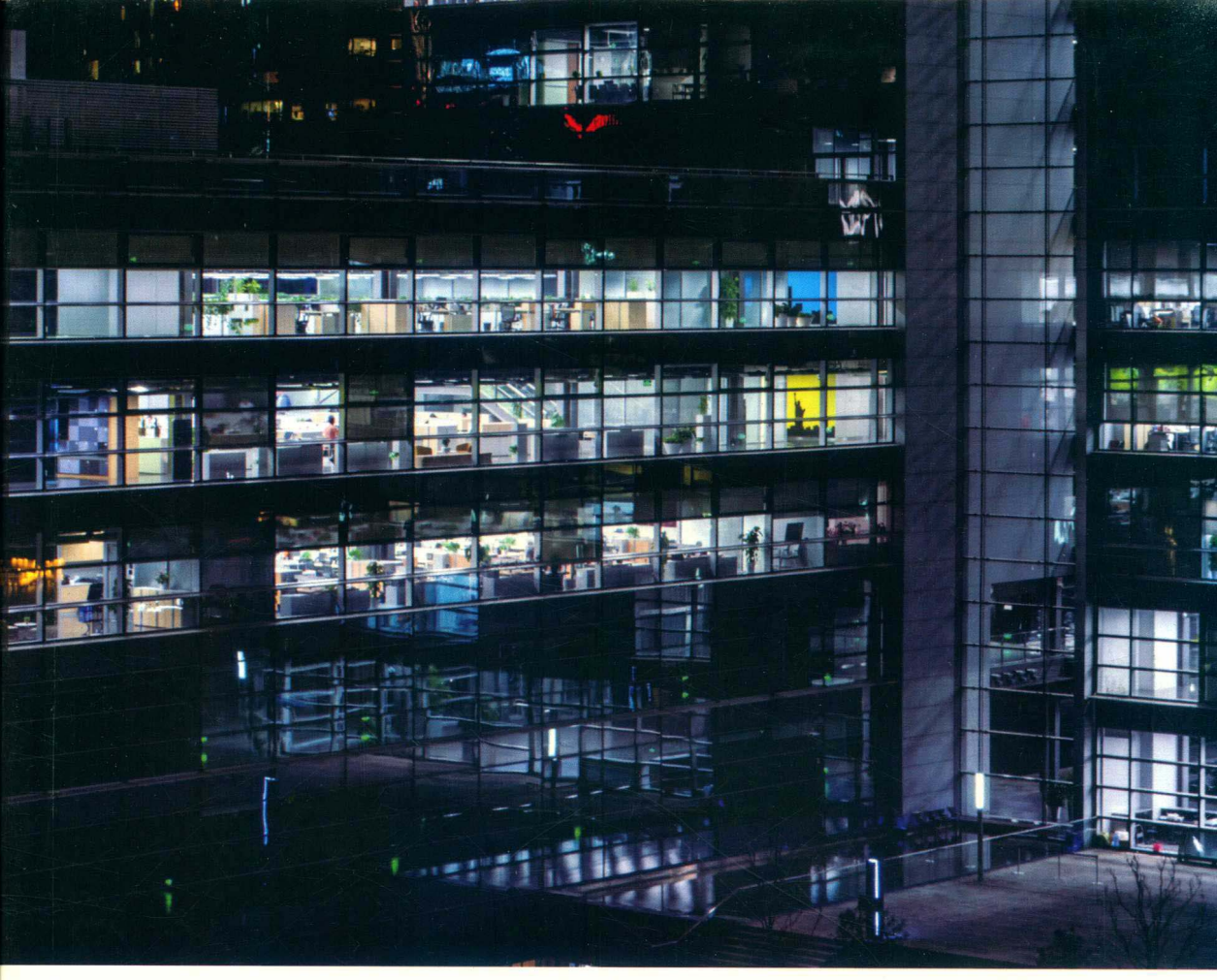

A Review of Global Cyberspace Security Strategy and Policy (2018)

全球网络空间安全战略与政策研究（2018）

本书编写组 ◎ 编著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

A Review of Global Cyberspace Security Strategy and Policy (2018)

全球网络空间安全战略与政策研究（2018）

本书编写组 ◎ 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

全球网络空间安全战略与政策研究. 2018 / 全球网络空间安全战略与政策研究编写组编著. -- 北京 : 人民邮电出版社, 2019.12
ISBN 978-7-115-52553-6

Ⅰ. ①全… Ⅱ. ①全… Ⅲ. ①网络安全－研究 Ⅳ. ①TN915.08

中国版本图书馆CIP数据核字(2019)第238863号

内 容 提 要

本书聚焦网络空间安全领域的战略与政策问题，从顶层设计、安全防护、数据治理、犯罪治理、内容管理、基础设施保护、未成年人保护、情报获取等方面系统梳理了2018年全球网络空间安全政策动态，分析了每个月的安全形势特点，重点研究了美国、加拿大、俄罗斯、日本等国的网络安全政策变化情况，介绍了一些国家和地区的有关战略和文件，全景式展现了全球网络空间安全领域的政策变化形势。本书主要面向党政机关、事业单位、高校、科研机构、企业等相关从业人员，可以帮助读者了解网络安全的方方面面。

◆ 编　　著　本书编写组
责任编辑　唐名威
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：20.75　　2019 年 12 月第 1 版
字数：340 千字　　2019 年 12 月北京第 1 次印刷

定价：139.00 元

读者服务热线：（010）81055493　印装质量热线：（010）81055316
反盗版热线：（010）81055315
广告经营许可证：京东工商广登字 20170147 号

前　言

这是互联网大发展的时代，也是网络空间大博弈的时代。

2013 年，震惊全球的“棱镜门”事件揭露出的真相让各国从享受互联网发展福祉的和谐氛围中惊醒。短短几年过去，已经有 60 多个国家发布了国家网络战略，70 多个国家建立了网络作战部队，网络空间安全已经成为各国国家安全政策的优先事项，以及各大安全论坛和国际会议的重要议题。各国都认识到，互联网的力量不仅削弱了经济壁垒，碾平了沟通障碍，同时也创造了一个更加复杂的国际竞争空间。如果说，五百年前谁控制海洋，谁就能在大国竞争中掌握主导权，那么，五百年后的今天，谁可以利用和治理好网络，谁就能掌握国际竞争和未来发展的优势。

我国是互联网发展大国，党和国家高度重视网络安全在经济社会发展和国家安全中的重要作用。习近平总书记指出，没有网络安全就没有国家安全。党的十八大以来，我国始终把网络安全摆在国家安全和发展的优先地位。2014 年，中央网络安全和信息化领导小组成立，开启了我国网络强国建设事业的宏伟篇章。几载磨砺，我国已经在信息化发展、核心技术突破、加强网信领域军民融合、参与网络空间国际治理等方面取得了长足进展，维护我国网络空间主权、安全和发展利益的实力得到了大幅提升。与此同时，我们也清醒地认识到，面对百年未有之变局、面对网络斗争的风波诡谲、面对世界各国的千帆竞逐，我国网络空间安全能力与有些国家相比仍存在一定差距，仍需要不断追赶和进步。推进网络强国建设，制定合理的政策措施，需要全面掌握网络空间发展态势，不断学习各国网络安全发展建设的政策经验。为了整体把握全球网络安全

战略和政策形势，本书编写组全面跟踪全球一些国家制定的网络安全战略与政策，以动态跟踪为基础，编写形成了这本《全球网络空间安全战略与政策研究（2018）》。此书力图全景式地对2018年一些国家的网络安全政策进行梳理，期待能够为政府、企业、高校、科研机构的有关从业人员提供一定的借鉴和参考，也欢迎大家批评指正。

全书共5章：第1章对2018年全球网络空间安全政策内容和特点进行了概览性评述；第2章对有代表性的几个国家2018年的安全政策及部分专门政策进行了研究分析；第3章对2018年每月全球网络空间政策形势进行了综述；第4章是2018年部分国家（地区）的政策文件译文；第5章则是本书编写组对相关信息的动态汇编和整理。其中，第1章至第4章由赵志云编写，第5章由袁钟怡完成。此外，谭丝妲、徐阳华也对本书内容的收集和整理做出了贡献。全书在描述事件发生的时间时，若没有特意指出具体年份，均默认为2018年。

风云多剧变，正是奋发时。应对网络空间威胁风险，把握网络空间战略机遇，是时代考验，更是国家使命。网络空间是一个涉及政策立法、技术应用、社会治理等多层次、宽领域、跨学科的研究领域，安全形势的快速复杂变化令这个领域的研究只有休止符，没有终结音。未来，我们将坚定初心，继续在网络空间安全的技术和政策研究领域深耕厚植，久久为功，不断推出更多技术和政策研究成果。

本书受到国家社会科学基金重大项目“总体国家安全观视野下的网络治理体系研究”（No.172DA107）的资助。

本书编写组

2019年5月

目 录

第 1 章

2018 年总体形势

2018年，国外网络与信息安全整体形势不容乐观，信息泄露、漏洞隐患、黑客攻击等网络安全事件频发。对此，一些国家从安全策略、安全防护、战略立法、国际治理与合作等多方面加快网络与信息安全体系建设，重点加强数据监管和治理，加速布局人工智能、5G、区块链等领域，推进前沿技术研发及应用。热点网络安全事件中，脸谱（Facebook）公司数据泄露事件、美国中期选举期间网络安全动向备受关注。

一、信息泄露、漏洞隐患、黑客攻击等网络攻击事件频发，整体安全态势堪忧

2018年全球网络安全总体态势不被看好。一是亚太地区网络安全态势堪忧。美国火眼公司2018年1月发布的《亚太地区网络攻击报告》显示，亚太地区网络攻击驻留时间全球最长。全球网络攻击驻留时间中位数为99天，亚太地区则为172天，欧洲、中东和非洲地区为106天，美国为99天。二是核设施网络安全状况堪忧。英国皇家战略研究所2018年1月公布的《全球核武器系统网络安全调研报告》显示，由于设计年代久远，核武器系统存在许多非常明显的安全漏洞，对黑客攻击活动基本没有抵御能力，网络攻击可能会破坏核武器的控制装置，其后果不堪设想。

（一）信息泄露事件频发

影响范围最广的是2018年3月曝光的脸谱公司数据泄露事件，超过5 000万名用户的数据被一家名为“剑桥分析”的公司非法收集，用于协助特朗普在2016年美国大选期间预测并影响选民投票倾向，该事件引发了多国政府启动对脸谱公司的调查。此外，2018年度信息泄露事件频发。泰国最大的4G移动运营商TrueMove H的一名操作人员将亚马逊AWS S3中总计32 GB的4.6万人的数据公开在互联网上，其中包括身份信息、护照和驾驶执照等数据；英国在线购物网站DronesForLess.co.uk交易数据库无加密保护遭意外在线暴露，致数千名警方、军方、政府以及个人消费者的购买记录以及个人信息泄露；澳大利亚

一家人力资源公司基础设施遭恶意程序感染，导致超过200万活跃用户的数据泄露；以色列一家DNA检测公司遭黑客攻击，导致超过9 200万名用户的信息泄露；美国国防部表示其差旅记录遭黑客窃取，这些记录包含美国军方和文职人员的个人信息和信用卡数据。据悉，此次数据泄露可能影响了多达3万名国防部雇员。美国网络安全公司UpGuard称，100多家车厂的机密数据泄露，包括通用汽车、特斯拉、丰田、蒂森克虏伯、大众等。火眼公司旗下的安全团队在地下黑客论坛发现了一组正在被出售的数据集，涉及大量的敏感资料，其中就包括超过2亿条日本网民的个人身份信息。近期，网上出现疑似查询泄露邮箱密码信息的网站，初步统计该网站涉嫌泄露约14亿个邮箱密码，涉及Gmail、Hotmail、Yahoo等知名邮件服务运营商用户。

（二）各类漏洞隐患曝光

一是工控系统、加油站软件、固件漏洞。网络安全公司IOActive和Embedi的研究发现，工控系统APP存在严重漏洞，或导致设备被摧毁或工厂爆炸。研究人员随机挑选了34款由西门子和施耐德电气等工控系统供应商开发的APP进行测试，结果发现了147个安全漏洞，只有2款APP不存在安全漏洞。加油站软件漏洞曝光。卡巴斯基实验室研究人员发布报告称，可通过软件漏洞在线访问全球1 000多个加油站控制器，不仅能够擅自更改汽油价格，还可以窃取记录在控制器上的信用卡信息和车牌号码。固件漏洞威胁依然严峻。美国消费者协会使用基于Insignary的Clarity扫描工具，测试了14个制造商销售至美国市场的186个SOHO Wi-Fi路由器的样本，其中，83%的路由器固件中有可被潜在的攻击利用的漏洞，平均每个路由器有172个漏洞。

二是芯片漏洞。英特尔披露了其芯片的新漏洞“预兆”，能让黑客有机会获取内存数据，影响到2015年以来发布的酷睿和至强处理器。以色列网络安全公司CTS Labs披露AMD芯片存在13个安全漏洞，这些漏洞允许攻击者向芯片注入恶意代码并破坏硬件，其严重程度不亚于“熔断”和“幽灵”漏洞。

三是通信和可穿戴设备漏洞。4G LTE网络协议中的漏洞可被恶意利用，发起监视用户通信行为、跟踪设备位置、发送虚假警报等网络攻击。西班牙电信存在一个能访问用户完整个人数据的安全漏洞，可导致数百万用户的完整个人数据泄露。芬兰穿戴设备品牌Polar生产的运动手环存在漏洞，可泄露用户位置信息和2014年至今的运动路径，进而可导致情报机构、军事基地、机场或核武器存放地点曝光。美国三大运营商AT&T、Sprint和T-Mobile的系统被

发现存在安全漏洞，不良分子可利用漏洞获取用户数据。美国位置数据公司LocationSmart向客户提供的实时获取公民位置信息的应用程序接口（API）存在漏洞，他们不需要经过授权许可，就能在几秒内获取任何公民的实时位置，其精度可以达到几百米。

（三）黑客攻击愈演愈烈

一是政治性网络攻击不断，国际重大活动成为黑客攻击的重要目标。德国外交部及内政部网络疑遭俄罗斯黑客入侵，部分数据被窃取。俄罗斯国防部网站在2018年3月23日为最新的国产武器选名投票过程中，遭到了密集的分布式拒绝服务（DDoS）攻击，攻击主要来自西欧、北美等地区。据美国网络安全智库披露，美国、朝鲜首脑会晤前，韩国遭受网络攻击次数显著增加；会晤期间，新加坡作为会议地点，遭遇网络攻击超过4万次，其中，92%为侦查扫描，8%为攻击行为。

二是国家关键信息基础设施频遭攻击。网络安全研究团队FortiGuard称，近期俄罗斯多个电子产品服务中心网站遭受攻击。赛门铁克安全公司于2018年6月19日称，监测发现黑客组织正针对美国和东南亚国家的卫星通信、电信、地空成像、军事系统等设施发动攻击。卡巴斯基实验室于2018年8月1日称，俄罗斯制造业、石油、天然气、物流等领域的逾400家工业公司遭遇“鱼叉式”网络钓鱼攻击。

三是黑客攻击情报获取活动仍处于高发态势。电子前沿基金会和安全公司Lookout联合调查发现，与黎巴嫩总安全局有关的监控间谍活动Dark Caracal APT，从世界各地的安卓手机和微软视窗系统中窃取大量数据，并且有黑客组织将Dark Caracal间谍软件平台出售给某些国家，2012—2018年已盗取21个国家的记者、军事人员和其他目标的敏感信息。美国国土安全部公开表示，他们在华盛顿特区发现了电子监控设备。这些被称为国际移动用户识别码（IMSI）捕捉器的设备，通过伪装成手机信号塔并截获手机信号的方式来达到监听通话和信息的目的。

四是黑客网络攻击大肆破坏社会生活。意大利警方测速摄像头数据库被黑客攻破，约40 GB文件被删除。新加坡2018年8月遭遇了历年来最大规模的网络攻击，包括李显龙总理在内的约150万人的公共医疗个人信息失窃。芬兰赫尔辛基新企业中心负责维护的某网站在2018年4月3日遭到匿名黑客的攻击，造成约13万用户信息以及其他一些机密信息失窃。

二、多国（地区）发布网络安全立法和战略计划，加强网络安全监管顶层设计

（一）通过网络安全相关法案，加强网络安全监管举措

2018年2月，新加坡国会通过《网络安全法案2018》，旨在对提供基本服务的计算机系统加强保护，防范网络攻击。澳大利亚通过了“国家面部生物特征匹配方案”，并将其纳入立法，授权其内阁收集、使用和披露身份信息，以用于用户身份和社区保护及其他活动。2018年3月，美国参议院国土安全和政府事务委员会通过《重新授权法案》，批准了多项网络安全监管举措，包括设立网络安全和技术设施安全局，负责保护联邦网络和关键基础设施免受物理和网络威胁；实施“漏洞悬赏”计划，以挖掘国土安全部网络中的更多漏洞；实施“人才交流”计划，让私营部门的网络安全工作人员进入国土安全部工作；指导相关部门及时报告区块链技术的潜在威胁等。2018年5月，波兰政府通过一项关于国家安全体系的法律草案，详细说明了国家网络安全体系的组织、实施监督和确保遵守法律的方法以及建立《波兰网络安全战略》的程序等。乌克兰的《关于保障乌克兰网络安全的基本原则法》于2018年5月9日正式生效，明确了网络安全的管理对象和关键设施基础清单。英国执行欧盟《网络与信息安全指令》（也称NIS指令）的新法律于2018年5月10日生效，旨在确保英国的最关键行业提高网络安全。2018年6月，欧洲议会通过《著作权指令》，要求在线平台借助技术手段审查用户上传内容。美国联邦通信委员会宣布，《恢复网络自由命令》正式生效，这也意味着其2015年制定的“网络中立”政策被废除。2018年7月，美国众议院推出《推进网络安全诊断和缓解法案》，推动美国国土安全部对其“持续诊断与缓解（CDM）”网络监测计划进行定期更新和技术升级。欧洲议会工业委员会批准《网络安全法》草案，拟对入网设备引入新的安全认证体系，只有达到最低“安全性设计”标准的设备才能进入市场。保加利亚通过了引入新框架的网络安全法草案，以更好地防范国家网络安全风险和事故。2018年8月，美国总统特朗普签署《2019财年国防授权法案》，允许美国使用“国家权力的所有工具”对国外势力发起的损害美国利益、造成美国公民伤亡、严重破坏美国民主以及攻击关键基础设施的行为予以反击。此外，特朗普签署命令，推翻奥巴马2012年签署的《第20号总统政策指令》。《第20号总统政策指令》制定了一

个复杂的跨部门流程，美国在使用网络攻击之前必须遵循这一流程，特朗普此举旨在放松对此类行动的限制。美国科罗拉多州共和党参议员科里·加德纳和得克萨斯州民主党参议员克里斯·库恩斯提出《网络威慑与响应法案》，要求对所有对美国发动的网络攻击负有责任或参与其中的实体和人员实施制裁。波兰总统签署了2018年5月通过的《网络安全法》，为波兰的国家网络安全系统搭建了框架。

（二）发布网络安全战略计划，加强网络安全防护

2018年3月，英国发布《智能设备网络安全草案》提案，要求制造商强化防护措施，以提高联网智能设备的安全性，该提案被认为是英国《国家网络安全战略》的重要组成部分。2018年5月，美国能源部发布了长达52页的美国《能源行业网络安全多年计划》，为美国能源部的网络安全、能源安全和应急响应办公室勾画了一个“综合战略”。2018年6月，加拿大颁布新版网络安全战略，旨在加强网络安全防护、打击网络犯罪。2018年7月，乌克兰内阁批准了《实施国家网络安全战略的行动计划（2018年）》，确定了支持网络安全监管、提升国家网络安全技术手段、建立国际伙伴关系和加强人员培训等18项任务。2018年9月，美国总统特朗普签署《国家网络战略》，确定了联邦政府为保护美国免受网络安全威胁和加强美国在网络空间的能力采取的新举措。2018年10月，沙特阿拉伯国家网络安全管理局发布了核心网络安全控制文件，以便在各个国家机构中应用最低标准，降低网络安全风险，保障沙特阿拉伯的经济安全和国家安全。美国智库情报和国家安全联盟发布“网络指标和警告（I&W）框架”白皮书。

（三）成立专门工作组，加强组织机构建设

2018年2月，美国司法部成立网络安全特别工作组，研究制定一项针对加密货币的“全面战略”，以处理使用加密货币进行洗钱的违法行为。美国国防部旗下的信息网络联合部队总部已经获得完全运作能力。美国司法部宣布将成立一个名为“网络数字工作组”的全新网络安全工作组，旨在评估和解决恐怖分子及一般用户恶意利用互联网的问题。2018年9月，英国国家计算中心为保障政府、央行、监管机构等多家组织的网络安全，创立新一代威胁保障中心，该中心为境外央行与监管机构提供全球网络安全咨询服务，协助有关机构设计网络安全监管制度。2018年11月，美国签署的《网络安全信息共享法案》中，批准成立网络安全和基础设施安全局，该机构将成为独立联邦机构，

负责监督民用和联邦网络安全。美国国土安全部成立信息通信技术供应链风险管理特别工作组，以防范黑客入侵重要信息系统。保加利亚议会与部长理事会成立网络安全委员会，委员会主席由副总理担任，成员包括内政部长、国防部长和外交部长等，旨在加强国家层面的统筹协调。

三、持续加强以数据保护为重点的信息安全立法和战略计划，加速推进相关领域法治进程

（一）重点加强数据保护领域的立法和战略计划

2018年，一些国家积极发布、通过相关数据保护法案，拟定、出台国家数字战略。2018年1月，美国民主党参议员伊丽莎白·沃伦和马克·沃纳提交了《数据泄露预防和赔偿法案》，要求信用机构与联邦贸易委员会（FTC）共享数据保护策略和方法细节，以避免数据泄露。该法案要求，FTC成立一个新的网络安全办公室，负责检查和监督信用机构的数据保护。该法案授权FTC可对机构每泄露一条信息罚款50～100美元。2018年2月，爱尔兰发布2018年《数据保护法（草案）》，以使《一般数据保护条例（GDPR）》生效。澳大利亚《数据泄露通知法案》正式生效，该法案要求澳大利亚《隐私法》涵盖的机构和组织，一旦意识到存在可能导致“严重损害”的信息泄露，需尽快通知泄露事件中涉及的个人。2018年3月，美国总统特朗普签署《澄清境外数据合法使用法案》。2018年4月，澳大利亚政府表示正积极促成与美国签订获取跨境数据的协议。欧盟委员会正拟定新法，允许欧盟成员国的司法部门可以直接向在欧盟提供服务的提供商，以及设立在其他成员国的服务提供商或代理公司，请求电子证据（如应用中的电子邮件、文本或消息等），而不管数据位于何处，服务提供商需在6小时内提供对应数据。2018年5月，美国众议院提出《安全数据法案》，这项法案禁止联邦机构强制或请求厂商、开发人员、卖方来设计或修改产品或服务中的安全功能，以实施监控。2018年6月，越南通过一项法案，要求脸谱、谷歌等全球科技公司将越南本地“重要”用户数据存储在其境内，并开设办事处。英国政府宣布将制定一项全国性数据战略，旨在“释放政府数据力量”。荷兰政府公布了一项数字战略，旨在推进经济社会的数字化。澳大利亚宣布启动“国家基础设施数据收集和传播计划”，推动实现提升数据决策支撑、驱动经济创新发展的目标。2018年7月，巴西参议院通过《个人数据保护法案》，建立起保护国内个人数据的体系。法国国民议会

投票通过修正案，将“打击对个人数据的延伸或不合理使用”的条款列入修宪法案。新加坡政府拟于2018年年底试行“个人资料保护信誉标志计划”，有助于建立消费者对企业的信心。肯尼亚政府正制定一项数据保护和隐私法案，以保护肯尼亚公司处理的消费者数据。美国正在拟订的《联邦数据战略》草案的“原则”部分强调，数据的使用和治理应优先考虑数据安全、隐私和透明度，同时加强“联邦数据实践对公众影响”的评估。2018年8月，巴西总统特梅尔签署《通用数据保护法》，以减少私营企业收集个人数据的数量。西班牙发布更新《数据保护法》指令，引入一些新规则来解决《一般数据保护条例》和1999年制定的《数据保护法》这两个独立数据保护制度之间的冲突。埃及批准保护个人数据的法律草案，旨在提高国内数据安全水平，规范电子营销组织活动和数据传输行为。2018年11月，加拿大新版《数据泄露应对条例》生效，该条例要求对数据安全开展科学的风险评估。此外，加拿大公布新版《保护个人信息和电子文件法案》，要求加拿大的企业在发生数据泄露事件后尽快报告，否则将面临处罚，罚款金额最高可达10万加元（约合53万元）。

（二）通过法案积极打击虚假信息和有害信息

马来西亚于2018年4月2日通过了《反假新闻法》，将对在社交媒体或数字出版物上传播虚假新闻的公民处以最高50万林吉特（约合81万元）的罚款和最高6年的监禁。俄罗斯总统普京于2018年4月25日签署《互联网诽谤法案》，允许当局封锁发布诽谤公众人物信息的网站，并对拒绝删除者处以最高5 000万卢布（约合535万元）罚款。法国国民议会于2018年7月3日通过《反假新闻法》，根据该法，选举期间候选人可向法院申请删除存在问题的新闻报道，同时要求脸谱和推特（Twitter）等社交媒体平台披露相关内容的赞助方。埃及议会于2018年7月16日通过一项法案，允许埃及媒体监管最高委员会对社交媒体上粉丝数超过5 000个的用户账号进行监督。欧盟委员会起草打击“网络虚假信息”的政策。

（三）出台相关立法，加强网络犯罪打击力度

2018年1月，巴基斯坦联邦内阁批准了《防止电子犯罪法案（2016年）》的修正案，该修正案旨在将亵渎和色情内容纳入《网络犯罪法案》。此前，伊斯兰堡高等法院在听证有关在社交媒体上传不良内容案件时，处理了与亵渎有关的罪行问题。2018年4月，美国总统特朗普签署了《2017年允许州和受害者打击在线性交易法案》，提出了终止性贩卖的办法，为执法部门

和受害者提供打击性交易的法律支持。英国内政部表示在2018—2019年投入约5 000万英镑（约合4.45亿元）提升打击网络犯罪的能力，并加大力度打击“暗网”犯罪。2018年6月，埃及议会通过《网络犯罪法》，宣布对鼓励犯罪的网站或社交媒体账户的经营者处以罚款和监禁。白俄罗斯总检察长办公室宣布起草立法，对涉嫌在互联网传播“虚假消息”的人员进行起诉。2018年8月，阿联酋总统颁布了修订后的《阿联酋网络犯罪法》，明确了对危害网络安全行为的监禁及罚款细则。2018年9月，俄罗斯总统普京签署了一项“独立国家联合体（CIS）打击网络犯罪合作协议”，以共同应对日益增加的网络犯罪数量，维护国家安全。2018年11月，南非议会司法委员会正式通过了《网络犯罪和网络安全法案》，该法案除了将盗窃和数据干扰定为刑事犯罪外，也引入了涉及“恶意”电子通信的新法规。

（四）出台电信领域安全监管方案

欧盟创建信息通信技术（ICT）网络安全认证框架。欧盟委员会将在新的《网络安全法案》中确立欧洲地区ICT产品和服务的网络安全认证框架，包括认证的组织方式、职责归属，以及如何开发和管理认证计划，相关认证标准则由欧洲标准化委员会和欧洲电工委员会共同拟议。澳大利亚启动了电信部门安全改革（TSSR），旨在建立一个通信行业应对国家安全威胁的框架。该法案还规定，除了保护其网络外，电信运营商还被要求向政府报告正在规划的基础设施变化，以及这些变化可能会给政府部门安全带来的影响。

（五）加快数据中心建设，为信息安全提供技术支撑

俄罗斯国防部正筹划建立数据灾备处理中心云网络，以便让其情报系统“离网”运作，云网络预计在2020年全面投入使用。印度计划在博帕尔建立包含50万个虚拟服务器的数据中心，并在两年内投入使用。英国数字、文化、媒体和体育部于2018年6月宣布筹建新的数据创新中心。

四、强化信息安全内容监管和控制能力

（一）重点监管社交媒体，打击虚假信息、有害信息传播

一是设立专门监管机构。缅甸运输和通信部长宣布，建立一个社交媒体监控机构，专门负责监控和调查社交媒体网络。新加坡考虑设立一个专门的部长级委员会，负责对使用数字技术在网上散布虚假信息的情况进行评估，分析其