# 国盟信息安全通报

2020 年 8 月 30 日第 223 期

全国售后服务中心

# 国盟信息安全通报

（第 223 期）

国际信息安全学习联盟

2020 年 08 月 30 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 381 个，其中高危漏洞 135 个、中危漏洞 202 个、低危漏洞 44 个。漏洞平均分值为 5.91。本周收录的漏洞中，涉及 0day 漏洞 151 个（占 40%），其中互联网上出现“vBulletin 跨站脚本漏洞、vsftpd 操作系统命令注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3061 个，与上周（3721 个）环比减少 18%。

# 主要内容



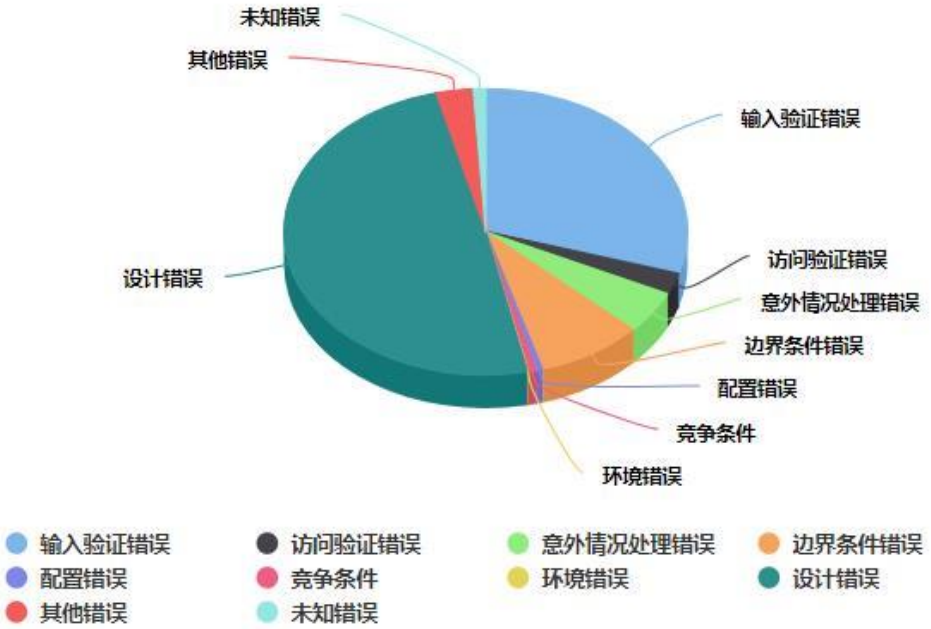
**注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。**

# 一、概述

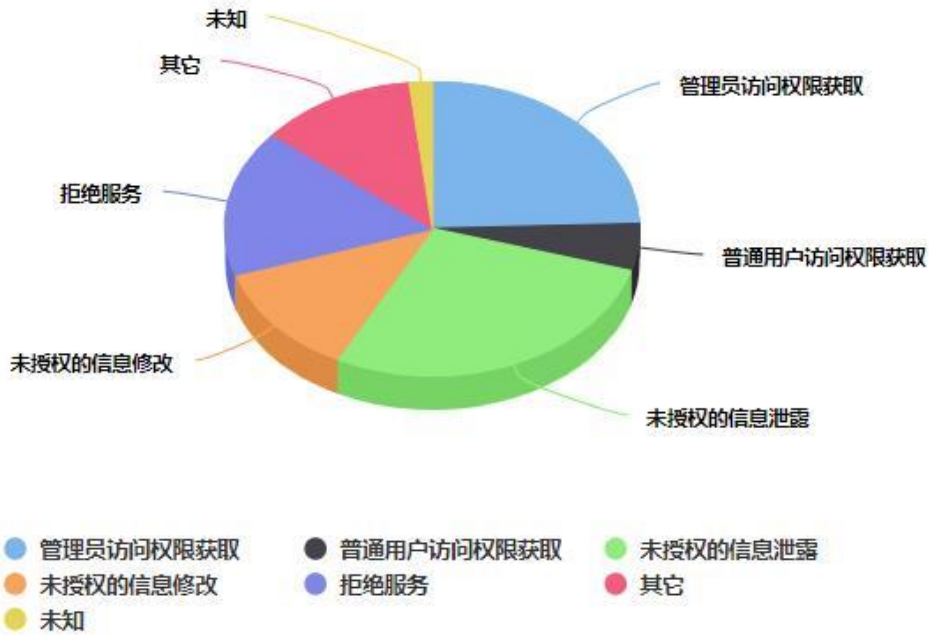
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 381 个，其中高危漏洞 135 个、中危漏洞 202 个、低危漏洞 44 个。漏洞平均分值为 5.91。本周收录的漏洞中，涉及 0day 漏洞 151 个（占 40%），其中互联网上出现“vBulletin 跨站脚本漏洞、vsftpd 操作系统命令注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3061 个，与上周（3721 个）环比减少 18%。

# 二、安全漏洞增长数量及种类分布情况

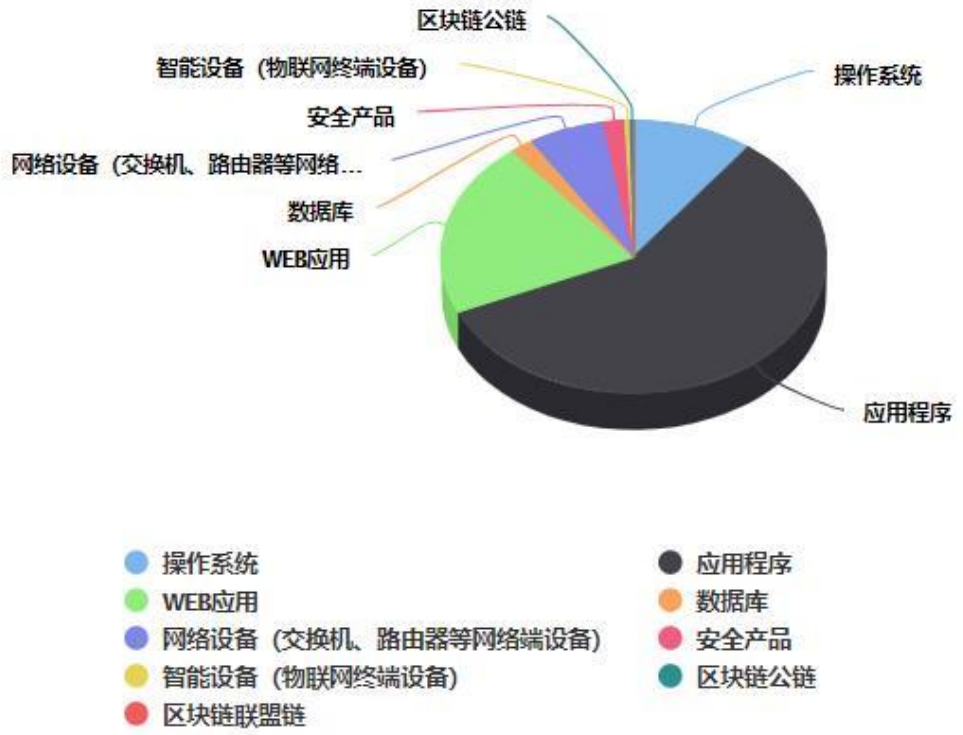
➢ **漏洞产生原因（2020 年 08 月 16 日—2020 年 08 月 30）**



## ➢ 漏洞引发的威胁（2020 年 08 月 16 日—2020 年 08 月 30）




## ➢ 漏洞影响对象类型（2020 年 08 月 16 日—2020 年 08 月 30）



# 三、安全产业动态

## ➢ 2020 年上半年全球网络犯罪趋势与应对

网络信息技术在 2020 年全球抗疫中扮演了重要角色，也集中暴露了长期以来存在的网络信息安全缺陷和短板，而疫情在一定程度上提前进行了一场多主体协同治理网络犯罪的场景预演。网络犯罪治理需要在不违反公民基本权利、保障公民个人信息与隐私权的前提下，综合提升网络犯罪治理能力，促进网络犯罪多主体协同治理模式的深化。

**一、上半年全球网络犯罪总体生态环境**

新冠疫情全球大暴发在一定程度上催化了社会整体网络化和数字化。一方面，为抗击疫情，政府各部门需要收集和共享更多的公民信息以追踪疾病的传播路径，实现事前预警和防范，以及事后处置；另一方面，基于隔离防范的需求，社会活动前所未有地从线下转为线上，整个社会对网络和信息技术的依赖程度大幅度提升。以上两项因素的结合，形成了疫情期间网络信息安全的特殊外部生态，其特征主要表现为以下四个方面。

第一，已经建立的个人信息保护制度门槛因紧急事态被降低。例如，匈牙利宣布暂停《一般数据保护条例》（GDPR）相关规则的效力；意大利通过《630 号公民保护令》（Civil Protection Ordinance No.630）以扩张个人数据数据处理范围；法国公共健康区域委员会（les Agencesrégionales de santé）发布信息通知，允许向任何涉及控制、预防和评估疫情的合作方传输个人数据；美国计划引入《2020 年 COVID-19 用户数据保护法》（COVID-19 Consumer Data Protection Act of 2020）；泰国将原本计划于今年生效的《个人数据保护法》（Personal Data

Protection Act）推迟至 2021 年。

第二，不同类型数据之间的规范界限被打破，特别是对健康数据、生物数据、行踪轨迹等敏感数据的收集和处理，在疫情防控的总体需求之下成为必须。例如，今年 5 月，苹果和谷歌联合开发基于设备蓝牙系统的追踪软件。

第三，收集和处理数据的主体更加广泛，并且主体间数据共享亦更加全面和深入，这一点在政府部门与互联网企业的合作方面尤为明显。特别是在疫情期间，一系列由网络信息技术公司开发的追踪、识别技术，被广泛应用于抗疫活动。

第四，信息不对称的情况加剧，关于疫情情况、抗疫措施、疫情防护和救治等方面的信息在真实性、可靠性、扩散速度和影响力方面呈现出较大差异，信息繁杂且真假难辨，并进一步引发社会信任危机。例如，世界卫生组织已经发布警告，提醒各国注意犯罪分子模仿世界卫生组织发送伪造的邮件和 WhatsApp 信息，以诱使收件人点击恶意链接。

**二、全球涉疫情网络犯罪主要形态和特征**

疫情充分暴露出网络信息技术安全在不同地区和领域的发展不均衡，现有关于犯罪治理的立法与司法实践的缺陷被放大，并且借由社会公众的恐慌情绪进一步发酵。

（一）涉疫网络犯罪发展态势

根据网络安全公司 ZScaler 的观察，自新冠疫情全球暴发以来，钓鱼软件、恶意网站和恶意软件的增长率一度高达百分之三万。互联网技术企业 AtlasVPN 基于谷歌数据的报告也显示，3 月，钓鱼网站的数量较之 1 月增长了 350%。

国际刑警组织（InterPol）4 月发布的《新冠疫情网络威胁全球态势》报告显示，即便是一些已经发现的恶意软件，也借新冠疫情改头换面，死灰复燃。根据该报告，以“COVID”或“corona”等关键词注册的恶意域名大幅度增加，犯罪分子通过制造虚假的新冠肺炎网站或软件欺骗民众，进而传播恶意软件、钓鱼软件或非法获取个人信息。

（二）涉疫网络犯罪主要形态

疫情为犯罪分子提供了新的犯罪契机，在此背景下网络犯罪呈现出新的形态。欧洲委员会总结出与疫情相关的七种网络犯罪形态，大致可以归为三类：第一类是非法获取和使用数据类犯罪，其中又以侵害个人信息类犯罪为甚；第二类是涉财类犯罪，又可区分为敲诈勒索犯罪和诈骗犯罪；第三类是涉社会公共秩序类犯罪，主要以虚假销售防疫物资与制造、散布虚假防疫信息为典型。

（三）涉疫网络犯罪的特征

就网络犯罪实施的具体方式上，可以观察到以下三方面的特征。

首先，远程办公网络成为安全弱点。受疫情影响，利用私网络进行远程办公被短时间大范围普及，而与之相关的应用也成为网络犯罪的重点攻击目标之一。有评论已经表示，“越多人在家庭网络工作，黑客们就有越多机会磨炼技巧和赚钱”。

其次，弱势群体受网络犯罪冲击严重。国际刑警组织的报告显示，疫情期间涉儿童色情的网络犯罪呈现出飙升的态势，这与隔离期间儿童接触网络时间延长、对网络社交依赖度提升有紧密关系。

再次，防疫设施成为犯罪分子攻击重点。疫情期间，疫情防护所需的医疗、科研或其他健康卫生设施遭到大量勒索软件攻击，同时，世界卫生组织等疫情防护组织或关键设施也成为主要攻击对象。这与疫情期间社会及公众对于医疗卫生资源高度且急迫的依赖度相关。

**三、国际社会应对涉疫情网络犯罪的措施**

在此背景下，打击网络犯罪面临前所未有的挑战。可以预见的是，这种挑战还有可能长期存在。对此，国际社会也已经开始探索多主体协同配合的机制，以共同抗击利用疫情实施网络犯罪的活动。

一方面，刑事执法机关站在打击利用疫情实施犯罪的最前线。国际刑警组织在 3 月 26 日发布了《新冠疫情期间执法机关指南》（COVID-19 Pandemic：Guidelines for Law Enforcement），针对疫情期间激增的网络犯罪提出一系列应对建议。欧洲刑警组织执行主任 Catherine de Bolle 在 4 月 30 日的报告《超越疫情：新冠疫情将如何塑造欧盟严重和有组织犯罪的图景》（Beyond the Pandemic: How COVID-19 Will Shape the Serious and Organized Crime Landscape in the EU）中表示，“疫情的整体影响尚不可知，但是，执法机关需要做好准备以应对疫情带来的危机。国际警力前所未有地需要在现实世界和虚拟世界联合起来。这次危机再次证实，犯罪信息的共享对于打击犯罪而言至关重要”。

另一方面，网络信息业者和社会组织积极参与到抗疫过程中。5 月，国际刑警组织发起主题为“清洁你的网络双手”（WashYourCyberHands）的全球警示运动，其核心在于警示公众防范涉及疫情的网络威胁，并促进全球执法机关和网络安全组织的合作，以打击犯罪分子利用疫情盗取数据、实施网络诈骗或单纯扰乱虚拟世界等活动。国际大型互联网企业开始对外共享涉新冠疫情的网络威胁情报。例如，微软在 4 月 21 日发动全球数据公开运动，号召打破数据壁垒，共同应对新冠疫情等全球面临的严峻挑战。

**四、下半年全球网络犯罪治理的总体思路**

疫情的突然暴发，暴露出一系列现有规制体系的盲点和缺陷，引发的次生灾害可能进一步影响未来网络犯罪治理活动。在此背景下，对于涉疫情网络犯罪治理的探讨和经验总结不

应仅限于疫情期间，更需要延伸至疫情之后。

（一）推进公私主体间的协同配合

疫情期间出现的网络犯罪数量激增，在一定程度上预演了社会生活高度网络化之后可能面临的现实障碍：数据壁垒之下不同国家和地区间刑事执法机关的能力受限。这一方面表现为执法管辖权的地域性与数据分布和流动的弱地域性之间的矛盾，另一方面则表现为不同国家和地区间网络信息技术融入执法活动的不均衡，进而反映为网络执法能力的差异。在疫情期间，国际刑警组织积极发挥了各国警力协调联动的中枢功能，其在疫情期间发布网络犯罪最新信息、提供执法机关打击涉疫情犯罪指南、加强各国警力数据与技术共享等方面发挥了重要作用。这一合作模式将成为未来网络空间治理的主要模式，并伴随社会网络信息化的不断深入而常态化。

除刑事执法机关之间的合作外，疫情期间网络信息业者的参与度也进一步提升，不仅表现在各类数据的收集、处理、共享方面，还表现在疫情防控相关技术的开发和使用。无论是在数据层面还是在技术层面，网络信息业者均发挥了补强执法机关短板的重要功能，并且一定程度上克服了传统刑事司法框架下的执法管辖权障碍。在疫情暴发前，刑事司法机关与网络信息业者的合作执法已经逐步凸显，疫情催化了这一趋势，并且促使双方快速调整角色加以适应。

可以预见的是，疫情之后，打击网络犯罪仍然需要强化执法机关与网络信息业者等的合作，并且这种合作不仅限于数据共享层面，还将深入拓展至技术共享层面。现有规则体系可能更为关注前者，但是，借由技术共享所形成的多主体协同配合，实则对于已有法律体系及刑事司法权力运行提出了同样严峻的挑战，需要在未来给予充分的重视。

（二）强化网络信息安全均衡发展

新冠疫情期间的网络犯罪态势具有较为鲜明的特征，暴露出不同地区和社会领域网络信息技术发展状况以及相关安全机制的不均衡。网络犯罪的全球性特征直接将这种不均衡转化为犯罪机遇和执法漏洞，从而形成网络信息安全的木桶短板，需要在疫情之后予以补强。具体而言，疫情期间网络犯罪主要暴露出以下三个方面的网络及数据安全差异。

1. 政府与行业企业网络的安全均衡

疫情期间，政府与行业企业在抗疫过程中在数据和技术方面形成紧密合作。长期以来，政府部门借由内网安全机制以及内外网联结过程中的安全技术应用，往往具有较高的网络及数据安全。相对而言，疫情期间其他非政府组织的网络安全形势则面临较为严重的挑战。例如，疫情期间公共卫生健康机构的网络信息系统频繁遭受攻击，或者成为网络诈骗的重点模

拟对象。此外，一些紧急开发或应用于疫情信息登记、健康状况监测、行踪轨迹监测等疫情防控工作的软件并未就收集和处理海量数据匹配充分的数据安全保障机制，从而短时间内极大提高了数据泄露和网络安全风险。根据 Navid Ali Khan 等人的研究，目前受到新冠网络犯罪攻击最为严重的机构或行业主要包括三类：健康卫生系统、金融服务系统、政府和媒体。

2. 公共网络设施与私人网络设施的安全均衡

疫情期间的隔离机制使远程居家办公被迅速推广和普及，私人设备和网络被迫在此期间承担起部分公共网络设施职能，从而形成网络与数据安全的新漏洞。这种漏洞主要体现在两个方面：其一是多样化的私人网络设备形成数据传输、存储和处理系统的碎片化，导致难以适用统一标准的网络和数据安全保障机制。例如，疫情期间急速推广的 Zoom 等远程办公系统成为用户数据泄露和非法交易的重灾区。其二是私人网络与公共网络之间进行数据传输时不可避免地造成公私网络的混用以及公私数据的混同，二者衔接区本身即可形成网络信息安全的短板。

3. 一般公众与弱势群体的安全保障均衡

在疫情期间，弱势群体在网络环境中变得更加脆弱，特别典型的是，针对儿童的网络犯罪呈现出激增的态势。这主要是由于疫情期间，无论是通过网络在线学习，还是进行社交活动，儿童接触网络的频率远高于平时，并且其情绪和认知更容易受到网络信息的影响。例如，欧洲刑警组织报告《疫情投机：犯罪分子如何利用新冠疫情危机》（Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis）显示，犯罪分子利用儿童在疫情期间的封闭状态和敏感情绪，诱使更多儿童成为网络霸凌或性犯罪的被害人。联合国儿童基金会（UNICEF）也发布报告《新冠疫情：强隔离措施下儿童面临的虐待、忽视、剥削和暴力风险提升》（COVID-19: Children at Heightened Risk of Abuse, Neglect, Exploitation and Violent amidst Intensifying Containment Measures），警示各国现有隔离措施使儿童面临更为严重的虐待、暴力、剥削等风险。

（三）秉持人权保障的底线

在疫情之后，一方面需要充分反思疫情期间暴露出的网络犯罪治理方面的问题，并在已有基础上进一步强化国家和社会适应网络信息革命的能力；另一方面也必须看到疫情本身的特殊性和应急性，这种属性意味着疫情过去之后，网络犯罪治理措施应当回归到正常社会生活状态，重新形成打击犯罪和保障人权的平衡。

可以观察到的是，疫情期间基于疫情防控的现实需要，整体社会治理在事项排序上进行了调整，尤为典型的是，近些年来世界各国普遍推进的个人信息保护制度和机制被暂停适用，

个人信息的收集和处理呈现出规模化扩张的趋势，这种扩张不仅体现在个人信息的类型上，也体现在其收集和使用范围上。个人信息保护制度所一贯强调的知情同意原则、目的原则以及最少收集原则在疫情期间均被突破；信息在不同公私主体之间以及不同公共事务部门之间的交互和共享被普遍化和正当化。

正是在这一背景下，有相关组织已经发出警示，认为必须警惕不加审慎评估地暂停适用个人信息保护等基本人权保障规则，并且从有效性和比例原则出发，遏制借疫情之名而过分干预公民基本权利的倾向。3 月，《个人数据自动处理中的个人保护公约》（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）委员会主席亚历山德拉·皮耶鲁齐（Alessandra Pierucci）和欧洲理事会数据保护专员让-飞利浦·沃特（Jean-Philippe Walter）发布联合声明，一方面承认数据保护并非拯救生命的障碍；另一方面强调即便在艰难环境下，数据保护的基本原则仍然应当受到尊重。国际商会（ICC）也在 5 月发布了《AOKpass 新冠疫情健康数据保护宣言》（AOKpass Declaration for COVID-19 Health Data Protection），认为“面对疫情造成的生命和生活的损失，采取紧急的全球行动确有必要。但是，这不应当被用作侵犯个人健康数据隐私权利的借口。通过与行业领袖合作，我们强烈支持根据严格的数据隐私原则制定新冠疫情合规标准和体系”。

此外，电气和电子工程师协会（IEEE）在《自动化与情报系统伦理国际倡议》（Global Initiative on Ethics of Autonomous and Intelligent Systems）的基础上，针对疫情期间的 AI 应用伦理问题发布了《涉疫情人工智能系统应用伦理的声明》（Statement Regarding the Ethical Implementation Artificial Intelligence Systems for Addressing the COVID-19 Pandemic），提醒人们重视人工智能技术不当应用可能造成的对基本人权的侵蚀。为预防或打击涉疫情网络犯罪而应用此类技术时，如果因特殊时期对个人信息、隐私权等权利的保障有所松懈，那么，在疫情结束之后，网络犯罪治理仍应当重新回归到人权保障的基本框架之中。（来源：中国信息安全）

## ➢ 《数据安全法（草案）》的立法背景、立法定位与制度设计

**引言：**作为数字化转型的核心要素和关键因素， 数据对经济发展的重要性不言而喻。伴生而来的数据安全问题亦愈发凸显，给个体权益保护、产业健康发展甚至国家安全带来诸多风险。网络攻击、侵入等外部威胁与安全漏洞、缺陷、人的因素等内部脆弱性叠加共振，

任何组织百分之百数据安全的目标都是不可实现的。2019 年底以来，席卷全球的新冠疫情和经济危机推动国际形势乃至国家秩序重建变化趋势加剧。

与公共卫生保持社交距离要求截然相反的是社会对高度互联数字世界的强烈依赖，网络世界和物理世界加速融合，无处不在的安全需求与泛滥的数据安全风险则形成鲜明对比。疫情后世界和全球化未来不稳定性与不确定性前所未有的凸显。我国正加快供给侧结构性改革，加快培育数据要素市场，稳定传统产业的同时科技创新驱动“新基建”发展。新时代、新形势、新发展和新业态背景下，数据安全问题纳入法治化轨道极具必要性和迫切性。

**一、立法背景：没有数据安全就没有国家安全**

数据是国家基础性战略资源，没有数据安全就没有国家安全。当前，我国数据安全顶层制度设计加速推进。2015 年《国家安全法》第 25 条明确提出“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”。作为网络安全综合性立法，2017 年《网络安全法》将数据安全纳入网络安全范畴，基于网络安全保障目的为个人信息保护与数据安全的部分重要、核心制度奠定了基础。2018 年《数据安全法》《个人信息保护法》纳入人大常委会立法规划。2019 年国家互联网信息办公室相继发布《数据安全管理办法（征求意见稿）》《个人信息出境安全评估办法（征求意见稿）》等多部《网络安全法》体系的下位配套文件，大力推进国家层面的数据治理规则构建和具体制度设计。2020 年《民法典》明确个人信息、数据、网络虚拟财产等属于合法权益。执法实践层面，围绕个人信息非法采集和滥用、数据三性破坏等活动的数据安全专项治理行动空前有力。地方层面围绕数据跨境、数据安全保障、数据开放、数据权等问题积极先试先行，典型如《天津市数据安全管理办法（暂行）》《贵州省大数据安全保障条例》《深圳经济特区数据条例（征求意见稿）》《中国（上

海）自由贸易试验区临港新片区总体方案的通知》《海南自由贸易港建设总体方案》等。2020 年 7 月 3 日，历时 3 年制定时间的《数据安全法（草案）》正式向社会公开征求意见，备受关注。

**新时代、新形势、新发展和新业态背景下，国家层面的数据安全立法推进面临着诸多难题。**

第一，数据安全问题本身复杂性凸显。数据安全问题横跨数据与安全两大领域，囊括数据静态安全与动态利用安全两大面向，涉及个人、企业、国家多方法益，同时还须考量区块链、人工智能、5G 等新技术新应用对传统法律规则的冲击。

第二，我国先前经验相对不足。相较于欧美等国家或地区，我国的数据相关立法起步较晚，基于法律传统、文化差异、产业发展水平等因素的不同，国际经验借鉴也需进行根植于国情的本土化改造。近年来，国际社会围绕数据资源的角逐与博弈日趋激烈，以欧盟《通用数据保护条例》（GDPR）、美国《加利福尼亚州消费者隐私保护法》(CCPA)等国际数据安全立法在互相融合的同时，诸多方面亦有明显分立。

第三，数据安全立法演变为全球范围内的利益协调与主权斗争工具。以美国《合法使用境外数据明确法》（Cloud 法）以及相关国家的效仿或配合、欧盟《通用数据保护条例》（GDPR）为代表，立法趋势表现为争夺数据话语权，积极推行符合本国利益诉求的国际社会数据规则体系，扩张本国法律的适用范围、提升执法行为的域外效力。随着近年来中国综合国力的提升，数据安全成为个别国家针对中国专门立法的重要关切，部分数据相关的立法条款更是成为个别国家抑制我国新技术新应用发展的重要借口，以此营造不利于我国的舆论氛围，挤压我国产业的国际发展空间。

第四，数据安全治理“中国方案”亟待突破。作为当前全球第一数据资源大国和全球第二大数字经济体，中国人工智能、5G 等新技术新应用场景越来越丰富，在某些领域和问题的规范与引导上已无成熟的国际经验可循。数据安全治理“中国方案”一直在探索，亟待突破和确立，为中国企业走出去、推进全球数字化进程、增进全球人民数字福祉贡献大国力量。

第五，数据权利保护的基础性问题尚未解决。现下正值我国国家通信信息技术发展应用从量变到质变的特定时期，国家层面的立法承担了“以安全保发展、以发展促安全”的数字经济支撑使命。在中央将数据定位为生产要素的背景下可以预见，未来数据的流通与共享将更加常态化，而现阶段以数据法律权属、数据法律性质为代表的诸多基础性问题还没有解决，部分已经确立的规则也未能在安全和产业发展之间找到一个很好的平衡点。

第六，立法衔接与协调问题亟待考量。如何与国家安全领域的《国家安全法》《网络安

全法》《密码法》《出口管制法》以及制定中的《个人信息保护法》等进行衔接与协调是国家层面立法体系安排中需要考虑的重要问题。

从研究视角来看，数据领域基础性法律问题的解决还需要不断探索，加强数据权利的本质、内涵、外延、客体、分类的研究，为数据权利保护提供底层支撑，在此基础上，完备的国家立法应覆盖数据主权维护、数据权利确认、生命周期保护、供应链条监管、跨境传输审查、境外要素（资本、技术、产品、人员、服务）审查、数据主体监管、数据滥用禁制等数据权利法律制度。

**二、立法定位：数据安全领域的基础性法律**

科学的立法定位是搭建立法框架与设计立法制度的前提条件。立法定位对于法的结构确定起着引导作用，为法的具体制度设计提供法理上的判断依据。与社会各界对《数据安全法》明确解决问题措施的预期有所差异，草案立法说明将《数据安全法》定位为“数据安全领域的基础性法律”，这一自身立法定位决定了其以下特点：

第一，该法是安全保障法。该法以公权介入数据安全保护，提供认识数据安全问题、处理数据安全威胁和风险的法律路线。具体来说，以其对数据、数据活动、数据安全的界定为出发点，厘清不同面向的数据安全风险，构建数据安全保护管理全面、系统的制度框架，以战略、制度、措施等来构建国家预防、控制和消除数据安全威胁和风险的能力，确立国家行为的正当性，提升国家整体数据安全保障能力。

第二，该法是基础性法律。基础性立法的功能更多注重的不是解决问题，而是为问题的解决提供具体指导思路，问题的解决要依靠相配套的法律法规。这也决定了其法律表述上的原则性和大量宣示性条款。但与此同时，预设好相关接口、整体立法语言的表述粒度均衡等也应特别注意。

第三，该法是数据安全管理的法律。数据安全作为网络安全的重要组成部分，诸多安全制度可被网络安全制度所涵盖。在数据安全管理上，与《网络安全法》充分协调，避免制度设计交叉与重复带来的立法资源浪费、监管重复与真空、产业负担是《数据安全法》制定过程中需重点关注的问题。

就安全保障法来说，作为数据安全领域的基础性法律和国家安全法律制度体系的重要组成部分，草案第1条明确立法宗旨之一为“维护国家主权、安全和发展利益”，这与《国家安全法》第25条国家网络与信息安全保障“主权、安全和发展利益”的宗旨一致。草案虽将数据界定为“电子或者非电子形式对信息的记录”，对数据这一概念做了最大化解释。

事实上，随着信息化、网络化、数字化的发展，无论是电子数据体量、影响的增长还是

“传统”非电子数据向电子数据的转化都呈不可逆趋势， 能带来“数据这一非传统领域的国家安全风险与挑战”的更多是电子数据。草案将数据安全定义为“通过采取必要措施，保障数据得到有效保护和合法利用，并持续处于安全状态的能力”，这与《国家安全法》对国家安全、《网络安全法》对网络安全的概念界定相似，都落脚到保障持续安全状态的能力，安全状态既包括了数据的静态安全保障（防止因数据泄露、篡改、灭失所导致的保密性、完整性和可用性破坏），也包括了数据的动态利用安全保障（包括不限于加工、使用、提供、交易等环节的依法有序自由流动）。

草案为数不多的创设性法律责任条款第 42、43 和 44 条中，第 42 条既是对违反静态安全保护义务的行政处罚，第 43 条和 44 条是针对非法交易、非法处理这两大动态利用不当的行政处罚。

**三、制度设计：数据安全治理的四梁八柱**

在我国数据产业正处于高速发展的当下，数据安全风险、安全保障能力均在不断发展、演变。尚不稳定的国际政治、经济等形势也成为影响数据安全制度设计的重要变量。在缺乏成熟经验与范例，又异常敏感的情况下，《数据安全法》应厘清自身定位，明确自身需要重点解决的问题，重在构建起数据安全治理的四梁八柱，明确预防、控制和消除数据安全风险的制度、措施，确立国家行为的正当性，这里仅对草案的一些制度规定简单予以评析。

数据安全监督管理体制。首先，草案第 6 条和第 7 条出现中央国家安全领导机构与国家网信部门两处“统筹协调”的职责分工。虽然第 7 条将国家网信部门的统筹职责划定在“网络数据”范畴，但随着我国信息化、数字化进程的快速推进，如此制度设计，未来中央国家安全领导机构与国家网信部门在数据安全领域的统筹协调职责将出现更多的重合，既不科学也不严谨，会造成理解和实施上的困难。

其次，各地区各部门承担数据安全监管工作。数据安全监管工作具有较高的专业技术要求，行业主管部门对本行业的数据安全工作的指导和监督，受限于其工作重点、关注领域、专业能力、信息来源，难以代替数据安全职能部门的专业性监管。这一难题在动用国家之力对数据实行分级保护和重要数据目录确定的责任落实中会表现得更为明显。持续了三年有余的《网络安全法》关键信息基础设施认定工作历程可作为参考。再次，第 7 条第 1 款的主体责任规定明显不适合合并于职责分工这一条中，建议另行放置。

分级分类和重要数据重点保护制度。草案第 19 条规定了数据分级分类和重点数据保护制度。首先，鉴于数据同样是影响网络安全等级保护制度中定级、关键信息基础设施认定的重要因素，此处的数据分级与等保、关保是否采用同样的分级标准、如何协调需要进一步明

确。近年来，《工业数据分类分级指南（试行）》《证券期货业数据分类分级指引》《个人金融信息保护技术规范》等各部委发布的指引性文件及行业标准，对特定行业的数据分类分级具体标准进行了非常有帮助的尝试。

其次，“重要数据保护制度”是本法的重要制度之一。重要数据也是《网络安全法》的重要概念，需注意保持不同法律文本同一概念内涵和外延的一致性。重要数据概念、认定机制、保护方式、法律责任应当在本法中予以确立。针对维护国家核心利益和国家安全需要，应明确对基因、生物、医疗、地理等类别数据实施重点保护。鉴于“重要数据”一般具有攸关国家安全的高度敏感性，立法中应限制重要数据认定权授予、设置严格认定程序、强化认定结果监督。若“重要数据”将其交由各地自行决定，不仅可能不当扩大或缩小重要数据范围，还可能导致数据跨地区流动和处理引发法律规避。建议由中央国家机关划定重要数据的类型，各地区在上述划定范围内有权确定本地区重要数据目录，在不同地区出现冲突的情况下，可上报中央国家机关决定。

最后，鉴于重要数据处理者需要履行更多的义务，政府部门认定是否属于重要数据之后应当给予相关主体提出异议的权利和渠道。

数据跨境安全流动规则。数据跨境作为影响数据安全的重要因素，应当属于《数据安全法》的重要规范对象。草案总则第 10 条明确提出要“促进数据跨境安全、自由流动”，但正文目前并未明确具体的规则。虽然第 23 条的数据出口管制、第 33 条的境外执法机构的跨境数据调取涉及数据出境问题，但无法涵盖一般商业场景下的数据跨境流动问题。数据跨境流动规则的设计需充分研判以下因素，实现跨境的破局和流动性价值：

（1）各国数据跨境的的基本政策框架，找寻不同框架下的政策、法律差异，以及形成这些差异的缘由；

（2）不同的跨境政策，其后也有不同的技术能力、算法认同的支撑，应从历史沿革和技术演化的长期过程充分考究逻辑、统计、生物等不同学科对数据技术和算法的影响，以及当前和未来的发展趋势；

（3）尝试局部、先行的区域或双边的数据跨境流动框架，在数据分级分类的前提下，可以进行某些行业、领域数据的跨境流动，避免数据流动性停滞导致的单一性，以及创新不足问题。

数据安全审查制度。草案第 22 条确立了数据安全审查制度，但未明确该制度的实施主体、实施机制、审查内容等。当前我国已通过《国家安全法》《网络安全法》《外商投资法》等法律法规，建立起了网络安全审查、外商投资审查等在内的国家安全审查体系。关于网络

安全审查，从 2020 年颁布的《网络安全审查办法》第 9 条的规定可看出，产品和服务使用后带来的重要数据被窃取、泄露、毁损的风险属于网络安全审查的内容之一。在此背景下，网络安全审查、外商投资审查与数据审查存在一定的交叉。如何处理数据安全审查与前述审查制度的关系，包括审查机制、审查内容、审查标准等需要重点考量。

数据出口管制制度。草案第 23 条建立了数据出口管制制度与《出口管制法》及数据出境安全评估制度之间的配合及衔接问题。当前《出口管制法》尚在制定中，从 7 月 3 日全国人大网公布的二次审议稿来看，目前的版本在第 32 条对信息出口管制做出了仅原则性的规定。

此外，《网络安全法》《数据安全管理办法（征求意见稿）》及《个人信息出境安全评估办法（征求意见稿）》规定了重要数据及个人信息的数据出境安全评估要求。本条建立的数据出口管制制度与《出口管制法》及数据出境安全评估制度之间的配合及衔接需要通盘考虑。

境外执法机构数据调取的阻断机制。草案第 33 条规定了境外执法机构获取我国境内数据的报告和批准机制。本条是对美国 CLOUD 法为代表的执法数据跨境获取体系威胁国家主权的阻断。2018 年 10 月我国通过的《国际刑事司法协助法》中第 4 条第 3 款规定被视为对 CLOUD 法的直接回应。但鉴于该条款规定抽象，也未设立相应的罚则，可操作性不足。草案第 33 条应为阻断提供充足而有力的规定。

首先，建议将“境外执法机构”扩展至“境外机构”。从现实情况来看，境外要求提取数据的除执法机关外还有其他组织，对其提供数据同样会对我国的国家安全带来隐患。

其次，建议增加法律责任。本条缺乏对应的法律责任，一方面难以切实落实阻断，另一方面法律责任的落空会让企业依据 CLOUD 法做“礼让分析”中缺少“不一致的法律要求”实质性依据。

此外，草案第 20 条、第 21 条所确立的国家数据安全风险评估、报告、信息共享与监测预警机制、数据安全应急处置机制也与《网络安全法》监测预警与应急处置一章的规定高度重合，需做好配合与衔接。

**四、总结**

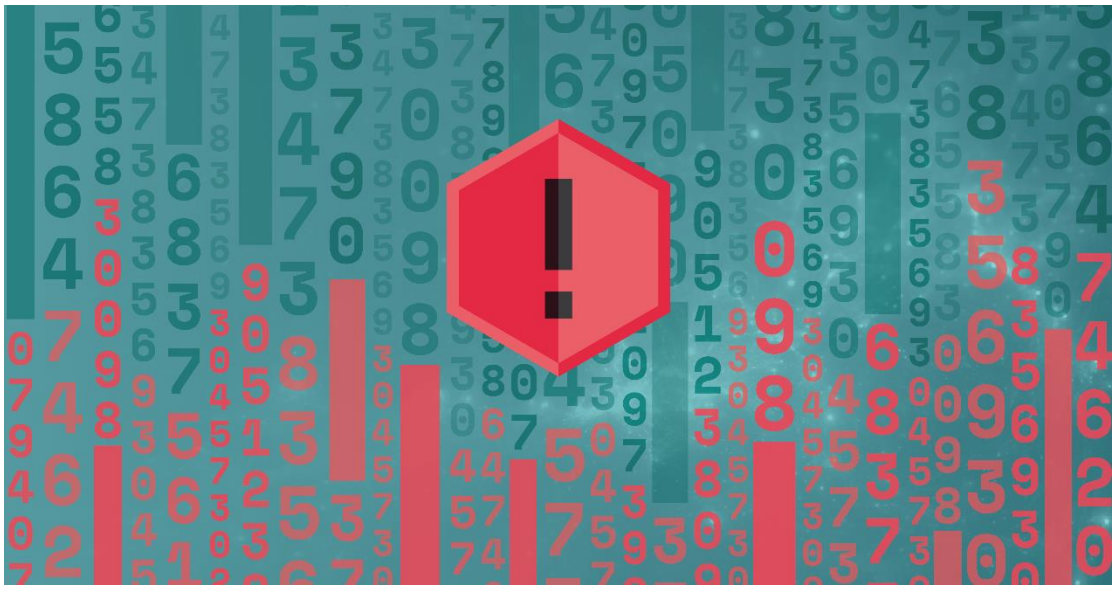
在技术日新月异的今天，如何有效地利用法治资源，在产业技术政策中确立以技术创新为核心的法治目标，是企业获得生命力和国家谋求长足发展的基础性保障。中国特色社会主义法治体系加速构建，《数据安全法》将与《国家安全法》《网络安全法》《密码法》、制定中的《个人信息保护法》和二次审议稿阶段的《出口管制法》等共同构建起一个横向内部体系更加协调、外部辐射范畴更为广泛，纵向制度、原则、规则更为立体化的国家安全保障体系。

鉴于数据安全问题的复杂面向，草案存在各种问题和争议，如数据主权维护机制、与其他基础性立法的有效衔接、数据要素资源利用与数据安全协同治理的平衡考量、引进来走出去的法治营商环境构建、制度设计的合理性与可操作性、条款完整性和结构平衡性的立法技术问题等，这一方面须得各界人士脚踏实地地研究、调研和论证，为草案多提建设性意见；一方面有待有关部门加速《数据安全法》及其下位配套制度的设计、规划、协调工作，推动数据安全治理“中国方案”不断完善；另一方面基于国家统一层面的立法实施执法检查、立法影响评估等工作也是国家治理现代化与中国特色社会主义安全法治体系构建的必然要求。

（来源：公安三所网络安全法律研究中心）

## ➢ 提高网络安全意识 构筑网络安全屏障

“没有网络安全就没有国家安全。”党的十八大以来，以习近平同志为核心的党中央高度重视网络安全，统筹协调多领域信息化建设和网络安全重大问题，作出一系列重大决策部署，推动网络安全事业取得了历史性成就。



从第一封邮件的发送成功，到当代云计算、大数据、区块链等网络高科技的突破性发展，网络正在把全人类带入一个以信息技术为核心资源的新时代。

网络发展有力地推动了全球各国围绕网络信息技术开展新一轮技术革命，不断加快重塑了社会发展的物质基础。特别是在全球一体化进程不断深化的当下，网络凭借其互联、互通特性将世界逐渐紧密地融为一体，但与此同时，在有利于信息共享、资源共通的良性前提下，也存在着风险和挑战。

一方面，网络技术的发展，加强了一国之内民众间的交流联络，拓展了民众政治参与途径，促进了世界范围内民众个体间的文化信息融合和政治参与程度。另一方面，网络技术已在国家政治、经济、军事、文化、教育等各领域广泛应用，成为社会和经济发展的强大助推力，且受依赖程度愈发增强，大有“牵一发而动全身”的关键作用。如果网络安全出现问题，轻则影响国家正常运转，重则可导致国家关键领域门户洞开，直接导致国家颠覆的巨大风险。

互联网是人类共同家园，一个安全稳定繁荣的网络空间，不只是一国的需要，更是世界的需要。保障网络安全与守护国家安全是统一的。

“网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线”。以习近平同志为核心的党中央高瞻远瞩、高屋建瓴，将网络安全问题提升至国家战略层面，在总体国家安全观引领下系统落实网络强国建设。

近年来，我国从出台网络安全法、国家网络空间安全战略，到开展移动互联网应用（APP）违法违规收集使用个人信息专项治理，再到建立关键信息基础设施安全保护制度，一系列关乎个人、国家的网络安全举措出台落地，织密了网络安全的“安全网络”，为通往“网络强国”奠定了基础。

首先，自觉规范网络活动行为。随着移动互联网技术的广泛应用和网络自媒体时代的开启，网络信息已从单向获取转为双向传输，网络空间已成为多渠道汇集、多层面共享的信息聚合平台。网民在享受网络空间带来便利的同时，需自觉规范网上活动行为，不破坏网络空间技术基础，不发布违法有害信息，不传播负面及谣言内容，主动弘扬正能量，主动维护网络空间“风清气正”和“和谐清朗”。

其次，落实网络服务主体责任。提供网络服务的企业、单位及个体，要依照国家相关法律法规落实主体责任，在保障网络技术领域安全的前提下，及时有效开展网络信息内容监管，严守信息发端，严控违法信息传播，加强网络内容建设，培育积极健康、向上向善的网络文化。同时，还应有效开展网络服务主体间的互相监督，有力加强行政管理部门对网络服务的管理工作，多措并举营造健康向上的网络服务空间。

最后，加强网络空间建设国际合作。习近平同志指出，“一个安全稳定繁荣的网络空间，对各国乃至世界都具有重大意义”，“国际社会应该本着相互尊重和相互信任的原则，共同构建和平、安全、开放、合作的网络空间”。我国在承认各国网络空间主权的前提下，要积极推动并参与国际合作，进一步构建国际网络安全体系，不断推动国际网络技术交流和安全共识，逐步提高网络空间规划治理主动权和话语权。

网络空间不是法外之地，网络安全更是事关国家安全和国家发展，也直接关系到每一个网民的切身利益。只有保护好每一个网民的安全，共同构建良好的网络空间秩序，才能让网络安全落地生根，构筑起国家网络安全的坚固长城。（来源：法制网）

## ➢ 数字化时代个人金融信息保护的思考

当前，全球正迎来一场更大范围、更深层次的科技革命和产业变革，数字化浪潮正深刻改变着包括金融业在内的经济社会各领域，数据作为新生产要素和基础性战略资源的重要地位日益突显。如何建立完善更加符合数字化时代要求的个人金融信息保护体系，并在更高水平实现信息安全和合理应用之间的适度平衡，已成为摆在我国金融管理部门、行业协会、从业机构和广大金融消费者等面前的一项重要课题。

**建设个人金融信息保护体系的必要性和紧迫性**

个人金融信息一般指个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化，是从业机构在提供金融产品和服务的过程中积累的重要基础数据。加强个人金融信息保护既是落实人民至上理念、保护金融消费者合法权益的应有之义，也是促进个人金融信息安全合规应用、发挥金融数据要素价值的必要之举。在互联、开放、共享的数字化时代，建设个人金融信息保护体系的必要性和紧迫性更为突出。

首先，这是金融业贯彻以人民为中心的发展思想的关键举措。金融业是跟老百姓钱袋子打交道的特殊行业。个人金融信息与个人财产状况、信用水平等高度相关，涉及金融消费者

的个人隐私。移动网络的发展和数字技术的应用，在提升金融服务覆盖面和便利性的同时，也增加了个人金融信息泄露和不当使用的风险。近年来，金融领域个人信息非法收集、滥用、泄露等现象时有发生，引起了广泛的社会关注，给金融行业声誉和消费者信任带来极大冲击。建设个人金融信息保护体系，有助于落实个人金融信息全流程安全防护要求，使金融消费者合法权益免遭各种不当行为的侵害，从而提升金融消费者的安全感和满意度。

其次，这是金融业落实国家网络和数据安全制度的迫切需要。随着网络强国和数字中国战略的推进，我国网络普及率已提升至 64.5%，网民规模超过 9 亿，网络和数据安全相关法律制度加速出台。其中，《网络安全法》对网络运营者收集和使用个人信息的基本原则、负面清单、管理要求等进行了明确规定。《民法典》对隐私和个人信息进行了基本界定，并对隐私权和个人信息保护提出了原则性要求。此外，《数据安全法（草案）》已进入征求社会公众意见环节，《个人信息保护法》已列入 2020 年全国人大常委会立法规划。上述法律规范为加快建设个人金融信息保护体系提供了坚实的制度条件，也提出了更高要求。

最后，这是金融业推进数字化转型与高质量发展的必然要求。当前，经济数字化转型已是大势所趋。数据显示，2019 年我国数字经济增加值规模达到 35.8 万亿元，占 GDP 比重达 36.2%。金融业正加速迈入一个与数字经济相对应的数字化新时代，日益呈现出“无科技不金融、数据驱动金融”的特征。在依法合规并做好信息安全保护的前提下，充分发挥个人金融信息类型多、应用领域广、集聚增值效应强等优势，将其分级分类运用于营销获客、信用评估、风险管理等核心业务环节，有助于充分释放技术红利和数据红利，推进金融业数字化转型和高质量发展。

**我国个人金融信息保护现状与面临的挑战**

近年来，随着数字技术与经济金融活动的加速融合，我国金融管理部门、行业协会以及广大从业机构在个人金融信息保护的制度建设和业务实践方面做了大量工作，取得了阶段性成效，总体呈现出以下几个方面的特点。

1.法律规范不断完善。目前，我国已初步形成涵盖法律、行政法规、部门规章、规范性文件等在内的多层次和广覆盖的个人金融信息法律规范体系。《民法典》《网络安全法》《消费者权益保护法》等法律明确了个人信息保护基本原则和相关权利义务。《商业银行法》《证券法》《保险法》《反洗钱法》等金融法律确立了专门领域个人金融信息保护的基本原则。《个人存款账户实名制规定》《储蓄管理条例》《征信业管理条例》等行政法规对账户管理、征信服务等领域个人金融信息保护提出了规范性要求。《个人信用信息基础数据库管理暂行办法》《中国人民银行金融消费者权益保护实施办法》等部门规章以及《关于银行业金融机构做好

个人金融信息保护工作的通知》等规范性文件，从个人金融信息类别范围、工作原则、业务规则等方面，对从业机构开展个人金融信息保护工作提出了细化具体的要求。此外，《个人金融信息（数据）保护试行办法》作为专门针对个人金融信息保护的部门规章，已列入人民银行 2020 年规章制定工作计划。

2.技术标准配套实施。2017 年 12 月，国家标准化管理委员会发布国家标准《信息安全技术个人信息安全规范》，规定了开展个人信息处理活动应遵循的原则和安全要求，并将银行账户、财产信息、征信信息等个人金融信息列为个人敏感信息，提出了明示同意、信息加密等要求。2020 年 2 月，人民银行发布金融标准《个人金融信息保护技术规范》。该标准从安全技术和安全管理的角度，规定了个人金融信息在生命周期各环节的安全防护要求。此外，在近年来陆续发布的云计算技术金融应用、声纹识别安全应用、移动金融客户端应用软件、网上银行系统信息安全、金融分布式账本技术、商业银行应用程序接口等领域相关金融标准中均对个人金融信息保护和安全管理提出了明确要求。这些技术标准在信息系统和技术安全层面有效促进了个人金融信息保护有关法律制度的落地实施。

3.行政监管持续发力。近年来，金融管理部门通过监督管理、投诉处理、风险排查、专项治理、宣传教育等多种方式，不断加强个人金融信息保护工作力度，督促从业机构履行客户个人金融信息保护义务，切实保障金融消费者信息安全权。比如，银保监会持续深化银行业保险业市场乱象整治工作，对有关从业机构未采取有效措施保护客户信息安全、违规泄露和滥用客户信息等行为予以严厉整治。2020 年 4 月，人民银行启动针对移动金融客户端应用软件、应用程序编程接口、信息系统等重要领域的金融科技应用风险专项摸排工作，并将个人金融信息保护作为摸排重点之一。此外，金融管理部门在监管执法过程中，注重综合运用约谈高管、限期整改、行业通报、监管评级挂钩、行政处罚等各类措施，不断提升个人金融信息保护工作针对性和监管有效性。

4.行业实践扎实推进。从业机构在金融管理部门的指导和各金融行业协会的组织下，认真贯彻落实有关法律规范、监管要求和标准规则，注重将个人金融信息保护纳入金融消费者权益保护、数据治理、网络信息安全等工作规划，明确个人金融信息保护牵头部门和管理机制，建立健全个人金融信息保护相关内控制度，开展个人金融信息保护员工教育培训，加强金融消费者信息安全和金融知识普及教育，规范第三方合作机构和外包服务机构管理，明确外包合作各方的个人金融信息保护职责和保密义务。

5.多重挑战仍待破解。尽管取得了一定进展，我们还应清醒地看到，数字化时代个人金融信息保护在立法、监管、自律等方面依然有一些新老问题相互交织、亟待破解。一是个人

金融信息保护专门制度尚未出台，现有规定以原则性、框架性规定居多，且零散分布在不同效力层级的法律规范中，制度衔接和统合存在不足。二是金融管理部门在个人金融信息监管执

法方面的职责分工有待进一步明确，监管统筹、信息共享和工作联动机制需要加强，与行业协会有机协调配合的治理机制尚未成熟。三是部分从业机构在个人金融信息保护方面的主体责任意识有待加强，在内部控制、数据治理、消费者保护和教育等方面仍需进一步补短板、强弱项、堵漏洞。四是一些金融消费者个人信息保护意识和风险识别能力依然薄弱，在数字金融产品、信息安全防护、投诉维权等方面的知识和技能存在欠缺。

**政策建议**

数字化时代下建设个人金融信息保护体系是一项长期复杂的系统工程，需要包括政府、市场、社会多方协同，科学施策，久久为功。具体来说，建议着力做好以下几个方面的基础性工作。

一是强化法律规范。立足中国现实国情和经济金融数字化转型实际，科学借鉴欧盟、美国、英国、日本等国家和地区立法经验，合理吸收目的限定、最小必要、隐私安全、权益保护等国际共识原则，探索实现信息可携带权等具有数字化时代特征的新型权利形式的可行路径，适时出台《个人信息保护法》《个人金融信息（数据）保护试行办法》及相关配套标准规则，进一步健全符合中国国情、具有中国特色、接轨国际规则的个人金融信息法律规范体系，统筹实现信息安全与合理应用之间的更好平衡。

二是严格行政监管。进一步加强个人金融信息保护领域的统筹监管，持续完善各部门职责分工、信息共享、工作联动等机制，以保护金融消费者合法权益和督促从业机构履行主体责任为切入点，以个人金融信息采集和处理机构为主要对象，探索运用人工智能、大数据、

区块链等监管科技手段，持续深入开展个人金融信息保护有关监管执法和检查评估工作，以“零容忍”态度依法加大对个人金融信息相关违法违规行为的惩处力度。

三是推进行业自律。发挥行业协会贴近市场和会员组织优势，深入研究行业在统筹个人金融信息保护和合理应用方面所面临的共性问题，搭建从业机构信息共享和国际交流平台，通过信息基础设施、统计监测、标准规则、教育培训等行业自律管理手段，督促和引导从业机构落实个人金融信息保护有关法律规范和监管自律要求，完善个人金融信息保护有关举报受理和线索移交机制，对行政监管形成有益补充和有力支撑。

四是加强机构自治。从业机构应牢固树立以客户为中心、负责任创新的正确理念，切实落实个人金融信息收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，加强内控制度和数据治理体系建设，明确各部门、岗位和人员在个人金融信息保护方面的责任权限，完善内部监督和责任追究机制。此外，从业机构还应在依法合规前提下探索应用数据脱敏、多方安全计算、联邦学习、差分隐私、同态加密等隐私保护和数据融合技术，加强个人金融信息保护技术支撑，促进信息合理开发利用。

五是加强公众参与。加强违法违规行为举报奖励、举报人保护等机制建设，充分调动社会公众参与个人金融信息安全治理的积极性。通过司法解释等方式，明确网络环境下个人金融信息侵权形式，丰富和畅通个人金融信息保护的救济渠道。广泛运用线上线下宣传教育渠道，针对性开展个人金融信息保护教育，定期发布个人金融信息保护风险提示和典型案例，提高公众对个人金融信息保护的意识和能力。

为者常成，行者常至。中国互联网金融协会作为国家金融行业自律组织，始终注重将个人金融信息保护要求贯彻落实在互联网金融登记披露、统计监测、信息共享、移动金融客户端应用软件备案、金融科技创新监管试点支撑等有关行业自律管理工作的各个环节。下一步，协会愿继续与社会各方一道，在金融管理部门指导下，共同建设一个涵盖法律规范、行政监管、行业自律、机构自治、公众参与且更加具有数字化时代适应性的多层次、综合化个人金融信息保护体系。（来源：金融电子化）

# 四、政府之声

## ➢ 工信部印发《运用大数据推进防范治理电信网络诈骗长效机制建设工作方案》

2020 年 8 月 19 日，为深入落实国务院打击治理电信网络新型违法犯罪工作部际联席会议有关部署，充分运用大数据等新一代信息技术强化电信网络诈骗精准治理、有效治理，加快健全完善行业防范治理长效机制，近日工业和信息化部印发了《关于运用大数据推进防范治理电信网络诈骗长效机制建设工作方案》(工信部网安〔2020〕121 号，下称《方案》)。


中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

邮箱登录 | 移动版网站 | 工信微报 | RSS订阅

统一搜索

看新闻 找文件 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏 疫情防控专题

首页 > 工业和信息化部 > 机关司局 > 网络安全管理局 > 工作动态 > 正文

工信部印发《关于运用大数据推进防范治理电信网络诈骗长效机制建设工作方案》

发布时间：2020-08-19 来源：网络安全管理局 分享：

为深入落实国务院打击治理电信网络新型违法犯罪工作部际联席会议有关部署，充分运用大数据等新一代信息技术强化电信网络诈骗精准治理、有效治理，加快健全完善行业防范治理长效机制，近日工业和信息化部印发了《关于运用大数据推进防范治理电信网络诈骗长效机制建设工作方案》（工信部网安〔2020〕121号，下称《方案》）。

近年来，信息通信行业坚决贯彻落实党中央、国务院决策部署，在各相关部门大力支持下，持续深入开展防范治理电信网络诈骗工作，取得阶段性成效。当前，电信网络诈骗方式和手法不断翻新，诈骗活动呈现从电话诈骗向互联网诈骗、从全国分布向重点边境地区集聚、从“短平快”诈骗向长线套路诈骗转变等趋势特点，技术对抗性日益加大，亟需运用大数据推进构建长效机制，为行业防范治理工作提供更加有力的数据支撑和能力支撑。

《方案》明确要坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中全会精神，坚持以人民为中心的发展思想，按照“整体推进、分步实施、数据驱动、技管结合、务求实效”的总体思路，坚持数据融合、数据驱动和数据共享，加快推进大数据反诈长效机制建设，深入巩固治理成效，不断提升人民群众的获得感、幸福感、安全感。

《方案》围绕技术平台、监管能力、工作机制，明确了相关具体工作任务。在技术平台方面，《方案》提出打造信息通信行业反诈大数据技术手段，持续提升大数据技术管控水平。在提升监管能力方面，《方案》明确进一步强化行业源头治理，健全创新事前防范、责任落实、成效评价、信用管理等制度。在完善工作机制方面，《方案》指出持续优化跨政企、跨

行业、跨部门的联防联控工作机制，充分释放大数据在防范治理电信网络诈骗方面的强大效能。

针对技术平台建设，《方案》提出了三项工作要求。一是建设完善行业互联网反诈数据统一资源库和互联网反诈平台，加大数据汇聚范围，具备线索发现、追踪溯源等能力，实现对涉诈 IP、域名、APP 有效研判和处置。二是开展省级反诈大数据平台建设试点，提升属地反诈大数据运用能力，逐步在全国范围内推进反诈大数据平台建设。三是开展反诈大数据技术标准研究，研究制定电信网络诈骗治理标准体系架构，推进急需标准出台。

针对提升监管能力，《方案》明确了三项工作任务。一是强化事前预防能力建设，建立全网疑似涉诈网络资源交叉核验机制，对高危码号、IP 地址、域名等及时清理整顿，提早防范化解涉诈风险。二是强化事中责任督导机制建设，深化企业责任清单管理，完善问题通报和公开曝光机制，探索实施行业涉诈失信企业“黑名单”，有效落实企业主体责任。三是完善事后反诈成效评价体系，完善基础电信企业防范治理电信网络诈骗评价指数，研究重点互联网企业防范治理电信网络诈骗评价指标，客观准确评价治理成效。

此外，《方案》还就进一步完善协调推进治理、创新反诈技术与应用、加强基础保障等工作机制明确了有关要求。（来源：工业和信息化部网络安全管理局）

## ➢ 密码管理局《商用密码管理条例（修订草案征求意见稿）》公开征求意见

2020 年 8 月 20 日，为了贯彻落实《中华人民共和国密码法》，国家密码管理局起草了《商用密码管理条例(修订草案征求意见稿)》，现向社会公开征求意见。


2019 年发布的《密码法》 对商用密码管理制度进行了结构性重塑，为了落实党和国家

要求、贯彻《密码法》精神，适应新时代商用密码事业发展需求，亟需对《商用密码管理条例》（简称《条例》）进行修订（注：1999 年 10 月 7 日国务院发布《商用密码管理条例》）。公众可在 2020 年 9 月 19 日前，通过信函或电子邮件方式对《条例》征求意见稿提出意见。（来源：国家密码管理局）

- **《商用密码管理条例（修订草案征求意见稿）》**
- **全文：**http://www.oscca.gov.cn/sca/hdjl/2020-08/20/content_1060779.shtml

## ➢ 工信部就《工业互联网标识管理办法》公开征求意见

2020 年 8 月 14 日，为贯彻落实国务院《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，规范工业互联网标识服务，推动工业互联网标识发展和应用，促进工业互联网健康发展，工业和信息化部组织编制了《工业互联网标识管理办法》（征求意见稿）。

《工业互联网标识管理办法》是为了促进工业互联网标识健康有序发展和应用，规范工业互联网标识服务，保护用户合法权益，保障工业互联网标识系统安全、可靠运行，根据《中华人民共和国网络安全法》、《中华人民共和国电信条例》、《互联网信息服务管理办法》、《互联网域名管理办法》、《电信业务经营许可管理办法》、《通信网络安全防护管理办法》等法律法规和规章，制定。（来源：中国网信网）

- **《工业互联网标识管理办法》**
- **全文：**http://www.miit.gov.cn/n1278117/n1648113/c8054148/content.html

## ➢ 中央网信办等六部门下发通知联合开展未成年人网络环境专项治理行动

2020 年 8 月 19 日，当前，未成年人沉迷网络游戏、网络不良信息、网络不良社交等问题较为突出，严重影响未成年人身心健康成长。为营造良好安全的未成年人网络环境，日前，教育部、国家新闻出版署、中央网信办、工业和信息化部、公安部、市场监管总局等六部门联合下发《教育部等六部门关于联合开展未成年人网络环境专项治理行动的通知》，启动开展未成年人网络环境专项治理行动。

通知要求，本次专项整治的重点是影响未成年人健康成长的不良网络社交行为、低俗有害信息和沉迷网络游戏等问题。


重点采取五项举措：一是集中整治未成年人沉迷网络问题。重点对未落实网络游戏用户账号实名注册制度、控制未成年人使用网络游戏时段时长、规范向未成年人提供付费和打赏服务等方面要求的网络游戏企业或平台进行全面整治。二是集中整治网络不良行为。加大对“饭圈”“黑界”“祖安文化”等涉及未成年人不良网络社交行为和现象的治理力度，重点对涉及未成年人网络社交中出现的侮辱谩骂、人身攻击、恶意举报等网络欺凌和暴力行为，以及敲诈勒索、非法获取个人隐私等违法活动予以查处。三是专项治理低俗有害信息。集中对学习教育类网站平台和其他网站的网课学习版块推送网络游戏、低俗小说、娱乐直播等与学习无关的信息问题进行治理。四是加强对企业监督监管。督促互联网企业严格落实主体责任，加大对涉未成年人信息内容审核力度，及时发现和处置有害信息。加强信息通报，引导企业切实履行社会责任，规范有序经营。五是加强教育宣传引导。部署各地中小学集中开展学生网络素养和网络自我保护教育，有效提高中小学生网络安全意识。开展普及家庭教育科学理念的宣传活动，指导家长履行监护人职责，引导未成年人限时、安全、理性上网，学习使用文明、健康的网络语言，预防和制止未成年人沉迷网络。

通知要求，营造良好的网络环境，是促进未成年人身心健康发展、维护人民群众切身利益和社会和谐稳定的重要举措，各地教育、新闻出版、网信、公安、电信、市场监管等部门要高度重视，周密部署，建立联动协调机制，深入摸排网站、平台和应用程序中存在的问题，坚决打击取缔违法违规的网站平台，全面净化未成年人网络环境。（来源：教育部）

- **教育部等六部门关于联合开展未成年人网络环境专项治理行动的通知**
- **全文：**http://www.moe.gov.cn/srcsite/A06/s7053/202008/t20200826_480306.html

# 五、本期重要漏洞实例

## ➢ Microsoft Windows Graphics Components 远程代码执行漏洞

**发布日期：**2020-08-18
**更新日期：**2020-08-18
**受影响系统：**
Microsoft Windows Server 2008 R2 SP1
Microsoft Windows Server 2008 SP2
Microsoft Windows 7 SP1
Microsoft Windows Windows Server 2012
Microsoft Windows 8.1
Microsoft Windows RT 8.1 SP0
Microsoft Windows Server 2012 R2
Microsoft Windows 10
Microsoft Windows 10 1607
Microsoft Windows Server 2016
Microsoft Windows Server 2019
Microsoft Microsoft Windows Server 1803
Microsoft Microsoft Windows Server 1903
Microsoft Windows 10 1709
Microsoft Windows 10 1803
Microsoft Windows 10 1809
Microsoft Windows 10 1903
Microsoft Microsoft Windows Server 1909
Microsoft Windows 10 1909
**描述：**

---

CVE(CAN) ID: CVE-2020-1153
Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Graphics Components 是其中的一个图形组件。
Microsoft Windows Graphics Components 中存在远程代码执行漏洞该漏洞，该漏洞源于 Microsoft 图形组件处理内存中对象的方式存在问题，攻击者可利用该漏洞在目标系统上执行任意代码。
**建议：**

---

厂商补丁：
Microsoft
厂商已发布了漏洞修复程序，请及时关注更新：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1153

## ➢ 深信服终端监测响应平台（EDR）远程命令执行漏洞

**发布日期：**2020-08-17
**更新日期：**2020-08-17
**受影响系统：**
深信服终端检测响应平台 EDR
**描述：**

---

CVE(CAN) ID: CNVD-2020-46552
深信服终端检测响应平台 EDR 可通过云网端联动协同、威胁情报共享、多层级响应机制，帮助用户快速处置终端安全问题，构建轻量级、智能化、响应快的下一代终端安全系统。
深信服终端监测响应平台（EDR）存在远程命令执行漏洞。攻击者可通过构造 HTTP 请求来利用此漏洞，成功利用此漏洞的攻击者可以在目标主机上执行任意命令。

**建议：**

---

厂商补丁：
深信服
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.sangfor.com.cn/product/net-safe-mobile-security-edr.html

## ➢ Apache Shiro 权限绕过漏洞

**发布日期：**2020-08-18
**更新日期：**2020-08-18
**受影响系统：**
Apache Shiro <1.6.0
**描述：**

---

CVE(CAN) ID: CVE-2020-13933
Apache Shiro 是美国阿帕奇（Apache）软件基金会的一套用于执行认证、授权、加密和会话管理的 Java 安全框架。Apache Shiro 存在权限绕过漏洞。攻击者可利用漏洞导致绕过身份验证。
**建议：**

---

厂商补丁：
Apache
厂商已发布了漏洞修复程序，请及时关注更新：
https://lists.apache.org/thread.html/r539f87706094e79c5da0826030384373f0041068936912876856835f%40%3Cdev.shiro.apache.org%3E

## ➢ IBM QRadar SIEM 跨站脚本执行漏洞

**发布日期：**2020-07-13
**更新日期：**2020-08-25
**受影响系统：**
IBM QRadar SIEM 7.4.0<= Version <=7.4.0 Patch
IBM QRadar SIEM 7.3.0<= Version <=7.3.3 Patch
**描述：**

---

CVE(CAN) ID: CVE-2020-4513
IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。
IBM QRadar SIEM 7.4.0 至 7.4.0 Patch 2 版本和 7.3.0 至 7.3.3 Patch 3 版本存在跨站脚本执行漏洞。攻击者可利用该漏洞在 Web UI 中注入任意 JavaScript 代码从而改变预期的功能，这可能导致可信会话中的凭据泄露。

<*链接：https://www.ibm.com/support/pages/node/6246131
*>
**建议：**

---

厂商补丁：
IBM
IBM 已经为此发布了一个安全公告（6246131）以及相应补丁：
6246131：Security Bulletin: IBM QRadar SIEM is vulnerable to cross-site scripting (CVE-2020-4513)
链接：https://www.ibm.com/support/pages/node/6246131

# 六、本期网络安全事件

## ➢ GPS 定位器变身窃听器 有公司因此损失上千万

2020 年 8 月 17 日，一提起窃听，很多人可能最先想到的都是谍战剧的剧情。然而，这些我们在电影电视里看到的情节很有可能就发生在我们身边。最近，北京一家安防公司就因为商业机密被窃听，企业竞标失败，蒙受了重大损失，而窃听器竟然是我们常见的 GPS 定位器。


在北京一家安防公司，记者见到了这样一个小黑盒。工作人员告诉记者，企业讨论营销方案的会议是高度保密的，但没人想到，座椅下却藏着这个小黑盒。由于商业机密泄露，企业竞标失败，从而蒙受了上千万元的损失。这种小黑盒子，叫做 GPS 定位器，它广泛用于汽车防盗和企业运营车辆管理。

**而这样的产品是如何用来非法窃听的呢？**记者尝试买了一个产品进行测试，拆开产品的包装，是一个火柴盒大小的塑料盒，记者按使用说明书在手机上安装好 APP，打开 APP，果然在上面就能实时观察车辆的行驶轨迹。接下来要尝试的是远程监听。两位记者约定，一位和定位器一起留在车内，另一位记者回到办公室准备听音。结果证实，不管被窃听者的声音是大还是小，监听到的声音就像跟对方打电话那么清楚。此外，在 APP 的界面中，还有一个“远程录音”的按钮，启动后，这段对话就被存到了手机里。

也就是说，只要在被窃听者身边放置这样一个 GPS 定位器，就相当于放了一个保持通话的手机。一切声音会被传到窃听者的手机上，甚至被录音，被而窃听者对发生的这一切却

浑然不知。

GPS 定位器广泛用于私家车的防盗和企业进行车辆管理。但是，当 GPS 定位器被设计成小巧易于隐蔽、能远程听音的时候，就让产品变了味。而且一些生产厂家和销售商家也正是利用监管盲区，在一些电子产品销售推广广告中进行或多或少的明示暗示其隐藏功能。

**这种能够远程收音的 GPS 定位器，内部结构非常简单：**一块物联网芯片，还有一块为它供电的电池。芯片接收卫星数据，将数据传输至信号塔，再经信号塔将定位数据传至服务器，使用者向服务器发送请求，就能获取芯片的精准位置。相比一般的物联网芯片，这块芯片上多加了一个微型的麦克风。


目前，GPS 定位器这类产品尚未列入国家强制性产品认证目录。但在此基础上增加麦克风收音等功能却没有相关管理规定，形成监管的盲区。而生产厂家和销售商家也正是利用这种监管盲区，在这类产品销售推广广告中，进行或多或少的明示暗示其隐藏功能。

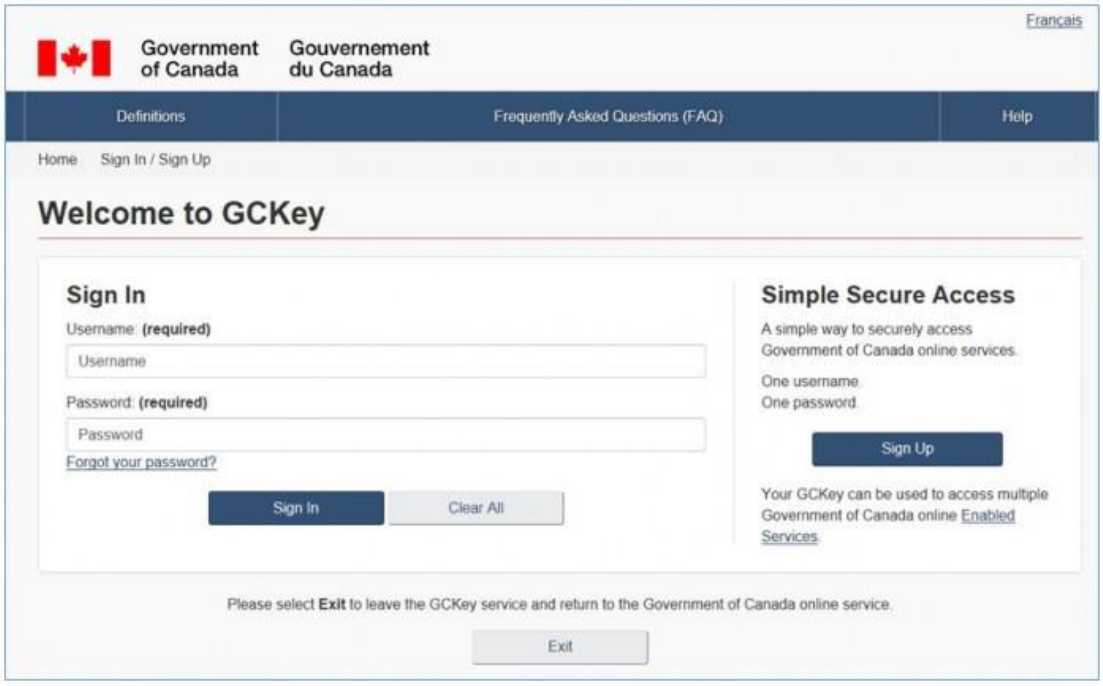
2015 年起实施的《禁止非法生产销售使用窃听窃照专用器材和“伪基站”设备的规定》明确禁止自然人、法人及其他组织非法生产、销售、使用窃听窃照专用器材。我国《最高人民法院关于行政诉讼证据若干问题的规定》第五十七条也明确规定，以窃听手段获取的材料不但不能作为定案依据，行为人很可能还要承担相关的法律责任。对此，专家指出，随着科技的发展，法律应该同步跟进，对利用新技术手段实施的各类违法行为进行规范。

**中国政法大学传播法研究中心副主任朱巍：**“对个人信息实际上在各个国家，包括中国在内都是一个最高位阶的保护。不能靠企业自律，也不能通过个案来处理，应该是一个常态化的过程。必须是线上线下结合起来，从它的生产源头开始堵截才可以。”（来源：央视网）

## ➢ 加拿大税务网站被攻击 黑客入侵账户给自己发救济金

2020 年 8 月 18 日，据加拿大广播电视台报道，加拿大联邦官员表示，加拿大税务网站遭黑客攻击，11200 个账户被入侵，黑客利用漏洞访问政府网站并给自己重新发放紧急救济金。加拿大财政部秘书处首席信息官马克·布劳拉德（Marc Brouillard）17 日表示，此次攻击是“凭证填充”的一种形式，黑客通过这种方式欺骗性地获取用户名和密码，并利用了许多人在不同账户上使用相同密码这一点，获得利益。

**布劳拉德表示，所幸由于拥有适当的系统，因此能够及早发现这些攻击，并在很大程度上减轻了对加拿大人的影响。**




布劳拉德说，总共有 11200 个帐户受到攻击，其中包括 9000 多个 GCKey 帐户和另外 5600 个加拿大税务局帐户，几乎一半的 CRA 帐户与 GCKey 都遭到黑客袭击。布劳拉德表示，网页一旦发现受到威胁，受影响的帐户就会被取消，现在部门正在联系被盗用户，并提供有关如何接收新 GCKey 账户的说明。

加拿大税务局网站与 CGkey 是安全在线门户网站，为加拿大人提供就业保险、退伍军人福利以及移民申请等服务。疫情期间，加拿大人通过该网页领取救济金，该门户网站也是此次被攻击的主要对象。8 月初，有许多加拿大人收到邮件说他们的用户名、邮箱地址以及直接存款信息被更改，与此同时，尽管他们没有申请的救济金却也以他们名义发放。

加拿大税务局首席信息官安妮特·布蒂科弗（Annette Butikofer）表示，近日税务局网站

已经受到 3 次黑客攻击，第一次攻击是在 8 月 7 日。受到攻击后，税务局于 8 月 11 日与加拿大皇家骑警联系，并开始加强安全措施。本周末由于税务局再次受到攻击而关闭了各项服务后，加拿大市民才收到有关违规行为的通知。 布蒂科弗表示，加拿大雇主使用的“我的企业帐户”已通过其他安全措施重新上线，以便雇主可以申请最新一轮的紧急工资补贴。她还表示，个人账户有望在本周中恢复运行，现在所有网络服务将转为电话服务。加拿大税务局正在向其帐户遭到破坏的加拿大人发送通知，通知上将说明人们将如何确认自己的身份并重新获得访问权限。任何受害者都将有资格获得债权人保护。

联邦机构加拿大反欺诈中心发布的信息显示，2020 年共有 1.3 万多名加拿大人成为欺诈行为的受害者，总金额为 5100 万加元（约合人民币 2.55 亿元），共有 1729 名为涉及新冠肺炎欺诈的受害者，其受骗金额达到 555 万加元（约合人民币 2775 万元）。（来源：海外网）

## ➢ 涉案 3000 余万虚拟货币黑客案，主谋曾从事信息安全工作

2020 年 8 月 19 日，日前，苏州园区警方通过缜密侦查，循线追踪，成功侦破苏州首起针对虚拟货币的黑客犯罪案件，抓获多名专门利用黑客手段盗取账户密码、窃取虚拟货币，通过暗网联系职业洗钱销赃团伙变现的犯罪嫌疑人，涉案金额高达 3000 余万元。

“警察同志，有人盗取了我的虚拟货币。”不久前，郑女士(化名)至苏州工业园区公安分局报案称：其拥有的价值 100 余万元的虚拟货币被盗。接报后，园区公安分局高度重视，立即汇同苏州市公安局网安支队成立专案组，对该案件进行侦查。

通过对被盗虚拟货币走向进行梳理，专案组民警深挖细查，经过不懈努力，成功锁定了一个藏匿于云南昆明、广东广州的家族式洗币团伙，并先后远赴云南、广东，成功打掉了一个专门负责转移黑客手段窃取来的虚拟货币团伙，抓获以姚某为首的 4 名洗币嫌疑人。

归案后，经对姚某等嫌疑人的审讯，专案组民警发现，姚某就是黑客团伙联络人。民警继续对直接窃取虚拟币的黑客团伙展开追查。然而，作案的黑客团伙在听到消息后销声匿迹了。不抛弃不放弃，民警紧盯该案循线侦办，经过大量的研判追踪，从纷繁复杂的网络线索中发现了利用黑客手段盗窃虚拟货币的犯罪嫌疑人线索。该团伙两名犯罪嫌疑人宁某、陈某均为某网络科技公司前工程师，技术水平高、犯罪手段隐秘。

在充分查明两名嫌疑人落脚点及生活、作案规律之后，专案组民警远赴福建厦门、福州两地，分别抓获两名黑客犯罪嫌疑人宁某、陈某，查获涉案资金 3000 余万元。在大量的证据面前，两名黑客对犯罪事实供认不讳。

据悉，犯罪嫌疑人宁某曾在某网络科技公司从事计算机信息安全方面的工作。工作期间通过社交论坛了解到一些专业人员利用企业网络漏洞进行攻击以窃取巨额网络资产的“成功”案例，这令他心动万分。辞职后，宁某利用专业优势，打起了侵占他人网络资产的念头。但苦于没有目标公司的网络地址，一直未行动。

后来，宁某通过社交软件结识了合作的姚某，通过姚某的“牵线搭桥”，宁某锁定了目标，挨个儿地寻找网络漏洞，实施渗透入侵，借此来获取相关程序的管理权限，以便操作实施资产转移。在面对一些较难入侵的系统时，宁某想到了专业能力更强的前同事陈某，在他的利诱之下，利欲熏心的陈某同意入伙，一同参与违法犯罪活动。短短数月，仅两名黑客就获利 3000 余万元。

就在宁某赚得盆满钵满之际，姚某被抓的消息传了过来，看到形势不妙，妄图摆脱嫌疑的陈某立即联系了宁某，还丢弃手机、电脑，想要暂避风头，借此躲避公安机关追捕。然而法网恢恢，疏而不漏，等待他们的将是法律的严惩。目前，园区警方已对宁某、陈某等黑客嫌疑人以及姚某等嫌疑人采取刑事强制措施，案件仍在进一步调查中。

**警方提示：**在处理网络财产的电脑或手机上，切记不要轻易点击来历不明的链接，或者下载路径不明的软件，对相关查杀软件要经常更新和升级，定期对后台进行安全更新维护，尽量多设置“网络密钥”，最大程度增加黑客攻击的成本和难度，也最大限度保障自身财产权益不受侵害。（来源：现代快报）

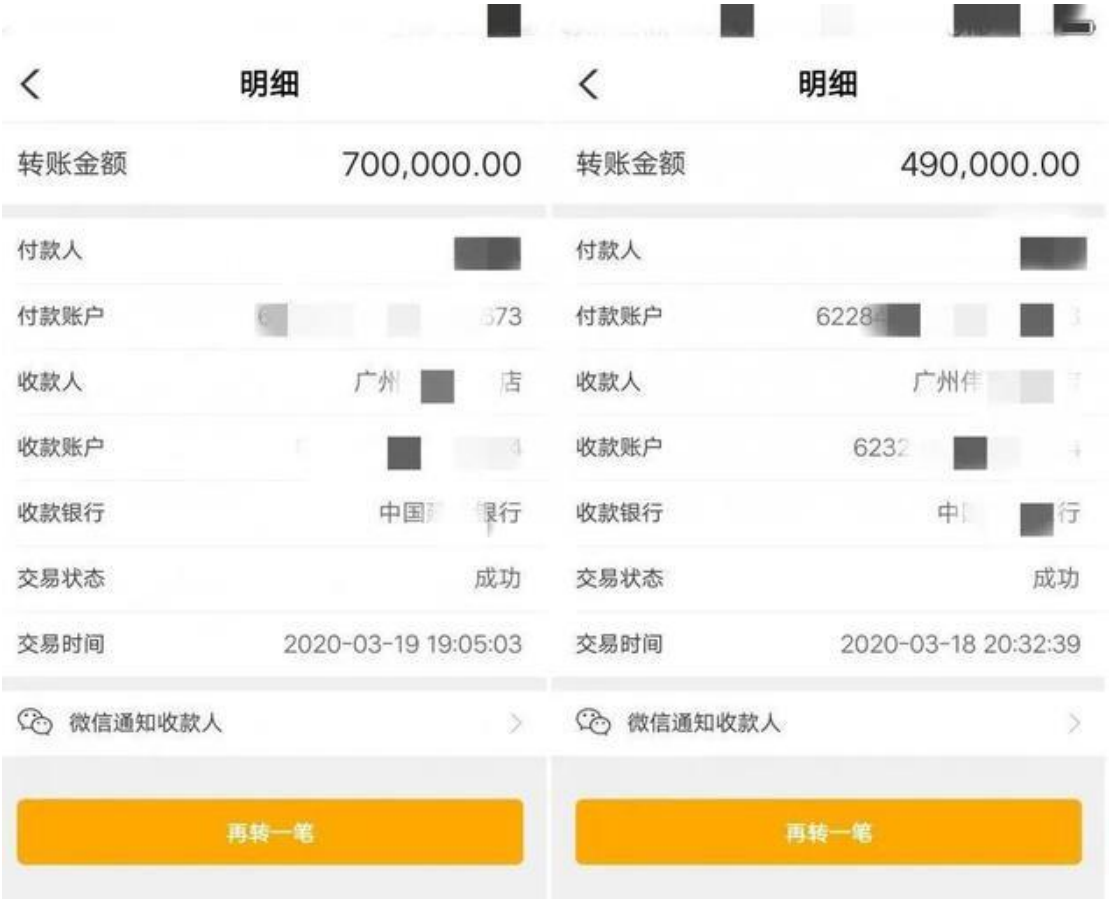
## ➢ “杀猪盘”牵出侵犯公民个人信息案，通信公司员工成骗子帮凶

2020 年 8 月 24 日，记者从四川凉山州警方获悉，近期，凉山德昌县公安刚办理了一起

案件，一个跨境“杀猪盘”诈骗团伙，诱导受害人下载使用假冒赌博平台，进入导师教你博彩的骗局，在四川、辽宁、重庆、内蒙古、新疆、湖南等十余省成功作案 20 起，涉案金额高达 1200 余万元。这起案件中，通信公司人员竟成了幕后黑手，精准筛选用户信息倒卖，成为诈骗团伙的“秘密武器”。

**抓获犯罪嫌疑人女子遭“杀猪盘”被骗 120 万 警方打掉跨境诈骗团伙**

2020 年 3 月 21 日，德昌县公安局接到本地居民吴某报案，因网名为“初恋少冰”的人诱导，下载某 APP 软件，步入导师教授参与网络赌博“杀猪盘”骗局。




转账凭证起初，吴某试着下注几百、上千都是翻了几番的赢，连续一个星期赢钱，尝到了甜头的她不知不觉越陷越深。随后，她追加了投注，但“运气”急转直下，最多一天输了 70 多万元，输红眼的她再也停不下来，直到借不到钱，才恍然醒悟已经输了 120 余万元。

案件金额大、危害程度深，德昌县公安局立即展开追查，侦查人员陷入电信网络诈骗常规套路，犯罪分子藏身国外作案，银行账户也只是花钱购买的空壳，账户上的钱早已转移。案件陷入僵局，但德昌县公安局坚持不懈，全力开展追查。经过专案警力三个多月不分昼夜的摸排、走访，辗转四川、辽宁、重庆、内蒙古、新疆、湖南等十余省数千公里地收集线索。案件告破，团伙头目陈某被抓后，心中不忿，连声说：“居然阴沟里翻船、居然阴沟里翻船”。

**抓获犯罪嫌疑人通信公司人员成幕后黑手 精准筛选用户信息倒卖**

在侦办该这起电信诈骗案件中，德昌县公安局网情大队查明受害人一笔资金流向非常可疑，经过层层核查，细化摸排，打掉一个层级分明的贩卖公民个人信息黑色产业链，揪出隐藏在幕后的“内鬼”。罪魁祸首落网，幕后黑手渐渐浮出水面。某电信、联通下属公司营销人员，使用网络编程技术，将非法程序放至电信、联通的云主机、堡垒机、租户平台上窃取访问特定网页 URL 的电话号码，即是将访问浏览过赌博、彩票、股票等信息的用户，精准确定用户手机号码。

运营商内部不法人员，非法获取公民个人信息后，将信息倒卖给兜售贩卖公民个人信息的中间商，再转卖致境内外诈骗团伙，这些团伙利用轻松获取特定人群的电话号码，实施各种违法犯罪。

警方介绍，德昌县公安局打掉的是一个组织有序、分工明确的电信网络“诱导赌博”诈骗犯罪团伙。该犯罪团伙涉及境外实施诈骗、境内洗钱、境内贩卖公民个人信息黑色产业链。在短短的数月时间，购入电信 800 余万条、联通电话号码 8000 余万条，并通过精准筛选出信息正好成为犯罪分子的“优质客户”，成为诈骗团伙致胜的“秘密武器”。

目前，已抓获涉嫌侵犯公民个人信息罪嫌疑人 6 人，妨害信用卡管理秩序罪嫌疑人 7 人，掩饰、隐瞒犯罪所得罪 1 人，采取其他强制措施 9 人，扣押作案手机 30 部、银行卡 60 张、汽车 3 辆、诈骗资金 800 余万，扣押涉案固定资产 850 余万元。案件正在进一步全链条深挖中。（来源：红星新闻）

## ➢ 自家网站怎么变身赌博主页了？别到被处罚时才发现

2020 年 8 月 26 日，小伙伴们有过这样的经历么登录一些经常上的小型网站时熟悉的网页没有出现却突然弹出了“一本万利”“美女荷官”是输错网址了吗？你急忙检查没错啊，什么时候变成赌博网站了你的脑袋充满了问号……通常来说，遇到上述情况的朋友，你访问的网站很有可能已经被黑客非法“光顾”了。原有网站的域名遭到劫持，被篡改指向某些境外赌博网站。更让人啼笑皆非的是，这些网站的运营者甚至都不知道自家网站已经无法访问，直到被用户投诉、网警上门时才发现。近年来，这样的情况在互联网上时有发生，并非个案。

**案例揭秘**


**案例一：**2020 年 6 月 28 日，云南省大理州洱源县公安局网安部门巡查中发现，当地某技术公司网站主页被篡改为 XX 境外赌博网站，公司主页无法正常访问。经深入调查，网安部门发现该公司将网站交由第三方公司建设、维护。双方合同到期后，公司未予续期，且该公司未建立网络安全管理制度，也未采取安全保护技术措施，网站处于无人管理状态，最终导致公司网站被劫持，并篡改为境外赌博网站。

**案例二：**2020 年 3 月 10 日，云南省大理市公安局网安部门在工作中发现，大理市某商贸有限公司网站被黑客入侵，并篡改页面，植入大量违法信息。经调查，自网站开办以来，该公司未采取防范计算机病毒、网络攻击、网络侵入等网络安全保护技术措施，也未落实网络安全保护责任，导致网站被入侵篡改。

**网站发生上述情况公安机关将如何处理呢今天就给大家普及一个重要知识点**

一案双查针对网络乱象，公安机关已实行“一案双查”制度，即在针对涉网违法犯罪案件调查中发现互联网运营者不履行法定网络安全责任义务，存在安全问题的情况，同步开展侦查调查和执法监督检查。举个例子，如果你们公司的网站发生上述类似网络安全事件或未履行网络安全责任义务被违法犯罪分子利用实施违法犯罪活动，公安机关就会同步开展“一案双查。”一查破坏网站的违法犯罪分子，比如黑客，并依法打击。二查你们公司是否落实网络安全责任，即有没有按照《中华人民共和国网络安全法》规定，履行网络安全义务。如果没有，那你们公司也将受到处罚。

**对“一查”大家应该没有疑问，而对“二查”可能会产生疑惑，有人可能会说：“我也**

**是受害者啊，为什么要处罚我？”。让我们看看法律是怎么规定的。**


**法律依据：《中华人民共和国网络安全法》对网络运营者应当履行的网络安全义务有明确规定，下面让我们来划划重点：**

第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其他义务。

第二十五条：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第五十九条：网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

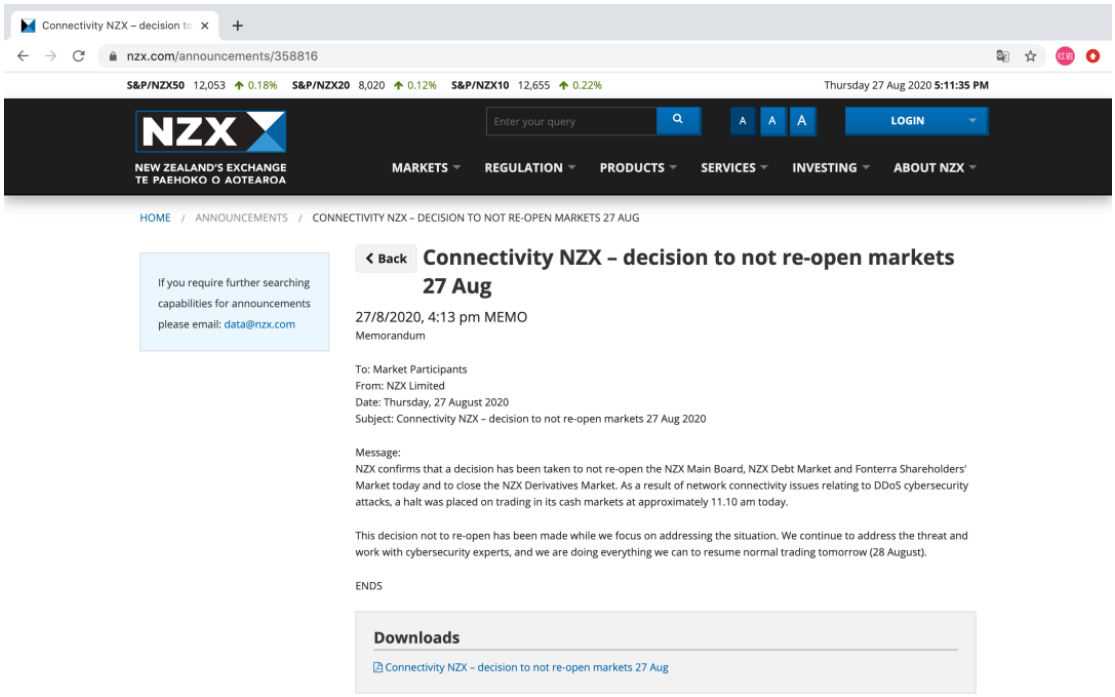
此外，《计算机信息网络国际联网安全保护管理办法》（公安部令第 33 号）也对此作出明确而具体的规定。网络运营者对维护网络安全是存在义务的。也就是说，如果没有按照要

求进行防护，就没有履行义务，而没有履行义务，那就涉嫌违法，而违法就将面临处罚。在上述两个案例中，公安机关开展“一案双查”，在对破坏公司网络的违法犯罪分子进行依法打击的同时，也对两家公司没有履行网络安全保护义务的行为依法作出了警告的行政处罚。

**网警提示：**网络安全是矛与盾之间的较量，不想受伤，仅仅祈祷矛永远不会出现，是不可能的。网站必须打造出能够保护自己的坚固盾牌，并时刻紧盯攻击方向，及时调整应对。只有这样，才能在动态博弈中立于不败之地。（来源：公安部网安局）

## ➢ 新西兰证券交易所遭到 DDoS 攻击：连续关闭三天！

2020 年 8 月 27 日，新西兰证券交易所网站 27 日受到网络黑客攻击，被迫暂停交易。这已经是该交易所连续第三天因黑客攻击暂停交易。




**攻击事件的具体性质尚不清楚：**NZX 发言人称，今天周四之所以决定关闭股市大约 70 分钟，是由于“DDoS 网络安全攻击引起了网络连接问题”。股市在周二和周三也关闭过，NZX 表示遭遇这些事件后希望迅速恢复正常。发言人称：“鉴于我们专注于应对这一情形，决定不重新开放股市。我们继续应对威胁，并与网络安全专家合作；我们在竭尽全力，争取明天（8 月 28 日）恢复正常交易。”

当地媒体猜测，攻击目标是新西兰证券交易所的网站，而不是其核心交易系统。然而，新西兰证券交易所之所以关闭交易，是由于如果该网站停运，影响股市走向的公司信

息无法发送到投资者手中。为 NZX 提供网络服务的新西兰电信公司 Spark 表示，周二晚些时候它发现并缓解了 DDoS，并恢复了服务。Spark 让我们向 NZX 征求进一步的评论，我们还不知道到底什么受影响或如何受影响。

NZX 运营新西兰的资本市场、风险市场和大宗商品市场，提供市场信息，包括实时股票行情、市场数据和新闻。NZX 不是全球主要证券交易所之一，但是由于 NZX 的几个主要成员获得的回报可观，全球托管基金投资的主力股票在其上面交易。该交易所下面还开有恒天然集团股东市场（Fonterra Shareholders Market），这个交易所专供大型乳制品合作社恒天然集团的农民股份进行交易，恒天然集团约占全球乳制品出口总量的三分之一。

虽然 NZX 的警告并未提到发动攻击的威胁分子的名称或用来发动 DDoS 攻击的方法，但不法分子很有可能使用了提供 DDoS 租用服务（又叫 stresser 或 booter）的网站的服务。

最近，全球各地的执法机构一直在关闭恶作剧者、威胁分子或黑客活动分子对在线服务和网站发动大规模 DDoS 攻击所使用的众多 DDoS 租用服务。比如说，4 月初荷兰警方反网络犯罪小组与外部各方开展了联合行动，在短短一周内打掉了 15 家提供 DDoS 租用服务的网站，包括主机托管服务提供商或域名注册服务提供商、其他国际警察部门、欧洲刑警组织、国际刑警组织和 FBI。

除了打击提供 DDoS 租用服务的网站外，执法机构还在追查使用这种服务的那些人，“断电行动”（Operation Power Off）开展后，数百人已经遭到了调查。作为这场行动的一部分，提供 DDoS 租用服务的网站 WebStresser 在 2018 年 4 月被关掉，这项 DDoS 租用服务关闭时有 151000 个注册用户。之后，DDoS 缓解公司 Link11 报告欧洲境内的 DDoS 攻击减少了约 60%。赛门铁克的报告估计，DDoS 事件对小公司造成的经济影响可能高达 12 万美元，而大公司在每次攻击后最后可能平均花费 200 万美元才能恢复服务。（来源：新华网）

## 信息安全意识产品服务


**021-33663299**