总体国家安全观下网络安全对我国国家安全的影响及社会治理探索

于国欣¹, 李 鹏², 郑 军³, 袁 畅^{2,*}

(1. 山东省政法委综治服务中心, 济南; 2. 山东中网云安智能科技有限公司, 济南;
3. 北京理工大学前沿技术研究院, 济南; * 3962202@qq.com)

摘 要: 在习近平总书记总体国家安全观的指导下, 通过解析具体事件来分析研究当前网络安全影响我国国家安全的典型事件, 深入剖析其对我国国家安全带来的种种危害, 对网络安全危害我国国家安全的具体途径进行分类, 并总结探索社会治理解决网络安全危害国家安全的方式, 为今后相关领域的研究提供思路。

关键词: 总体国家安全观; 网络安全; 国家安全; 社会治理; 法治建设

1 引言

1.1 习近平总体国家安全观的提出

党的十八大中, 以习近平总书记为核心的党中央科学研判我国所处的国内外环境, 指出影响我国国家安全的“内外因素比历史上任何时候都要复杂”, “当前我国国家安全的内涵和外延比历史上任何时候都要丰富”。《朱子家训》¹有如下论述: “宜未雨而绸缪, 毋临渴而掘井。”自党的十八大以来, 习近平总书记在重要会议讲话中多次提到要增强忧患意识, 在《习近平新时代中国特色社会主义思想学习纲要》²、《习近平谈治国理政》系列丛书³中“忧患意识”被提到 20 余次, 可见他对其重视程度 [1]。疫情爆发引发的全球经济衰退、局部国家地区冲突导致的全球粮食供应短缺、以美国为首的西方国家恶意制裁引起的制造业供应链断裂等, 这些事件的发生无不在印证“居安思危、未雨绸缪”这一论断。

为应对新的复杂动荡的国外局势, 同时面对国内产业升级带来经济社会巨大变化的情况, 习近平总体国家安全观应运而生。这不仅是新时代我国保持繁荣发展的必然需求, 同时也是保障国民安居乐业的必要途径。习近平总体国家安全观强调, 要在维护国家安全的实践中注重“外部安全与内部安全”、“国土安全与国民安全”、“传统安全与非传统安全”、“发展问题与安全问题”、“自身安全与共同安全”这五组辩证关系的探究 [2]。在当前“逆全球化”的势头下, 新的总体国家安全观的提出为我们描绘了一个多元凝聚、价值包容、赋权扩能、韧性稳定的治理蓝图, 为新形势下我国国家安全工作铸成了强大的思想武器。

党的二十大报告指出, “推进国家安全体系和能力现代化, 坚决维护国家安全和社会稳定。必须坚定不移贯彻总体国家安全观, 把维护国家安全贯穿党和国家工作各方面全过程, 确保国家安全和社会稳定”, “强化经济、重大基础设施、金融、网络、数据、生物、资源、核、太空、海洋等安全保障体系建设”。

1.2 没有网络安全就没有国家安全

2018 年 4 月, 习近平在全国网络安全和信息化工作会议上提出“没有网络安全就没有国家安全, 就没有

¹ 《朱子家训》又名《治家格言》, 是以家庭道德为主的启蒙教材, 作者朱柏庐 (1627—1698), 明末清初人 (今昆山市), 著名理学家、教育家。

² 《习近平新时代中国特色社会主义思想学习纲要》, 是中央宣传部组织根据中央要求编写的政治理论著作, 学习出版社、人民出版社联合出版, 首次出版时间为 2019 年 6 月 9 日。

³ 《习近平谈治国理政》系列丛书共四卷, 收入了习近平总书记在 2012 年 11 月 15 日至 2014 年 6 月 13 日这段时间内的讲话、谈话、演讲、答问、批示、贺信等 79 篇, 分为 18 个专题, 外文出版社出版。

经济社会稳定运行，广大人民群众利益也难以得到保障。”

互联网经过二十余年的高速发展，早已深入国家社会经济的各个角落，其所形成的网络空间已经成为继陆、海、空、天之后的第五大战略空间，是影响国家安全、社会稳定、经济发展和文化传播的核心、关键和基础，是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。《中华人民共和国网络安全法》⁴明确规定要维护我国网络空间主权，网络空间主权是一国国家主权在网络空间中的自然延伸和表现。由此可以判断，网络安全已经成为我国面临的最复杂、最现实、最严峻的非传统安全问题之一。

网络具备传播速度快、影响范围大的特点。网络安全问题在这一特点下已不仅仅是影响个人、企业的局部问题，而是可以切实危害国家安全的“大问题”。新时代的国家安全不再局限于传统国土安全、军事安全、反奸防谍等狭义范畴，而是涵盖政治、经济、文化、社会、网络等多个领域，是一种广义的“大安全”观 [3]。对于每一个国民来说，个人每天通过手机、电脑等智能终端在网络上从事各种活动，这些活动都会留下足迹，而这些足迹又形成了庞大的数据网。一些个人或组织利用网络安全的漏洞非法窃取数据信息，侵害到我们的个人与国家利益，因此提高网络安全意识，自觉维护网络安全，是互联网时代的全体国民、组织共同的责任和义务，维护网络安全就是维护国家安全。

2 网络安全危害我国国家安全实例分析

2.1 滴滴事件

事件脉络：2021 年 6 月 30 日，“滴滴出行”正式在美国纽约证券交易所上市，上市首日市值最高达到了 800 亿美元；同年 7 月 2 日，国家互联网信息办公室（以下简称“网信办”）宣布对“滴滴出行”实施网络安全审查，审查期间“滴滴出行”停止新用户注册；两天后的 7 月 4 日，网信办再次发布了关于下架“滴滴出行”App 的通报；7 月 5 日，事件产生联动效应，网信办接连宣布对“运满满”“货车帮”“BOSS 直聘”实施网络安全审查，要求审查期间停止新用户注册；7 月 9 日，网信办再次通报，要求“各网站、平台不得为‘滴滴出行’和‘滴滴企业版’等上述 25 款已在应用商店下架的 App 提供访问和下载服务”。

网信办发布的公告中提到，审查原因是“为防范国家数据安全风险，维护国家安全，保障公共利益”，审查依据是“《中华人民共和国国家安全法》⁵、《中华人民共和国网络安全法》及《网络安全审查办法》⁶” [4]。这是自《网络安全审查办法》发布以来的首次公开审查行动，随即引发了一系列对类似“滴滴出行”的以大数据智能驱动的企业进行审查。系列事件通过网络引起了巨大的社会讨论，从国家监管、到社会舆论都对重点领域行业企业探索全球发展模式过程中存在的网络安全隐患产生了更加深刻的认知。2021 年 6 月 10 日，《中华人民共和国数据安全法》正式颁布，并于 2021 年 9 月 1 日起正式实施。该事件对我国网络安全监管以及数据伦理治理产生了深远的影响，具有标志性的变革意义。

2.2 西工大事件

事件脉络：2022 年 4 月，西安市公安机关接到一起关于西北工业大学信息系统发现遭受网络攻击痕迹的报警，公安机关高度重视并与网络安全技术专家成立联合专案组立案调查；2022 年 6 月 22 日，西北工业大学发表公开声明，经过国家计算机病毒应急处理中心和 360 公司联合技术团队的技术分析，初步判明相关网络攻击活动源自美国国家安全局（NSA）下属的“特定入侵行动办公室”（Office of Tailored Access Operation，简称 TAO）；2022 年 9 月 5 日，国家计算机病毒应急处理中心发布报告中提到 TAO 在此次网络攻击行动中，先后使用了 41 种 NSA 的专用网络攻击武器装备，同时发现近年 TAO 对中国国内的网络目标实施了上万次的恶

⁴ 2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》，自 2017 年 6 月 1 日起施行。

⁵ 2015 年 7 月 1 日，第十二届全国人民代表大会常务委员会第十五次会议通过新的国家安全法。国家主席习近平签署第 29 号主席令予以公布。法律对政治安全、国土安全、军事安全、文化安全、科技安全等 11 个领域的国家安全任务进行了明确，共 7 章 84 条，自 2015 年 7 月 1 日起施行。

⁶ 2021 年 11 月 16 日，国家互联网信息办公室 2021 年第 20 次室务会议审议通过《网络安全审查办法》，自 2022 年 2 月 15 日起施行。

意网络攻击，窃取了超过 140GB 的高价值数据；同日，外交部发言人毛宁在答记者问中表示该事件证据链清晰完整，美方行径已严重危害中国国家安全和公民个人信息安全，并要求美方作出解释并立即停止不法行为 [5]。

西北工业大学隶属工信部，为我国国防科研作出了巨大贡献，其在“三航”研究方面特色优势显著，是“为中国首次载人航天飞行作出贡献单位”的两所高校之一，建有我国高校唯一的无人机专业化飞行试验测试基地。正是因为这些突出的成绩，引发了美国的忌惮，进而对其研究机密实施攻击窃取。根据事件调查结果来看，近年来 TAO 对我国各重要行业领域网络实施了大规模的攻击以窃取高价值数据，本次事件的披露是对我国重要行业领域网络安全防范的重要警示，未来应更加警惕攻击窃取的隐蔽性，加速相关行业对防御、漏洞发现等技术的研究，全面提升软硬件设施防御水平。

2.3 间谍渗透系列案件

近年来，国家安全机关加大了对境外间谍渗透窃取我国重要数据危害国家安全事件的披露，可以看出境外势力对我国长期实施间谍活动，其渗透手段之多元和渗透范围之广泛深入都引入深思。

标志案件一航运数据窃取案。2021 年 5 月，国家安全机关破获一起某境外咨询调查公司刺探窃取我国航运基础数据案件。该咨询公司通过网络、电话等方式，频繁联系我大型航运企业、代理服务公司的管理人员，以高额报酬聘请行业咨询专家之名，与我境内数十名人员建立“合作”，指使其广泛搜集提供我航运基础数据、特定船只载物信息等。其与所在国家间谍情报机关关系密切，承接了大量情报搜集和分析业务，相关数据的非法收集可以反映航运线路、吞吐量以及运行状态，对我国航运运营造成重大威胁 [6]。

标志案件二高铁运行数据窃取案。2022 年 4 月，国家安全机关破获一起为境外刺探、非法提供高铁数据案件。上海某科技公司为谋取利益，持续采集、传递数据给某境外公司，该境外公司以进入中国市场提前调研名义，委托境内公司采集中国铁路信号数据，包括物联网、蜂窝和 GSM-R⁷等数据，而 GSM-R 敏感信号是高铁移动通信专网，直接用于高铁列车运行控制和行车调度指挥，承载着高铁运行管理和指挥调度等各种指令。这些数据足以使得高铁通信中断，影响高铁的正常运行秩序，对我国铁路运营构成重大威胁 [7]。

标志案件三敏感气象数据窃取案。2021 年 3 月，国家安全机关破获一起私人向境外传输敏感气象数据案。国家某重要军事基地周边存在可疑气象观测设备，设备具备采集精确位置信息和多类型气象数据功能，设备系个人购买并私自架设，并向全国多地售出 100 余套，均架设在我国重要区域周边，所采集数据传送至境外某气象观测组织网站，网站由某国政府部门以科研之名发起成立，搜集分析全球气象数据信息，旨在为其军方提供服务，对我国国防安全造成重大威胁 [7]。

3 网络安全危害我国国家安全途径分析

通过对上述典型案例的分析，我们可以概括出三个当前网络安全危害我国国家安全的主要途径，一是客观环境下的主动泄露，二是遭受被动攻击引发泄露，三是外部势力渗透加之内部管理薄弱产生泄露。

3.1 客观环境下的主动泄露

滴滴事件是这一类型的代表，以数据赋能智能的高新技术企业为寻求全球化发展，通过在海外上市或接受境外大股东持股投资等形式，拓展其业务范围，从而扩大经济效益谋求更高地发展 [8]。其本质是客观因素环境下的一种对经营方式这一的探索，本着信任与向好的原则，我们可以认为其没有主观上的泄露意图，但实际情况却并不按照主观意图发展。根据境外上市规定，相关企业将提供包括平台运行、公民个人数据在内的全场景化原始数据。借助前沿信息技术手段，这些数据的跨境流动将侵犯个人、群体乃至国家的利益，数据已然转换为关乎国家安全价值的利益形态，特别是涉及关键信息基础设施的运营数据直指国家隐私的核心，其泄露将会引发国家安全问题。

这一类型事件所造成的危害反映出了我国相关法律法规、行业准则制定的滞后性，其背后所隐含的正是对

⁷ GSM-R (Global System for Mobile Communications - Railway) 是一项用于铁路通信及应用的国际无线通信标准。欧洲铁路交通管理系统的子系统使用 GSM-R 完成列车和调度中心的通信。

数据主权认识的缺乏，数据主权即包含在网络空间这一第五大战略空间安全范畴内。数据主权主要指一个国家对其政权管辖地域范围内个人、企业和相关组织所产生的数据拥有的最高权力，未来，处于信息技术领先地位的国家将更多拥有对海量数据开发、传播和控制主动权和主导权的数据主权 [8]。

3.2 遭受被动攻击引发泄露

西工大事件是这一类型的代表，境外组织利用网络攻击手段窃取我国重要行业领域关键数据，从而掌握我国重大设施、重点行业的国家机密。其特点主要是攻击范围广泛、攻击力度和规模强大、技术手段先进、具有一定的隐匿性。一旦成功，则无需经过大规模的数据分析挖掘，而直接获取关键机密信息，其危害性更大。

这一类型事件所造成的危害反映出了相关行业、组织安全防御软硬设施存在一定的技术漏洞。当前我国信息安全与网络安全的防护能力整体较差，相关从业人员安全意识薄弱，很多关键行业领域重要系统设防水平不足，受攻击危险系数极高，同时我国对于网络信息软硬件设备的更新速度相较于发达国家仍存在一定的差距 [9]，企业及组织对安全投入的主观能动性不足，涉及关键重大基础设施的行业安全标准执行不到位，监管力度不强，都是导致这一类型泄露频发的主要原因。

3.3 外部渗透加内部薄弱产生泄露

间谍渗透系列案件是这一类型的代表，文中列出的窃取案件均针对我国重要行业领域，通过假借商业行为隐秘间谍组织真实意图，借助经济贿赂、予以好处等手段渗透行业薄弱处，其渗透路线已不再局限于政府关键部门或重要领导职务，而是采用广泛撒网的形式获取大量数据，并据此利用信息技术手段挖掘提取非公开秘密数据，意图全面掌握我国重要信息。

这一类型案件所造成的危害反映出了行业组织及个人的国家安全意识淡薄，法律知识欠缺，管理体系存在巨大漏洞，监管措施不利等一系列问题。往往个体的行为将对国家安全造成不可挽回的重大影响，其防治难度相对更大，且短期不易见到成效，需自上而下、自下而上全面增强国家安全意识，同时加强各级管理体系，增大违法犯罪处罚力度，扩大宣传范围引导行业、民众树立正确的国家安全观、提升国家安全防御意识、强化个人对国家的责任与义务。

4 探索社会治理新举措保障国家安全

社会治理是国家安全体系的重要组成部分，面对当今世界百年未有之大变局，我国国家安全的内涵和外延比历史上任何时候都要丰富，时空范围比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂，网络空间对抗已成为大国博弈的常态化手段，筑牢网络安全防线已成为维护国家安全和社会稳定的关键。面对网络安全对我国国家安全的危害，本文基于政法体系的实践探索提出三个方面的社会治理措施，一是进一步完善我国国家安全及网络安全法制体系建设；二是持续加强网络安全技术创新，完善相关领域技术标准；三是扩大宣传警示力度，增强全民国家安全及网络安全意识。

4.1 完善国家安全及网络安全法制体系建设

党的二十大报告提出，“要强化经济、重大基础设施、金融、网络、数据、生物、资源、核、太空、海洋等安全保障体系建设”。为实现这一目标，应进一步完善我国国家安全及网络安全法制体系的建设，自顶向上规划，开展重大基础设施领域数据安全试点，加强对人工智能、车联网、工业互联网等新兴领域的监管政策研究，进一步完善风险监测预警体系，明确个人、组织、单位、行业、政府各级主体责任。

在法律体系方面，我国现已形成由《数据安全法》（2021）、《国家安全法》（2015）、《网络安全法》（2017）、《网络安全审查办法》（2020）共同组成的我国数据安全法律框架体系。《数据安全法》中对数据分级分类保护、数据安全审查、重要数据风险评估、数据出境管理以及数据歧视对等措施等做了明确的规定，《网络安全审查办法》、《国家安全法》等对关键信息基础设施的运营商可能存在的危害国家安全的行为做出了明确的阐述。此外，对个人网络信息范围而言，2021年3月，网信办、工信部等多部门联合发布的《常见类型移动互联网应用程序必要个人信息范围规定》，明确了地图导航、网络约车、即时通信、网

络购物等 39 类常见类型 APP 必要个人信息范围，要求其运营者不得因用户不同意提供非必要个人信息而拒绝使用 App 基本功能服务 [8]。

4.2 持续加强网络安全领域技术创新

深究网络安全防护，其本质是网络攻防对抗技术的争锋。这需要全方位提升网络安全防护能力，筑牢这张广覆盖、强立体的网络安全防护网。为实现这一目标，需要加强技术创新，研究制定重点行业领域网络安全、数据安全标准，对技术的违规滥用和非法使用依法治理；通过区块链、隐私计算等技术，破解数据安全与数据流通难题，同时要强化网络风险预警、态势感知、应急处置等能力，搭建一个全方位立体化的防护网络，实现“看得见威胁”“打得赢攻击” [10]；要加强全链条、多领域的网络安全防护，在不同的行业领域，不断丰富技术监测手段，实现关键安全防御检测技术自主可控。

新兴的几种重要防治技术手段包括：一是渗透测试，是指在计算机上测试工作人员通过模拟黑客的恶意攻击，并利用所掌握的技术和相关知识，利用人工和工具对网络系统的弱点进行分析。通过对各类常见的黑客攻击方法的研究，可以发现传统的安全防护方法所不能探测到的漏洞，是一种全新的工具测试方法；二是 APT 攻击检测，高级持续性威胁（Advanced Persistent Threat, APT）一般受国家或大型组织操控，受国家利益或经济利益驱使，由具有丰富经验的黑客团伙实施，具有技术性强、持续时间长、危害性较大等特点，是近年来出现的新型综合性网络攻击手段。针对 API 攻击的反制极为重要，目前亟待解决的问题主要有即渗透防护能力脆弱、检测精度较低、攻击范围取证困难及对新型未知攻击反应速度慢；三是网络异常检测与网络安全态势感知，其优势在于其可以综合各个方面的因素整体反映网络安全状态，通过大数据技术，可以对网络安全运行过程中的风险作出及时预测和报警，从而有针对性地启动攻击保护屏障；四是网络威胁情报分析，威胁情报可以通过大数据、分布式系统及其他方式来获取，其优势在于大大弥补了传统防御方式的不足，可以从攻击者的角度开展防御性工作。分析者可以全面性掌握互联网风险，继而采取高效和准确的防御行动，降低网络攻击所带来的损失，尤其在反恐主义、漏洞检测、网络犯罪防范及恶意软件清理中能够发挥更加显著的作用，有很强的实用性和适用性。

4.3 增强全民国家安全及网络安全意识

人民安全始终是我国国家安全工作的出发点和落脚点，要坚持以人民安全为宗旨，增强全民网络安全意识。当前，滥用个人信息、数据泄露、电信网络诈骗等问题严重影响了人民群众的财产安全和切身利益。党的二十大报告提出，要加强个人信息保护。全行业必须深刻认识到当前网络安全的严峻形势和新时期面临的新挑战、新任务，将网络安全视为发展之根基、稳定之前提、强盛之保障。对此，要持续整治危及用户安全的问题，压实网络安全责任，规范个人信息的搜集和使用，纵深推进防范治理电信网络诈骗，切实维护人民群众的利益。

通过设立全民国家安全教育日⁸，开展国家网络安全宣传周⁹等方式，集中宣传普及危害国家安全及网络安全信息，公开披露间谍渗透、电信诈骗、违法收集数据等典型案件，围绕金融、电信、电子政务、电子商务等重点领域和社会公众关注的热点安全问题，邀请国安专家、法律专家、技术专家解读背后的安全知识，同时加强《国家安全法》、《网络安全法》及《数据安全法》等法制教育，营造网络安全人人有责、人人参与的良好氛围，有效增强全民、全行业的安全意识。特别是针对防止个人信息遭受诈骗问题，《网络安全法》通过布置四道防线严防间谍诈骗渗透，第一道防线是实行网络实名制，第二道防线是从公民个人信息的收集、保管、出售三个环节加强监管；第三道防线是强化公民个人防诈骗意识，第四道防线是阻止诈骗信息广泛快速传播。

5 结语

面对当前新形势下的我国国家安全，网络安全作为其中重要一环早已成为各国关注的焦点，随着大数据、人工智能技术的飞速发展，网络安全的内涵也不再局限于传统的物理攻防或设置保密屏障，而是逐步发展为囊括了攻击、防范、检测、控制、管理、评估等多方面的综合理论与技术，这给我国防治网络安全危害国家安全

⁸ 2015 年 7 月 1 日，全国人大常委会通过的《国家安全法》第十四条规定，每年 4 月 15 日为全民国家安全教育日。

⁹ 2014 年起，我国正式开启“国家网络安全宣传周”活动，现已连续举办 9 年。

提出了更新更高的要求，从政法制度体系建设，到创新技术手段，再到提升全民安全意识，可谓任重道远，其意义极其重大。习近平总体国家安全观已为我们指明了方向，多元协同的治网格局正在形成发展，未来将继续为维护我国国家安全、营造清朗网络空间发挥更大作用 [2]。

参考文献

- [1] 李孟鸽. 习近平国家总体安全观研究. 江西财经大学硕士研究生学位论文. 2022.
- [2] 莫非, 王子玥. 总体国家安全观视域下的网络信息内容生态治理: 模式、路径与可持续性. 上海法学研究集刊. 2022;6.
- [3] 杨好. 习近平网络安全观研究. 长江大学硕士研究生学位论文. 2022.
- [4] 纪正坦. 平台数据安全治理优化路径探析—以“滴滴公司网络安全审查案”为切入视角. 信息安全研究. 2023;9(1).
- [5] 中国小康网. 西北工业大学遭 NSA 网络攻击事件调查: 使用 41 种网络攻击武器. 2022-09-06.
- [6] 网信文安. 国家安全部公布三起危害重要数据安全案例. 2021-11-04.
- [7] 安全 419. 2022 年上半年全国数据安全及个人信息泄露大事记. 2022-07-05.
- [8] 韩洪灵, 陈帅弟, 刘杰, 陈汉文. 数据伦理、国家安全与海外上市: 基于滴滴的案例研究. 财会月刊. 2021;15.
- [9] 郭鹏. 从网络勒索病毒事件分析科技领域安全对国家安全的影响及对策. 网络安全技术与应用. 2022;8.
- [10] 苏德悦. 筑牢网络安全防线维护国家安全 五论信息通信业学习贯彻党的二十大精神. 人民邮电. 2022-11-08;001.