12 个小时算下来总损失超过 1200 万美元。

真实原因仍扑朔迷离

5 月 28 日，遭遇噩梦的不仅只有股市，还有携程。

记者在第一时间发现之后，点击携程官方网站，页面显示 404 报错，点击“返回首页”后依然可进入携程，但其功能和其他链接均无法使用；APP 的酒店查询页面则显示“Error 503 Service”，其他业务线的产品均不能查询和预订。携程此番“宕机”范围覆盖全国范围，网站及 APP 处于全线崩溃状态。因携程未在第一时间公布原因，随后，各种猜测甚嚣尘上。

一则消息在微信朋友圈风传：携程数据库被物理删除（指文件存储所用到的磁存储区域被真正地擦除或清零，不可恢复）。

“宕机”一个半小时后的 12:38，携程在微信上首次回应媒体称：因部分服务器疑似遭到不明攻击，携程官方网站及 APP 于 11:09 起无法正常使用。目前，系统正在逐步恢复中。经紧急排查，携程数据没有丢失，预订数据也保存完整，正在恢复过程中。对用户造成的不便，我司深表歉意。

回应中的“疑似”二字，引发了更多网友的猜测。

一位自称为携程员工的网友在微博上爆料：“网站根目录被删除，所有节点上的业务代码包括发布日志都被干掉了，个人猜测是有人内部报复。”另有网友分析，携程数据庞大，从外部直接攻击的难度可想而知，应该是内部人员动了“手脚”，“最大的可能性是某人破解公司内部密码和验证条件，放置了某些恶意程序”。

“大部分情况下，互联网企业都能在第一时间解决技术性问题。如果第一时间无法解决，也会说明故障原因，以此来打消公众的猜测和恐慌。多个途径的消息都显示此事系内鬼所为，而不是外界因素，也有点蹊跷。”速途研究院院长丁道师告诉记者。

“如果真是内部人搞破坏，这就难以阻止了，只能用法律责任以及相关的流程控制，以此降低风险和损失。”一名旅游网站的创始人分析道。

艺龙、同程受牵连

当天下午 3:00，携程的官网及 APP 查询和预订服务仍未恢复。刚刚收归携程门下的艺龙，暂时承担起了崩溃后的导流任务。

就在携程导流艺龙两个小时后，艺龙首页也无法正常访问；几乎同时，同程旅游因接入携程的酒店数据，酒店预订服务也出现瘫痪。去年 4 月，携程以逾 2 亿美元的价格战略投资同程，成为其第二大股东。

对于同程和艺龙网站短时间崩溃的原因，华南地区一名从事互联网信息安全的人士分析说：“携程过大的流量导入，使得同程和艺龙首页的承压过大而致首页崩溃，艺龙最后借助腾讯的流量清洗系统解决了该问题。”

“宕机”近 11 个半小时后，携程在官方微博上发布声明称：5 月 28 日 22:45，经抢修，除个别业务外，携程官方网站及 APP 恢复正常。经过排查，携程郑重声明数据没有丢失，预订数据也保存完整。对用户造成的不便，携程再次深表歉意。

此时，携程依旧未能恢复所有功能，但也未就确切原因作出进一步解释，除了对数据被物理删除辟谣外，对坊间传闻未作其他说明。

5 月 29 日 0：18，携程微博称：5 月 28 日 23:29，经技术人员抢修，携程官方网站及 APP 全面恢复正常。经过排查，携程郑重声明，数据没有丢失，预订数据也保存完整。

互联网信息安全成短板

从全线瘫痪到完全修复，携程用了将近 12 个小时，刷新国内互联网公司“宕机”处理时间的新纪录。

5 月 29 日凌晨 4 点，携程官方公布网站崩溃具体原因称：经携程技术排查，确认此次事件是由于员工错误操作导致。由于携程涉及的业务、应用及服务繁多，验证应用与服务之间的功能是否正常运行花了较长时间。携程官方网站及 APP 已于 5 月 28 日 23:29 全面恢复正常。

对于携程的官方声明，魏建称：“携程说的是内部操作失误，估计是一个组合原因，内部操作失误显示了漏洞，漏洞被抓住之后估计被‘黑客’设计了后门，持续删除代码，导致系统无法发布。”前述互联网信息安全从业人士表示，携程 12 个小时恢复网站，在互联网公司实属罕见，足以说明内部管理、系统、技术投入都存在问题，如果有灾难恢复机制，不太可能花如此长时间，“此前携程的支付系统调试接口被泄露，已足以暴露它在互联网信息安全管控这块的短板”。

携程“宕机”事件，再次敲响了安全信息防护的警钟。不过，当下现实依然严峻。“很多互联网安全信息防护因投入资金量大而被忽视，很少有公司真正去做好这一块，大部分都只追求利益产出相关的技术投入。”多名业内人士感叹说。