ISSN 2096-2282
CN 10-1421/TP

网络空间安全

Cyberspace Security

CCiD 赛迪出版物　2023年第5期　10月25日出版　总第147期　邮发代号：80-893

ISSN 2096-2282
9 772096 228231 10>

国家新闻出版广电总局（原）首批认定学术期刊
中国计算机学会（CCF）审定优秀期刊

本刊已被以下期刊数据库收录：
中国科学引文索引库期刊（CSCI）　中文核心期刊（遴选）数据库
中国知识资源总库（CNKI）源期刊　中文科技期刊数据库
中国学术期刊网络出版总库

网络空间安全 Cyberspace Security
二〇二三年十月　第十四卷第五期　总第一百四十七期

本刊已被以下期刊数据库收录：
中国科学引文索引库期刊（CSCI）
中国知识资源总库（CNKI）源期刊
中国学术期刊网络出版总库
中文核心期刊（遴选）数据库
中文科技期刊数据库

网络空间安全
Cyberspace Security
（Wangluo Kongjian Anquan）
（双月刊）
2023年10月
国际标准连续出版物号：ISSN 2096-2282
国内统一连续出版物号：CN 10-1421/TP
广告发布登记：
京海工商广登字 20170178 号
邮发代号：80-893

Contents 目次

网络空间安全　总第147期　第14卷　第5期　2023年10月

政策与研究

数据与治理

密码与应用

系统与网络

可控与防御

目次 Contents

网络空间安全　总第147期　第14卷　第5期　2023年10月

应用与安全

技术与应用

人才与教研

专题：打击网络犯罪

网络安全为人民
网络安全靠人民

保护知识产权
就是保护创新

手机APP个人信息安全的法律保护

张泽昊
（中国人民公安大学，北京100038）

摘要：

［目的/意义］ 通过对手机APP个人用户信息的研究和保护，以及对网络空间态势的展开梳理，让大众对手机APP的信息安全保护意识和在网络空间的法律保护意识更强。手机APP在给人们生活和工作带来便捷的同时，也出现了一些安全风险问题。例如，个人信息和隐私数据的泄露就是一个影响社会发展的严重问题，并给很多手机用户造成极大的困扰，有的甚至给人们带来经济损失。结合网络空间的大环境，整治手机APP信息安全已经迫在眉睫。

［方法/过程］ 针对目前手机APP个人信息保护现状，确保个人信息安全和网络空间安全，尽早提出防范措施和治理手段是一项非常关键和重要的工作。通过立法与手机APP中的隐私协议相结合来完善立法是核心。加快手机APP信息泄露防治，与网络空间的法律保护建立快速的连接，从而使得手机APP信息保护程度更高。

［结果/结论］ 在网络空间的发展和完善过程中，进一步细化网络空间的立法，并加强对手机APP个人信息保护，让网络空间环境变得更加良善，信息流更加顺畅，用户的权益能够得到进一步的保障。

关键词： 手机APP；个人信息；隐私保护；网络空间安全；立法

中图分类号： D925.1 **文献标识码：** A

Protection and legalization of personal information in mobile APP

Zhang Zehao
(*People's Public Security University of China,Beijing 100038*)

Abstract:

[Purpose/Significance] This article sorts out the research and protection of mobile app user information, as well as the overall situation of the online space. Enhance the public's awareness of information protection and legal protection of mobile apps throughout the online space. Mobile apps are the core of mobile phones. However, while mobile phones bring convenience to people's lives and work, some new problems may also arise. For example, the leakage of personal information and privacy data is a serious problem that affects social development and causes great distress to many mobile phone users, some even causing economic losses to people. It is urgent to rectify the information security of mobile apps in the context of the network environment.

[Method/Process] In response to the current situation of personal information protection in mobile apps, it is crucial and important to propose preventive measures and governance measures as soon as possible to ensure personal information security and cyberspace security. The core of legislative improvement is to combine legislation with privacy agreements in mobile apps. Speed up the prevention and control of information leakage of mobile APP, and establish a fast connection with the legal protection of cyberspace, so as to improve the protection of mobile APP information.

[Results/Conclusion] In the process of development and improvement of the cyberspace, further refinement of legislation in the cyberspace has been made, and information protection for mobile app users has been strengthened. Let the environment of the entire cyberspace become more benign, the information flow more smooth, and the rights and interests of users can be further protected.

Keywords: mobile APP;personal information;privacy protection;cyberspace security;legislation

0 引言

信息安全与当今社会的经济、政治发展已不可分割，网络空间中传递信息的一个主要端口就是手机APP（Application）。手机APP具有用户客流量大的特征，而且很多手机APP已经成为人们生活当中不可分割的一部分。例如，一些社交类的手机APP和娱乐休闲类的软件，人们对其已经形成生活娱乐的依赖性。为此，信息安全、网络安全和个人隐私保护等问题同时被提上议事日程。由于大量的手机APP下载、用户注册和使用，都需要使用者输入相关的个人信息才能使用手机，所以会涉及到的一系列问题，包括个人信息泄露、涉及个人隐私等情况，需要网络空间安全管理部门与社会大众、政府部门、立法部门和执法部门共同出击，打好保护个人信息、隐私预防泄露和交易的攻坚战。

手机是现代网络空间中，最为直接且最多的网络端口，手机APP是手机的核心。在使用手机APP时，会在初次登录和使用过程中，要求获取使用者的个人信息。手机APP获取使用者的个人信息，在一定程度上可以理解。因为在大型的网络虚拟空间中，要进行一定的约束与框规。但是，手机APP背后运营商的素质与获取手机APP使用者的目的差强人意，有的甚至不那么单纯。很多手机APP用户的个人身份信息（包括但不限于姓名、性别和年龄等），甚至是工作单位与银行卡账号都被手机APP背后的运营商，在获取收集后泄露给第三方，给手机APP用户带来了不必要的困扰，甚至是物质和精神上的损失与伤害。

很多网络用户表示，个人信息泄露较多；一部分的用户表示，自己遇到过个人信息被侵害；很大一部分的网民要求个人信息保护应有立法方面的保护。在使用手机APP给我们带来快捷与方便的同时，对个人信息的泄露和个人身份信息保护等问题的解决也迫在眉睫。

1 手机APP侵犯个人信息的途径

可以说，现在的手机APP在视觉效果上做的是非常不错的。尤其是一些偏于社交类或者是游戏类的手机常用休闲的手机APP，深受年轻人的喜爱。这些软件的开发运营商深挖年轻消费者和使用者的心理，采用鲜艳和动态的视觉冲击，给手机APP带来强烈的吸引力度。所以说，在这些看似给手机APP初始界面的高度美化，抓住了年轻人的眼球和需求，但却让使用者和消费者在安全方面放松了警惕性。甚至，更多的消费者，在被吸引后，根本忽略了网络和信息安全问题，直接点击下载进行安装。

手机APP背后的运营方主要是通过一些“经同意”或者是“允许”等，一类不附具体通知义务的隐形条款，来获取和收集使用个人的主体信息。而在此，大部分手机APP使用者，对自己的个人信息是如何被泄露出去的，甚至是如何被侵害的却一无所知。那是因为通过下载、点击或者是使用手机APP。手机APP背后的运营平台所获取的个人用户信息，大多也是通过网络链状的交易形式进行的，隐蔽性之高，令人难以想象。

2 手机APP泄露用户信息的分析

2.1 个人信息泄露的类型

有多数手机APP用户表示，在使用运营商开发的手机APP过程中，APP运营平台泄露了自己的个人基本信息，包括用户姓名、性别、年龄、地址、电话号码、身份证号码等。同时，一部分手机APP使用者认为，泄露了自己的个人身份信息，像工作和家庭情况乃至婚姻状况等。相对一部分手机APP用户表示，自己的个人账户信息被泄露，包括电子信箱和个人银行卡账号等。而个人账户信息直接与个人财产信息紧密相关，一旦泄露就会对手机APP用户的财产安全造成严重的威胁。还有很多手机APP用户认为，自己的个人行为信息被泄露，例如出行路线信息，像手机APP的旅游路线、跑步轨迹、网站上浏览过的痕迹残余等。运营平台的后台系统会根据自己用户的浏览信息、所在位置和地域，进一步给用户提供下一步的后续服务。同时，会根据平台所掌握的APP用户的账户信息和个人基本信息，分析确定用户的消费水平和支付能力。

2.2 手机APP用户信息保护协议

虽然手机APP泄露个人信息的现象较多，但是不能说每一款手机APP都是这样，只要是通过正规渠道，像正规手机自带的手机应用市场下载的手机APP，在下载安装前，大部分都会出现“是否阅读安装协议”“权限内容”“用户须知隐私保护协议”等个人信息隐私保护协议。

但是，这些看似很有保障性的手机APP个人信息保护协议，大部分手机APP用户是不理解它本身的法律性质。有部分手机APP用户，从来没有阅读过。少部分的手机APP用户略有了解。在调查数据中，只有极少的的手机APP用户仔细阅读过这些关于个人信息的保护协议。以上几组调研数据充分表明，绝大部分的手机APP用户对个人信息保护的协议是不了解的，手机APP的背后运营平台对手机APP用户个人信息的过度索取，甚至是被泄露与交易的事实几乎完全不知情已成为事实。

经分析，造成以上情况的主要原因主要集中在两点：一是从事实角度出发，手机APP信息被泄露的实害程度较低；二是个人信息主体用户对自身的个人信息程度保护意识、法律意识以及重视程度较低。

2.3 手机APP信息泄露的影响

在信息加速发展的时代，信息流传递之快、影响之大是无法预知的。手机APP平台在网络空间中运作的背后是一个具有链状形、集合性、利益性的庞大且复杂的网络整体。手机APP使用者根本无法根据自身对互联网以及虚拟空间的一知半解，来设想自己的个人信息被泄露，甚至是被交易之后，给自身的生活与工作造成的物质和精神层面不同程度的影响与伤害。

很多的手机APP用户反馈，个人信息在泄露给平台后，骚扰性的电话与短信对其生活已经造成了严重的影响与困扰。有很多的用户，由于法律意识以及自身保护不够强，在受到困扰后，选择不作任何处理。部分手机APP用户，在个人信息被泄露，受到不同程度骚扰后，选择将其设置成消息免打扰模式，然后继续使用。其中，也会有一些用户在受到不停的电话或者是短信骚扰后将其号码拉黑；更有极少的用户在受到以上的困扰后，会直接选择将该APP卸载。

2.4 手机APP用户的法律保护意识

随着时代的发展，法律的普及教育，已经进入常态化。但是，由于法律知识本身的特质与属性，可能会给人们一种比较晦涩的感觉。所以，大部分人可能会在必不得已的情况下去了解法律知识。平时的时候，人们并不会主动的去了解与法律相关的知识。

但是，随着这几年的一些关于个人信息类事件的发生，使得人们越发注重关于隐私的保护，尤其是在涉及自己的私生活方面，像是一些私密性较强的照片等。因为确实网络流量的伤害程度实在是太高，正常人根本抵抗不住网络舆情的攻击。所以，针对手机APP个人用户对于个人信息保护的法律法规的了解程度，做了一定分析。大部分的人仍了解较少，甚至处于朦胧状态；少部分的手机APP用户表示只是简单了解。只有很少的手机APP用户表示了解的程度与层次上透彻一些。

从这几组数据上看，人们对于个人信息的法律保护还处于不够了解的层面。加大我国公民的个人信息法律保护势在必行。法律的制定与出台很重要，但是公民懂得如何运用现行有效的法律，作为武器来维护自己的切身利益更重要。大家只有先了解，然后才能去学习和掌握。然后在必要的时候，去帮助自己、家人与朋友去维权。

目前，手机APP用户大部分都是一种放任状态。可能大家都是想着我只是用个手机软件而已，没有什么。再说，就算出现什么事情，我也不先采取措施，会有第一个敢于吃螃蟹的人。这种想法并不仅仅代表公民的维权意识差强人意，更为重要是，其根源性原因是普法事业可能做的不到位。“法者，应公之于众”。但是，现在的普法如果仅仅是将法律公布出来，是达不到现今我国经济社会的高速发展对法律的需求。我们要在一定程度上，通过加大宣传力度、普法力度，让社会公众能够适时地拿起法律武器，维护自己的切身利益。

3 手机APP个人信息保护对策

3.1 立法与隐私保护协议的连接

手机APP在进入智能手机时代，可以说是获得了超级升级性发展。再加上，互联网领域的技术具有受众的广泛性与超地域性，还有手机APP自身的登录和使用上的公开性、自由性等特征，使得手机APP用户的个人信息无时无刻地不暴露在互联网中。

因为现在关于个人信息的立法已经不再是空白，所以说，最为关键与主要的不只是再简单的推出立法，或者是完善现有的立法。我们应该靶向性地再强一些，直接在手机APP现有的关于手机APP用户的个人信息保护协议上，直接与我国信息保护相关的法律进行搭建与连接。

例如，可以运用现有法律层面上的信息保护法律法规，由国家相关法律部门出面对手机APP开发商在手机APP中的个人信息与隐私保护的选项设置，提出法律层上的强制性规定与要求。要求手机APP开发运行公司的隐私政策设计，必须符合特定的程序与形式，并且在一定程度上，对手机APP对个人信息保护协议的内容长度与知识层面进行合理要求与规制。努力减少手机APP运营商超范围收集与业务功能无关的信息，为用户无法自由注销账户和手机APP软件侵犯用户隐私提供个性化推荐等。这样既在实质层次上完善了对于个人信息保护，又不仅仅是将个人信息保护落实在纸面上，而是将我国个人信息保护的相关立法，与现行有效的手机APP运营商开发的软件手机APP中的个人信息隐私的保护条款联系起来，形成真正的能够保护手机APP用户的个人隐私与信息的保护性屏障。

3.2 加强政府部门的监管力度

尽管法律的出台、完善以及对手机APP用户个人信息的完善，是一个刚性的设计。但是，不该忽略的是，政府与市场的联系是最为紧密的，比起法律部门的刚性介入与调整，更能调整经济市场的各种问题。同时，在现有的法律维权行为中，法律部门是主力军，但是其他部门、团体与个人，不乏也是维护市场秩序井然有序、正常运转、不可或缺的有生力军。政府部门可以根据自身的定位，要求手机APP开发商及相关企业改进隐私政策中的默认选项设置，来帮助个体做出最优化的选择。

由于手机APP用户对个人信息的保护及相关法律政策的了解与掌握程度不高，为此手机APP用户在首次使用手机APP时，面对极其繁杂的相关信息或者是隐私条款以及一些未知的选项，仅凭借自身的理性，信息主体未必能够作出最优选择。此时，需要政府部门出面，通过政府对手机APP开发商提出强制性的要求，将精心设计、经过深思熟虑，并经过权威审核的较优选项呈现在信息主体面前，以降低个人用户作出不理性决策的概率。

除此之外，政府及相关部门可以联合设定民意咨询网站广泛征集群众意见，集中收集、处理民众意见，对手机APP运营商进行监督和管理，其更好地为手机APP用户进行服务。与此同时，各手机APP开发运营商，也应该注意自身的良好形象及注重加强自身的道德修养，争取尽量从根本与源头上杜绝违规事件的发生。

3.3 针对年龄段，加强普法教育

随着国家社会经济的空前发展，手机在中国家庭成员中的使用已非常普遍，尤其是青少年中，占比很重。我们的普法教育宣传要有出针对性：一个是针对于社会广大群众层面，一个是大学生层面，一个是中小学等青少年层面。这样区分层次的普法教育会使得普法教育的力度更大，层次性更强，从而针对防治手机APP用户信息泄露问题的效果会更好。

关于手机APP用户信息的隐私保护及防泄漏问题，在普法教育方面应该重之又重。可以通过“法律课堂”“手抄报”“普法期刊”“大型讲座”等各种容易让社会大众接受的形式进行。

4 结束语

本文旨在通过对手机APP用户个人信息保护现状的调查研究，进一步呼吁手机APP用户提升

个人信息保护意识和法律维权意识，让自己的切身隐私与信息利益不受伤害。提倡进一步通过完善立法，并建议将立法与手机APP的个人信息隐私协议进行连接，从而更好地保护社会大众的隐私与个人信息，使社会大众在享受网络世界带来便捷与高效的情况下，更好地保护与维护好自己的个人信息，从而营造一个运转更流畅、 人文素质更良善的网络空间环境

参考文献：

[1] 秦华,高允菁.个人信息保护的当下困境及司法应对——以手机APP对个人信息的使用为切入点[J].天津法学,2022,38(02):55-70.

[2] 郭伟栋,周志中,乾春涛.手机App列表信息在信用风险评价中的应用——基于互联网借贷平台的实证研究[J].中国管理科学,2022,30(12):96-107.DOI:10.16381/j.cnki.issn1003-207x.2021.0359.

[3] 刘龙军,杨妍.破解手机APP侵犯个人信息公益诉讼监督难题[J].中国检察官,2021(12):14-17.

[4] 于游,于锦秋.大数据时代个人信息侵权的民法规制——以手机APP收集使用个人信息为视角[J].学术交流,2021(05):64-73.

[5] 赵利杰,王红云.关于手机APP用户信息安全的调查分析[J].科技风,2020(34):109-110+147.

[6] 陈银平,刘艳.手机APP个人信息安全现状分析——基于30款手机APP的测试结果[J].中国管理信息化,2020,23(18):192-193.

[7] 徐璐瑶,白书豪,赵楠楠,刘军,戴莉娜.手机APP服务提供者信息收集的行政保护机制拟态[J].现代盐化工,2020,47(04):115-116+146.DOI:10.19465/j.cnki.2095-9710.2020.04.055.

[8] 武煜熹,安小米.大数据时代APP用户个人信息保护的困境和解决对策[J].网络空间安全,2020,11(10):22-25.

[9] 程韵.APP共享个人信息二次授权问题法律规制研究[J].网络空间安全,2022,13(02):28-36.

作者简介：

张泽昊（1995-），**男**，**汉族**，**山东济南人**，**山东财经大学**，**本科**；**中国人民公安大学法学院**，**在读硕士**；**主要研究方向和关注领域**：**民事诉讼法、个人信息保护和网络安全**。

网络平台刑事监管义务新探讨

周子扬
（上海市静安区人民法院，上海200040）

摘要：

［目的/意义］ 随着网络平台的普及，犯罪分子利用网络的数字化和交互化等特征，在刑事监管中呈现出取证难、追赃难等新特点，使得网络安全面临严峻挑战。

［方法/过程］ 针对利用网络平台犯罪带来的安全挑战，仅仅依靠以公安为主的传统打击刑事犯罪模式已不足以应对，将网络平台刑事监管义务引入到刑事犯罪治理体系中是必要且合理的。

［结果/结论］ 通过对网络平台刑事监管义务具体路径的构建，既可以提升网络安全，也是网络平台履行刑事合规对自身的保护。

关键词： 网络平台；网络安全；数字化；刑事监管；刑事合规

中图分类号： D9 **文献标识码：** A

Discussion on criminal supervision obligations of network platforms

Zhou Ziyang
(*Shanghai Jing'an District People's Court, Shanghai 200040*)

Abstract:

[Purpose/Significance] With the popularization of online platforms, criminals have taken advantage of the digitization and interactivity of the internet, making it difficult to obtain evidence and recover stolen goods, posing serious challenges to network security.

[Method/Process] It is necessary and reasonable to introduce the criminal supervision obligation of online platforms into the criminal crime governance system, as relying solely on the traditional criminal crime crackdown model dominated by public security is no longer sufficient to address the security challenges brought about by crimes committed on online platforms.

[Results/Conclusion] By constructing specific paths for criminal supervision obligations on online platforms, it is not only possible to improve network security, but also to protect the platform by fulfilling criminal compliance obligations.

Keywords: network platform; network security; digitization; criminal supervision; criminal compliance

0 引言

根据“360数字安全”在2023年2月16日发布的《2022年度反诈报告》显示，截至2022年底，共识别恶意网址总量为180余亿，每日新增恶意网址500余万，犯罪手法从刷单、投资理财到原宇宙、Web3.0层出不穷[1]。基于对涉网络平台刑事案件司法实践的归纳与整理，发现网络平台刑事案件风险明显增加，网络安全问题日益突出，仅仅依靠传统的犯罪打击模式难以遏制，有必要让网络平台自身监管参与进来，对网络平台在刑事案件中的监管义务重新定义。

1 网络平台刑事案件对网络安全的挑战

从刑事案件的立案侦查再到定罪量刑，利用网络平台的刑事犯罪衍生出了多种不同的犯罪模式，但无论何种模式都对网络安全产生了巨大的挑战。

1.1 传统侦查手段的安全挑战

由于网络平台具有双边关系，可以使人与人之间断点式的产生数字性的交互，使得网络平台刑事案件对网络安全的挑战远大于传统模式。首先，侦查难度极具增加，证据采集困难。例如，在利用网络非法集资类案件中，涉及的被害人呈现出人数众多、地域分布四散、资金流向复杂等特点。其次，社会危害性更加大，但防范效果不佳。线上犯罪就等于将犯罪陷阱放在每一位运用网络平台的人员身边，对网络安全的破坏从某种程度上来说已经超越犯罪人的控制。例如，在传播淫秽物品罪中，犯罪人将淫秽视频上传至网络平台，但是点击量的多少、有无二次传播等就不受犯罪人的控制。最后，执行周期长，追赃困难[2]。例如，在网络赌博案件中，跨国犯罪属于常态，犯罪人利用境外假设的网络服务器在境内开展赌博活动，所有的赌资均通过一系列洗钱的手段流入到境外账户，即便侦查机关查获了违法赌场，涉案赌资仍旧难以追回。

1.2 新型犯罪行为的安全挑战

原本不常见的传统犯罪，因为网络平台的出现，一些犯罪率明显升高的犯罪行为，对网络安全带来了新的挑战。一方面，部分涉破坏金融管理秩序罪的犯罪率明显上升。例如，消费者在网络购物平台上购物，商家并不会主动开具发票，之后虚假开具增值税发票行为给无真实交易的第三方赚取钱款，构成虚开增值税专用发票罪。另一方面，新类型的犯罪行为亟需法律规范。例如，犯罪人将从网络平台处非法获取的微信等社交媒体账号、手机验证码等信息出售，提供给他人的行为，应当如何认定、是否可以认定为侵犯公民个人信息等问题，尽管相关法律和司法解释明确规定了什么样的信息属于公民个人信息，并追究犯罪人的刑事责任，但是法律和司法解释的滞后性，远远跟不上信息种类的变化速度。

2 刑事监管义务的引入与价值

针对网络平台刑事案件对网络安全带来的挑战，传统的刑事侦查手段受到严重限制，只有将网络平台自身监管义务引入刑事犯罪治理体系，才能更好地应对网络安全风险。

2.1 刑事监管义务的逻辑基础

对于网络平台刑事犯罪，我国司法层面已经出台了相应的法律、司法解释以及指导性案例，以应对网络平台犯罪的复杂性和多变性。相关法规的出台，一方面表现了法律对于网络平台犯罪的重视，另一方面也显示出传统刑事案件的模式对网络平台犯罪的应对不足。法律作为对行为人事后的评价，本身就具有一定的滞后性，更何况刑事法律作为法律的最后一道底线具有谦抑性和后置性。由于网络平台特有的多边性特点，在某种程度上构成了一种特有的社会经济结构。在这种社会经济结构下，网络平台不仅仅是市场的参与者，也是市场的组织者，对于要求使用者提供个人信息、提供交易平台进行交易等行为，也应当认为是对社会经济结构规则的制定[3]。有学者提出，平台在某些领域的运行应嵌入公共义务，承担一定的公共责任，这既是通过扩大平台注意义务的形式实现，也可以是改变归责原则的方式落地[4]。网络平台可以通过制定一些非正式规范来约

束网络用户的行为[5]。这种网络平台对于平台规则的制定、执行以及产生相应的预警机制，体现的是网络平台刑事监管的过程，也是有效提升网络平台安全性的重要一环节。

2.2 刑事监管义务的法律保障

从刑事案件中被保护的客体到参与刑事案件的部分环节，网络平台的角色转变在某种程度上突破了传统刑法理论中对权利义务的规定。在传统理论中，刑罚是同一切犯罪行为作斗争的工具，而刑罚的适用是由国家侦查机关和各司法机关一系列司法活动的最后结果，网络平台只是作为被保卫的公民私人所有的财产范畴，属于被保护的对象。但是，随着网络平台在人类生活中扮演越来越重要的角色，从社会治理到打击犯罪，法律已经离不开网络平台所能提供的数字能力和技术能力，国内外立法层面也确认了网络平台监管责任的变更。《中华人民共和国刑法修正案（九）》（以下简称《刑法修正案（九）》）增设的罪名在某种程度上消除了对网络平台行为进行刑事责任分析的障碍[6]。2021年，国家网信办、工信部和公安部联合起草的《互联网信息服务管理办法（修订草案征求意见稿）》（以下简称《征求意见稿》）第21条，提到了互联网服务提供者对于防范犯罪的必要措施和后续的存证、报告制度，并规定了违反上述规定的法律后果。在2022年12月通过的《中华人民共和国反电信网络诈骗法》中，也规定了网络服务提供者的审核义务、监测义务、内控义务以及协助办案义务。尽管目前网络平台对于犯罪行为的规范义务散见于各个规定和仅有的几个刑法条文，但是随着犯罪行为对网络平台的依赖越来越强和网络平台对犯罪行为打击效果的日渐显现，更多不同法律位阶的规范将会出现并逐步统一和综合，为网络平台打击刑事犯罪提供了更多法律保障。

2.3 刑事监管义务的技术支持

相比于国家侦查机关的技术手段，网络平台拥有大数据和算法优势[7]，使得其作为侦查手段更加具有灵活性。实际上，网络平台看门人理论提出的依据之一，也是因为具有“执法成本优势”[8]。首先，从网络平台的准入到内容的发布，犯罪人的一切行为都是在网络平台上数字化交互的直观体现，所有的数据均在网络平台后台的服务器中储存，即网络平台一直闭眼看着所有的犯罪行为；其次，现在的网络平台已经不仅仅是数据的储存和交换，基于大数据的算法模式和云计算的发展，网络平台对于用户在平台上的行为是有一定监控和分析的，即网络平台的“眼睛”时不时地也是睁开的；最后，网络平台本身作为一个专业化的数字交换平台，后台庞大的数字网络能够在国家侦查机关和用户之间建立起有效的联系。对于网络平台来说，充分发挥网络平台自身的技术优势，通过对信息网络技术、产品和服务等开展安全审查来维护国家安全，借助国家安全的模糊化、抽象化的特点，为国家处理涉外纠纷和争端留有较大的制度余地[9]，不仅是法律法规明确的要求，也是对司法资源的一种社会优化。

3 刑事监管义务的具体构建

为了提升网络安全，在明确了网络平台刑事监管义务引入的必要性、合法性和专业性之后，就必须结合相关的法律法规，构建网络平台刑事监管义务。

3.1 从消极静态监管到积极动态监管。

消极监管，即事后监管，在违法犯罪行为被发现之后，网络平台具有删除相关犯罪内容的义务，即《征求意见稿》第21条规定的行为。此外，《征求意见稿》也多次提及物联网服务提供者“应当采取技术措施和其他必要措施，防范、发现、制止违法犯罪行为”，即对于平台刑事监管义务的要求从消极监管衍生到积极监管。积极监管，即事前、事中、事后的全流程主动监管。网络平台应建立全流程的动态风险识别制度，例如对于网络诈骗内容的识别与提示、对于重点银行账户的识别与冻结、对于个人信息的发布屏蔽、对于明显不符合交易习惯交易行为的预警等，对犯罪人假以合法手段实施的犯罪行为做出识别并制止。

3.2 从部分监管到全面监管

部分监管，即仅对网络平台中部分重点内容进行监管。传统的监管包括用户信息的监管、内容发布的监管等。

《征求意见稿》第16条除了要求网络服务提供者建立信息发布审核制度之外，还应当建立网络安全和信息安全管理制度等，第26条也列举了网络平台8个可能涉及的犯罪行为，并以法律和行政法规禁止的其他信息作为兜底，即对网络服务提供者要求上中下游全面监管。《中华人民共和国反电信网络诈骗法》第24条也对域名解析、域名跳转和网址链接转换服务，提出了明确的监管义务。

网络平台的全面监管不应该仅仅包括本平台自我的监管，还应当包括多平台之间的网络链接地带的全面监管，避免出现模糊地带导致危害网络安全的犯罪发生。

3.3 从刑事监管到刑事合规

网络平台自身监管在于对监管规则的全面完善，最终方式是对现有刑事法律规范在平台规则上的政策回应，目的是避免犯罪行为导致在刑法上映射，即避免网络平台构成单位犯罪，无论是不作为犯罪还是共同犯罪。

尽管网络平台具有对犯罪的预防、识别以及制止等义务，但是刑事案件谦抑性导致事前治理不能完全防止犯罪行为的发生，刑事合规制度有利于避免网络平台陷入无尽的义务之中，刑法介入企业合规管理体系的目标，是将涉案企业的正常业务行为对法益的损害预期值，降低到法律能够容忍的标准。

网络平台应当根据自身的特点，形成一套全流程化、标准化和可操作化的监管流程，并成立相关部门保证监管流程的落实，以达到刑事合规的程序化要求。

同时，网络平台应当积极落实并且有效地实施监管流程，确保在能力范围之内，或者平台特点涵盖下有效阻止犯罪行为，以达到刑事合规的实质化要求。

4 结束语

随着《中华人民共和国反电信网络诈骗法》的颁布，以及后续《征求意见稿》等相关法律的陆续出台，网络平台在刑事案件中的权利义务将更加明确，网络平台的监管义务将趋于规则化、主动化和常规化，网络安全问题将得到净化。“大力发展数字经济，提升常态化监管水平，支持平台企业在引领发展、创造就业、国际竞争中大显身手”是总书记在中央经济工作会议上对平台经济的要求和展望。网络平台承载的功能已经不仅仅是虚拟与现实的链接，更代表着在数字时代下新型网络社会安全和网络市场经济。网络平台做好刑事监管措施，履行刑事监管义务，从被保护对象到参与社会治理的一部分，不仅仅是对网络平台刑事案件中监管义务的具体要求，也是国家信息网络安全的有力保障。

参考文献：

[1] 360数字安全.2022年度反诈报告.[EB/OL]. https://new.qq.com/rain/a/20230218A079GH00/2023-02-18

[2] 刘茹.交易平台类网络投资诈骗犯罪侦查对策研究[J].网络空间安全.2022(5).113.

[3] 王一彪.新时代呼唤构建良好网络舆论生态——深入学习贯彻习近平同志“4·19”重要讲话精神[N].人民日报,2018-04-19(07).

[4] 刘权.网络平台的公共性及其实现——以电商平台的法律规制为视角[J].法学研究,2020(2):54-55.

[5] 刘哲.对网络平台信息安全责任的反思与重塑[J].网络空间安全,2022(5).p3-4.

[6] 刘宪权.论信息网络技术滥用行为的刑事责任——《刑法修正案(九)》相关条款的理解与适用[J].政法论坛.2015(6):105.

[7] 付新华.论超级平台数据垄断的法律规制[J].学习与探索,2022(2):64-65.

[8] Assaf Hamdan.Gatekeeper Liability.[J].California Law Review,2003(77):58-59.

[9] 许长帅.网络立法与监管[M].北京:中国政法大学出版社,2019:110.

作者简介：

周子扬（1992-），**男**，**汉族**，**上海人**，**上海师范大学政法学院**，**硕士**；**上海市静安区人民法院**，**法官助理**；**主要研究方向和关注领域**：**刑法学和网络安全**。

面向全流量的网络安全大数据系统研究

朱俊芳[1]，李彦泽[2]，郭超[1]，韦崴[1]
（1.中国电子产业工程有限公司，北京100084；2.北京百分点科技集团股份有限公司，北京100096）

摘要：

［目的/意义］ 传统的网络安全应对策略已无法满足新的网络空间安全需求，亟需结合人工智能、大数据等先进技术手段对网络全流量进行监控、分析和防护，才能最大化地保证网络空间安全。

［方法/过程］ 基于先进的数据智能技术，规划和设计了融合数据采集、大数据处理与存储、人工智能、内容安全、网络安全等数据智能技术构建的网络安全大数据系统技术框架，并将相关技术应用在多网络空间安全场景。

［结果/结论］ 通过相关技术能力建设，实现网络内容监管、网络犯罪预防、关键基础设施防护和安全合规审计等复杂网络安全场景的有效应对。

关键词： 数据智能；网络空间安全；网络安全；内容安全；人工智能；大数据

中图分类号： TP393 **文献标识码：** B

Study of big data cyber security system processing all network traffic

Zhu Junfang[1], Li Yanze[2], Guo Chao[1], Wei Wei[1]
(*1.ELINC China Co.,Ltd.,Beijing 100084; 2.Beijing Percent Technology Group Co., Ltd.,Beijing 100096*)

Abstract:

[Purpose/Significance] Traditional cyber security countermeasures have been unable to meet the new cyber space security needs, and it is urgent to combine artificial intelligence, big data and other advanced technologies to monitor, analyze and protect all network traffic, so as to maximize the security of the cyber space.

[Method/Process] This article proposes and designs a technical framework and network security process workflow for the new generation of cyberspace security requirements, including data acquisition, big data processing and storage, artificial intelligence, content security, network security and other core modules, to achieve cyber space security with multiple scenarios.

[Results/Conclusion] By building these technical capabilities, the system achieves effectively response to multiple network security scenarios, such as network content supervision, cybercrime prevention, critical infrastructure protection and security compliance audit etc.

Keywords: data intelligent;cyberspace security;cyber security;content security;artificial intelligence;big data

0 引言

当今，网络空间逐渐被视为继“陆、海、空、天”之后的“第五空间”，成为国际社会关注的焦点和热点[1]。网络空间安全既要保护信息通信技术系统及其所承载的数据免受攻击，也要防止、应对运用或滥用这些信息通信技术系统而波及政治、经济、文化、社会、国防安全等情况的发生[2]。在此背景下，数据智能技术的出现正是为保障网络空间安全带来曙光，其善于对海量多源异构的网络数据高效治理，以及通过结合大规模数据挖掘、机器学习和深度学习等预测性分析技术，快速提取有价值的安全信息或情报，提升复杂实践活动中的管理与决策水平。数据智能的最终目标是将大数据和智能算法应用于各类实际场景并创造价值，数据智能技术为网络空间安全建设带来了新的技术机遇[3]。

1 网络空间安全现状

近年来，全球网络安全形势愈来愈严峻，软件漏洞、黑客入侵、病毒木马、恶意攻击等问题频频爆发，对全球经济发展和各国社会稳定带来极大冲击。此外，互联网上与日俱增的内容也导致了巨大的内容风险，新技术和新应用也加速了暴恐、低俗和分裂等不良内容信息的传播，引发社会政治层面的不稳定[4]。

网络空间安全理念也正在发生重大转变，网络安全目标正从防止数据泄露、资产破坏、网络瘫痪等传统网络安全领域，延展到安全智能感知、基础设施保障、内容犯罪管控等新一代网络空间安全领域。在传统的网络空间安全建设中，内容安全和网络安全防护相对独立，缺乏对海量的网络日志、网络威胁、网络犯罪情报结合起来的统一思考，在危害发生时容易形成“信息孤岛”。同时，随着云计算、移动互联网等信息技术的迅猛发展，网络空间中累积的信息量正以惊人的速度不断增长，使得网络空间承载的信息具有前所未有的广度和深度，这也导致了传统的统计分析和人工研判，已无法有效应对海量多源异构网络数据所带来的安全分析挑战。网络空间安全所面临挑战的应对策略，亟需从传统对抗的网络安全思路，升级到以数据智能、分析研判等融合技术实现的工程化、自动化和规模化的网络空间安全应对理念。

基于此，设计了一种基于数据智能技术的网络空间安全系统架构，提出了把流量情报、网络安全[5]与实际网络犯罪分析场景结合起来，深度挖掘分散在各系统中的攻击痕迹，以及跟踪和保障流通的信息安全，及时发现和屏蔽不实、危害信息，形成全网、多层次和多渠道延伸的网络安全综合监测能力，从内容安全和网络安全两个维度为构建网络安全系统提供了构建思路，从而保障网络空间中的设备、基础设施和信息内容的安全传播，最终实现保障网络空间安全。

2 网络空间安全系统架构

本文规划和设计了实现对网络流量数据的采集、识别、分析、管控和安全的一体化处理的网络空间安全系统架构图，具体由数据采集层、大数据处理与存储层、智能分析层、业务应用层组成。数据采集层实现流量原始数据的采集接入和流量还原，大数据处理与存储层实现对多源异构安全数据要素加工、处理与存储，智能分析层提供针对流量特征分析、安全威胁检测与内容风险分析等多场景人工智能模型构建的支撑，业务应用层则从内容安全和网络安全两个维度实现综合的安全防护功能，最终实现对网络空间中多安全应用场景的有效支撑。

网络空间安全系统架构如图1所示。

3 关键技术

3.1 数据采集

数据采集技术主要完成流量原始数据的采集和还原。首先，通过部署网络流量采集器，在不影响网络正常运行条件下，实现对多个接入点大规模网络流量数据的采集接入，需要串接或并接的接入模式，以及灵活选择手动上传流量或离线流量采集的方式。

流量采集器的核心是流量分析技术，通过嗅探分析通信流量（通常是加密流量）的各种模式

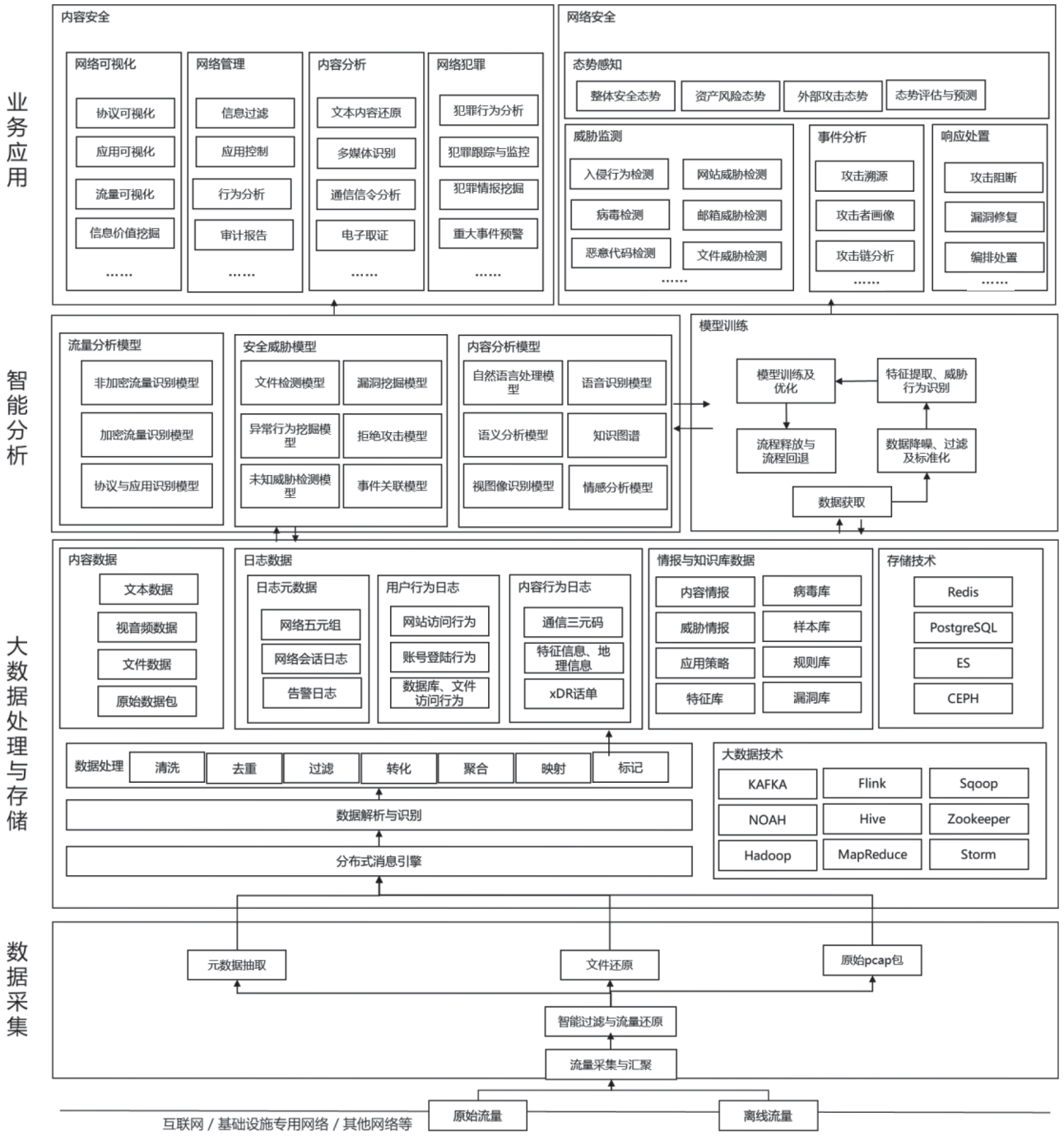

图1 网络空间安全系统架构

以获取有价值信息的一种技术.。现如今的网络流量呈现非加密、加密和匿名流量三种不同模态。随着加密流量、匿名流量在网络流量中所占的比例快速增长，对应的流量分析技术也产生了相应变化。流量分析技术采用深度包检测技术（Deep Packet Inspection），既可以被动地抽取分析网络流量特征的技术，能够对数据包全字段解码，通过监控网络流量、连接和对象，进而识别内容合规，发现注入攻击、数据夹带等网络攻击行为，也可以通过对通信传输施加干扰。例如，修改、重放、丢弃或延迟等操作，从而高效地进行流量特征分析和抽取，具体常用的包括采用深度流检测技术（Deep Frequency Inspection）和匿名协议缺陷等技术。

3.2大数据处理与存储

网络流量数据多呈现结构复杂、更新频繁、语义不明、内容散落、关键数据项缺失等情况，需要通过开展大数据处理，解析生成相关元数据和内容数据，再利用高效的数据治理能力，结合内容安全与网络安全业务不同分析场景需求，网络安全数据要素提取、加工处理以及建库存储，支撑数据分析和情报挖掘。

首先，需要对流量等网络数据开展解析还原。通过消息队列集群接入数据采集模块发送的原始报文和流记录，再由数据解析模块针对业务的关键报文进行深度解析，根据捕获的网络数据报文还原会话流，分层解析、智能过滤并抽取网络层、传输层和应用层的头部信息和重要负载信息，实现对常见协议、应用和行为的识别与还原，还原成不同协议类型数据、日志元数据以及对应的行为日志，并提取关键字段内容，为后续日志分析和数据挖掘提供基础数据支撑。

其次，对流量数据开展数据治理能力建设。开展对多源异构数据的检查和校验，从数据完整性、一致性、准确性、关联性和规范性维度开展数据质量管理，帮助归并重复数据，规范数据格式，纠正数据错误，保证数据一致性。围绕安全业务分析需求，通过本体映射、实体消歧、共指消解等手段，开展相关实体、属性、关系等网络空间安全数据要素的提取、融合和补全，并通过数据标签对数据刻画，从多角度映射实体特征，开展对数据要素地统一维度、统一语境下的描述、分析和处理，形成标准范式下的数据资源。

最后，对各类型数据建立不同的数据存储应对。针对系统运行、用户行为、内容行为等全流量日志类数据，采取白名单、多通道、数据压缩和反序列化等存储手段，能够最大程度地提高数据存储效率。针对内容数据，主要是非关系型数据，包括文本、音视频及原始数据包数据，通过数据结构化加工与处理后按顺序依次存储效率低。同时，采用按照时间先后顺序先暂存在缓存中，记录具有相同类型属性的数据在缓存中的位置，利用记录的内容将缓存中的数据按照属性类型排序后存储到硬盘的方式，则能明显地提高存储读取效率。

3.3 智能分析

智能分析技术是实现内容安全、网络安全等安全场景分析的关键支撑。智能分析技术主要包括流量分析模型、安全威胁模型和内容分析模型。

在流量分析模型方面，现如今随着流量加密与混淆的手段不断升级，传统的基于端口、有效载荷和机器学的分类技术，因存在效率低且精准度差的问题，基于原始数据包数据和提取的流量特征，结合多层感知器、卷积神经网络、循环神经网络、自编码器等深度学习模型框架，构建的加密流量识别模型能够具有较高的识别准确率[6]。

在安全威胁模型方面，随着攻击手段的不断发展，很难采用统一模型识别各种网络威胁行为，针对不同的威胁构建不同的模型，除了采用特征匹配技术实现对各类已知威胁的检测外，聚焦高级威胁检测和未知威胁检测[7]，结合威胁情报体系能力，分类建模不同的高级威胁模型，覆盖异常检测、漏洞检测、行为检测、未知威胁检测、隐蔽攻击检测等模型等，覆盖的深度学习模型包括卷积神经网络、长短时记忆网络、深度置信网络和堆栈自编码网络模型等。在内容分析模型方面，针对社交媒体情报挖掘分析等舆情领域，常通过社交网络分析、信息传播模型、虚假新闻识别、恶意机器人识别等挖掘和跟踪重点人物言论及动态，以及事理图谱和新闻聚类等算法模型，开展事件溯源与分析。针对网络流量情报挖掘分析，常采用知识抽取、知识融合等知识图谱相关算法，开展情报溯源、分析及预警等能力建设。

人工智能模型的实现要经过数据获取、数据预处理、特征构造、模型架构设计与训练和流程释放等环节实现。首先，数据获取阶段以公共数据集和原始数据为先验数据，作为模型训练的数据输入，其中公共数据集主要来源于公开的网络数据，原始数据为通过数据包采集工具收集的原始数据。然后，对数据进行预处理，常见的操作包括数据包过滤、填充或截断和归一化等操作。之后，对高质量的先验数据进行特征提取，特征构造根据不同的识别模型及实际需要动态调整。随后，根据不同的模型开展模型设计与训练，进而进行参数修改等模型优化。最后，在模型训练完成后进行流程释放与回退。

3.4 内容安全

网络内容安全技术实现对网络信息的获取与挖掘、内容识别与管理以及行为的安全审计，侧重对网络空间中流动的信息流内容层面的分析等，具体包括网络可视化、网络管理、内容分析和网络犯罪。

对于网络可视化应用，系统通过全面分析从网络层到应用层的数据，识别L2~L7层的协议和应用，并对协议、流量和应用进行可视化展示，并支持实时统计和多种专业报告格式。此外，通过提取有用信息加以概括总结，实现高效分析、挖掘数据隐藏价值，帮助用户进行业务分析与决策。

网络管理应用包括信息过滤、网络应用控制、行为分析和审计报告等方面。其中，信息通过配置相应策略，实现按URL（Uniform / Universal Resource Locator）或关键字过滤恶意网站及面向DNS（Domain Name System）的过滤技术，从而实现不良网站和钓鱼网站过滤，防止不良信息和内容的传播。网络应用控制支持根据应用程序及会话的流量属性，确定是否允许、拒绝、监视或拦截会话。上网行为分析通过分析URL类别、网站、关键字和访问计数来分析用户上网行为，支持根据标记、分组和报告生成，辅助精细化运营和准确信息推送。审计报告通过制定网站访问、文件传输、邮件收发、远程终端访问等监控策略，系统根据策略记录相应的网络访问行为和内容，从而实现访问可追溯和访问合规性评估。

内容分析对信息网络中的流量或应用内容进行识别、还原与分析。内容分析主要包括文本内容还原、通信信令分析、多媒体识别和电子取证。文本内容还原采用协议识别和内容深度智能分析，实现对网络流量中承载的HTTP、Mail、VoIP等网络内容中的关键字和敏感信息的实时监控。通信信令针对移动网信息生成信令面和用户面话单，进行生成xDR话单。多媒体识别对从海量视音频及网络流量中图片的识别与还原，并通过对比分析和智能检测，快速有效地发现不良信息。电子取证实现对以上内容信息的留存和检索分析。

网络犯罪实现对网络犯罪活动的分析和管控，针对用户行为元数据和信息内容，系统基于大数据、人工智能分析技术，对犯罪行为进行特征、时空、轨迹、关联等维度的分析，支撑犯罪安全情报的挖掘，例如犯罪画像描绘、犯罪行为跟踪、重大时间预警和关联关系挖掘等，保障犯罪可以目标的跟踪与监控，支撑对犯罪事实的调查和研判。

3.5 网络安全

网络安全技术侧重保护网络空间的使用免受网络攻击并能够可靠正常运行的能力。系统架构支撑的网络安全应用，主要包括态势感知、威胁监测、事件分析、响应处置和集中管理，从全局视角提升对安全威胁的发现识别、理解分析和响应处置能力。

网络安全态势感知全面感知和动态洞悉网络及应用运行健康状态，系统支持使用可视化技术，将相应资产风险态势、外部攻击态势、态势预测等信息直观可视化展示，以达到对网络状态的整体把控，为网络安全及网络管理人员的决策分析提供依据。

威胁监测包括实时攻击监测和潜在威胁监测，一方面通过威胁识别模型识别威胁行为，对相关威胁进行实时监测，另一方面基于大数据的关联归并、融合分析和深度挖掘等多种技术手段，从离散的、孤立的数据中探测发现潜在的安全威胁并实时监测。具体的威胁监测范围包括入侵威胁、病毒检测、恶意代码检测、网站威胁检测、邮箱检测和文件威胁检测等。

安全事件分析实现对APT（Advanced Persistent Threat）攻击事件、Botnet事件、恶意样本传播事件、信息传输攻击[8]等重点事件的分析。首先，通过全流量分析技术实现完整的网络攻击溯源取证，回溯已经发生网络攻击行为，分析攻击路径、受感染面和信息泄露状况。从资产角度出发，结合攻击链模型快速定位需要关注和处理的失陷资产。从攻击者角度出发，结合威胁情报，分析攻击行为和通信行为，分析攻击者画像。

处置响应根据告警和事件分析结果构建相应处置动作，例如攻击阻断、漏洞修复、木马杀毒、蠕虫清除等。此外，编排处置借助

SOAR（Security Orchestration Automation and Response）编排技术完成自动化响应处置工作，提升响应处置的速度与准确性。

4 网络空间安全系统的应用场景

4.1 网络监管

面向具有监管义务的政府机构部门，对互联网内容实现综合治理。随着固网、移动网的发展，网络上传播的不良信息、淫秽色情、虚假信息、恐怖主义和公共危机等有害信息持续增加，针对固网和移动网的网络内容监测势在必行。

通过对对网络空间中传输数据进行内容安全层面的分析，通过分级、过滤技术和信息监控来监管、治理各种非法信息、不良信息及有害信息并及时预警，达到净化网络环境、规范网络行为和维护国家安全的目的。

网络内容监管功能实现如图2所示。

图2 网络内容监管功能实现

4.2 网络犯罪

面向国家公安部门，实现网络犯罪的侦破和遏制。目前，网络犯罪呈上升趋势，网络诈骗、身份盗用、商业机密和敏感信息窃取、网络赌博成为网络犯罪的主要形式。

通过网络内容情报和数据智能技术，对犯罪分子的网络行为和通信行为进行监控和多维度关联分析，并对犯罪行为进行深度挖掘和预测，辅助公安机关决策和犯罪管控。例如，阻碍相关犯罪行为的通信、信息过滤和封堵，及时锁定并将其抓获归案。

网络犯罪调查功能实现如图3所示。

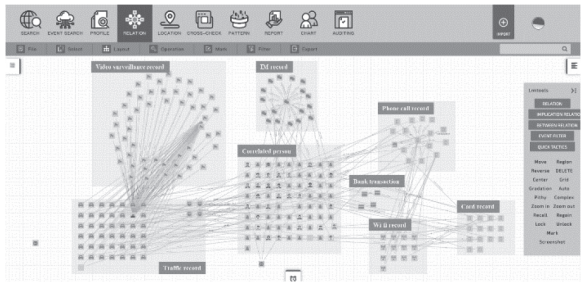

图3 网络犯罪调查功能实现

4.3 关键信息基础设施防护

面向政府部门和重要行业，全面提升网络威胁监测、分析、响应和预测能力。随着关键基础设施频繁面临黑客攻击、病毒破坏等境内外的网络安全风险和威胁，制作传播计算机病毒、入侵和攻击计算机与网络的犯罪日趋增多。

建立关键信息基础设施威胁感知和防护系统，及时发现潜藏在网络中的安全威胁、网络攻击和控制行为，对威胁的恶意行为实现早期的快速发现，对受害目标及攻击源头进行精准定位，对入侵途径及攻击者背景的研判与溯源，尽可能地减少安全威胁对政府、企业带来的损失，提升防御能力，从而保障基础通信设施和重要信息系统的安全稳定运行。

4.4 安全合规审计

面向政府机构、重点行业和大中小企业，实现从内容安全和网络安全双层面的合规审计。信息系统遭受的很多与内部用户的非法使用密切相关，非法盗取内网重要数据的不合规行为也非常普遍。通过对内网流量分析、网络行为监测、网络内容分析，帮助用户事前规划预防、事中实时监控、违规行为响应、事后合规报告和事故追踪溯源，可以最大限度地减少内网风险，防止网络泄密，保护内部安全，满足政府网络管理和内控要求。

网络行为安全合规审计如图4所示。

5 结束语

网络安全目标正从传统网络安全领域，跃升

图4 网络行为安全合规审计

到安全智能感知、基础设施保障、内容犯罪管控等新一代网络空间安全领域。基于此，亟需将数据智能技术与网络空间安全有机结合，探索出适用于网络空间安全新模式的新系统。本文围绕网络空间的内容安全和网络安全两个业务维度，聚焦互联网网络、基础设置专用网络及特定监控范围的其他网络，基于数据智能技术，提出对网络流量的采集、识别、分析、管控和安全防护的综合解决方案，覆盖海量的流量情报、网络情报和网络犯罪，构建了一个全程全网、多层次、多渠道延伸的网络安全综合监测平台，从而有力地保障了基础通信设施和重要信息系统的安全稳定运行。

参考文献：

[1] 金潇,陈兴,董胜亚.电信行业商用密码的个人信息保护实践[J].网络空间安全,2021,12(Z4):43-53.

[2] 李凤华.信息技术与网络空间安全发展趋势[J].网络与信息安全学报,2015,1(01):8-17.

[3] 方滨兴.定义网络空间安全[J].网络与信息安全学报,2018,4(01):1-5.

[4] 吴俊杰,刘冠男,等.数据智能:趋势与挑战[J].系统工程理论与实践,2020,40(08):2116-2149.

[5] 郭宇斌,李航,丁建伟.基于深度学习的加密流量识别研究综述及展望[J].通信技术,2021,54(09):2074-2079.

[6] 邹莉萍,顾峰.网络安全数据分析平台的设计与实现[J].网络空间安全,2021,12(Z3):33-36.

[7] M.Lotfollahi,R.S.H.Zade,M.J.Siavoshani, M.Saberian,《DeepPacket: A Novel Approach For Encrypted Traffic Classification Using Deep Learning》.arXiv,2022,6.22.:http://arxiv.org/abs/1709.02656

[8] T.Shapira, Y.Shavitt.FlowPic: A Generic Representation for Encrypted Traffic Classification and Applications Identification,IEEE Trans.Netw.Serv.Manag.

[9] 王易风,陈迅,纪添.内容和功能分发网络的安全机制研究[J].网络空间安全,2022,13(04):40-47+54.

作者简介：

朱俊芳（1988-），女，汉族，河南安阳人，清华大学，硕士；中国电子产业工程有限公司，高级工程师；主要研究方向和关注领域：网络与信息安全。

李彦泽（1989-），男，汉族，河北乐亭人，黑龙江大学，本科；北京百分点科技集团股份有限公司，高级工程师；主要研究方向和关注领域：网络安全、大数据与人工智能。

郭超（1988-），男，汉族，陕西榆林人，北京大学，硕士；中国电子产业工程有限公司，高级工程师；主要研究方向和关注领域：网络与信息安全。

韦崴（1972-），男，汉族，江苏扬州人，西安电子科技大学，硕士；中国电子产业工程有限公司，工程师；主要研究方向和关注领域：电子信息系统。

社会工程学与大数据环境下的商业秘密保护

韩峰，宋力，李涵睿
（南京晨光集团有限责任公司，江苏南京210006）

摘要：

［目的/意义］ 随着信息技术日益发展，大数据技术的应用逐渐广泛，与之带来的信息安全问题也日益突出，个人隐私信息、企业商密信息，甚至国家秘密信息被泄露的现象呈上升趋势。商业秘密作为一种资源，重要性愈发明显，对商业秘密的非法获取不但可以获利，有时还会威胁到企业的发展乃至威胁到国家安全，甚至影响到国家的政治安全和社会安全。如今，越来越多的黑客开始利用社会工程学方法绕过网络防御窃取信息资源，再通过对信息的大数据分析窃取商业秘密。

［方法/过程］ 基于对社会工程学的认知，结合对商业秘密和国家秘密的探讨，首先介绍了社会工程学的概念，接着讨论了商业秘密与国家秘密的关系和区别，着重论述了利用社会工程学手段，对大数据环境下商业秘密实施窃取的行为，最后提出了在大数据环境下对商业秘密的保护措施。

［结果/结论］ 基于大数据等信息技术广泛、深入地应用到我们的工作和生活中，为了有效地保护大数据环境下的商业秘密安全，有效应对社会工程学攻击，在加强制度建设和政策研究的同时，要加强技术投入，做好数据加密、访问控制和日常的审计，从技术层面加强对数据的保护。

关键词： 大数据；信息安全；社会工程学；商密秘密；国家秘密

中图分类号： TP393 **文献标识码：** A

Social engineering and trade secret protection in big data environment

Han Feng, Song Li, Li Hanrui
(*Nanjing Chenguang Group Co. , Ltd.,Jiangsu Nanjing 210006*)

Abstract:

[Purpose/Significance] With the increasing development of information technology,the application of big data technology is becoming more and more widespread, and the information security problems brought about by it are becoming more and more prominent. The leakage of personal private information,corporate confidential information and even state secret information is on the rise.As a resource,the importance of commercial secrets is becoming more and more obvious. Illegal acquisition of commercial secrets can not only make profits,but sometimes even threaten the development of enterprises,the security of national secrets,and even affect the political and social security of the country. Nowadays,more and more hackers are beginning to use social engineering methods to bypass network defenses to steal information resources,and then steal business secrets through big data analysis of information.

[Method/Process] Based on the cognition of social engineering, combined with the discussion of commercial secrets and state secrets, this paper first introduces the concept of social engineering, then discusses the relationship and difference between commercial secrets and state secrets,and focuses on the use of social engineering methods to analyze big data. The commercial secrets are stolen in the environment, and finally the protection measures for the commercial secrets in the big data environment are proposed.

[Results/Conclusion] Based on the extensive and in-depth application of information technology such as big data in our work and life, in order to effectively protect the security of trade secrets under the environment of big data and effectively cope with the attack of social engineering, we should strengthen the system construction and policy research on the one hand; At the same time, it is necessary to strengthen technical input, do a good job in data encryption, access control and daily audit, and strengthen the protection of data from the technical level.

Keywords: big data; information security; social engineering;business secrets; state secrets

0 引言

随着市场经济的不断发展，国家重点高新企业、核心科研院所甚至国防军工企业越来越多地参与到市场竞争中，逐步认识到商业秘密的重要性和大数据背景下保护商业秘密的必要性和紧迫性。与此同时，多数重要的商业秘密承载的信息与国家秘密信息密切相关，在不同的背景下，商业秘密承载的信息经过大数据的汇聚分析后，具有国家秘密信息的属性。目前，政府部门、国防军工企业、核心科研院所对国家秘密的保护有一套成熟完整的机制。但是，对商业秘密的认识和意识相对淡薄，对商业秘密的保护还处于探索阶段。在商业秘密的使用和保护过程中，应该谨防一些别有用心的组织和个人，利用社会工程学手段窃取商业秘密或敏感信息，同时通过对所获得信息的大数据收集、分析和推断，非法获取企业、科研机构等的核心关键信息甚至获取国家秘密信息。

1 社会工程学概念

社会工程学（Social Enginrrging）也被称为信息刺探，是由美国网络安全工程师凯文·米特尼克在《反欺骗的艺术》中第一次提出，出发点是让人们懂得信息防护，避免个人信息泄露所造成的不必要损失[1]。严谨地说，社会工程学不是一门纯粹的学科，是利用公众的粗心大意、贪心不足、轻易相信和缺乏警惕性等特点，来操纵人们去执行预先设定好的行为动作或泄露信息的一门学问和艺术。同时，社会工程学通过建立自然的、社会的或制度的理论基础，通过实践进一步达到解决各种问题，实现个人目的的一门学问和艺术。近年来，利用社会工程学实施信息窃取的行为日益严重，许多组织和个人深受其害。

2 商业秘密与国家秘密

《中华人民共和国刑法》第219条对商业秘密的定义：“商业秘密是指不为公众所知悉，能够为权利人带来经济利益、具有实用性，并经权利人采取保密措施的技术信息和经营信息”。《中华人民共和国保密法》和《保密法实施条例》对国家秘密的概念、密级、保密期限、知悉范围的确定、变更和解密都做了具体规定[2]。国家秘密是指关系国家安全和利益，依照法定程序确定，在一定时间内只允许一定范围人员知悉的事项。

2.1 商业秘密与国家秘密的区别

从国家法律对商业秘密和国家秘密的定义上，可以看出二者有着一定的区别。

首先，商业秘密和国家秘密涉及的利益主体不同，前者主要涉及企事业单位、科研院所等权利人的经济效益、市场竞争优势等层面；后者则主要涉及国家的安全和国家的利益。

其次，二者的所有权属性不同，前者为自然人或者法人所有；后者的所有权则为国家。

其三，二者的定密主体不同，商密的定密主体是企业、科研院所等经营、研究性的企事业单位，国家秘密的定密主体则是依照国家法律和法定程序拥有定密权限的国家政府机关和依照国家法律被授予定密权限的企事业单位。

其四，二者的确定程序不同，相较于国家秘密的确定程序，商业秘密的确定程序相对简单，而国家秘密的确定程序必须严格按照国家法律法规确定的程序进行。

其五，二者所适用的法律法规不同，商业秘密主要受国家反不正当竞争相关的法律法规保护，主要归其权利人自行管理和保护；国家秘密则受到国家保密法律法规管理，保密管理要求和措施由国家法律明文规定。

2.2 商业秘密与国家秘密的关系

虽然商业秘密与国家秘密存在着显著的区别，但是二者也存在着千丝万缕的联系。在我国现有的制度体系下，科研院所、军工企业的诸多核心商业秘密，在一定程度上直接关系到国家利益和安全。国家秘密和商业秘密在一定条件下可以互相转变。例如，随着科学技术的不断发展和时间的推移，在一定时间段和一定条件下属于国家秘密的信息会被降低密级或解除密级，此时的国家秘密如果具备商业秘密价值，则可以被定义为商业秘密加以保护。又如，企业利用军工技术开发、研制属于商业秘密的科技项目，此时的商业秘密就可能要被定义为国家秘密。

3 利用社会工程学窃取信息的手段

应用社会工程学手段实施信息收集、信息刺探等窃取国家、组织和个人敏感信息的行为越来越多，且方式多种多样。越来越多的黑客在研究网络安全技术的同时，开始学习、研究并利用社会工程学手段，辅助相应的信息安全技术，突破网络防御措施、利用人的弱点实施信息窃取[3]。

3.1 社会工程学的攻击形式

运用社会工程学窃取商业秘密一般分为三个步骤[4]，即“信息收集”“假冒身份”和“信息窃取与大数据分析”。这三个步骤相互依存，紧密结合，攻击者在实施攻击时，通常会根据实际情况混用这三种手法以达到最终目的。

3.1.1 信息收集

信息收集是指通过各种手段去获取被攻击者的一些不敏感信息。不敏感信息访问控制策略设置的门槛较低，攻击者容易得手。同时，在获取的过程中，不易引起被攻击者的注意，降低了攻击者的风险，例如收集被攻击者的个人信息、企业信息和产品信息等。信息收集为攻击者进入下一阶段的攻击做了前期铺垫。

3.1.2 假冒身份

假冒身份是根据攻击需要“包装”自己。攻击者根据攻击目的为自己设置一个合适的身份，再把选好的身份稍加粉饰，使被攻击者不产生怀疑。在包装的过程中，攻击者会充分利用和挖掘人感性的弱点，通过博取信任、好感和树立权威性等技巧达到逼真的包装效果。例如，通过参加展会、假装洽谈、提供订单等方式，与被攻击者建立一种事先设定好的个人关系和商业关系。

3.1.3 信息窃取

在顺利完成信息收集和假冒身份之后，攻击者便可以通过施加影响、实施攻击等手段来达到窃取信息的目的。例如，以商业合作的方式索取一些人员信息、产品信息和生产周期等。继而对汇聚到的各种信息进行大数据分析，推断出被攻击者的产品类别、研发能力和生产能力等情况。

由于被攻击者对商业秘密信息的敏感度和防护意识不强，会根据攻击者的需要，提供一些不涉及国家秘密但可能是商业秘密的信息。攻击者通过对信息的大数据采集、分析和提取，把获取的非密信息、一般商业秘密信息，汇聚为核心重要商业秘密甚至国家秘密，进而威胁到企业的发展，乃至危害到国家的安全。

4 大数据环境下的商业秘密特点

大数据在经过搜集、加工、整合后形成大量数据群。在信息技术高速发展的今天，数据资源作为企业、国家的重要资源，特别是商业秘密数据资源对企业发展、国家安全稳定起着举足轻重的作用。在大数据环境下，商业秘密具有两个明显的特点。

4.1 形式多样

在大数据环境下，企业经营、科学研究等各个环节都有可能产生商业秘密或敏感信息，即使原本不具备商密性质的信息，经过对信息的大数据分析处理，也可能会形成具有使用价值的商业秘密信息。因此，商业秘密呈现的形式多样，可以是企业日常运作过程中产生的客户信息、产品类别和招投标信息等。同时，商业秘密还可以是科研院所日常研究过程中建立的数据库和研究数据样本等，还可以是政府发布的政务信息，例如在新型冠状病毒疫情期间，政府内部发布的疫情信息、医疗资源分布情况等信息。上述信息单独存在、或片段存在时，不一定涉及商业秘密或国家秘密，但是经过大数据的搜集、整理加工后，就有可能形成企事业单位商业秘密，一旦被泄露，就会给企事业单位甚至国家造成损失。

4.2 存储电子化

商业秘密存在于企业科研、生产和运营的各

个环节，多以纸介质、光介质和电磁介质等形式存在，存储方式主要是以电子化和数字化的方式存在。作为商业秘密载体的信息，大多是依靠互联网产生、保存、传递、处理和存储。电子化的方式存储对信息的搜集、处理和整合，乃至辅助支撑决策都带来诸多的便利，在很大程度上提高了工作质量和工作效率，但是也带来了一定的风险。由于信息存储电子化，如果对信息的使用和传递等控制不严格，极易造成信息被窃取、商业秘密被泄露的风险，或者不是商业秘密的碎片信息被收集后，经过大数据分析形成涉及商业秘密的信息。

5 大数据环境下的商业秘密保护措施

在大数据环境下，商业信息数字化和信息化的程度越来越高，数据集中存储、信息网络传递、远程视频办公等，均使得商业秘密信息或片段信息被非授权获取、大数据分析、非法使用，进而导致商业秘密信息泄露。因此，在大数据时代，对商业秘密的保护愈发重要。

5.1 防范社会工程学攻击

社会工程学的主要攻击对象是人。人是整个信息安全链中一个非常薄弱的环节，同时也是防范社会工程学攻击最坚固的“防火墙”[5]。企业的商业秘密事关企业的生存、发展和市场竞争力，大量商业秘密的汇聚甚至关系到国家秘密安全。

5.1.1 构建商业秘密保护体系

在应对利用社会工程学手段窃取商业秘密时，起码应做到两点。首先，制定完善、合理的管理体系和奖惩机制，并定期做好宣传工作，使人对社会工程学攻击有认识、有意识、有防备、有应对，不泄露企业敏感信息。其次，加强日常相关知识的教育，提高人们的保密知识、保密意识和防范措施，使人们在日常工作和生活中，时刻保持保密防线不松懈、保密底线不触碰。企业等组织还应根据信息的重要程度，制定不同的等级标准，严格控制核心商业秘密的知悉范围。

5.1.2 明确商业秘密管理要求

应该建立完备的商业秘密保护细目，明确具体的商业秘密保护条款。依据信息的重要性进行分类处理，控制信息的知悉范围。首先，明确商业秘密的提供途径，不擅自提供商密秘密信息，利用信息化手段将商业秘密的保护融入到业务的各个环节，实现过程管控。其次，按规定程序及时销毁不再使用的商业秘密文件，不随意丢弃、不随意带出工作区。第三，加强对离职离岗人员的教育和脱密期管理，在人员离岗时，除了教育其要保守国家秘密外，还要提醒其保守企业商业秘密，并定期回访。最后，应该建立事故应急响应小组，在发生失泄密事件时，应急小组能够及时作出有效响应。

5.2 防范大数据泄密

大数据等信息技术的高速发展是机会和挑战并重、发展和安全共存的时代。我国高度重视大数据技术的发展，国家网信办在《国家网络安全战略》中，提出我国要实施国家大数据战略，同时提出要建立相应的大数据安全管理制度，大力支持大数据的创新和应用。在享受大数据价值的同时，应面对并解决带来的网络安全挑战，从技术层面做好信息保护，谨防大数据泄密。

5.2.1 做好数据加密

在大数据环境下，对信息的加密是保护数据安全最直接和最基本的措施，加密的一个重要环节是如何对密文信息进行处理，对这一问题可采用同态加密和可搜索加密[6]。1978年，Rivest等首次提出秘密同态的概念，在后续的相当一段时间，构造同态加密算法体系一致是密码学的难题。后续的学者和研究人员在同态加密理论和实践上不断取得突破和成就，所形成的同态加密方案越来越简洁和实用，并且具有更高的安全性，为大数据的处理提供了数据保护功能。2000年，Song等经过深入研究和大量实践提出了可搜索加密方案。他们用伪随机数和流密码的方法，构建了基于对称算法的可搜索加密算法。这一算法，

解决了对密文信息的查找和检索困难的问题。可搜索加密算法分为非对称可搜索加密和对称可搜索加密。在对数据加密时，应该根据自身特点选择合适的加密算法，有效地降低数据被窃取的风险。

5.2.2 做好访问控制

在日常工作中，要做好对数据访问策略的设置，严格控制数据信息访问。大数据的访问控制思路和方案主要有两种。其一，是基于访问者角色的访问控制，依据角色和职责的不同，配置相应的访问权限，只有满足策略要求时，访问者才可以查看相应的数据信息。其二，是基于数据自身属性的加密访问控制，将访问策略直接与用户密钥或数据加密关联。它是利用密文机制实现对访问客体控制的方法，在此方案中，访问者只要掌握密钥即可访问对应的数据。

5.2.3 做好日志审计

企业还应根据自身的技术特点，定期做好数据平台的日志审计。通过审计用户访问行为、审计用户权限开放、审计数据的访问记录等来分析是否存在数据违规被获取的风险。在发现违规事件或潜在风险时，应及时上报，有效处理。在发现重大风险时，应及时响应和补救，将风险降低。

6 结束语

随着数字中国概念的提出，“大数据”“云计算”“信息化”和“智能化”等技术高速发展，并广泛应用到我们的工作和生活中，极大地便利了人们的生活、企事业单位的发展和政府的运营。在技术为企业发展创造更多经济效益的同时，也使企业面临更大的挑战和威胁。

商业秘密作为企业发展的无形重要资产，在技术高速发展的时代，对商业秘密的保护提出了更高的要求。同时，通过社会工程学手段有目的、有针对性地搜集获取企业非涉密信息，通过对搜集数据的大数据分析，进而推断出敏感信息、商密信息甚至国家秘密信息，会造成商业秘密的泄露和国家秘密的泄露[7]，给企业发展带来了严峻挑战。

为了有效地应对社会工程学攻击，有效地保护大数据环境下的商业秘密安全，在加强制度建设和政策研究的同时，要加强对人的保密“两识”教育，使人们懂安全、知法规、有意识、保底线、守秘密，同时还要加强企业技术投入，从技术层面加强对数据的保护。

参考文献：

[1] 凯文·米特尼克.欺骗的艺术[M].北京:中国铁道出版社,2008.

[2] 远东.国家秘密标志的作用不可忽视[J].保密工作,2016(8).

[3] 建中.黑客社会工程学攻击[M].济南:齐鲁电子音像出版社,2008.

[4] 王宏波.社会工程学的意义、内容与学科特征[J].西安交通大学学报（社会科学版）,2011(1).

[5] 黄明祥.信息与网络安全概论[M].北京:清华大学出版社,2010年1月.

[6] 张博卿.我国大数据安全现状、问题及对策建议[J].网络安全空间,2018(08).

[7] 杨光子鉴.军工科技企业对外合作中的商业秘密防护措施[J].网络安全空间,2022(03).

作者简介：

韩峰（1986-），男，汉族，江苏邳州人，中国矿业大学，硕士；南京晨光集团有限责任公司，工程师；主要研究方向和关注领域：信息安全和保密技术管理。

宋力（1980-），男，汉族，河南南阳人，哈尔滨工程大学，硕士；南京晨光集团有限责任公司，高级工程师；主要研究方向和关注领域：保密政策法规、保密管理。

李涵睿（1996-），女，汉族，山东济宁人，大连大学，硕士；主要研究方向和关注领域：网络安全、数据安全。

探析使用国密算法进行个人信息保护

张德强
（成都市住房和城乡建设信息档案中心，四川成都 610015）

摘要：

［目的/意义］ 随着数字经济的高速发展，特别是在国家关于数据安全治理和个人信息保护相关法律法规颁布和实施后，数据安全治理和个人信息保护作为强制性要求得到了进一步巩固和提升。数据信息保护最重要的措施之一就是对数据信息的加密。信息加密必然会影响信息的使用效率，基于国密算法并兼顾信息使用效率，提出了一种个人信息保护方法。

［方法/过程］ 通过对重要数据信息进行SM3密码杂凑算法、线性变换和异或处理生成“一次一密”密钥，再使用生成的密钥和SM4分组密码算法，对需保护的个人信息进行加密保护。在使用个人信息时，利用个人信息的SM3杂凑值进行精准高效查询，查询到信息后使用密钥进行国密SM4算法解密使用。

［结果/结论］ 基于国密算法的个人信息保护方法，在满足信息使用的业务需求场景下，经过实际使用显示加强和提升了数据和个人信息的保护。

关键词： 个人信息保护；敏感信息；国密算法；SM3算法；SM4算法；数据安全治理；一次一密

中图分类号： TP309.2；TP309.7 **文献标识码：** B

Exploring the use of national security algorithms for personal information protection

Zhang Deqiang
(*Chengdu Housing and Urban Rural Construction Information Archives Center, Sichuan Chengdu 610015*)

Abstract:

[Purpose/Significance] With the rapid development of the digital economy, especially after the promulgation and implementation of national laws and regulations on data security governance and personal information protection, data security governance and personal information protection have been further consolidated and improved as mandatory requirements. One of the most important measures for protecting data information is to encrypt it. Information encryption will inevitably affect the efficiency of information usage. Based on the national security algorithm and taking into account information usage efficiency, a personal information protection method is proposed.

[Method/Process] The "one-time key" secret key is generated through the SM3 password hash algorithm, linear transformation and XOR processing of important data information, and then the generated secret key and the SM4 block cipher algorithm are used to encrypt and protect the personal information to be protected; When using personal information, use the hash value of the SM3 of personal information for precise and efficient query. After finding the information, use the secret key to decrypt it using the SM4 algorithm.

[Results/Conclusion] The personal information protection method based on the national security algorithm has strengthened and improved the protection of data and personal information through practical use and display in scenarios that meet the business needs of information usage.

Keywords: personal information protection;sensitive information;state secret algorithm;SM3 algorithm;SM4 algorithm;data security governance;one-time key

0 引言

中共中央、国务院在2020年4月9日印发了《关于构建更加完善的要素市场化配置体制机制的意见》，明确提出数据是一种新型生产要素，要通过加快数据要素市场培育，充分发挥数据要素对其他要素效率的倍增作用，使大数据成为推动经济高质量发展的新动能。数据参与经济建设、社会治理、生活服务，发挥着重要作用。数据信息安全是数据信息应用的基础，发展数字经济、加快培育发展数据要素市场，必须把保障数据安全放在突出位置，安全问题是所有工作的前提和底线。这就要求我们着力解决数据安全领域的突出问题，有效提升数据安全治理能力。在数字化建设过程中，会收集、使用和加工大量个人信息，如果这些信息不采取措施妥善保护，不法之徒将会利用这些个人信息侵扰人民群众生活安宁，危害人民群众生命健康和财产安全。加强数据信息的保护，提高数据安全治理能力，维护国家安全和个人权益迫在眉睫。

2021年9月1日正式实施的《中华人民共和国数据安全法》（以下简称《数据安全法》）第4条规定“维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。”要建立健全数据安全治理体系，需在数据的收集、存储、使用、加工、传输、提供、公开等各个处理环节，实施完善的安全策略、人员责任、安全作业等治理手段，并部署相关的数据安全产品。构建数据安全治理体系，还需对数据进行分类分级管理。但是，考虑到成本，数据加密技术的应用能在业务快速迭代背景下使数据安全得到显著提升。同年11月1日《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）正式颁布实施，进一步明确了个人信息处理规则、跨境提供规则、个人在个人信息处理活动中的权利和义务、履行个人信息保护职责的部门及法律责任。《个人信息保护法》统筹了个人主体和公权力机关的义务与责任，同时兼顾个人信息保护与利用，为个人信息保护工作提供了法律依据，保护信息所有人的隐私权，避免个人隐私遭到泄露。个人信息保护已成为人民群众最关心的现实利益问题之一。

加强数据信息的保护，使用户在主动化、自动化、智能化、服务化和实战化等需求时得到保护，有助于清除个人信息的无序滥用、私下转卖等行业弊病的发展障碍，有利于推动形成利于数字经济快速、健康、平稳发展的市场环境，保障数字经济高速发展。个人信息保护是经济发展的需要，也是时代进步的需要。

1 国密算法

国密算法即国家商用密码算法，通常用SM表示,简称国密，是国家用于非国家机密信息保护所采用的一系列密码技术和密码产品的总称。密码算法标准及其应用规范由国家密码管理局认定和公布，其中部分密码算法已经成为国际标准。2020年1月1日颁布实施的《中华人民共和国密码法》（以下简称《密码法》）规定“密码分为核心密码、普通密码和商用密码”“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，运营者应当使用商用密码进行保护”。《密码法》进一步明确使用国密算法来保护关键信息基础设施和个人信息。

国密算法如表1所例。

表1 国密算法

序号	密码分类		国密算法
1	对称加密	分组加密/块加密	SM1(SCB2)、SM4(SMS4)、SM7
2		序列加密/流加密	ZUC（祖冲之算法）、SSF46
3	非对称/公钥加密	离散对数	SM2、SM9
4	密码杂凑/散列		SM3

在对称加密算法中，SM1、SM7密码算法目前还没有公开，仅以IP核的形式存在于芯片中，使用该算法需使用对应的芯片、加密卡或者加密机。对称加密SM4分组密码算法和SM3密码杂凑

算法的算法均对外公开，可以根据公开的算法编写不同语言的程序供系统使用。

1.1 SM3密码杂凑算法原理

SM3密码杂凑算法通常称作摘要算法、散列算法，或者Hash算法，是密码学中的基础算法，是现代密码学中的核心组成部分。密码杂凑算法是将任意大小（例如文本消息）的输入信息数据转换为固定大小（例如256位长度）的结果，这个结果称为杂凑值（或消息摘要、哈希码、哈希值）。比如，SM3密码杂凑算法，可将任意输入转换为256位长度输出。

SM3密码杂凑算法采用默克尔·达姆加德（Merkle-Damgard）结构，消息分组长度为512Bit，输出的摘要值长度为256Bit。SM3密码杂凑算法的输入长度为lBit($l<2^{64}$)的消息，经过填充、分组、迭代压缩后生成杂凑值，杂凑值输出长度为256位，算法过程分为三步。

第一步：填充。通过填充使加密数据的长度是512Bit的整数倍。首先在数据的末尾加一个1，然后把原始数据的长度用64Bit表示，并放在最后面，再看现在的数据的长度值离512的整数倍还差多少位，差多少位就在加的这个1和64Bit的之间填多少个0。

第二步：分组。把填充后的信息按照512Bit一个组进行分组，例如分成了N组，标注为b(0),b(1)……b(N-1)。

第三步：迭代压缩。SM3算法的压缩函数和SHA-256算法的压缩函数类似，但是SM3的压缩函数更复杂。通过迭代压缩得到最后的杂凑值IV(n)=CF(IV(n-1)，b(n-1))，其中CF为压缩函数、IV为初始值，如果信息分为N组，那么IV（N）就是最后得到的杂凑值。

SM3密码杂凑算法主要有三个特点：一是具有确定性，相同的消息总是能得到同样的摘要值，并且不管消息长度是多少，最终的摘要值长度也是相同的；二是难以分析且不可逆，算法具有雪崩效应，对输入消息的微小改变会对杂凑值产生巨大影响，通过杂凑值很难逆向计算出原始消息；三是没有碰撞性，试图找到两个具有相同杂凑值的不同消息几乎不可能。正是基于SM3密码杂凑算法的这些特点，才被广泛用于数字签名与验证、消息认证码的生成与验证和随机数的生成。

本文探索的信息保护方法也是利用SM3算法来进行消息验证和“一次一密”密码的生成。

1.2 SM4分组密码算法原理

对称分组密码算法SM4是一种迭代分组密码算法，采用非平衡费斯妥（Feistel,以德国的物理学家和密码学家霍斯特·费斯妥命名）结构，分组长度为128Bit，密钥长度也为128Bit。加密流程分为明文加密与密钥扩展（每次密钥的生成）两部分。加密算法与密钥扩展算法均采用32轮非线性迭代结构，以字（Word，长度为32Bit的组）为单位进行加密运算。SM4分组密码算法的数据解密和数据加密的算法结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

分组密码算法只能处理特定长度的信息数据，而在实际应用中待加密的明文数据的长度是不固定的，这就需要对分组密码的算法进行迭代，将一段很长的明文全部加密，而迭代的方法就是分组模式，一次迭代运算为一轮变换。

迭代分组加密流程如图1所示。

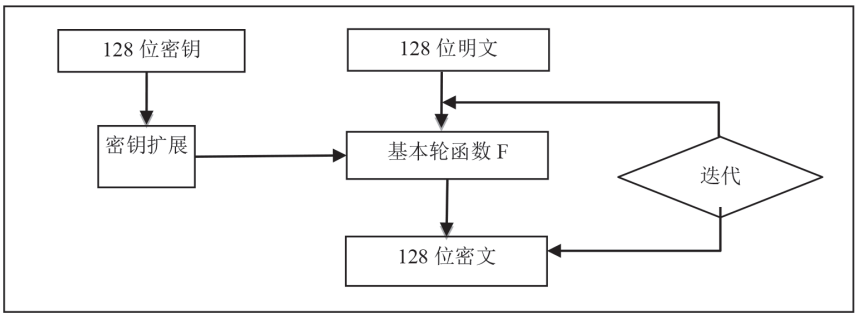

图1 迭代分组加密流程

分组密码在加密中有5种分组工作模式，分别为电子密码本（Electronic Code Book，ECB）模式、密码块链接（Cipher Block Chaining，CBC）模式、密码反馈（Cipher Feedback，CFB）模式、输出反馈（Output Feedback，OFB）模式和计数器（CounTeR，CTR）模式。推荐使用CBC和CTR模式，其中CBC密码块链接模式的密文分组像链条一样互相连接在一起。

CBC分组工作模式加密过程如图2所示。

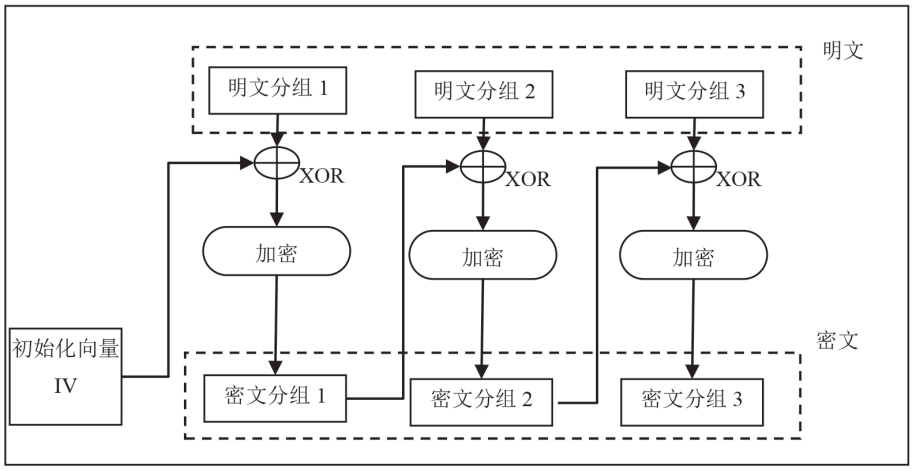

图2 CBC分组模式加密过程

这种分组工作模式，将一个明文分组和一个密文分组进行异或（Exclusive OR，XOR）运算，然后再进行加密。其特点就是每个密文块都依赖与它前边的所有明文块，明文分组在加密之前一定会与“前一个密文分组”进行XOR运算，因此即使明文分组1和明文分组2的值是相等的，密文分组1和2的值也不相等，算法的抗攻击性和安全性都更高了。

3 基于国密的保护方法

个人信息的保护就是最大限度地保障个人信息在采集、传输、存储和应用过程中的安全。在个人信息的保护过程中通常需要解决三个关键问题：一是如何选择适当的信息数据加密方式及机制，同时考虑加密效率；二是在信息数据以加密形态存储的情况下，如何实现对目标信息数据的精确查找和搜索，并兼顾信息的使用效率；三是在确保信息数据隐私性安全的情况下，要保证数据的一致性和可用性。

基于国密的个人信息保护方法，将充分利用SM3密码杂凑算法和SM4分组密码算法等国密算法特点，依靠关键信息的杂凑值产生“一次一密”密码，对个人信息进行加密，实现对相同的个人信息因密码不同使加密后的密文也不同，同时使用个人信息的杂凑值进行高效的精确查找和搜索。

3.1 实现方法

为便于对信息系统收集到的个人数据信息的管理和利用，在实际使用中，通常采用数据库进行存储和使用。个人信息保护的首要措施是对个人信息的加密，个人信息加密分为存储加密和传输加密。存储加密是在数据写入存储介质前将数据进行加密，实现对数据的加密存储，实现的方式复杂多样，是一种对个人信息最有效的保护方式。传输加密是对传输中的信息数据流加密，保证传输通道、传输节点和传输信息数据的安全，防止通信线路上的窃听、泄露、篡改和破坏。通常系统使用Web服务，只需启用安全传输层协议（Transport Layer Security，TLS）就能实现个人信息传输中的安全。

基于个人信息保护过程中的三个关键问题，可通过SM3密码杂凑算法对需要防串改的关键信息进行信息认证形成摘要信息（即256Bit杂凑值），取信息认证的杂凑值第一位使用y=（ax+b） mod 32和Substring（y,y+32）截取128Bit值，并和128Bit密码进行异或形成“一次

一密”密码。用生成的“一次一密”密码对需要保护的个人信息使用SM4分组密码算法进行加密，利用SM3密码杂凑算法对个人信息形成的杂凑值用于精确查找和搜索，实现基于国密算法、兼顾效率和安全的个人信息保护模式。

个人信息加密保护过程如图3所示。

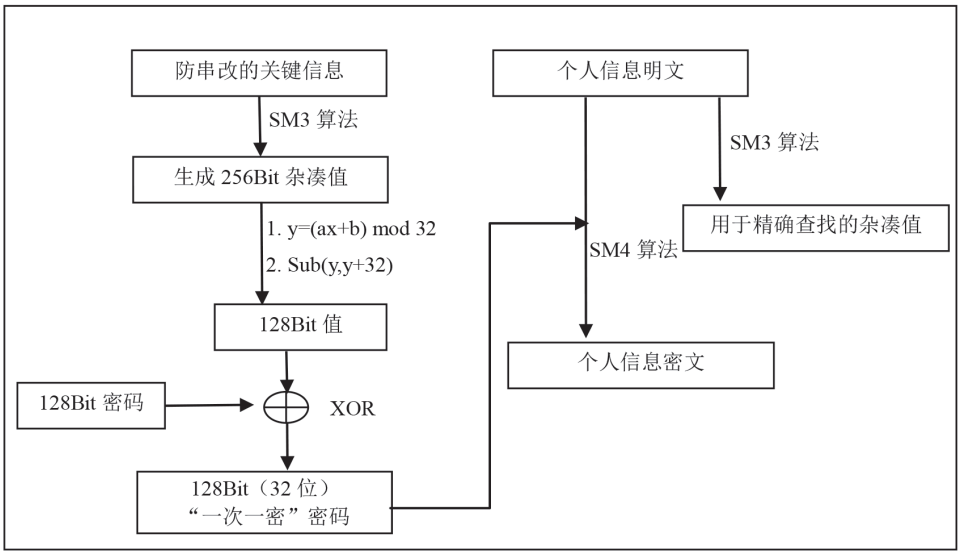

图3 个人信息加密保护过程

例如，在房屋交易业务过程中系统需采集购房人信息和购房合同信息。在数据库中建立房屋交易合同表，用来保存采集的购房人姓名、身份证号和签订的合同文本信息等。如表2所例。

表2 房屋交易合同表

序号	字段名称	类型	字段含义
1	id	Bigint	ID号
2	username	Varchar(200)	购房人姓名
3	idnumber	Varchar(200)	身份证件号码
4	idnumberhash	Varchar(200)	证件号码杂凑值
5	idnumberciphertext	Varchar(1000)	证件号码加密信息
6	contract	Text	合同文本原文信息
7	contracthash	Varchar(200)	合同杂凑值
8	inserttime	Timestamp	系统录入时间

合同信息作为关键信息需防范被串改，身份证件号码作为重要个人信息需进行加密保护。为了测试加密后信息的使用效率，数据库表中保留了身份证件号码的明文，实际使用不保存身份证件号码明文信息。

为了便于演示说明个人信息加密保护过程，模拟系统采集购房合同信息。使用随机函数生成购房人姓名、身份证件号码，再向PostgreSQL数据库中循环插入100万条购房信息记录。信息数据生成后，使用SM3密码杂凑算法对身份证件号码和合同信息进行杂凑计算形成对应的杂凑值。身份证件号码的杂凑值用来对身份证号码进行精确查找和搜索，合同信息的杂凑值用来校验合同信息防止信息被非法修改，同时合同信息的杂凑值也用来生成“一次一密”密钥。

按照图3所示流程，对身份证件号码的杂凑值首位数值进行线性变化，取余后，从余数位开始截取32位字符串，并和固定密钥进行异或计算，生成“一次一密”的128Bit（32位字符串）密码，利用生成的“一次一密”密钥使用SM4分组密码算法（CBC模式）加密身份证件号码，使存储的个人身份证件号码信息为加密字符串，达到保护个人信息的目的并生成“一次一密”的程序代码。

个人信息身份证件号码通过SM4分组密码算法加密得到保护，并且使用“一次一密”秘钥可以使相同的身份证件号码加密的密文不一样，加强了个人信息的保护。相同身份证件号码使用“一次一密”加密信息后结果，因身份证号为系统随机产生，非实际真实号码，图中身份证号信息为方便表述说明，未进行脱敏处理。

加密后数据库存储信息如图4所示。

“一次一密”加密结果如图5所示。

一次一密程序代码：

```
//取 16 进制杂凑值第一位并转化为 10 进制
Integer i1=Integer.valueOf(sm3hash.substring(0,1),16);
//线性变换 f(x)=ax+b，取 a=3,b=5
Integer i2=3*i1+5;
//对 32 取余
Integer i3= Math.floorMod(i2,32);
//从余数的位数开始截取 32 位字符串
String hash32=sm3hash.substring(i3,i3+32);
//和固定秘钥进行异或，生成“一次一密”的 128 比特（32 位字符串）密码
String rkey= xorHex(key,hash32);
```

id [PK] bigint	usernam characte	idnumber character varying (20	idnumberhash character varying (200)	idnumberciphertext character varying (1000)	contract text	contracthash character varying (200)
916548	叶手	44270820210920...	E913EE4C12DEB8D2AFC29689C3C10...	1b928f9fa445773dd8b6ed8769ed88...	购房合同信息，购房人为:叶手,身份...	931782BC0558A813F659C2FE7D59BC9652CE
100030	糜粘锐	31100719980505...	D91A0A3D57CA54E449C1B3DF93166...	1337163d71373b8870fb6fa34e667c...	购房合同信息，购房人为:糜粘锐,身...	A8FEBAF0BF53C157DB85793145695DD2A61...
100036	冯芬菌	23260819700728...	98315ABF9339D70D7971DD67245836...	3dba0a216226d53dda864907d904a...	购房合同信息，购房人为:冯芬菌,身...	7065D4C893498F38E0257EB94C2A4C9EE6D9
100039	梅苍	22083619990602...	9DDF2CB43367D6B56B1DB34F00A53...	9bb0da8bd7f56f236262ea2fcc0e6f2...	购房合同信息，购房人为:梅苍,身份...	CD1B4240CFFE7CEB40A132382A4BC0BA741...

图4 数据库存储的加密数据

id [PK] bigint	username character var	idnumber character varying (200)	idnumberciphertext character varying (1000)
100063	史田放	632632193206254441	0022c1576178ed027fc4a94598aff139d76d9ad7e6348af1ccd59660ef6c6b91
100034	史田放	632632193206254441	de2f487c737fb24ad4753912786396f0d01a67362e647fda821e9fa27ce4f1f2

图5 “一次一密”加密结果

3.2 信息加密后的使用效率

个人信息加密后信息得到了保护，但是个人信息采集存储的目的是个人信息的使用。个人信息的加密保护不能为了保护而不考虑信息使用，如何高效地利用个人信息是采集个人信息后首先需要考虑的问题。通过个人身份证号码明文查询和加密密文查询进行对比，检验个人信息加密后使用效率的损耗。

明文查询。根据个人身份证号码明文直接进行数据库精确匹配查询并显示，记录系统所耗时间，这种利用方式也是最普通常见的，主要代码：

```
//明文查询所需时间
startTime = System.currentTimeMillis();
List<HashMap<String, Object>> select = sqlUtil.Select("select * from contractTable where
idnumber='"+idnumber+"'");
for (int i = 0; i < select.size(); i++)
{
System.out.println(select.get(i).get("id").toString()+"明文查询的身份证号：
"+select.get(i).get("idnumber"));
}
endTime = System.currentTimeMillis();
elapsedTime = (endTime - startTime) ;
System.out.println("明文查询总共耗时：" + elapsedTime + "ms");
```

密文查询。对要查找的个人身份证件号码信息进行SM3杂凑计算，用生成的杂凑值进行数据库精确匹配查询，利用检索结果中的关键信息计算“一次一密”密钥，再利用密钥使用SM4（CBC模式）解密个人身份证号码并显示主要代码。

系统运行后效率为明文查询948ms，加密查询1160ms，得出运行结果。因数据库未做优化处理，在100万数据库记录里面查询，个人信息加密后精确查询比直接明文查询慢了22.36%。效率损失不大。损耗的效率可以通过提高硬件计算能力、优化数据库弥补。在一个约500万数据记录的

解密后显示的个人身份证号码代码：

```
//加密查询需要时间
startTime = System.currentTimeMillis();
String idnumberHash= Util.generateSM3HASH(idnumber);//SM3 杂凑计算
List<HashMap<String, Object>> select0 = sqlUtil.Select("select * from contractTable where
idnumberhash='"+idnumberHash+"'");//杂凑值数据库精确匹配查询
String contractHash=null;
String oneTimePassword=null;
String Key="11DDBAF3386AEA1F2974EEE984542152";//固定秘钥
String decidnumber=null;
for (int i = 0; i < select0.size(); i++)
  {
contractHash= Util.generateSM3HASH(select0.get(i).get("contract").toString());
oneTimePassword=Util.xorString(Key,contractHash);//生成“一次一密”秘钥
decidnumber=Util.SM4DecForCBC(oneTimePassword,select0.get(i).get("idnumberciphertext").toString());
//SM4（CBC 模式）解密
System.out.println(select0.get(i).get("id").toString()+"解密后身份证号："+decidnumber);//显示解密后身
份证号
}
endTime = System.currentTimeMillis();
elapsedTime = (endTime - startTime) ;
System.out.println("加密查询总共耗时：" + elapsedTime + "ms");
```

房屋交易信息系统的实际使用中，加密后的精确检索带来的效率损耗在可接受范围内，不影响业务的正常办理。

信息的查询效率比较如图6所示。

```
C:\Users\Administrator\.jdks\corretto-1.8.0_342\bin\java.exe ...
100050 明文查询的身份证号：212130196304197204
明文查询总共耗时：948ms
100050 解密后身份证号：212130196304197204
加密查询总共耗时：1160ms

Process finished with exit code 0
```

图6 信息的查询效率比较

4 结束语

数据安全是数据应用的基础，个人信息作为数据资源的重要组成部分，应该受到严格保护。特别是在《数据安全法》《个人信息保护法》和《密码法》等法律法规颁布实施后，对个人信息的保护和使用国密算法具有强制力。个人信息的安全隐患主要集中在信息的传输、存储和使用三个环节，核心是对信息数据的加密保护。结合数据安全治理和个人隐私保护要点和具体要求，健全数据治理体系，遵循《数据安全法》《个人信息保护法》等数据安全的有关法律法规和标准技术规范，建立数据安全保护体系，防止重要数据和个人信息被泄露、篡改和滥用。

针对数据安全治理和个人信息的加密保护，在国密算法的合规性要求下，提出了一种兼顾个人信息使用效率的保护方法。这种保护办法通过SM3密码杂凑算法、线性变换和异或处理生成“一次一密”密钥，利用生成的密钥和SM4分组密码算法对个人敏感信息进行加密保护。在使用个人信息时，通过个人信息的杂凑值进行高效精准查询，查询到信息后再利用密钥和SM4分组密码算法解密使用。基于国密的这种个人信息保护方法，在房屋交易信息系统中进行了实际应用，以应用带动了发展和技术创新，同时兼顾个人信息的利用，构建了新的数据信息保护方案，为数据全生命周期安全管理和防护提供了技术支撑。

参考文献：

[1] 金潇,陈兴,董胜亚.电信行业商用密码的个人信息保护实践[J].网络空间安全,2021,12(Z4):43-53.

[2] 陈伟,张平,戴华等.新型网络安全风险的管控技术与对策[J].南京邮电大学学报（社会科学版）,2021,23(04):1-10.

[3] 程子栋,王鹏彪,罗海宁.对数字政府安全技术合规分析的建议[J].中国信息安全,2022(08):35-38.

[4] 杨婕.解析我国规制个人信息泄露问题的法律路径[J].信息

（下转第66页）

基于灰狼优化算法的障碍物检测识别技术研究

孙佩茹，柳祖鹏，王子怡，田钧元
（武汉科技大学，湖北武汉430065）

摘要：

［目的/意义］针对当前的交通安全问题，无人驾驶中交通障碍物识别技术是保证交通安全的核心技术之一。

［方法/过程］传统的GS算法识别准确率低，深度学习技术虽然具有很强的表征能力，但是迭代过程久且精度不高，研究引入灰狼算法在卷积神经网络基础上解决这些问题。通过运用障碍物图像识别系统，在Matlab软件中创建卷积神经网络模型，对数据库中障碍物图片进行特征学习，然后研究进行仿真实验验证，使用灰狼算法优化后迭代10次后的验证成功率为96%。

［结果/结论］优化后的算法检测时间更短且精度略高，明显优于现有的两种模型。

关键词：障碍物识别；图像识别；深度学习；灰狼算法；卷积神经网络

中图分类号：TP391 **文献标识码：**A

Exploration of obstacle detection and recognition technology based on grey wolf optimization algorithm

Sun Peiru, Liu Zujpeng,Wang Ziyi , Tian Junyuan
(*Wuhan University of Science and Technology ,Hubei Wuhan 430065*)

Abstract:

[Purpose/Significance] In response to current traffic safety issues, the identification technology of traffic obstacles in unmanned driving is one of the core technologies to ensure traffic safety.

[Method/Process] The traditional GS algorithm has low recognition accuracy. Although deep learning technology has strong representation ability, the iterative process is long and the accuracy is not high. Therefore, the study introduces the Grey Wolf algorithm on the basis of convolutional neural networks to solve these problems. Firstly, establish an obstacle image recognition system and create a CNN model in MATLAB to learn the features of obstacle images in the database. Secondly, simulation experiments were conducted to verify the success rate of 96% after 10 iterations using the Grey Wolf algorithm optimization.

[Results/Conclusion] The results show that the optimized algorithm has a shorter detection time and slightly higher accuracy, significantly superior to the existing two models.

Keywords: obstacle recognition; image recognition; deep learning; grey wolf algorithm; convolutional neural network

0 引言

城市交通驾驶情况主要依靠驾驶员进行观察，由于主观因素的不稳定性，驾驶员对于前方障碍物容易存在误判。针对交通安全问题，各个国家根据自身情况建立了符合本国国情的障碍物检测识别系统，我国最早也是借鉴国外技术及经验[1]。目前，深度学习已经广泛应用于图像识别检测领域，在图像特征提取和智能化检测方面发挥出了巨大的应用优势[2]。随着深度学习的发展，卷积神经网络在图像识别也得到快速的发展[3]。丰晓霞[4]回顾了图像识别中的深度学习技术和表示方法，并比较了几种流行的基于卷积神经网络的深度模型。罗先圣[5]分析了典型深度网络的架构，例如深度信念网络（DBN）、卷积神经网络自编码器（AE）等。寇大磊[6]等回顾了的大量深度学习方法，提出了Fast R-CNN，并对目标检测方法的性能和优缺点进行了对比分析。郑远攀[7]等提供了基于新的、更全面和丰富的多层次分类的图像识别解决方案的调查。

本文介绍了传统图像识别模型和深度学习识别模型，在传统间隙统计聚类（GS）算法的基础上，引入灰狼优化算法，将灰狼优化算法与卷积神经网络相结合，并在自建障碍物数据库上进行试验，与原模型比较得到研究结论。

1 GS算法

基于间隙统计聚类算法，也称GS（Gap Statistic，GS）算法[8]被提出用于从两个已知的强度信息中恢复相位信息。GS算法通过输入、输出之间的FFT和输入、输出表面的约束条件，重复迭代，直到达到设计要求为止。在GS算法中，由于计算精度不随迭代数的增大而增大，故这种算法又被称作“错误降低”算法。但是，GS算法存在一个停顿的问题，仅通过最初几个迭代步骤，降低错误数值，在后面的迭代过程没有明显的减少，即GS算法仅能得到最优解。

2 障碍物识别系统设计

2.1 卷积神经网络理论

卷积神经网络（Convolutional Neural Networks，CNN）是一种前向神经网络，包括了卷积运算，并具有深度结构，是一种典型的深度学习算法[9]。最为传统的卷积神经网络由输入、卷积、池化、全连接和输出五层结构组成。卷积神经网络不仅适用范围广泛，而且能够自动提取图像特征然后进行深一步学习，现已被广泛应用于图像特征识别、图像分割、图像分类[10]。

2.2 灰狼算法

灰狼优化算法具有全局搜索能力强、简单易实现的特征。

灰狼优化算法具体数学建模过程：根据狼群中的等级分类，把最优解的搜索个体作为α，取得次优解和第三优解的搜索个体分别作为β、δ，其他搜索个体为ω。灰狼算法的优化过程可以类比为狼群的群体狩猎过程，首先追踪逼近猎物，然后追逐包围至猎物停止逃跑，最后攻击猎取猎物。

灰狼优化的实现过程如图所示。

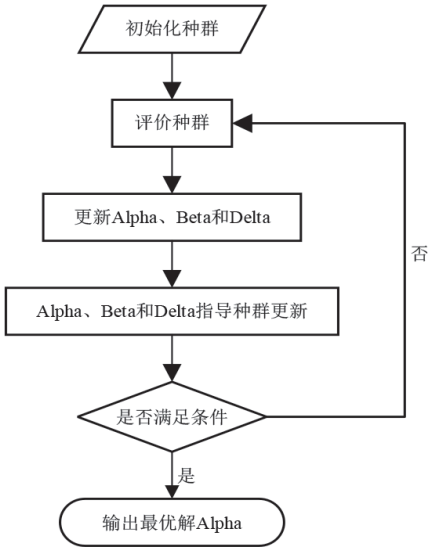

图 灰狼优化实现过程

2.3 障碍物识别模型

研究建立一个基于神经网络的障碍物识别模型，其中输入不同的数据库中的数据。首先定义了一个目标函数并使用梯度下降算法进行迭代，以针对所有权重最小化目标函数，并设计了网络结构利用卷积和密集层的数量和大小来获得梯度下降算法的最佳收敛性，从而在预定义的测试数据集上产生比联合得分更好的交集。

2.3.1 模型框架

根据上述研究算法，以卷积神经网络为依托，改进设计得到本文的灰狼算法卷积神经网络，目的是把多个时序数据转化成一个二维网路输出，即从一个完整的连接到一个卷积层的转变。

2.3.2 数学建模

完全连接的层尝试使用矩阵乘以未知权重来学习层的输入和其输出之间的所有连接，对Ntrain×Nfeatures输入大小特征（训练样本数乘以代表每个样本特征的数值数）的输入矩A和大小为Ntrain×Nfeatures个特征的未知矩阵W，层输出表示为：

$$\Phi(A)=W\cdot A+b^{T} \tag{1}$$

其中，b表示未知权重的偏置向量。

在训练过程中使用梯度下降算法，卷积层学习数据中的局部模式。它们由一组权重未知的图像数据组成。将层的输入与每个图像数据卷积产生层按公式（1）输出，然后在训练过程中使用梯度下降算法对图像数据权重进行近似。使用深度学习的池层来降低层输出的维度，每一层后面都有一个非线性激活——以适合数据的方式操纵输出。本文选用sigmoid激活函数：

$$(x\rightarrow \max(0,x)) \tag{2}$$

和

$$(x\rightarrow \frac{1}{1+e^{-x}}) \tag{3}$$

对于卷积神经网络，定义损失函数的梯度下降算法来确定所有权重以最小化函数，产生一个以高精度预测分割的输出。网络的输出是一个大小为M×M的概率矩阵，用B表示，B的每个坐标表示该坐标在图像Ω内的概率，即B是像素位于散射体内部的概率。转换B使用阈值转换成二值图像以获得B并检查准确性。将数据集分成两个子集——一个包含Ntrain个样本的训练集和包含Ntest个样本的测试集：

$$Ntrain+Ntest=Nsamples \tag{4}$$

在训练阶段中，建立一个可微的损失函数来比较样本的真实标签和预测标签以实现最小损失优化，该损失函数：

$$NLL=-\frac{1}{Ntrain\cdot M\cdot M}\sum_{q=1}^{Ntrain}\sum_{i=1}^{M}\sum_{j=1}^{M}(B'_q)_{i,j}\log(B_q)_{i,j} \tag{5}$$

式中，B'_q表示样本的真实标签，B_q表示样本的预测标签。

然后，训练网络以最小化这个目标函数。同时，建立一个近似IOU损失的替代损失函数soft-IOU损失函数，并使用联合近似交集：

$$\frac{1}{Ntrain}\sum_{q=1}^{Ntrain}\frac{<B'_q,B_q>}{|B'_q|+|B_q|-<B'_q,B_q>} \tag{6}$$

在第一次梯度下降迭代（Epoch）中使用NLL损失函数，当达到饱和后，即Epoch之间的NLL损失差异非常小，立即切换到在另外几个Epoch（~15）中使用Soft-IOU损失，同时仍然在这些时期计算NLL损失并观察到更小的NLL损失。

比较B_q和B'_q有几种测量误差的方法，其中1≤q≤Ntest：

1）均方误差：

$$\frac{1}{N^2\cdot Ntest}\sum_{q=1}^{Ntest}\|B'_q-B_q\|^2 \tag{7}$$

其中$\|B'_q-B_q\|=\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{M}|(B'_q)_{i,j}-(B_q)_{i,j}|^2}$

2）IOD：

$$\frac{1}{Ntest}\sum_{q=1}^{Ntest}\frac{|B'_q\cap B_q|}{|B'_q\cup B_q|} \tag{8}$$

其中，$|B'_q\cap B_q|$表示B'_q和B_q中值为1的像素数，$|B'_q\cup B_q|$表示B'_q或B_q中值为1的像素数。

3 实验验证

3.1 卷积神经网络模型搭建

使用Matlab代码搭建本项目所使用的卷积神经

网络模型，可以实现对给定的障碍物图像库进行特征学习后加以识别，并在Matlab软件中搭建运行的卷积神经网络模型。

3.2 灰狼优化算法搭建

利用Matlab构建所使用的灰狼优化算法，构建好的灰狼优化算法进行迭代训练，优化图像寻找最优参数。

3.3 障碍物数据集建立

实现障碍物识别关键需要满足待检测和验证的输入。因此，必须设置图像传感器或典型的相机记录或捕捉图像。在研究中共获取障碍物图像100张，包括减速带图像、路障栏杆图像和路障柱图像等常见障碍物图像。

3.4 实验结果

对数据库测试集进行训练之前，将卷积神经网络加载到灰狼算法模型中，得到一个预训的网络模型，通过对网络模型测试CNN的图像识别成功率，以得到最优的模型，最后进行检测验证。从数据训练迭代结果可以看出，改进的模型在迭代速度更快，识别精度也略高与现有模型。从数据上看，使用灰狼算法改进的模型平均检测速度为3.84s，传统模型的平均检测速度为4.67s，改进的模型检测速度更快。观察迭代10次后改进模型的检测精度为95.7%，且逐渐趋于稳定。

4 结束语

研究并定义了损失函数NLL和近似IOU损失的替代损失函数Soft-IOU，分别计算样本实际值与预测值之间的损失并用联合近似交集表示，使用梯度下降算法进行迭代得到最佳收敛性。同时，利用卷积神经网络的密集性和前向性，加快灰狼算法迭代时的信息交互，提高了模型的检测速度。在障碍物数据集上进行的实验结果表明，基于灰狼算法的改进模型明显优于现有的传统模型，且在检测速度和识别精度上均有优势。

基金项目：

受武汉科技大学大学生创新创业训练计划项目资助（项目编号：23Z096）。

参考文献：

[1] 超木日力格.机车司机视野扩展系统及路轨障碍物检测的研究[D].北京:北京交通大学,2012.

[2] 李先锋,徐森,花义明.深度学习在舰船前方障碍物图像识别中的应用[J].舰船科学技术,2022,44(6):157-160.

[3] 张文乐.基于深度学习的交通路标图像识别研究[D].西安:西安石油大学,2020.

[4] 丰晓霞.基于深度学习的图像识别算法研究[D].太原:太原理工大学,2015.

[5] 罗先圣. 基于深度学习的图像目标识别技术研究[D].北京:中国地质大学（北京）,2021.

[6] 寇大磊,权冀川,张仲伟.基于深度学习的目标检测框架进展研究[J].计算机工程与应用,2019,55(11):25-34.

[7] 郑远攀,李广阳,李晔.深度学习在图像识别中的应用研究综述[J].计算机工程与应用,2019,55(12):20-36.

[8] Robert Tibshirani,Guenther Walther,Trevor Hastie. Estimating the Number of Clusters in a Data Set via the Gap Statistic[J]. Journal of the Royal Statistical Society. Series B (Statistical Methodology),2001,63(2).

[9] 邓虚睿,贾蒙磊.基于深度学习与双目立体视觉的物体管理应用[J].网络空间安全,2019,10(04):89-95.

[10] 陈振昂,黄星期,秦中元.基于图像处理和卷积神经网络的文本验证码识别方案[J].网络空间安全,2020,11(08):75-80.

作者简介：

孙佩茹（2003-），女，汉族，湖北武汉人，武汉科技大学汽车与交通工程学院，本科；主要研究方向和关注领域：交通运输和图像识别。

柳祖鹏（1979-），男，汉族，浙江兰溪人，同济大学，博士；武汉科技大学汽车与交通工程学院，副教授；主要研究方向和关注领域：交通管理与控制、微观交通仿真。

王子怡（2001-）女，汉族，湖北荆门人，武汉科技大学智能汽车工程研究院，本科；主要研究方向和关注领域：交通运输和图像识别。

田钧元（2002-），女，汉族，甘肃天水人，武汉科技大学智能汽车工程研究院，本科；主要研究方向和关注领域：交通运输和图像识别。

基于目标分布的模型提取攻击方法研究

罗基，刘洋
〔哈尔滨工业大学（深圳），广东深圳518055〕

摘要：

［目的/意义］ 在模型提取攻击中，攻击者使用的数据极大地影响了攻击的有效性。在实践中，攻击者往往很难获取到精确的目标数据。相比之下，目标模型所用数据的分布可能更容易获得。基于目标分布进行模型提取攻击的方法，为攻击提供了新的思路和方法，同时也提醒拥有有价值模型的云平台和个人，需要采取措施防止攻击者获取目标分布。

［方法/过程］ 使用一些生成对抗网络来学习目标分布并生成数据，并使用此数据执行模型提取攻击。研究了提取部分类攻击方法，并提供了两种提取部分类的方法，丰富了模型提取攻击的攻击手段。

［结果/结论］ 实验结果表明，基于目标分布进行模型提取是可行的，得到的替换模型甚至在某些类别上超过了目标模型的性能，同时攻击效果随着使用的分布接近目标分布而增强。

关键词： 模型提取攻击；生成模型；目标分布；云平台；模型安全

中图分类号： TP309 **文献标识码：** A

Research on model extraction attack method based on target distribution

Luo Ji, Liu Yang
〔*Harbin Institute of Technology (Shenzhen), Guangdong Shenzhen 518055*〕

Abstract:

[Purpose/Significance] In model extraction attacks, the data used by the attacker greatly affects the effectiveness of the attack. In practice, it is often difficult for an attacker to obtain the exact target data. In contrast, the distribution of the data used in the target model may be more readily available. This paper investigates a method for model extraction attacks based on target distributions. This provides new ideas and methods for attacks and also reminds cloud platforms and individuals with valuable models of the need to take steps to prevent attackers from obtaining target distributions.

[Method/Process] This paper uses several generative adversarial networks to learn the target distribution and generate data and uses this data to perform model extraction attacks. This paper also investigates the method of extracting partial class attacks and provides two methods for extracting partial classes. This enriches the attack tools for model extraction attacks.

[Results/Conclusion] The experimental results show that model extraction based on the target distribution is feasible, and the resulting replacement model even outperforms the target model in some categories. Moreover, the effectiveness of the attack is enhanced as the distribution used approaches the target distribution.

Keywords: model extraction attack; generative model; target distribution; cloud platform; model security

0 引言

深度学习技术能够构建复杂的模型，以解决多样化的问题，实现效率提升和价值创造，因此在智能化世界的发展中得到广泛应用。然而，深度学习模型也面临多种攻击形式，例如中毒攻击[1-2]污染被攻击模型的训练数据，导致性能下降；在逃逸攻击[3]中，攻击者小心地扰动恶意的样本，试图逃避模型的检测；模型提取攻击[5]尽力获取被攻击模型提供服务的能力，威胁模型的知识产权。这些攻击可能影响模型的训练和部署，并最终影响其可用性[4]。

就模型提取攻击而言，其中被攻击的模型称为目标模型，通常是为特定任务而精心训练的。模型提取攻击是一种旨在通过交互目标模型并获取其输出来构建一个等价的模型的攻击。攻击者可以使用这种攻击来窃取目标模型的知识产权，并在不经过授权的情况下使用知识产权。此类攻击可能会给模型拥有者带来极大的恶性影响。例如，攻击者可能会利用被窃取的知识产权来制造竞争对手或者从事其他商业活动，从而削弱目标模型的市场价值。

模型提取攻击特别威胁一些云平台提供的模型和服务，例如AWS、Azure和Google Cloud等。用户可以通过这些平台快速地利用机器学习模型优化业务，而平台也能从中获得收入。然而，一旦平台上的模型被盗用，则平台和用户为训练模型所付出的成本就会白费。因此，平台应审慎评估并避免这种攻击的影响。

为了更好地理解模型提取攻击并为进一步提出此类攻击的防御手段做准备，本文在图像分类任务上对模型提取攻击进行了研究，希望利用目标模型的输出建立一个等价的分类模型。

针对模型提取攻击的研究通常会对攻击者的能力做出设定。例如，对攻击者能否获取目标模型所用的训练数据的信息做出了不同的假设。更宽松的假设的攻击，可以获取目标模型的部分训练数据集或测试数据集；更严格的假设的攻击则不可以获取这些数据，攻击者需要自行搜集数据查询目标模型，或者使用生成模型生成合成数据进行攻击；更强的攻击者往往能够进行更成功的攻击。

做出一项新的假设，即攻击者知道目标模型训练数据的分布，也就是目标分布。这是一种介于宽松假设和严格假设之间的一种假设，旨在研究攻击者是否可以基于这些信息成功地进行模型提取攻击。实验结果表明，向攻击者揭示目标分布是危险的，因为攻击者仍然能够进行相对成功的模型提取攻击。

实验使用了一些由生成对抗网络学习到的数据分布。然而，这些网络无法为所有类别生成高质量的图像，导致攻击只能在部分类上获得成功，进而对是否可能仅在部分类上进行提取攻击进行了研究。对于只提取一个类和提取两个或更多类的情况，分别提出了相应的攻击方法。

（1）提出了基于目标分布的攻击方法，并通过实验证明了该方法可以实现较为成功的攻击。

（2）提出了提取一个类和提取两个及以上类的两种提取部分类的攻击方法，丰富了模型提取攻击的攻击手段。

在介绍了所作研究相关的工作之后，介绍了面向的威胁模型，包含了攻击的一系列设定，实现的攻击是在设定下进行，然后提出了的攻击方法，同时进行了相关实验验证并对实验结果进行了分析给出结论。

1 相关工作

模型提取攻击被应用于提取多种类型的神经网络中。Takenura等[6]在分类问题和回归问题上，阐明了模型提取攻击对循环神经网络的威胁。Hu等[7]系统地研究了针对生成式对抗网络的模型提取攻击的可行性。Chen等[8]提出了第一个针对深度强化学习的模型提取攻击，使外部对手能够仅从其与环境的互动中精确恢复黑盒深度强化学习模型。Wu等[9]首次全面研究并开发了针对图神经网络模型的模型提取攻击。文献[10]进行了提取目标检测器的研究，文献[11]对顺序推荐器进行了模型提取。

关注面向图像分类任务的模型提取攻击。这些攻击使用不同的假设，例如攻击者对用于目标模型的训练数据了解多少。文献[12]假设可以获取目标模型测试数据集的部分数据，并基于此进行了提取攻击。文献[5]假设攻击者使用的数据集

可以是一个包含几个较小数据集的大数据集。文献[13]在代理数据集（不同于用于训练目标模型的数据）上生成图像，作为后续攻击的基础。文献[14]在了解目标模型任务的基础上，用搜索引擎搜索任务相关的数据。攻击者使用这些数据进行攻击。文献[15]是一种使用零阶梯度估计的无数据模型窃取攻击，只使用生成模型创建的合成数据来执行模型提取。与上述工作不同，假设攻击者能够获取目标模型训练数据的分布，进而生成该分布的数据，使用这些数据进行攻击。

文献[16]提出了特殊用途的模型提取攻击。做法是将目标模型的一些类别汇总到替代模型的一个类别中，得到一个类别少于目标模型类别的替代模型。但是，本文没有通过聚合目标模型的类别来减少类别，而是通过丢弃不想要提取的类别的数据减少类别，也就是说仅针对部分类进行提取攻击。

2 威胁模型

从目标模型、攻击者的动机与能力、替代模型、攻击步骤等角度，分别对面向威胁模型进行介绍。

2.1 目标模型

模型提取攻击的目标是针对特定任务的预训练模型，这些模型在执行任务时表现良好并具有价值。在实践中，这些目标模型可能是由云平台和用户共同训练的，平台提供基础设施、资源和设计精良的模型，用户提供数据。一旦模型训练完成，用户可以自行使用或分享给其他人，而平台则通过对用户使用的资源和对用户通过应用程序编程接口（Application Programming Interface，API）使用模型的查询行为进行收费而获得收益。在研究中，将一些在本地训练的特定任务上表现良好的目标模型作为攻击目标，并将这些模型视为类似于平台提供的预训练模型的黑盒。

2.2 攻击者的动机

攻击者在进行模型提取攻击时的动机在于，目标模型是具有实用价值的，攻击者需要付费才能使用这些模型。然而，如果攻击者可以在本地构建替代模型，就可以规避掉这些费用。更进一步地，攻击者甚至能够将提取过来的模型提供给其他人，从而获得经济上的收益。这些因素均构成了攻击者进行模型提取攻击的动机。

2.3 攻击者的能力

攻击者在进行模型提取攻击时，可以利用对目标模型面向任务的了解，通过合适的数据查询目标模型，并获得目标模型的输出。除此之外，攻击者需要具备机器学习、计算机视觉、自然语言处理等方面的知识，并能够编写流畅的代码和使用深度学习框架等技能，以便在攻击中使用。攻击者拥有更多资源和能力，可以实现更成功的攻击。然而，攻击者无法总是获得有助于攻击的信息，例如目标模型的架构、超参数、训练方法和具体数据等。在本文中，假设攻击者能够获取接近目标分布的分布，并基于这些分布进行模型提取攻击。

2.4 替代模型

在进行模型提取攻击时，攻击者需要设计一个替代模型的架构，使其能够适应目标模型所面向的任务。在图像分类任务中使用了预训练模型作为替代模型的架构，预训练模型已经被广泛应用，表现良好且容易获得，因此被作为一种合适的替代模型架构。

2.5 攻击步骤

目标模型使用私有目标数据进行了很好的训练，具有一定的价值。为了替代目标模型，攻击者使用一个数据集查询目标模型，获得目标模型返回的输出。攻击者基于这些输出与原始的数据构建完整的数据集，使用该数据集在本地训练替代模型。在这个过程中，攻击者往往会仔细选择使用的数据集。为了能有更好的攻击效果，攻击者也会精心设计与目标模型的交互方式，以及尽力从目标模型的输出中挖掘出有帮助的信息。

攻击步骤如图1所示。

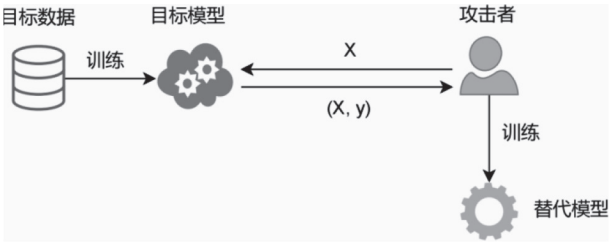

图1 攻击步骤图

3 方法

3.1 基于目标分布的攻击方法

基于目标分布的模型提取攻击方法，假设攻击者可以获得目标分布。攻击者从分布中采样获得数据，基于这些数据进行提取攻击。具体来说，使用生成模型学习目标模型数据的分布，然后从中采样得到一些数据。这些数据被目标模型所标注，得到带有标签的数据。然而，不会使用所有的数据训练替代模型，而是使用文献[14]中的方法找到确定性的数据，并用这些目标模型确定的数据训练替代模型。

攻击方法如图2所示。

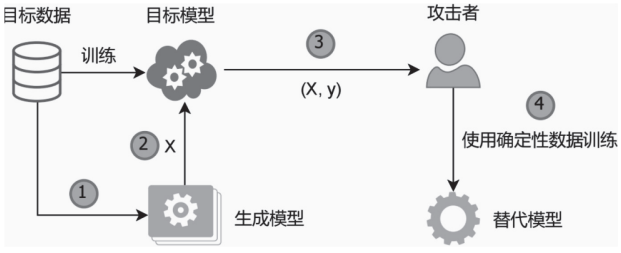

图2 攻击方法示意图

第一步，使用生成模型学习目标模型数据的分布；第二步，使用生成模型生成的图像查询目标模型；第三步，攻击者获得目标模型返回的输出，得到带有标签的数据集；第四步，使用该数据集的确定性数据训练替代模型。

使用深度生成模型学习目标分布。深度生成模型是一类训练深度神经网络来模拟训练样本分布的技术[17]。深度生成模型的目标是从少量的独立和相同分布的样本中学习一个未知的或难以解决的概率分布。在训练成功后，可以用深度生成模型来估计给定样本的可能性，并创建与未知分布的样本相似的新样本[18]。深度生成模型包括基于能量的模型、变异自动编码器、生成式对抗网络、自回归模型、归一化流，此外还有许多混合方法。本文的方法并不限制所使用的生成模型的类型，只要生成模型足够强大，能有效地学习数据集的分布并生成数据就可以。

根据文献[14]，使用目标模型更加确定的数据训练替代模型，会显著提升模型的性能。生成模型生成的数据并非都是可靠的，生成模型可能会输出一些令人感到奇怪的数据，所以并没有使用所有生成的数据及目标模型给的标签，而是仅使用目标模型确定的数据。度量模型对数据是否确定的公式：

$$P(\boldsymbol{y}_{t,k_1}|x_t) \geq \tau \tag{1}$$

$$P(\boldsymbol{y}_{t,k_1}|x_t) - P(\boldsymbol{y}_{t,k_2}|x_t) \geq \tau \tag{2}$$

$$\sum_{i=1}^{n} P(\boldsymbol{y}_{t,k_i}|x_t) \log P(\boldsymbol{y}_{t,k_i}|x_t) \geq \tau \tag{3}$$

其中，P为对模型的输出做Softmax运算后得到的值，k_i是第i个最自信的类，τ为确定程度的阈值。公式的值大于阈值的话，则认为模型对该数据的分类结果更加确定，否则认为模型对该数据的分类结果不确定。公式（3）受到了熵的概念的启发，熵是不确定性的度量。可以看出，公式（3）的值越大，确定性越大，因此可以作为度量模型确定程度的指标。在实际使用时，可以根据具体任务和数据特点，从这三个指标里选择合适的指标应用于攻击中。

3.2 提取部分类的攻击方法

即使仅使用确定性数据，实验结果表明，针对某些类别的攻击仍然不是很成功。这引起了进一步探索的兴趣，即仅提取部分类的攻击。

在提取部分类的攻击中，目标模型为多分类模型，能够很好地将多个类别的数据区分开来。攻击者不需要替代模型区分所有原始类别，而是希望替代模型只区分部分类的数据，即只攻击目标模型的部分类。这可能因为目标模型的类别太多，而攻击者只对其中少数的类别感兴趣。或者攻击者不能对所有类别进行成功的攻击，便可以仅关注少数表现良好的类别。所以，在提取部分类的攻击中，替代模型分类的类别少于目标模型分类的类别。如果替代模型能够很好地将这些类别的数据区分开来，则攻击是成功的。

本文将提取部分类的攻击分为两种情况，即

仅提取一个类的攻击和提取两个及以上类的攻击。在这两种攻击中，也仅使用目标模型确定的数据。如无特殊情况，这点将不再赘述。

对于仅提取一个类，方法是先查询所有的基于分布生成的无标签的合成数据，获得目标模型给的标签。但是，只保留所要攻击的这个类的标签及其数据，将其他类的数据的标签都统一设为另一个标签，所以替代模型的训练数据集如公式（4）所示：

$$D = \{D_0, D_1\},\ |D_0| = |D_1| \tag{4}$$

D为替代模型训练数据集，D由D0和D1组成。D0为所要攻击的类的数据及标签，标签为0；D1为其他类的数据及其标签，这些数据的标签都设置为1。|D0|和|D1|为这两个类的数据的规模。在训练时，保持这两部分数据的数量大致相当。

使用上面的数据集D训练二分类的替代模型。如果模型能够很好地将这个类的数据与其他类的数据区分开来，则认为仅提取这个类的攻击是成功的。

对于提取两个及以上类的攻击，方法是先查询所有的基于分布生成的无标签的合成数据，获得目标模型给的标签。但是，只保留这些被攻击的类的标签及其数据，简单地扔掉其他类的数据。所以替代模型的训练数据集如公式（5）所示：

$$D = \{D_0, D_1, ..., D_t\},\ |D_0| = |D_1| = ... = |D_t| \tag{5}$$

D为替代模型训练数据集，D由D0, D1, ..., Dt组成。D0, D1, ..., Dt为所要攻击的类的数据及标签，标签为0, 1, ..., t；。|D0|, |D1|, ..., |Dt|为这些类的数据的规模。在训练时，保持这些数据的数量大致相当。

使用上面的数据集D训练多分类的替代模型。如果模型能够将这些类的数据区分开来，则认为仅提取这些类的攻击是成功的。

4 评估

4.1 实验设置

本文在CIFAR-10数据集上进行了实验。CIFAR-10数据集由60 000张32×32的彩色图像组成，分为10类，每类有6 000张图像。有50 000张训练图像和10 000张测试图像，并有多种类别：“飞机”“汽车”“鸟”“猫”“鹿”“狗”“青蛙”“马”“船”“卡车”。CIFAR-10被广泛用作计算机视觉研究的基准。

4.1.1 目标模型

目标模型基于VGG19，可以使用CIFAR-10训练。目标模型的测试准确率为93.18%，将这个训练好的模型作为攻击的目标。攻击者对这个模型的了解是有限的，不知道模型的架构、参数、训练方法等信息，只知道模型面向的任务，并使用合适的数据查询模型并获得输出。

4.1.2 替代模型

替代模型基于Squeezenet[19]，是一个卷积神经网络，有18层深度，在ImageNet数据库的100多万张图片上训练过。SqueezeNet在ImageNet上达到了AlexNet级别的准确性，而参数却减少了50倍。

为了得到训练替代模型的数据，用一些生成模型学习CIFAR-10的数据分布，并从中分别采样100 000张图像。用这些图像查询目标模型，得到目标模型给的概率向量。接着用文献[14]中的方法，挑出某一概率分量大于0.995的数据，将这些数据视为目标模型的确定性数据。每种生成模型的信息及其生成的100 000张图像的确定性数据的数量如表1所例。使用这些确定性数据训练替代模型，替代模型被训练100-200轮，批量大小为128，优化器为Adam，学习率在0.001-0.00001之间。

生成模型及其生成数据信息如表1所例。

表1 生成模型及其生成的数据的信息

生成模型	FID	KID	确定性数据	总数据
SNGAN	16.79	0.0124	54 350	100 000
SSGAN	14.63	0.0101	57 544	100 000
InfoMax-GAN	15.07	0.0111	54 194	100 000

4.1.3 评价指标

使用CIFAR-10的测试数据集测试训练好的替代模型。由于更关注提取过来模型的可用性，即更关注替代模型在测试数据集上的表现，所以使用替代程度（Substitution）指标，如公式（6）

所示。其中，S为替代程度，f'为替代模型，f是目标模型，用两者的测试准确率之比表示替代模型替代目标模型的程度。

$$S = \text{Accuracy}(f') \ / \ \text{Accuracy}(f) \quad (6)$$

在实验中，发现基于目标分布进行模型提取攻击并不能在所有类别上都获得成功，所以引起了探索只提取部分类的攻击。对于这些攻击，评价指标并不能用公式（6）所述的总的替代程度。因为并不存在仅在部分类上训练的目标模型，所以不能计算总的替代程度。在这种情况下，计算每个类的替代程度，计算方法如公式（7）所示。其中，S_i表示模型在第i个类上的替代程度。$\text{Accuracy}(f'_i)$为替代模型将测试数据集中第i类的数据正确分类为第i类的比例，$\text{Accuracy}(f'_i)$为目标模型的。

$$S_i = \text{Accuracy}(f'_i) \ / \ \text{Accuracy}(f_i) \quad (7)$$

4.2 实验结果及分析

4.2.1 基于目标分布的攻击实验结果

分别使用实验设置部分所提到的SNGAN，SSGAN和InfoMax-GAN生成的确定性数据训练替代模型。得到的三个替代模型在每个类上的准确率和替代程度以及总的准确率和替代程度如表2所例。替代模型在一些类上的表现甚至超过了目标模型在该类上的表现，倒如基于SSGAN，替代模型对Ship类的替代程度达到了100.6%。为了更清楚地分析表中的数据，绘制了目标模型和三个替代模型准确率的折线图。

替代模型的准确率和替代程度如表2所例。

替代模型及目标模型在各类上的准确率及总准确率如图3所示。

从图3可以看出，基于SSGAN生成的数据进行

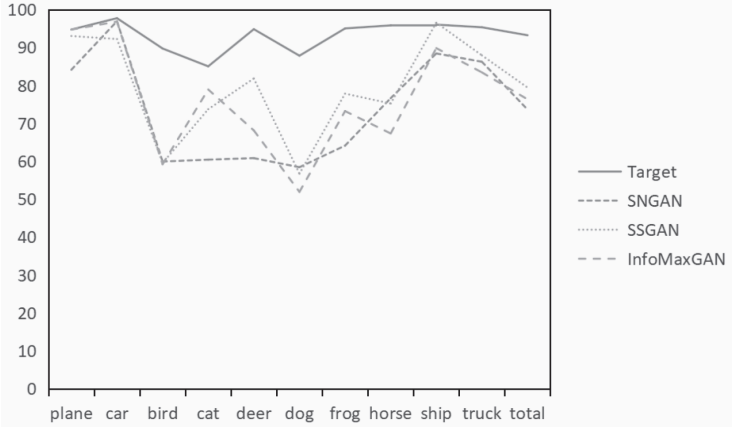

图3 替代模型及目标模型在各类上的准确率及总准确率

表2 替代模型的准确率和替代程度

	Target model	SNGAN		SSGAN		InfoMax-GAN	
	Accuracy(%)	Accuracy(%)	Substitution(%)	Accuracy(%)	Substitution(%)	Accuracy(%)	Substitution(%)
plane	94.7	84.1	88.8	93.0	98.2	94.7	100.0
car	97.7	96.9	99.2	92.2	94.4	96.8	99.1
bird	89.7	59.9	66.8	59.5	66.3	59.2	66.0
cat	85.0	60.4	71.0	73.7	86.7	78.9	92.8
deer	94.8	60.8	64.1	81.8	86.3	68.1	71.9
dog	87.8	58.4	66.5	56.7	64.6	51.9	59.1
frog	95.0	64.1	67.5	77.8	81.9	73.2	77.1
horse	95.8	76.6	79.9	75.2	78.5	67.3	70.3
ship	96.0	88.4	92.1	96.5	100.6	89.8	93.5
truck	95.3	86.2	90.4	87.9	92.3	83.4	87.5
total	93.2	73.6	79.0	79.4	85.2	76.3	81.9

攻击得到的替代模型的测试准确率总体上优于基于其他两个生成模型的。基于SNGAN的替代模型和基于InfoMax-GAN的替代模型的准确率则差不多。这可以由三个生成模型的FID值和KID值来解释。SSGAN的FID值和KID值为14.63和0.0101，优于SNGAN和InfoMax-GAN的FID值和KID值。SNGAN的FID值和KID值为16.79和0.0124，InfoMax-GAN的FID值和KID值为15.07和0.0111。同时，从表1可以看出，SSGAN生成了更多确定性数据。此处可以得到结论：学习目标分布的生成模型生成的数据越接近目标数据，越有可能被目标模型认为是确定性数据，也越有可能得到更好的攻击效果。

从图3所示中可以看出，三个替代模型的总测试准确率并没有太突出。这是由于替代模型在一些类别上的表现不够好，拖累了总测试准确率。例如，在狗这个类别上，三个替代模型都表现不够好，准确率没有超过60%。这可能是因为生成模型没有有效学习到一些类别的数据分布，导致生成的图像质量不高，影响了攻击效果。这也与观察到的一致，生成模型鲜有生成高质量的狗的图像。令人欣慰的是，替代模型在另一些类别上的表现足够好。例如，基于SSGAN的替代模型在Ship类上的准确率达到了96.5%，甚至超过了目标模型在该类上的准确率，为96.0%；基于InfoMax-GAN的替代模型在Plane类上的准确率达到了94.7%，这与目标模型的一样。这引发了探索只提取表现好的类别的兴趣。

4.2.2 提取部分类的攻击实验结果

（1）提取一个类的实验结果

替代模型分别基于SNGAN、SSGAN和InfoMax-GAN生成的数据提取一个类。例如，用基于SNGAN生成的数据提取Car类。SNGAN生成的数据查询目标模型，获得标签。目标模型所给标签为Car的数据归为一类，其他所有标签的数据归为一类，使这两类数据的规模大致相当，然后用这两个类的数据训练一个二分类替代模型。如果替代模型能够很好地将这两类数据区分开来，则认为提取单个类的攻击是成功的，总共进行了提取6个类的实验，每个攻击仅提取一个类。具体来说，基于SNGAN生成的数据提取Car类和Ship类，基于SSGAN生成的数据提取Plane类和Ship类，基于InfoMax-GAN生成的数据提取Plane类和Car类。得到的6个二分类替代模型在测试数据集上的测试准确率和替代程度如表3所示。

表3 提取一个类的替代模型的准确率和替代程度

	Class	Total Accuracy(%)	Other Classes(%)	Attacked Class(%)	Target Model(%)	Substitution(%)
SNGAN	car	87.3	80.3	94.4	97.7	96.6
SNGAN	ship	90.5	88.7	92.3	96.0	96.1
SSGAN	plane	85.7	82.4	89.1	94.7	94.1
SSGAN	ship	91.1	90.3	92.0	96.0	95.8
InfoMax-GAN	plane	86.1	84.6	87.5	94.7	92.4
InfoMax-GAN	car	86.9	87.4	86.3	97.7	88.3

表3中最后一列的数据为替代程度，其他列的数据为准确率。Class列为要提取的类，Total Accuracy列为替代模型的总准确率，Other Classes列为替代模型在其他类上的准确率，Attacked Class为替代模型在被攻击的类上的准确率，Target Model列为目标模型在被攻击的类上的测试准确率，Substitution列为替代模型在被攻击类上的替代程度，为Attacked Class列的数据除以Target Model列的数据所得到的值。

从表3可以看出，训练的6个二分类模型能够很好地在测试数据集上将被攻击类的数据和其他类的数据区分开来，替代程度也在88.3%-96.6%之间。本文的方法可以应用于更多的提取一个类的任务中去。

（2）提取两个及以上类的实验结果

替代模型分别基于SNGAN、SSGAN和InfoMax-GAN生成的数据提取若干个类。例如，用基于SNGAN生成的数据提取Car类，Ship类和Trunk类。SNGAN生成的数据查询目标模型，获得标签。目标模型所给标签为Car的数据归为一类，所给标签为Ship的数据归为一类，所给标签为Trunk的数据归为一类，扔掉其他类的数据。保证这三类数据的规模大致相当，然后用这三个类的数

据训练一个三分类替代模型。如果替代模型能够很好地将这三类数据区分开来，则认为提取这三个类的攻击是成功的。总共进行了三个提取部分类的攻击实验，每次攻击提取若干个类。具体来说，基于SNGAN的数据提取Car类，Ship类和Trunk类，基于SSGAN的数据提取Plane类，Car类和Ship类，基于InfoMax-GAN的数据提取Plane类和Car类和Ship类。得到的三个多分类替代模型在测试数据集上的测试准确率和替代程度如表4、表5和表6所例。

表4 提取若干个类的替代模型的准确率和替代程度（1）

	car(%)	ship(%)	trunk(%)	total(%)
SNGAN	75.6	92.1	80.8	82.8
Target model	97.7	96.0	95.3	-
Substitution	77.4	95.9	84.8	-

表5 提取若干个类的替代模型的准确率和替代程度（2）

	plane(%)	car(%)	ship(%)	total(%)
SNGAN	87.3	88.0	77.7	84.3
Target model	94.7	97.7	96.0	-
Substitution	92.2	90.1	80.9	-

表6 提取若干个类的替代模型的准确率和替代程度（3）

	plane(%)	car(%)	ship(%)	total(%)
InfoMax-GAN	85.2	85.6	86.3	85.7
Target model	94.7	97.7	96.0	-
Substitution	90.0	87.6	89.9	-

表4、表5和表6为基于不同的生成模型生成的数据的替代模型的测试准确率和替代程度。替代模型分别只提取了三个类。表中第一行数据为替代模型在三个类上的准确率。第二行数据为目标模型在各个类上的准确率。由于不存在仅在三个类上训练的目标模型，所以这一行的总准确率不存在，替代模型在三个类上的总替代程度也不存在。第三行为替代模型在三个类上的替代程度，为第一行数据除以第二行数据得到的值。

从表4、表5和表6可以看出，训练的三个多分类模型能够较好地在测试数据集上将被攻击的若干类的数据区分开来，替代程度也在77.4%-95.9%之间。本文的方法可以应用于更多的提取若干个类的任务中去。

5 结束语

研究主要集中在探索基于目标分布进行模型提取攻击的可行性问题。具体而言，使用生成对抗网络学习目标分布并从中采样数据进行攻击。实验表明，这种方法可以进行较为成功的模型提取攻击，并且攻击效果与使用的分布和目标分布的接近程度有关。除此之外，还探索了提取部分类的方法，并提供了两种方法，进一步丰富了模型提取攻击的方法库。在目标分布中，采样的数据被认为是非常适合进行模型提取攻击的数据，因为它们接近目标数据。希望引起对基于目标分布的模型提取攻击的进一步研究，例如通过结合其他攻击，把进行模型反转攻击，以黑盒的方式探索并接近目标分布。同时，拥有有价值模型的云平台和个人需要采取措施，防止攻击者通过其他攻击方式获取目标分布，以保护隐私和安全。

基金项目：

1.深圳市基础研究项目（项目编号：JCYJ20190806142601687）；

2.深圳市高等院校稳定支持计划（项目编号：GXWD20201230155427003-20200821160539001）；

3.深圳市基础研究项目（项目编号：JCYJ20200109113405927）；

4.广东省安全智能新技术重点实验室（项目编号：2022B1212010005）；

5.鹏城实验室新型网络基础设施体系架构与关键技术研究（项目编号：PCL2021A02）。

参考文献：

[1] Ahmed Im,Kashmoola My. Threats on machine learning technique by data poisoning attack: A survey[C]// Proceedings of the Third International Conference on Advances in Cyber Security, 2021: 586-600.

[2] 田继伟,王布宏,李腾耀,等.智能电网虚假数据注入攻击研究进展与展望[J].网络空间安全,2019,10(09):73-84.

[3] Biggio B,Corona I,Maiorca D,et al. Evasion attacks against machine learning at test time[C]// Proceedings of European Conference on Machine Learning and

Principles and Practice of Knowledge Discovery in Databases, 2013, 3: 387-402.

[4] 张嘉楠,王逸翔,刘博等.深度学习的对抗攻击方法综述[J]. 网络空间安全,2019,10(07):87-96.

[5] Orekondy T,Schiele B,Fritz M.Knockoff nets: Stealing functionality of black-box models[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019.

[6] Takemura T,Yanai N,Fujiwara T. Model extraction attacks on recurrent neural networks[J]. Journal of Information Processing, 2020, 28: 1010-1024.

[7] Hu H, Pang J.Stealing machine learning models: Attacks and countermeasures for generative adversarial networks[C]// Proceedings of the Annual Computer Security Applications Conference, 2021: 1-16.

[8] Chen K, Guo S,Zhang T, et al. Stealing deep reinforcement learning models for fun and profit[C]// Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, 2021: 307-319.

[9] Wu B, Yang X,Pan S,et al. Model Extraction Attacks on Graph Neural Networks: Taxonomy and Realisation[C]// Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022: 337-350.

[10] Liang S, Liu A,Liang J,et al. Imitated Detectors: Stealing Knowledge of Black-box Object Detectors[C]// Proceedings of the 30th ACM International Conference on Multimedia, 2022: 4839-4847.

[11] Yue Z,He Z,Zeng H,et al. Black-box attacks on sequential recommenders via data-free model extraction[C]// Proceedings of the 15th ACM Conference on Recommender Systems, 2021: 44-54.

[12] Papernot N,Mcdaniel P,Goodfellow I,et al. Practical black-box attacks against machine learning[C]// Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017: 506-519.

[13] Barbalau a, Cosma a, Ionescu Rt,et al. Black-Box Ripper: Copying black-box models using generative evolutionary algorithms[C]// Proceedings of the Neural Information Processing Systems conferences, 2020, 33: 20120-20129.

[14] Liu Y, Luo J, Yang Y, et al. ShrewdAttack: Low Cost High Accuracy Model Extraction[J]. Entropy, 2023, 2: 282.

[15] Kariyappa S,Prakash A,Qureshi Mk,et al. Maze: Data-free model stealing attack using zeroth-order gradient estimation[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2021: 13814-13823.

[16] Okada R,Ishikura Z,Shibahara T,et al. Special-Purpose Model Extraction Attacks: Stealing Coarse Model with Fewer Queries[C]// Proceedings of the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2020: 1995-2000.

[17] Bond-Taylor S, Leach A, Long Y, et al. Deep generative modelling: A comparative review of vaes, gans, normalizing flows, energy-based and autoregressive models[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021.

[18] Ruthotto L,Haber E. An introduction to deep generative modeling[J]. GAMM Mitteilungen, 2021. 2(44): 8.

[19] Iandola Fn,Han S,Moskewicz Mw,et al. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and < 0.5 MB model size[EB/OL]. arXiv preprint arXiv:1602.07360, 2016.

作者简介：

罗基（1996-），男，汉族，陕西商洛人，哈尔滨工业大学（深圳），在读硕士；主要研究方向和关注领域：深度学习模型及安全、强化学习和多模态大模型。

刘洋（1988-），男，汉族，山东日照人，牛津大学，博士；哈尔滨工业大学（深圳），助理教授；主要研究方向和关注领域：数据安全和隐私计算。

商用密码在机场旅客个人信息保护中的实践

杨琪[1]，朱明娟[2]，王勇[2]
（1.北京首都机场餐饮发展有限公司，北京100621；2.北京首都国际机场股份有限公司，北京100621）

摘要：

［目的/意义］ 民航机场为了向旅客提供便捷服务，采集、存储、使用了大量旅客个人信息，一旦发生泄露、被盗用或滥用事件，后果严重。随着我国《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》的颁行，民航机场的个人信息保护在实战和合规双轮驱动下，已由“或有”变为“刚需”。商用密码是数据安全防护的核心手段，通过商用密码技术保障民航机场个人信息安全成为数字时代的必然要求。

［方法/过程］ 通过分析民航机场在旅客个人信息保护工作中面临的安全挑战，结合当下安全防护的实战与合规需求，提出基于免改造安全技术和高性能商用密码技术，在不需要对民航机场业务系统升级改造、不影响数据系统运营的前提下，对系统中存储的包括个人信息在内的敏感数据进行安全保护，为民航机场打造密码安全一体化的数据保护体系。

［结果/结论］ 基于“网络”与“数据”并重的建设思路，为民航机场设计出多维度、多种安全技术有机组合的纵深防御战法，进一步增强民航业务系统的安全防护能力，提升民航数据资产的保护水平。

关键词： 旅客个人信息；商用密码；数据安全；防护体系；密码安全一体化

中图分类号： TN918.4 **文献标识码：** A

The application of commercial cryptography in the protection of personal information of passengers in airport

Yang Qi[1], Zhu Mingjuan[2], Wang Yong[2]
(*1.Beijing Capital Airport Food Management Co.,Ltd., Beijing 100621;2.Beijing Capital International Airport Co.,Ltd., Beijing 100621*)

Abstract:

[Purpose/Significance] In order to provide convenient services to passengers, civil aviation airports collect, store and use a large amount of passengers' personal information, and once an incident of leakage, theft or abuse occurs, the consequences will be serious. With the successive promulgation of China's "Data Security Law of the People's Republic of China" and "Personal Information Protection Law of the People's Republic of China", the protection of personal information of civil aviation airports has changed from "contingent" to "just needed" driven by practical combat and compliance. Commercial cryptography is the core means of data security protection, and ensuring the security of personal information of civil aviation airports through commercial cryptography technology has become an inevitable requirement in the digital era.

[Method/Process] By analyzing the security challenges faced by civil aviation airports in the protection of passengers' personal information, combined with the actual combat and compliance needs of current security protection, it is proposed that based on transformation-free security technology and high-performance commercial cryptography technology, the sensitive data stored in the system, including personal information, be safely protected without upgrading the business system of civil aviation airports and not affecting the operation of the data system, so as to create a cryptographic security integrated data protection system for civil aviation airports.

[Results/Conclusion] Based on the construction idea of "network" and "data", this paper designs a multi-

dimensional and in-depth defense method with an organic combination of multiple security technologies for civil aviation airports, which further enhances the security protection capability of civil aviation business systems and improves the protection level of civil aviation data assets.

Keywords: personal information of passengers;commercial cryptography;data security; protection system;cryptographic security integration

0 引言

随着数字化建设的不断演进，民航机场业务高度依赖网络与信息系统。民航机场信息系统承载着海量旅客个人信息，这使得数据安全问题日益凸显，加强数据安全建设迫在眉睫。在全面了解民航机场网络与信息系统安全状况的基础上，在不影响业务要求的数据流动和共享情况下，设计出基于商用密码技术的数据安全保护方案，才能有效地保障旅客个人信息的安全。

1 机场业务系统数据安全分析

1.1 数据安全面临挑战

信息化系统对民航机场业务的支撑作用日益突出，数据成为新的价值资源。民航机场掌握着旅客的大量个人信息，包括个人身份、生物识别、健康生理和位置等信息。在这些数据中包含有大量的旅客个人隐私信息，关系到每位旅客的切身利益，价值巨大，重要性不言而喻。同时，这些数据也是网络攻击者所觊觎的目标，一旦被泄露，不仅会使个人利益受损，也会影响到企业的形象和声誉，造成经济和信誉的双重损失。合法、适度地对旅客个人信息收集、利用和保护等，可以有效地促进航空业的商业发展和预防航空犯罪[1]。但是，必须正视的是，在实践中已经出现了越来越多的旅客个人信息被泄露、滥用和盗用的现象。

1.1.1 数据安全威胁

民航机场信息系统内部存储的大量包含了旅客个人信息的敏感数据，这些数据在整个生命周期中都面临着安全风险，主要来自于5个方面。

（1）存储数据的威胁。攻击者可从服务端入手，窃取集中存储的数据（包括数据库中的结构化数据和文件系统中的非结构化数据）。在内部没有安全防护措施的情况下，风险极大。

（2）数据防篡改威胁。数据在分发过程中，攻击者可能在截取数据并篡改内容后，再发给数据的接收方，而数据接收方无法识别文件是否被篡改，文件内容是否还是数据发送方的原意，存在接收错误信息的风险。

（3）应用内面临威胁。攻击者可以从数据库或者文件服务器上，直接窃取敏感数据。

（4）上云的泄露威胁。机场数据上云已经成为目前信息化建设的主要内容之一，但是每家上云用户都会担心敏感数据上传到云端的安全问题。云设施无法由用户物理掌控，数据存在泄露的风险。

（5）访问控制被绕过。数据在服务端可直接被窃取，访问控制可以被绕过，也可以对数据进行窃取，同时由于审计置信度较低，这既会带来数据被泄露的威胁，也是对安全保护机制本身的一种破坏。

1.1.2 数据安全建设面对的难题

如何实现在旅客个人信息流动的同时，做好安全保护工作，是民航机场亟待解决的问题。目前，在已建成的应用系统中，往往缺失对数据安全保护的能力，需要补充和增强。民航机场在数据安全改造方面，主要需要解决4个难题。

（1）系统不能大变动，全面改造增强安全无望。民航机场信息化建设往往都是投入了巨额资金，并且已经上线运行，为客户和业务部门提供在线服务。如果以开发改造的方式，为机场信息化系统增强和补充安全能力，特别是加入密码能力，要从应用底层架构入手，不仅需要继续投入大量的人力和物力，而且还需要较长的周期。同

时，对在线运行的应用系统进行改造和切换时，会带来运营风险，造成间接业务损失。

（2）积累数据量巨大，安全建设如何无碍效率。民航机场掌握着大量旅客的姓名、手机号码、证件号码等个人信息，数据量以亿条计，而且每时每刻都在高速流转。采用密码技术在对民航机场应用系统数据进行安全保护时，不能影响到数据的流转效率，不能影响到机场航空业务的正常开展，这对所采用密码的性能，提出了高要求。

（3）数据库品牌各异，增加了数据安全保护难度。在不同阶段建设的应用系统，或者直接采购的成套应用系统产品，带来了机构内部多个品牌数据库并存的情况，而且相同品牌数据库的版本也不统一。这就要针对每个品牌和版本的数据库进行数据安全保护，需要落地方案能够支持每一种数据库，而实现对每个品牌、每个版本数据库都进行各自的安全保护，这在成本和后期维护工作量上，对于机场而言一般是难以接受的。

（4）开发技术不统一，使得密码技术落地加难。各个时期建设的应用系统由不同的开发商供应，所使用的应用开发技术不统一，比如有Java、Net和Php等技术。要实现数据安全防护，就要对接不同的开发技术，实现密码技术与应用系统的结合，才能实现为应用系统中的数据提供安全防护。

1.2 安全防护实战需求

为了有效地化解针对包括旅客个人信息在内的敏感数据面临的安全风险，并有效地应对数据安全建设中的诸多挑战，民航机场在数据安全防护工作中存在6项需求。

（1）策略集中易管控。对于分布于各个应用系统中的敏感数据，在进行安全保护过程中所各自执行的安全策略，需要集中管控。平台要集中设置多个应用的加解密策略，并设置按照时间限制的管控策略。

（2）应用免开发改造。通过应用开发改造方式实现数据安全防护，需要投入大量的工作，而且已经上线运行的系统经过安全底层的改造，会影响到正常业务的开展。因此，理想状态是应用系统免改造方案要周期短和风险低。

（3）加解密须高性能。数据在共享中，是一个大数据量的高速流转过程，因此需要平台具备高性能的加解密能力。

（4）服务具备高可用。为了保持机场服务业务的持续不间断运行，为各个应用系统提供数据安全服务的平台，需要具备高可用的特性，目的就让数据加解密服务持续不间断运行。

（5）兼容各种数据库。在系统改造中，不可能针对每个数据库都要实现一种专门的方案，就需要有一种方案与数据库品牌和版本无关，并以统一的方式，实现数据库中的数据安全。其中的数据，既包含传统的基于SQL的数据库，例如Oracle、SQL Server和MySQL等，也要支持New SQL的新型数据库，例如MongoDB。

（6）使用密码须合规。在采用密码技术实现数据安全的同时，机场需要遵循国家密码管理局对于密码应用合规性方面的要求，使得实施方案能够通过由国家密码管理局认可的密评机构的密码安全性评测。

1.3 安全防护合规需求

个人信息作为数据资源的重要组成部分，应受到严格保护。个人信息处理者掌握着控制信息的主动权，只有规范个人信息处理行为，才能保障个人信息权益。通过调研证实，以往作为信息处理者的企业，在保护个人信息方面重视不够，不仅建设投入不足，而且安全建设滞后于业务功能建设。同时，在发生安全事件后，往往是企业责任不清晰。

自2018年欧盟《通用数据保护条例》实施以来，合规和风险的驱动使得数据保护的重要性日益受到重视，人们更加清晰地认识到数据能够产生的价值和可能带来的危害。近年来，我国关于信息保护的方面的法律及其配套政策规章陆续出台，对数据安全建设提出了明确要求。

1.3.1 法律明确数据保护的必要性

2021年，《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）施行。“两法”就“数据

安全保护义务”“个人信息处理规则”“个人信息跨境提供的规则”“个人在个人信息处理活动中的权利”“个人信息处理者的义务”“履行个人信息保护职责的部门”，以及相关各方的“法律责任”作出明确界定。“两法”统筹私人主体和公权力机关义务与责任，兼顾个人信息保护与利用，为个人信息保护工作提供了清晰的法律依据[2,3]。

1.3.2 行业监管督促数据安全保护

2020年10月1日实施的《民用航空旅客服务信息系统信息安全保护规范》（MH/T 0074-2020）要求：“运营者应制定安全策略和采取技术手段，确保旅客信息在使用、传输和存储各阶段的安全性，防止旅客信息泄露、非法越权使用。”“运营者应将在我国境内运营中收集和产生的旅客信息存储在境内，并采取数据备份和加密认证等技术措施和其他必要措施，防止信息泄露、毁损、丢失。”《GM/T 0054-2018 信息系统密码应用基本要求》要求采用国密算法保护重要数据的机密性、完整性等。

信息安全事件频发，安全威胁给个人信息处理者带来压力；《个人信息保护法》的实施，对个人信息处理者提出了“硬性”法律要求。客观的实战挑战和法律法规的明确要求，形成了“双轮”驱动，个人信息安全建设已经由“或有”变为“刚需”。面对数据安全现状，个人信息处理者应依照法律法规相关要求，采取技术措施，加强个人信息保护，使个人信息在安全的前提下，可以被有效开发和利用。

2 密码安全一体化新防护思路

2.1 数据安全需兼顾内外威胁

从总体上看，民航机场数据安全面临的风险主要来自于两方面。一是外部威胁与对抗的持续升级。黑客可以利用网络漏洞，远程窃取数据库中的敏感数据，同时新兴技术的演进也带来了不可预知的安全风险。二是来自内部的安全风险。机场内部工作人员有工作之便，存在无意泄露或出于商业目的有意倒卖包括旅客个人信息在内敏感数据的可能，即传统安全体系存在的固有问题。

数据安全乃至网络安全的本质，始终是攻击者和防御者之间的战斗，民航机场因为拥有海量价值数据，将会成为攻击者和防御者的重要战场。未来仍存在着大量不确定性，机场将会持续面临新的、不断演化的数据安全威胁与挑战。

2.2 防护思路由被动变为主动

传统的数据防护主流思路是应对式防御。通常是在系统遭受了攻击后，根据攻击情况采取行动，即“以网络为中心”的数据安全，主要是保护被传统物理网络多层包围的数据，包括且不限于传统杀毒软件、基于特征库入侵检测、病毒查杀、访问控制和数据加密等手段，这种防护体系仅适用于保护静态数据，“滞后于攻击手段”的弊端明显。目前，直接针对数据本身进行主动式防护，通过加密和去标识化等技术，为需要保护的数据穿上“防弹衣”，能够更有效地增强对数据本身的防护能力，即“以数据为中心”采取措施，是实现数据安全的最直接、有效的手段。以网络为中心的安全体系是保证数据安全的前提和基石，而以数据为中心的安全，是以数据为抓手实施安全保护。因此，以网络和数据并重的安全建设成为大势所趋。

3 以密码为核心构建防护体系

3.1 密码是数据安全的基石

密码技术是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务[4]。密码是网络安全的杀手锏技术和核心支撑，是保护网络与信息安全的重要手段[5]，是网络信任的基石。利用密码在安全认证、加密保护和信任传递等方面的重要作用，能够有效消除或控制潜在的“安全危机”，实现被动防御向积极防御的战略转变。密码支撑构建安全防护综合体，密码在网络安全防护中具有保底作用，是最后一道防线。密码技术可以实现OSI网络安全架构的“鉴别、访问控制、机密性、完整性和抗抵赖”等基本安全服务。

在以数据为中心的主动式数据安全防护体系

中，密码技术提供了重要价值。比如，在识别方面，密码可以为数据识别提供身份安全能力，为接口通道实现安全加密；在防护方面，数据加密技术本身就是在开放式信道中，构建了强制的防护措施，并结合身份实现访问控制；在检测、响应、恢复和反制方面，密码也能够提供身份鉴别、数据保护和水印追溯等能力。

3.2 安全技术从应对到主动

民航机场目前的数据防护主流思路仍然是应对式防御。但是，应对式防御的弊端比较明显，在应对拟人化和精密化的攻击时，很容易被攻击者快速发现漏洞，并针对薄弱点进行精准攻击，难以适应时代发展，难于达到数据安全防护的目的。

互联网难以避免地存在着各种先天性缺陷、日趋复杂的应用和网络的脆弱性，且已经成为一种常态。“找漏洞、打补丁和防病毒等被动式防御、局部式治理、增量式修复，已不能适应多变的网络安全形势。网络安全日益强调全域安全，强信任、强安全、强可控和强防护，已然成为必然要求。所以，必须以规范使用国家认可的密码技术为基础，以系统性、整体性和协同性为原则，构建以密码为基石的网络空间新安全[6]。”

从防御角度看，网络漏洞在所难免。应对式防御难以从根本上解决问题，必须更新思路，聚焦于核心保护目标“数据”，采取基于密码的系列技术手段，建立主动式防护机制才是解决问题的有效办法。

2019年12月1日起我国实行了等级保护2.0标准。在等级保护1.0标准基础上，更加注重了主动防御，建立事前、事中和事后全流程的安全可信、动态感知和全面审计。一方面实现了对民航机场传统IT系统和基础信息网络的等级保护，另一方面实现了对云计算、大数据、物联网和移动互联网等新兴技术下的等级保护对象的全覆盖。

3.3 安全产品从外挂到内嵌

边界往往是数据安全防护的焦点。从安全能力来看，个人信息在流动过程中没有边界，通过将数据放在一个安全增强点上进行加密，人为地塑造一个数据边界，然后在解密点上，再结合用户身份进行脱敏等访问控制，将数据安全防护从游离于业务的“外挂式”，提升到融合业务的“内嵌式”，从而构建出“防绕过”的访问控制、高置信度的访问审计。同时，基于此打造新一代安全产品，不仅能实现个人信息不受外部攻击，也能防范内部业务人员的越权访问，实现降低重标识风险，兼顾个人信息的安全性和有用性。

3.4 安全机制从单点到纵深

在数据安全防护过程中，不存在一招制敌的战法。只有建立防御纵深，凭借先发优势、面向失效的设计、环环相扣的递进式设防，才能铸造出有效的安全防护网。

3.4.1 建立先发优势

为了对抗体系化的攻击，防御体系的设计应用好“先发优势”，针对威胁行为模式，提前布置好层层防线，综合利用多种手段，实现各个维度防御手段的纵深覆盖，让进攻者在防守者布局的环境中“挣扎”。

3.4.2 面向失效设计

面向失效的设计原则是指任何东西都可能失效，且随时失效。需要考虑如果在前一道防御失效后，如何补上后手的问题。面向失效设计的整体思路是从传统静态、被动的方式，转向积极体系化的防御纵深模式。分析进攻者的进入路径，打造多样化、多层次递进式的防御“后手”。如图1所示。

基于面向失效的防御理念，从几个维度层层切入。当一种保护手段失效时，设计好后手应对措施，综合利用多种手段打造纵深协同。可以主要选择三个比较重要的维度：一是安全能力维度（识别、防护、检测、响应、恢复和反制）；二是数据形态维度（使用态、存储态和传输态等）；三是技术栈维度（SaaS/业务应用、Paas/平台和IaaS/基础设施）。这三个维度之间的 关系是独立的、正交的，三者叠加起来可以构建一套有效的数据纵深防御体系。

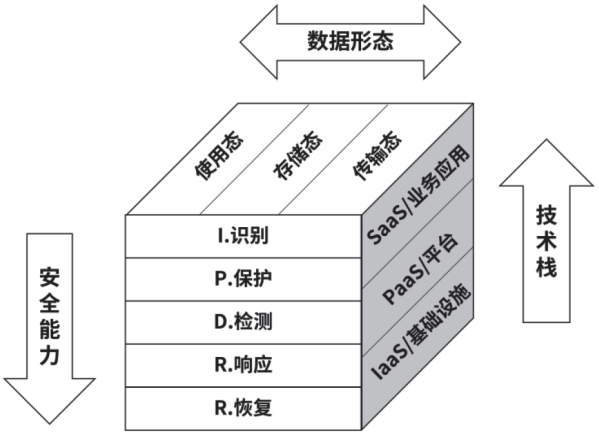

图1 面向失效的数据安全纵深防御新战法

3.4.3 安全纵深防御

纵深防御是一项体现在数据安全防御体系设计各个方面的基本原则，而不是一种“可以独立堆叠形成的解决方案”。

（1）从安全能力构建数据防御纵深。“IPDRRC”即识别（Identify）、防护（Protection）、检测（Detect）、响应（Response）、恢复（Recover）和反制（Counteract）数据保护环节，体现了数据保护的时间顺序，基于时间维度，可以有机地结合多种安全机制。识别是一切数据保护的前提，在数据识别、分类分级和身份识别的前提下，针对数据安全威胁的事前防护、事中检测与响应、事后恢复与追溯反制等多种安全机制，环环相扣，协同联动，可以有效地构建出面向失效的纵深防御机制。如图2所示。

从当前民航机场的数据安全建设重点看，越靠近“事前防护”，投资回报率越高，如果仅依靠检测/响应、恢复和反制等环节，损失已经发生，机场可能会因此付出更高成本。

（2）从数据形态构建数据防御纵深。数据状态大致可以分成传输态、存储态和使用态，而身份鉴别和信任体系则是对数据访问的补充或者前提，基于“数据三态”可延伸出数据全生命周

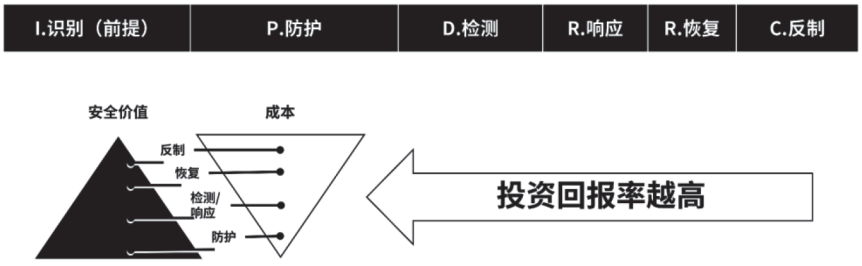

图2 IPDRRC投资回报率分布图

期。围绕数据形态，可以构建多种安全机制有机结合的防御纵深。目前，结合应用现状梳理出了20种密码应用模式，采用IPDRRC中数据防护段的密码技术，可以进行数据形态维度的纵深防御构建。如图3所示。

在信息系统中，数据在传输、存储和使用等不同形态之间的转化。在此过程中，可以利用多种安全技术构建协同联动的纵深防御机制。

（3）从技术栈构建数据防御纵深。信息系统的技术栈体现了空间维度，这也可以作为数据保护的纵深发展维度。沿着数据流转路径，在典型B/S三层信息系统架构（终端侧、应用侧、基础设施侧）的多个数据处理流转点，总结出适用技术栈不同层次的数据保护技术。综合IPDRRC中数据防护段的密码技术、数据存储态和典型信息系统的技术栈分层，可以从技术栈维度构建数据防御纵深。如图4所示。

如图4所示，列举了10种数据存储加密技术，在应用场景和性能优势方面各有侧重：DLP终端加密技术侧重于企业PC端的数据安全防护；CASB代理网关、应用内加密（集成密码SDK）、应用内加密（AOE面向切面加密），侧重于企业应用服务器端的数据安全防护；数据库加密网关、数据库外挂加密、TDE透明数据加密、UDF用户自定义函数加密，则侧重于数据库端的数据安全防护；TFE透明文件加密、FDE全磁盘加密则侧重于文件系统数据安全防护。其中，覆盖全量数据的FDE技术，可以作为基础

	身份鉴别及密钥管理	数据传输(通信安全)	数据存储(数据资产安全)	数据使用(数据共享与安全兼得)
应用层	③ 预共享密钥的身份鉴别 ④ 基于数字签名的身份鉴别 - 基于单一设备签名的身份鉴别 - 协同签名 -阈值签名	⑤ 离线通信消息加密 - PGP邮件加密 - S/MINE邮件加密 - Signal/OTR聊天加密 ⑥ 代理重加密受控分发消息	⑨ 应用内数据加密 - 应用内开发集成加密 - CASB代理网关加密 - AOE面向切面加密	⑫ 基于差分隐私的数据匿名化 ⑬ 基于属性加密的访问控制 ⑭ 锚点解密的防绕过数据安全 - TDF可控分享秘密信息 ⑮ 不可信环境中的数据运算 - FHE全同态加密 - MPC多方安全计算 - ZKP零知识证明、区块链隐私保护 ⑯ 可验证结果的计算外包 ⑰ 封装业务逻辑的可信运算环境 - 金融数据密码机
终端与基础设施层		⑦ 在线通信消息加密 - 基于SSL/TLS的HTTPS - VPN虚拟专用网络 - 链路密码机/网络密码机 ⑧ 可感知窃听的专线通信 - BB84量子密钥分发	⑩ 数据库存储加密 - DB-Proxy数据库代理加密 - 数据库UDF开发集成加密 - 数据库外挂加密 - TDE透明数据加密 ⑪ 文件存储加密 - TFE透明文件加密 - FDE全磁盘加密	⑱ 基于密码的数字水印追溯
基础密码产品	① PKI信任体系 - CA证书认证系统 - 安全认证网关 ② IBC信任体系			⑲ 基于密码校验的防篡改 - 电子签章 ⑳ 基于私钥签名的责任认定 - 签名验签服务器

图3 常见密码应用模式

安全增强点	终端侧	应用层			基础设施层					
	DLP 终端加密	CASB代理网关	应用内加密 (集成密码SDK)	应用内加密 (AOE面向切面加密)	数据库 加密网关	UDF用户自定义函数加密	数据库 外挂加密	TDE 透明数据加密	TFE透明 文件加密	FDE 全磁盘加密
实施特点	进程级管控，适用于企业终端数据的安全管理 优势：文件外发强管控 挑战：终端适配困难、运维成本高	1、通过适配应用层协议和上下文，为已有应用系统增强防护 2、复用CASB平台，降低实施工作量，解决云场景下的信任问题 优势：与业务结合的数据安全保护 挑战：实施成本较高	1、通过开发改造的方式，与封装了加密业务逻辑的密码SDK集成，调用其加解密接口，使目标应用系统具备数据加密防护能力 优势：适用范围广、灵活性高 挑战：需要对应用系统开发改造、对应用开发人员要求高	1、对流经切面的数据实施加密脱敏、日志留存及审计等 2、集成应用IAM的终端用户身份信息 3、支持结构化和非结构化数据 优势：数据加密与业务逻辑解耦、不影响业务运营、基于细粒度权限控制的数据安全防护 挑战：应用程序编程语言和框架需要做适配	1、为数据库提供“入库加密、出库解密”的防护，建立数据库用户的访问控制 优势：应用系统与加解密功能分离 挑战：只适合开源数据库、高性能和高可用实现难度大	1、改造数据库存储过程，手工编程实现数据加密 优势：扩展能力强 挑战：通用性低	1、给表增加“触发器+视图”改造，实现入库触发加密、出库视图解密 优势：独立权控体系 挑战：仅支持Oracle等少量数据库类型、数据库性能损耗较高、可扩展性差	1、国密替换数据库内置算法，支持MySQL/PostgreSQL等，支持国密合规的KMS密管集成 优势：独立权控体系、性能损耗较低 挑战：防护颗粒度较粗、数据库类型实用性有限制	1、主要执行策略包括文件加密 2、支持Windows/Linux/XC操作系统等 优势：可对应用进程授权 挑战：管理员风险、高性能实现难度大	1、原理：通过动态加解密技术，对磁盘或分区动态加解密 优势：性能优势突出、部署简单 挑战：数据防护颗粒度粗

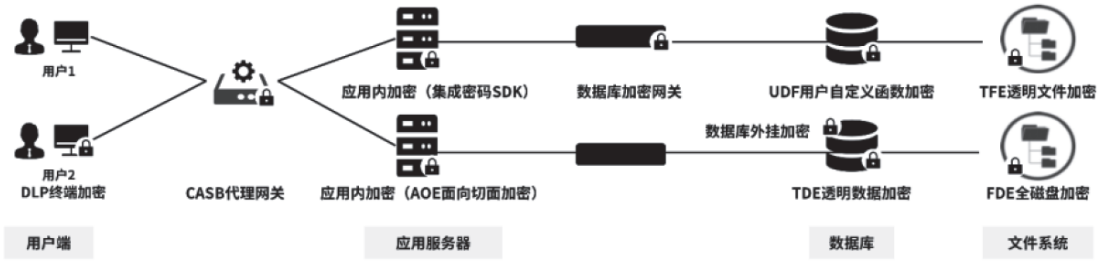

图4 覆盖不同技术栈的数据存储加密技术

设施层安全标配。针对特别重要的数据，再叠加AOE等技术实施细粒度加密保护，两者的结合可以面向技术栈构建出数据防护纵深防御机制。

综上所述，从安全能力、数据形态、技术栈等不同维度，有机地结合多种安全技术构建纵深防御机制，可以形成兼顾实战和合规、协同联动体系化的数据安全新战法。

4 机场数据安全体系建设落地

数字化升级为民航机场提高效率，降低成本提供了极大的助力，也对机场的管理支撑系统提出了更高要求，需要进一步提升管理系统运作效率，提高业务透明度，加强业务管控。为了满足机场数据安全建设的实战需求，基于纵深防御体

系建设落地的基本思路，是需要落地实现几项基本功能，以确保民航机场的数据安全。

4.1 保障业务性能与安全兼备

旅客信息在机场IT系统中流转、在实现数据的高效流转的同时，也带来了信息安全的挑战。传统的磁盘存储加密技术，虽然对业务性能影响不大，但是颗粒度较粗，很难有效地保护数据。机场客户端侧的加解密技术，会给客户使用造成不便，同时还会影响到数据的高效流转。分级隔离技术虽然能够有效地管控数据风险，但是却会间接地影响数据的共享。

要兼顾数据流转和安全防护，最好的方法是将加密等数据安全能力融合到业务流程中。可以根据机场实际的业务场景，制定针对性的数据安全保护方案，同时机场需要采用高性能的密码技术，将安全机制和用户的现有流程无缝对接，在不改变用户的操作习惯、不伤害用户粘性和不影响数据的流转性能前提下，实现两者之间的动态平衡。

4.2 兼顾多形态数据安全防护

民航机场的海量价值数据，不仅仅包括传统数据库中的结构化数据，同时还涵盖了文档、图片、视频和音频等大量高价值的非结构化数据。要想构建覆盖结构化与非结构化数据的纵深防御防御机制，可以将AOE面向切面技术和TFE透明文件加密等多种加密技术相结合，通过优势互补的方式，实现数据的全方位保护。如图5和图6所示。

对于机场结构化数据，采用AOE面向切面加密技术，其实现原理是将机场数据安全插件部署在应用服务中间件，并结合旁路部署的数据安全管理平台、密钥管理系统，通过拦截入库SQL，

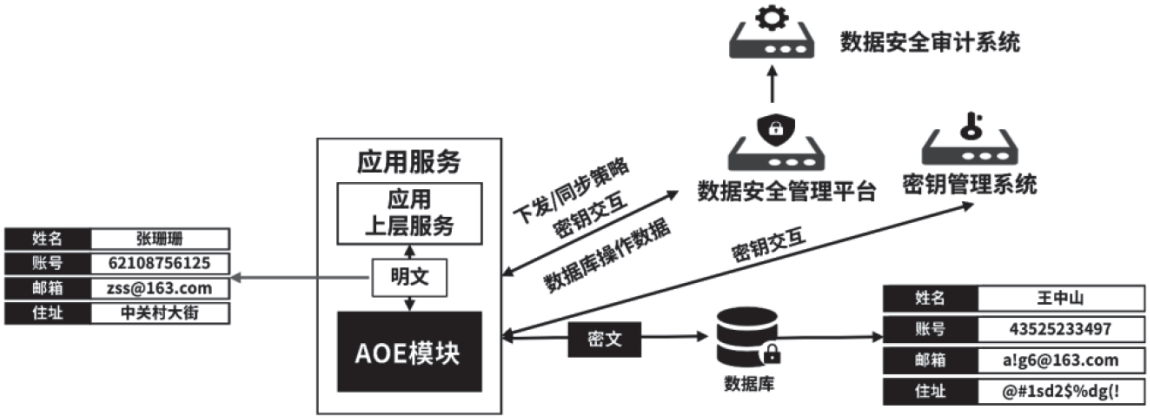

图5 AOE面向切面加密技术原理

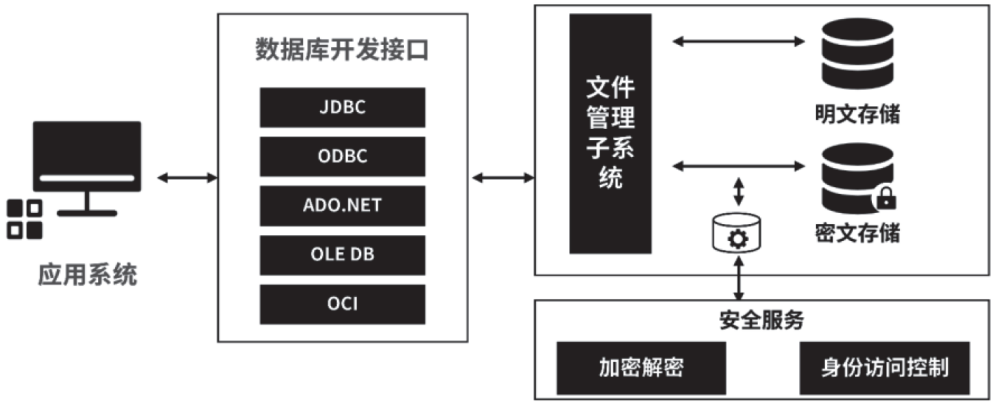

图6 TFE透明文件加密技术原理

将数据加密后存入数据库。对于非结构化数据，可以采用TFE透明文件加密技术，其实现原理是在机场操作系统的文件管理子系统上，以部署加密插件来实现数据加密，并基于用户态与内核态交付，实现“逐文件逐密钥”加密。

4.3 应用安全技术不影响业务运行

民航机场业务涉及的数据量非常庞大，在实现数据安全防护的过程中，如果影响到机场业务系统的正常运转，将会导致大量旅客的权益受到损害。传统技术路线一般会基于密码机硬件设备，提供SDK对机场的业务系统进行密码整改，一方面给机场信息系统的应用开发人员增加了负担，另一方面也带来了较大的业务风险。

机场可以利用AOE面向切面加密技术的特性，结合TFE透明文件加密等安全技术，实现整体安全方案的免开发改造敏捷实施，使安全与业务系统在技术上解耦，在能力上融合交织，最终实现批量化快速部署实施。在确保方案安全、可靠的前提下，可以实现方案在多场景、多地域下的快速复制，从而实现安全能力的快速升级迭代，更好地适应新技术下的安全挑战。

4.4 建立数据访问防绕过机制

很多数据泄露事件源于重要数据在数据库或备份的过程中被盗取，访问控制被不法分子利用网络或权限漏洞绕过，从而获取到海量价值数据。民航机场在构建数据安全防御体系的过程中，有必要考虑建立基于数据安全的防绕过机制。

在密码技术的基础上，将访问控制和审计等多种安全技术相结合，通过部署独立的数据访问审计，使每条日志都支持追溯到具体业务用户，并可以为审计日志提供完整的保护，从而实现对数据泄露源头的追溯，形成“以加密技术为核心，融合数据识别、防护、检测/响应和追溯等多种安全技术”的数据安全保护体系，解决了访问控制容易被不法分子轻易绕过的问题。

5 结束语

本文分析了当前民航机场在旅客个人信息保护工作中所面临的挑战，结合国家的相关法律法规、前沿的数据安全防护理念以及高性能商用密码技术，提出了针对民航机场数据安全的“网络”与“数据”并重的建设思路，设计出了多维度、多种安全技术有机组合的纵深防御战法，以期为民航机场加强包括旅客个人信息在内敏感数据的安全防护提供参考。

参考文献：

[1] 郑欣.论航空旅客个人信息的侵权责任[D].天津:中国民航大学,2020.DOI:10.27627/d.cnki.gzmhy.2020.000500.

[2] 中华人民共和国数据安全法[J].中华人民共和国全国人民代表大会常务委员会公报,2021(05):951-956.

[3] 中华人民共和国个人信息保护法[J].中华人民共和国全国人民代表大会常务委员会公报,2021(06):1117-1125.

[4] 中华人民共和国密码法[J].中华人民共和国全国人民代表大会常务委员会公报,2019(06):912-916.

[5] 白小勇.合规与实战推动密码产业发展[J].信息安全与通信保密,2021(01):92-98.

[6] 霍炜.构筑以密码为基石的智能时代新安全[J].网络空间安全,2018,9(05): 23-26+31.

[7] 刘佳,张琳.个人客户信息保护的法律法规及标准综述[J].网络空间安全, 2018, 9(10): 1-.

作者简介：

杨琪（1989-），**女，汉族，贵州凯里人，贵州师范大学，本科；主要研究方向和关注领域：民航信息化与网络安全。**

朱明娟（1979-），**女，汉族，天津人，中国民航大学，硕士；主要研究方向和关注领域：智慧机场和整体规划。**

王勇（1977-），**男，汉族，山东鄄城人，北京理工大学，硕士；北京首都国际机场股份有限公司，正高级工程师；主要研究方向和关注领域：民航信息化与网络安全。**

持续化网络安全运营体系在大中型企业的实践

董红涛，朱继建，刘书剑，姜昊
（中泰证券股份有限公司，山东济南250001）

摘要：

［目的/意义］ 大中型企业面临的网络威胁日益严峻，对网络安全的要求日益增强。企业通过持续化网络安全运营体系，建立自己的网络安全运营团队，将网络安全工作由静态的、碎片的安全运维转变为动态的、持续的安全运营，从而提升网络安全保障体系的及时性和有效性。

［方法/过程］ 企业通过组建网络安全运营团队、建设网络安全运营支撑平台等一系列方法，把持续化网络安全运营由理论转变为实践，以应对日益严峻的网络威胁形势，为企业生产经营提供有效的网络安全保障。

［结果/结论］ 企业建立持续化网络安全运营体系，可以有效地减少各类网络安全事件的发生，持续提升企业网络安全保障能力。

关键词： 安全运营体系；安全运营团队；企业信息安全；网络安全管理；网络安全保障能力

中图分类号： TN915.08 **文献标识码：** A

The practice of continuous cybersecurity operation system in large and medium enterprises

Dong Hongtao,Zhu Jijian, Liu Shujian, Jiang Hao
(*Zhongtai Securities Co.,Ltd., Shandong Jinan 250001*)

Abstract:

[Purpose/Significance] Medium and large enterprises are facing increasingly severe cyber threats, and the requirements for cybersecurity are increasing. By maintaining the cybersecurity operation system, enterprises establish their own cybersecurity operation team, and transform the work from static and fragmented to dynamic and continuous, so as to improve the timeliness and effectiveness of the cybersecurity guarantee system.

[Method/Process] Through a series of methods, such as the establishment of cybersecurity operation team and the construction of cybersecurity operation support platform, enterprises have transformed the sustainable cybersecurity operation from theory to practice, so as to cope with the increasingly severe cybersecurity situation and provide effective cybersecurity guarantee for enterprise production and operation.

[Results/Conclusion] The establishment of a sustainable cybersecurity operation system can effectively reduce the occurrence of various cybersecurity incidents and continuously improve the cybersecurity guarantee ability of enterprises.

Keywords: cybersecurity operation system; cybersecurity operations team; enterprise information security; network security management; cybersecurity guarantee capability

0 引言

自党的“十八大”以来，总书记高度重视网络安全和信息化工作，提出了“没有网络安全就没有国家安全”“网络安全和信息化是一体之两翼、驱动之双轮”“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”等一系列新思想、新理论、新论断、新战略。总书记关于网络安全的重要思想，为做好网络安全工作提供了指引方向。

随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规的相继出台，网络安全被提升到了国家战略高度，国内各大企业都开始不断倡导、建设和完善网络安全建设，以应对网络空间安全的严峻挑战。然而，大中型企业信息系统涉及网络系统、安全系统、业务应用系统、生产管理系统等，整体信息化规模庞大，信息资产数量繁多，如何确保如此庞大的资产量级下的网络安全，是大中型企业面临的现实问题。

鉴于此，企业应组建专业的网络安全运营团队，建设网络安全运营支撑平台及工具，制定并持续优化标准化的网络安全运营流程，建设和完善网络安全运营活动内容，快速实现从安全运维到安全运营转变以及安全能力的提升，强化安全风险的主动感知，提升对网络安全风险的掌控和处置能力，以应对日益严峻的网络威胁形势，为企业生产经营提供有效的网络安全保障。

1 安全运营体系的主体内容

网络安全运营是个复杂的工程化体系，安全运营需要人员、流程、运营支撑系统和基础安全资源的支撑，安全人员按照运营流程，有效使用基础安全资源中的各项安全工具，通过安全运营支撑系统进行协作并完成精细化的过程管理，从而开展各项安全运营活动。

1.1 组建网络安全运营团队

安全运营团队是安全运营体系的核心，用于实现安全策略的有效执行、运营支撑系统的有效使用、运营流程正常运转以及安全事件的有效分析和处置。为支撑完整的安全运营活动，安全运营团队主要由分析与响应团队、脆弱性管理团队以及系统维护团队构成。

分析与响应团队负责对信息系统进行实时监测和分析，承担安全运营中的持续威胁管理工作；脆弱性管理团队负责对受保护的网络空间进行持续扫描与测试，承担安全运营中的脆弱性闭环管理工作；基础架构团队承担安全运营基础设施的搭建、维护和运行保障工作，日常监控时长不低于7×8小时，重大活动安保期间升级为7×24小时。

1.2 建设网络安全运营支撑平台

安全运营支撑平台为持续性安全运营工作提供全流程支撑，以运营脚本为核心驱动运营团队精准稳定的开展各项运营活动，对于运营过程中的各项活动进行记录留痕、跟踪推进、质量监管，从而实现安全运营工作的精细化管理。

（1）安全数据采集存储能力

系统具备多种数据采集协议和采集方式，通过分布在不同网络区域内的采集节点实现各类安全日志的收集；系统采用大数据存储架构，对采集层收集的海量数据进行存储。

（2）安全大数据分析能力

系统具备事件、流量、脆弱性等多种数据维度的安全分析能力，通过大数据分析功能及安全算法，对异常攻击、异常流量进行分析识别。

（3）安全状态呈现能力

系统具备攻击态势、脆弱性态势、整体安全态势等多种态势呈现能力，并可实现针对新型安全问题或预警的快速定制能力。

（4）网络攻击检测预警能力

系统能够根据安全事件、网络流量以及威胁情报的解析，实现对恶意程序、网络攻击以及异常行为的有效检测，对安全威胁进行主动发现和预警。

（5）过程管理能力

系统具备精细化安全运营过程管理能力，支持运营流程的编排和运营质量评价。系统通过预设脚本规范各类安全威胁的处置动作，向运营团队人员自动化推送任务，驱动安全人员完成威胁分

析、事件提报、事件审核与威胁防御动作，实现对所有安全事件的闭环管理。

1.3 制定网络安全运营流程

安全运营不仅仅需要网络安全工具、安全运营平台和安全运营团队，更需要一套完善的标准化流程体系。完善的安全运营流程，要求每个安全相关要素都能根据威胁环境的变化进行调整，同时满足从顶层制度到防御、检测、响应、处置的各个环节，再到与人、工具、技术的各个因素有机结合。

企业安全运营团队通过安全运营流程规范各类安全运营动作，制定涵盖安全检查、运营支撑环境管理、资产安全、安全事件、运营交付、安全漏洞多方面、多项标准化的运营流程及规范，将标准化的流程及规范在日常安全运营工作中执行，推进安全工作的工程化、标准化。

（1）安全运营流程的制定

安全运营是一个持续的过程，需要执行一系列的步骤和流程来保障系统的安全性和稳定性。安全运营流程的制定，可以明确安全运营处理步骤，从检测阶段到分析阶段，再到最后的处置阶段，每个过程都有明确的处理方式，这样避免了对安全运营处理步骤的遗漏，增强了对安全运营整体的把握。

（2）安全运营流程的标准化

安全运营流程的标准化范围涵盖安全运营活动范围内的各项事务和操作流程，提高了安全运营团队人员在开展各项安全运营活动时的协作效率，加强了安全运营工作质量的监管和控制。

（3）安全运营流程的持续优化

安全运营流程是动态变化的，随着设备的更新、数据格式的更替、漏洞的发掘、攻击手法的发展，安全运营流程也要根据不断变化的具体情况作出持续性的优化。

1.4 开展网络安全运营活动

依托于专业安全工具和专业安全人员，由专职安全运营团队开展持续安全监控分析、重大活动保障、攻防演练以及安全工作的聚合管理等安全运营活动，通过持续安全监测、预警、处置，逐步实现自适应的安全保障能力。

（1）持续安全监控分析

开展安全运营应以持续安全监控和分析为核心，对信息系统提供安全事件检测、响应及动态防御三个维度的持续运营动作，包含安全事件监测、风险确认、事件遏制、风险修复、事件溯源分析、持续性威胁防御、持续威胁管理的工作流程管理等工作内容。同时通过分析威胁情报、热点安全问题，制定匹配企业信息系统的安全防护策略、更新策略配置要求，实时抵御攻击方的攻击行为。

（2）重大安保活动保障

在重大活动期间开展7×24小时安全监控和保障，开展高频度的内外网安全资产监控与重点保障目标的持续监测，提升安全监控级别，并开展相关应急及事件处置。

（3）实战攻防演练

举办真实网络环境下的攻防对抗，邀请可信的第三方专业团队担任红方，针对信息系统开展模拟攻击，验证企业安全保障能力以及安全运营体系对于攻击行为的监测与处置能力。

（4）安全工作的聚合管理

安全运营团队将安全设备维护管理、资产安全管理、系统安全评估等各类安全工作数据纳入至安全运营支撑系统，实现数据打通和共享利用，并通过相应的安全运营管理流程规范化各项工作开展。

2 安全运营体系的实践

2.1 安全事件运营

建立安全运营支撑平台和运营支撑工具，为日常安全运营工作提供技术能力支撑，并对运营成果进行归档。将安全设备纳入日常安全运营，并实现工作现场5~8天、远程7×24小时的安全事件监控机制。

建立每日、每周、每月复盘的安全运营模式，对安全运营工作期间发现的各类安全事件进行全面复盘，并根据复盘情况从源头解决安全隐患，促进安全事件管理到安全风险控制的转变。

2.2 安全资产及漏洞运营

对互联网侧暴露的资产进行持续探测，资产探测的内容包括IP、域名、端口、操作系统指纹、中间件指纹、应用指纹、数据库指纹、服务协议和设备指纹等。在进行资产探测的同时，安全运营团队同步开展互联网资产漏洞的安全探测，主要包括操作系统漏洞、中间件漏洞、常用软件漏洞、应用程序漏洞、网络设备漏洞和数据库漏洞等。

2.3 安全运营流程及规范标准化

制定涵盖安全检查、运营支撑环境管理、资产安全、安全事件、运营交付、安全漏洞等多个方面、多项标准化的运营流程及规范，将标准化的流程及规范在日常安全运营工作中执行，推进安全工作的工程化。

2.4 安全运营指标设计及实践

建立多类安全运营指标的安全运营指标体系，例如覆盖率、准确率、及时率、有效率、问题复发率、整改率、检出率等，通过运营指标驱动各项安全工作的开展，并对安全工作成果进行衡量评价。

2.5 实战攻防演习工作

定期开展实战攻防演习活动，邀请多支优秀攻击团队共同组成攻击团队，安全运营团队组成防守团队，通过实战化方式检验网络安全保障体系的有效性，并验证安全运营体系的有效性，及时发现并修复系统薄弱环节，逐步提升并完善系统纵深安全保障能力。

3 结束语

本文研究了持续化网络安全运营体系在大中型企业实践的问题。持续化网络安全运营体系能够在保障业务正常运行的基础上，提升组织整体安全能力。在当前严峻的安全形势下，安全威胁不断演变，需要可持续的安全运营不断提升对抗能力。面对复杂的网络安全事件，企业需要不断提升自身网络安全意识及安全防御能力，建立持续化网络安全运营体系，有效减少各类网络安全事件的发生，持续提升企业网络安全保障能力。

参考文献：

[1] 卢光明.企业安全运营中心将是支撑未来企业的核心[J].网络空间安全,2018,9(11):93-100.

[2] 王晟,赵建福,李超峰,等.持续化网络安全运营体系研究[J].电信工程技术与标准化,2020,33(12):37-41.

[3] 崔光耀.安全运营提升安全新境界[J].中国信息安全,2019,No.116(08):46-47.

[4] 孙磊.数据中心智能安全运营体系建设探索与实践[J].金融电子化,2021,No.314(11):31-32+6.

[5] 张剑,李韬.安全运营让网络安全更加有效[J].网络安全技术与应用,2020,No.229(01):6-7.

[6] 钱勍.网络安全运营与实践初探[J].中国信息安全,2019,No.116(08):71-73.

[7] 欧阳达诚.以银行业为例谈安全运营中心建设[J].金融科技时代,2020,No.301(09):28-32.

[8] 刘志诚.智慧城市网络信息安全体系建设浅析[J].网络空间安全,2018,9(06):74-79.

作者简介：

董红涛（1975-），男，汉族，天津人，贵州大学，硕士；主要研究方向和关注领域：信息技术治理和网络安全。

朱继建（1981-），男，汉族，山东济南人，四川大学，本科；中泰证券股份有限公司信息技术管理部，工程师；主要研究方向和关注领域：网络安全。

刘书剑（1986-），男，汉族，山东济南人，哈尔滨工业大学，本科；中泰证券股份有限公司信息技术管理部，工程师；主要研究方向和关注领域：网络安全。

姜昊（1986-），男，汉族，山东济南人，英国萨里大学，硕士；中泰证券股份有限公司信息技术管理部；高级工程师；主要研究方向和关注领域：网络安全。

企业网络安全态势感知系统设计与实现

莫永华，陈昱希，何淼
（桂林信息科技学院，广西桂林541004）

摘要：

［目的/意义］ 随着护网行动在全国展开，企业Intranet网络中暴露出来的安全问题日渐增多，需要一种新的网络安全方案来解决问题。

［方法/过程］ 通过对神经网络预测算法的改进，运用Logstash进行数据分析，采用Flask框架对数据进行处理，以及ElasticSearch和MongoDB数据仓库进行存储。

［结果/结论］ 实现企业网络安全可发现、可预警、可追溯和可视化呈现，安全设备可联动的企业网络安全态势感知系统，可以有效地提升企业网络安全管理水平，降低网络安全风险。

关键词： 信息安全；企业网环境；态势感知系统；数据仓库技术；网络安全；数据安全治理

中图分类号： TP393.0；TP274+ **文献标识码：** A

Design and implementation of enterprise network security situational awareness system

Mo Yonghua,Chen Yuxi,He Miao
(*Guilin Institute of Information Technology , Guangxi Guilin 541004*)

Abstract:

[Purpose/Significance] With the development of the national network protection action, there are more security problems exposed in the enterprise intranet network, and a new network security scheme is needed to solve the problem.

[Method/Process] This paper improves the prediction algorithm of neural networks, uses Logstash for data analysis, uses the Flask framework to process data, and ElasticSearch and MongoDB data warehouses for storage.

[Results/Conclusion] Therefore, the enterprise network security situation awareness system can be discovered, early warning, traced and visualized by enterprise network security, and the security equipment can be linked, which can effectively improve the level of enterprise network security management and reduce network security risks.

Keywords: information security;enterprise network environment; situation awareness system; data warehouse technology;network security;data security governance

0 引言

随着云计算、大数据和人工智能等技术的不断发展，传统的企业网以网络边界防护、终端准入和病毒防护为主的被动防御体系面临巨大挑战，多层面的网络安全威胁和安全风险也与日俱增。本文提出了一种适用于企业网的安全态势感知建设方案，从企业网中探测性、攻击性、侵入性、预警性、危害性和可用性方面的安全事件来描述网络态势，通过安全设备、网络设备、日志服务器、应用主机的数据采集和储存、威胁检测分析、安全事件应用展示等功能，实现可发现、可预警、可溯源、可视化、安全设备可联动的企业网络安全态势感知系统，有效地提高企业网络安全管理水平，降低网络安全隐患。

1 研究的目的和意义

1.1 目的

网络安全态势感知具体指的就是基于大规模网络环境对采集、评估、预测网络安全要素产生影响的过程。本文研究的主要目的就是通过安装在企业网中的探针系统，采集各系统中的敏感日志信息，集中到分析系统中进行数据储存和分析，并能通过管理端进行查看和处理，阻拦任何潜在的网络攻击或渗透动作。

1.2 意义

企业网目前存在网络和信息系统的安全隐患得不到快速修复、多种安全设备各自为战、检测响应周期长、网络攻击行为不能及时预警、网络安全事件溯源困难等问题。针对企业网网络安全解决方案，亟需提高企业的网络攻击防护、检测、预警能力，以及安全事件可视化呈现、安全设备联动协防等功能[1]。

网络安全态势感知技术通过全盘把握网络安全攻击事件的趋势和发展动向，以守为攻，能够极大地提高对常见攻击的防御能力。同时，能实时感知企业网中攻击的次数和方式，敏锐地察觉可能存在的攻击。网络安全态势感知平台还可与现有传统安全设备进行联防联控，全面提升企业网络的应急响应能力。

2 系统设计

2.1 主控端数据收集系统架构

考虑到数据收集系统的稳定性，系统主要是由成熟组件构成，包括日志存储（Logstash）、Redis、Mongo_DB和Elastic_Search等。系统采用这些基础组件进行日志的收集、储存，并供管理端进行分析和呈现用。数据收集系统会收集所有域控上的事件日志和Kerberos流量，通过特征匹配、Kerberos协议分析、历史行为、敏感操作和蜜罐账户等方式检测各种已知与未知威胁，功能覆盖了大部分目前常见的内网域渗透手法。

在设计上，系统支持敏感操作自动报警。（1）信息探测：查询敏感用户组、查询敏感用户、蜜罐账户的活动、PsLoggedOn信息收集；（2）凭证盗取：AS-REP Roasting、远程Dump域控密码；（3）横向移动：账户爆破、显式凭据远程登录、目标域控的远程代码执行、未知文件共享名；（4）权限提升：ACL修改、MS17-010攻击检测、新增组策略监控、NTLM 中继检测、基于资源的约束委派权限授予检测、攻击打印机服务 SpoolSample、未知权限提升；（5）权限维持：AdminSDHolder对象修改、DCShadow攻击检测、DSRM密码重置、组策略委派权限授予检测、Kerberos约束委派权限授予检测、敏感用户组修改、域控新增系统服务、域控新增计划任务、SIDHistory属性修改、万能钥匙-主动检测；（6）防御绕过：事件日志被恶意清空或日志服务被禁用。

主控端的架构设计如图1所示。

系统中使用到了Logstash来收集域控发来的原始日志数据，在经过初步解析后，会传到RabbitMQ消息队列。消息队列会把日志信息一边传到ElasticSearch进行原始日志的储存备用，一边发往分析引擎，并分析出具体事件类型、威胁程度等信息。发往ElasticSearch的原因是需要对原始日志进行储存，以便后期查证时调用对比。

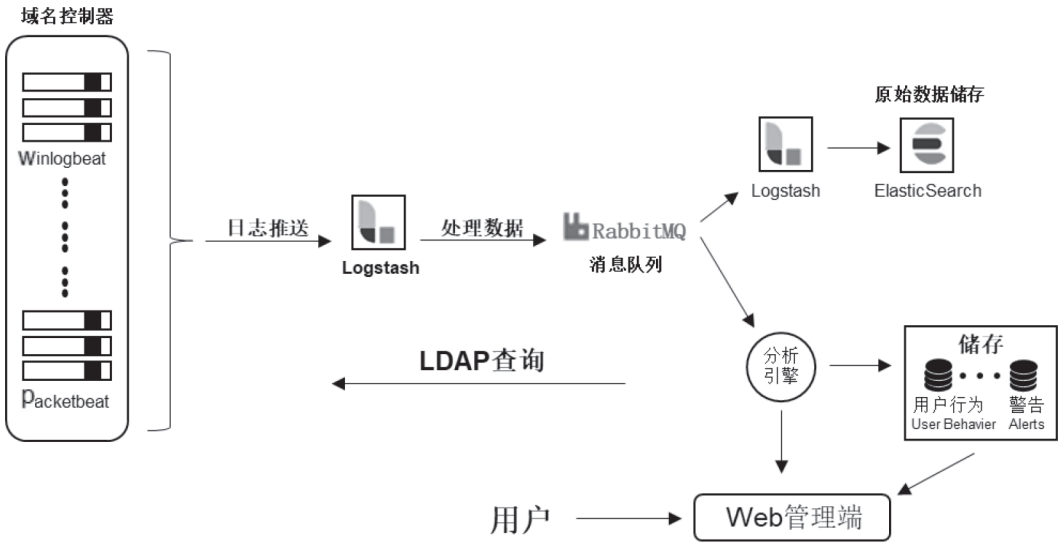

图1 主控端架构设计图

2.2 管理端

根据管理端基本的业务流程分析，系统对管理员页面与功能进行了详细的划分。在此重点叙述管理端的主要功能模块流程设计。

2.2.1 蜜罐系统模块

管理员在完成登录之后，可以进入蜜罐系统页面查看蜜罐相关的详细信息。在蜜罐系统页面，管理员可以进行蜜罐的相关配置，包括蜜罐账号等，以及蜜罐诱饵文件的生成，同时可以看到有关蜜罐系统的被入侵数、相关威胁事件数、威胁来源和威胁类型相应的趋势图。通过页面，管理员可以对整个网络有一个大体的把握，以便管理员决定接下来应该进行什么操作。例如，若短时间内蜜罐入侵事件数过多，管理员则可以决定开启应急响应模式，能够最大程度地缓解网络被攻击的情况。除此之外，蜜罐系统里的内容还可供管理员参考，以便管理员规划接下来对网络的维护计划，例如购置更多的安全设备、提升防火墙等级、升级服务器系统和修改网络口令等。

2.2.2 主机威胁模块

用户可以通过左侧的导航条跳转到主机威胁模块。在这里，管理员可以看到一个列表，其中包含近期所有威胁事件以及简单介绍。例如，若近期有服务器发生过管理员用户变更，则这个列表中就可以看到有一条威胁记录。

在左侧，管理员可以根据类型快速筛选，比如只看高风险或者只看之前忽略过的条目。这样，管理员可以有针对性地处理事件，例如针对低风险事件稍后处理等。在右侧，管理员可以根据来源IP、主机、日期、风险等级、事件类别等进行详细筛选，以便更为精确地搜索到想要的事件。

将鼠标放置在标蓝的IP、主机或事件上面，就会出现有关该对象的详细信息卡片，以便管理员快速预览该对象的具体内容。同时，若点击标蓝的内容，则会跳转到该对象的详细说明页面，里面会详细列出该对象的具体属性，以及曾经与哪些事件有关。

威胁条目右上角有一部分按钮，它们的功能包含屏蔽、删除和查看等，能供管理员快速操作使用。而点击威胁事件本身，则会跳转到威胁事件的详细页面，会列出威胁的来源、相关属性、原始日志等内容，以便管理员综合评判。

2.2.3 入侵威胁模块

使用左侧的导航条可以跳转到入侵威胁模块，可以看到入侵威胁的详细记录。入侵威胁模块与主机威胁模块类似，同样是展示入侵威胁的。不一样的是，这里会将威胁实体按IP进行分

类。这样，哪一个IP攻击次数比较多就一目了然了。

3 安全态势感知系统实现

态势感知系统的实现就是将系统所需要的功能进行设计并完成关键步骤，这是建立在系统的分析以及设计的基础上的。在这个过程中，结合国内现有系统和实际情况，完成了用户主要需求功能的实现。在这里着重讲述态势感知系统在实现过程中的关键性功能模块。

3.1 主机威胁模块

在管理员登录成功后，默认会跳转到主机威胁模块。在主机威胁模块中，可以看到最近的敏感事件信息，例如有人添加了管理员，或者进行了其他敏感操作。在这里，管理员可以对敏感事件进行处理，例如查看详细信息、标记已完成、标记误报或直接删除等。

除此之外，管理员还可以使用右侧的筛选功能，对数据进行详细筛选。例如，可以筛选源IP、源计算机，或者按开始时间和结束时间，或者按威胁类别和等级进行筛选。在输入条件完毕后，点击筛选按钮，列表就会刷新出筛选后的结果。如果想要快速筛选，也可以通过左侧的快速筛选列表，通过状态和威胁级别快速筛选出想要的事件。

主机威胁模块主要是从MongoDB中筛选出所有敏感事件（如果有筛选条件则一并加上筛选条件），通过NoSQL查询主机威胁事件列表。在进行查询的同时，还会查询威胁事件的详细信息。通过点击威胁事件的标题，还可以跳转到详细信息页面。在详细信息页面中，管理员可以看到更为详尽的有关敏感事件的信息，例如用户、用户组、计算机、时间和原始日志等，管理员可以据此做出处理判断。

3.2 入侵威胁模块

管理员可以通过左侧菜单跳转到入侵威胁模块。在入侵威胁模块中，可以看到最近的入侵事件信息，出现在这里的入侵事件更有可能是恶意入侵事件，所以更应该引起管理员的高度关注。通过点击威胁事件的标题，可以跳转到详细信息页面。在详细信息页面中，管理员可以看到更为详尽的有关敏感事件的信息，例如用户、用户组、计算机、时间和原始日志等，管理员可以据此做出处理判断。

入侵威胁模块主要是从MongoDB中筛选出高危敏感事件，通过NoSQL查询主机威胁事件列表。在进行该查询的同时，还会查询威胁事件的详细信息。

3.3 主机监控模块

主机监控模块主要采用Winlogbeat配合Logstash组件一起构成。Winlogbeat组件是一套自动化工具，可以自动读取Windows操作系统日志，并向指定的日志服务器发送消息，用以上传日志信息。通过这种方式，就可以将Windows的日志上传到中心服务器进行处理和分析。

在Winlogbeat配置中，可以设置自动向主控服务器Logstash传输的数据格式和服务器IP地址等信息。由于配置项目比较少，只需要使用默认的配置即可符合要求。如图2所示。

```
winlogbeat.event_logs:
  - name:Security
    event_id: -4662
    ignore_older: 1h

output.logstash:
  hosts: ["192.168.44.101:5044"]
```

图2 Winlogbeat配置文件

3.4 蜜罐模块

从根本意义上来说，蜜罐技术就是一种针对攻击者的防御方法。可以通过设置一些虚假的服务，开放一些虚假的端口，在背后部署一些监控软件。这样，当入侵者尝试侵入这些虚假服务时，就可以猜测他们的想法和目的。这样做，可以让防御者更全面地了解所面临的安全威胁，从而通过技术和管理手段，提高实际系统的安全防护能力。

蜜罐系统类似于信息收集系统，除非是故意吸引黑客的目标。因此，在攻击者入侵后，管理员可以了解攻击者是如何成功入侵的，并快速了解最新的攻击和服务器漏洞的增加情况。系统设计了一个简单的蜜罐账号系统，通过配置蜜罐账号布置蜜罐诱饵，当攻击者以为自己获取了关键账号密码而去登录时，就会在威胁事件中留下痕迹。由此，管理员可立即得知系统被入侵，从而做出快速反应。

蜜罐账号的报警是通过Windows的登录日志检测实现的，通过检索Windows登录日志，如果发现蜜罐账号被登录（蜜罐账号通常不允许被登录），则说明一般就是“并不知情”的黑客尝试登录。通过点击蜜罐威胁活动项目，可以进入查看蜜罐入侵事件的详情，看到入侵历史记录和入侵者来源IP，用以辅助管理员对蜜罐入侵事件进行综合判断和评估分析。

3.5 支持软件

客户端运行环境：操作系统选用微软Windows 10×64；服务器端运行环境：系统运行选用Linux、Unix等；数据库选用MongoDB、Redis和ElasticSearch；其他环境选用Docker和Python等。

4 结束语

这套态势感知平台架构比较复杂，主要由域控代理端和主控端以及管理端构成。通过在域控代理端部署日志监控和上传组件Winlogbeat，可以收集Windows的敏感日志，进而通过主控端上的Logstash配合MongoDB对敏感日志进行查询和分析，明显地增强了Windows日志的实用性和管理员面对网络安全威胁时的可操作性。同时，由于主控端仍然会在ElasticSearch组件中储存日志的原始副本，这样管理员在需要对日志进行复盘时仍然有据可循。在态势感知系统管理端的设计上，主要参考了微软ATA主要功能的布局和实现，做到了系统用户使用的简便性和易操作性，用户不需要通过特殊培训就能进行操作，并且能保障用户信息的安全，同时具备简单和安全性。目前，系统还存在一些不足之处，在后期的使用过程中，将会做出不断的完善和优化。

基金项目：

1.2022年大学生创新训练计划项目“基于深度学习的安全态势感知系统设计与实现”（项目编号：S202213644018）；

2.2022年广西教育厅项目:基于政校企多方协同的网络工程专业应用型人才培养探索与实践（项目编号：2022JGA415）。

参考文献：

[1] 杨凯雪.高校校园网网络安全态势感知研究[J].数字技术与应用,2019,v.37.

[2] 国家互联网应急中心.2020年我国互联网安全威胁报告[EB/OL].2021[2021-01-21].http://www.cert.org.cn

[3] Liu D.Prediction of network security based on DS evidence theory[J]. ETRI Journal, 2020.

[4] 杨怡.基于机器学习的网络安全态势感知[J].计算机科学与应用,2020,10(12):8.

[5] 包利军.基于大数据的网络安全态势感知平台在专网领域的应用[J].信息安全研究,2019.

[6] 陈金木.陈峰.郑少朋.高校计算机网络信息安全问题及其防范措施研究[J].网络空间安全,2023,14（01）.

[7] 靳燕.DDoS攻击特性分析与检测模型构建[J].网路空间安全.2023,14（01）.

作者简介：

莫永华（1978-），男，壮族，广西桂林人，桂林电子科技大学，硕士；桂林信息科技学院，副教授；主要研究方向和关注领域：云计算、网络和信息安全技术。

陈昱希（2003-），女，汉族，浙江温州人，桂林信息科技学院，本科；主要研究方向和关注领域：信息安全和大数据技术。

何淼（2000-），男，汉族，江西南昌人，桂林信息科技学院，本科；主要研究方向和关注领域：网络空间安全和软件开发。

比例原则在网络攻击中的适用困境及路径探索

焦雪晴
（中国人民公安大学，北京100038）

摘要：

［目的/意义］ 比例原则是国际人道法的基本原则之一，在规制网络军事行动、保护平民和民用物体方面起着关键性作用。

［方法/过程］ 比例原则在网络攻击中适用的核心是比例性分析，故应当明确附带性损害、具体与直接的军事利益和“过分”等关键要素的含义。

［结果/结论］ 比例原则在网络攻击中的适用面临两大困境，即网络攻击的内涵和外延不明、难以对对间接损害效果进行合理预期。因此，红十字国际委员会应当发挥作用，主导开展有关国际人道法规则在网络空间中适用的国际合作。

关键词： 比例原则；网络攻击；适用困境；国际合作；网络空间安全

中图分类号： D995 **文献标识码：** A

The application of the principle of proportionality in cyber attacks

Jiao Xueqing
(*People's Public Security University of China, Beijing 100038*)

Abstract:

[Purpose/Significance] The Principle of Proportionality is one of the fundamental principles of IHL and plays a key role in regulating cyber military operations and protecting civilians and civilian objects.

[Method/Process] The key to the application of the Proportionality Principle in cyber attacks is the proportionality analysis, so the meaning of the key elements of collateral damage, concrete and direct military advantage, and excessiveness should be clarified.

[Results/Conclusion] The application of the principle of proportionality in cyber attacks faces two major dilemmas, namely the lack of clarity about the meaning and scope of cyber attacks and the difficulty of making reasonable expectations about the effects of collateral damage. Therefore, the ICRC should play a role in leading international cooperation on the application of the rules of IHL in cyberspace.

Keywords: principle of proportionality;cyber attack;the dilemma in the actual application;international cooperation;cyberspace security

0 引言

比例原则是国际人道法的基本原则之一，指在计划或决定攻击时，应当注意不决定发动任何可能附带使平民生命受损失、平民受伤害、民用物品受损害，或三种情形均有且与预期的具体和直接军事利益相比损害过分的攻击。如果在攻击发动后发现可能出现上述情况，该攻击应予取消或停止。现代国际人道法以条约形式将其规定在《一九四九年八月十二日日内瓦四公约关于保护国际性武装冲突受难者的附加议定书》（以下简称《第一附加议定书》）第57条第2款中。

网络空间技术的发展催生了网络攻击的出现。根据《第一附加议定书》第36条和1996年国际法院《关于使用或威胁使用核武器的合法性问题》的咨询意见，国际人道法的基本原则和规则适用于过去、现在和未来任何形式的武器和战争，日内瓦公约的缔约国有义务对于新的作战武器、手段和方法，使用是否可能违反国际人道法基本原则进行审查。在诸多大规模网络攻击事件后，国际社会认识到，“在未来国家间冲突中使用信息和通信技术的可能性正在日益增加”，必须警惕网络空间成为新的“战场”。红十字国际委员会（International Committee of Red Cross, ICRC）在2019年发布的立场文件中提到，武装冲突中的网络行动，应当同任何其他武器、战争手段和方法的使用一样，受到国际人道法的规制。

目前，国际社会虽然并未就国际人道法的原则、某些规则和制度可以适用于网络攻击达成普遍共识，但是ICRC、联合国专家组、欧盟、北约等都已经认可和支持这一观点，并试图探索相关规则的适用路径。

本文将探讨比例原则在网络攻击中的适用问题，首先分析比例原则在网络攻击语境下的具体内涵，从而引出比例原则在网络攻击中的适用困境和难题，并以问题为导向探索更符合国际社会整体利益的适用路径。

1 网络攻击语境下比例原则的内涵

在网络攻击语境下，比例原则是指网络攻击的指挥者在决定发动网络攻击时，应当注意这一攻击不能造成与该攻击所预期取得的具体和直接的军事利益相比过分的附带性损害，这种附带性损害包括使平民受伤或死亡、计算机系统或网络基础设施等民用物体受损害或两种情形均有；如果在网络攻击启动后才发现该攻击可能造成上述损害，那么指挥者应当立即取消或停止这一攻击。比例原则的含义与具体适用应强调“比例性”，因此在网络攻击语境下对比例原则的理解应着重分析比例性，即所谓“过分”。但是，在分析这一比例性要素时，对于“附带性损害”以及“预期取得的具体和直接的军事利益”，也应当在网络攻击语境下进行一定的解读。

1.1 附带性损害的内涵与范围

附带性损害是指当平民和民用物体并非攻击的预期目标时所附带受到的损害。这表明当谈到“附带性损害”时，就已经默认攻击符合区分原则，所针对的是合法的军事目标。与传统动能攻击所造成的损害大多呈现为直接损害效果不同，网络攻击的损害效果往往是间接的，甚至有第三层或者更多层级的损害后果。因此，在预期网络攻击所可能造成的附带性损害时，应当不仅考虑第一序列的直接损害效果，还应当考虑第二、第三或是更高序列的间接损害效果。但是，应强调间接损害效果的可预期性，否则比例原则的适用将具有不确定性。因此，附带性损害的范围应当包括直接损害效果和可以合理预期的间接损害效果。

1.2 “具体和直接”的军事利益范围

ICRC认为，“具体和直接”的军事利益应当是指那些“实质性”、与攻击行为“有密切联系”的利益，那些“难以感知的”和“需要长时间才得以显现”的利益则不予考虑。故只有那些在特定时间内能够确定预见到的军事利益，才可能被纳入比例性分析，具有模糊性的“推测”就被排除在外。所谓“具体”，应当是指那些真实的或有形、可定义、可量化、有明确证据表明能够取得的军事利益。而所谓“直接”则应当是由攻击本身带来的、与攻击存在明确因果关系的军事利益。从明确性上看，对预期能够取得的军事

利益的“具体和直接”的要求，比对附带性损害“可预期性”的要求更高，这也体现了国际人道法保护平民和民用物体的宗旨。网络攻击一般会通过恶意软件、病毒等进行，而这些软件和病毒的设计与编码都是以被预期能够发挥的作用为导向进行的，故在不考虑意外和突发情况的条件下，网络攻击本身所能取得的效果具有确定性，所预期能取得的军事利益一般均能满足“具体和明确”要求。

1.3 “过分”的内涵与尺度

从定义上看，比例原则本身并非禁止造成任何损害，只是禁止造成与预期取得的具体和直接军事利益相比“过分”的损害，故“过分”这一程度要求是判断某一攻击行为是否违反比例原则的核心。“过分”与否的认定，基于攻击指挥者对所掌握的战场实际情况所进行的“诚实且合理”的判断，以及其后对攻击所预计取得的军事利益和攻击，可能造成的附带性损害进行的合理平衡，其依赖指挥者的自由裁量。但是，这种裁量并非没有边界，“过分”的相对性并不能作为发动造成大量附带性损害，同时也能取得大量军事利益攻击的理由，“偶然的附带性损害绝不能是大量的”。

在网络攻击中，用以实施攻击的恶意软件或病毒，一经运行便能取得较大的军事利益，但是这类软件或病毒一旦不受控地进入军事目标之外的民用计算机系统，便也会造成较大的附带性损害。这种情况一旦发生，即使在形式上符合比例原则的要求，造成的附带性损害与预期将取得的具体和直接的军事利益相比并不过分，但是在实质上却对民用计算机系统和网络基础设施造成了严重的损害，违反了国际人道法对平民和民用物体提供保护的宗旨。然而，《网络行动国际法塔林手册2.0版》（以下简称《塔林手册2.0版》）专家组的大多数专家，仍然主张如果预期的具体和直接的军事利益足够大，那么大范围的附带性损害仍然合法，对“过分”外部界限的要求尚未达成国际共识。

2 网络攻击下比例原则的适用困境

比例原则在网络攻击中的适用主要面临下两个最主要的困境：第一，世界范围内对于“网络攻击”的内涵与外延并未形成定论，这将导致比例原则的适用范围具有不确定性，也可能导致各国家或行为体对网络攻击的内涵和外延，进行肆意解释从而规避比例原则的适用；第二，受网络环境特性的影响，间接损害效果难以得到合理预期，由此可能导致比例性分析难以进行，从而导致比例原则难以得到有效适用。

2.1 “网络攻击”的内涵和外延不明

ICRC认为，为平民和民用物体提供一般保护的区分原则、比例原则以及预防措施原则，只适用于构成国际人道法所规定的“攻击”军事行动，故“攻击”的内涵和外延就成为了比例原则能在多大程度上得到适用的决定性因素。

比例原则在网络攻击中适用的第一重困境就是“网络攻击”的内涵和外延不明。根据《第一附加议定书》的规定，“攻击”是指在进攻和防御中针对敌人的暴力行为，“暴力”既可指暴力的作战手段，也可以指暴力的行动后果。网络行动主要是通过计算机系统开展，手段显然不具有暴力性，故网络行动的损害结果是否具有暴力性，就成为了判断某一网络行动是否构成网络攻击的关键。

网络行动的损害结果可以根据对象的不同分为对平民造成的损害和对民用物体造成的损害。网络行动能够对平民造成的损害与传统动能战争无异，即受伤或死亡，故认定对平民造成损害的暴力性时，完全可以沿用传统动能战争的标准，关注平民受伤或死亡的严重程度。

对于民用物体来说，网络行动对民用物体造成的损害，主要体现在对民用计算机系统和网络基础设施等的损害上，这种损害的表现形式不同于传统动能战争，国际社会对于网络行动对民用计算机系统和网络基础设施造成损害的暴力性认定标准存在不同看法。

第一类观点为“动能等效标准”，即只有当网络军事行动产生了和动能武器效果相当的暴力

后果时，才能被认定为网络攻击。根据《第一附加议定书》第57条的规定，传统动能攻击所造成的损害是指“平民生命受损失、平民受伤害、民用物品受损害或三种情形均有”，强调物理性的损害结果，故其具有较强的可操作性。《塔林手册2.0版》即采取这一标准，认为网络攻击是“可合理预见的会导致人员伤亡或物体损毁的网络行动”。

尽管这一标准获得了《塔林手册2.0版》大多数专家的肯定，但其仍有很大的局限性。网络军事行动的目标主要是计算机系统以及网络基础设施，故其所可能造成的损害与传统动能军事行动大不相同，许多网络攻击并不会造成物理性的损害结果。例如，病毒或恶意软件可能会导致电力系统瘫痪而并不损害电力基础设施的物理外观或部件，但若仅以未造成物理性损害为由而不将该网络军事行动认定为攻击，这显然是荒谬的，因为此时电力系统尽管物理状态完好但确已无法发挥效用。

因此，纵使动能等效标准可操作性强，并不符合网络军事行动的特性，对“攻击”的狭义理解也会导致只有极少数的网络行动能够被认定为网络攻击，区分原则、比例原则等原则和规则很难得到适用，不利于对平民和民用物体提供一般保护。

第二类观点为“功能性标准”，即只要网络军事行动造成了计算机系统或网络基础设施在功能方面的损害或失去效用，从而使其不能实现预期目的或功能，即可被认定为网络攻击。网络军事行动对于计算机系统造成的功能性损害就是使系统瘫痪从而无法运行并发挥功能，但网络军事行动干扰网络基础设施的功能是否可认定为构成功能性损害则存在分歧。有观点认为，网络基础设施失去可用性即可被认定为造成功能性损害；另有观点认为，只有当这种对功能的干扰需要通过更换网络基础设施的物理组件的方式来加以恢复时，才能被认定为构成功能性损害，但这种观点仍强调物理损害的必要性，与动能等效标准在实质上无异。

功能性标准强调功能上的损害而不要求物理损害，更符合网络军事行动的特性。因为网络军事行动特有的网站瘫痪、网络基础设施因恶意软件或病毒的影响而无法使用甚至报废等损害结果，都是传统动能战争所造成的损害结果无法覆盖的。因此，虽然究竟如何认定“可用性”等具体问题尚待商榷，但相比于动能等效标准，功能性标准在网络行动中能够对平民和民用物体提供更高程度的保护，也更有利于网络空间适用国际人道法时，在军事必要和人道原则间找到平衡。

网络攻击的内涵和外延对于比例原则等国际人道法基本原则，能否得以适用以及由此决定的国际人道法在网络空间对平民和民用物体的保护力度至关重要。纵使学理分析认为功能性标准更为合理，ICRC也同意“无论是通过动能手段还是网络手段，以使计算机或计算机网络失效为目的的军事行动构成国际人道法规定的攻击”。但是，这一观点仅反映在ICRC立场文件中，国际社会目前对于应如何认定网络攻击并没有形成定论，比例原则在网络攻击中的可适用性，可能会因各国家或行为体对“网络攻击”的认定标准不同而具有不确定性。

2.2 对间接损害效果难以进行合理预期

在上文分析中提到，只有可被合理预期的间接损害效果才能被纳入比例性分析，否则比例原则将难以得到适用。然而，对间接损害效果的合理预期，会受到网络空间技术普遍存在的军民两用性和网络环境固有的复杂多变性的桎梏。

一方面，间接损害效果具有发散性和延迟性。网络技术在应用中又呈现出较高的军民两用性，故网络攻击所可能造成的附带性间接损害效果的不确定性进一步提高。网络空间具有互联互通性，计算机系统和网络基础设施都具有较高的军民两用性。因此，恶意软件或病毒的准确性、所攻击的军民两用系统或基础设施的具体性质和民用化程度、网络环境、网络战斗员的技术水平、军用和民用系统之间“隔离带”的坚固程度等因素，都会影响民用计算机系统和网络基础设施受到附带性间接损害的程度。

由于间接损害效果固有的发散性与延迟性，网络攻击所使用的恶意软件或病毒，可能通过各种网络间的虚拟或物理通道传输并在民用网络中扩散，从而造成难以合理预期的、具有较高不确定性的附带性损害。

另一方面，网络环境的复杂多变性导致对间接损害效果进行合理预期的难度更高，进而存在

造成与预期取得的具体和直接的军事利益相比“过分”的，难以预期的附带性损害的可能。网络环境会因为协议、域名、系统连接、地域、网络结构等变化而发生改变，在这样的背景下，网络攻击的指挥者等，将更难以对间接损害效果进行具有确定性和全面性的合理预期。

因此，在发动网络攻击之前，相关人员可能很难预期到某些网络环境的突变从而在攻击中造成“过分”的附带性损害，而这种难以预期的附带性损害并不能被纳入比例性分析。因此，网络环境的复杂多变性，使网络攻击的指挥者对网络攻击所造成的附带性损害进行合理预期的难度较大，甚至由此导致比例原则的实际适用空间被压缩，无法发挥保护平民和民用物体的作用。

3 比例原则的网络空间适用路径探索

国际社会目前并未就国际人道法规则在网络攻击中的具体适用模式达成普遍的国际共识。由北约主导形成的《塔林手册2.0版》虽然对条约以及具有习惯国际法地位的实然法，如何适用于网络空间进行了解释和发展，在网络空间治理规则缺位的现实条件下，能够起到一定的参考和指引作用，然而本身并不具有国际法上的约束力，且在政治立场上首要反映西方国家的立场和关切，其本质亦是国家间在网络空间规则制定方面的博弈。

国际人道法规则在网络空间的发展和适用，事关对平民以及民用物体的保护。虽然网络空间目前尚未发生“珍珠港事件”，但是在各国已然意识到网络空间技术的滥用对国际和平与安全造成威胁的前提下，在网络空间开展国际合作以明确国际人道法相关原则、规则和制度在网络空间中的适用范式，并达成尽可能更广泛的国际共识具有必要性，开展网络空间的国际合作对于构建和谐、安全、开放的网络空间治理体系有着十分重要的作用。

必须申明的是，倡导以网络空间国际合作的形式，明确并完善了国际人道法在网络攻击甚至网络武装冲突中的具体适用规则，但并不意味着对网络空间军事化的鼓励和认同，更并不会为恶意网络行动赋予合法性。恰恰相反，以网络空间国际合作方式明确这些规则的适用范式，是为了最大程度减轻法律规则固有的滞后性，对未来网络攻击和网络武装冲突的受难者不利影响，更好地体现国际人道法保护平民和民用物体的宗旨。

3.1 ICRC主导网络空间IHL适用国际合作

ICRC成为国际人道法规则在网络空间适用方面的国际合作的主导者，兼具身份优势和平台优势。

首先，ICRC主导这一合作具有更强的身份优势。理论上，在网络空间技术飞速发展的背景下，ICRC和联合国均关注国际法现有规则是否以及如何适用于网络空间的问题，联合国大会通过联合国信息安全政府专家组（United Nations Group of Governmental Experts on Information Security，UNGEE）和开放性工作组（UN Open-Ended Working Group, OEWG）这一“双轨并行”的框架，推进国际法在网络空间的适用问题，其中包括国际人道法规则。

ICRC一直致力于敦促各国政府修订国际人道法，来应对作战方法和手段的现代化发展，鼓励世界各国就国际人道法的原则和有关规则如何适用于武装冲突中的网络行动达成共识，以应对网络空间的互联互通性与数字性，为解释国际人道法相关术语和作战规则所带来的挑战。故相比于联合国，ICRC在国际人道法规则适用方面更具有专门性。

其次，ICRC主导这一合作具有一定的平台优势。ICRC受联合国大会的长期邀请参加联大会议和工作，并有常驻联合国总部的办事处。在2019年11月28日发表的《国际人道法与武装冲突中的网络行动——红十字国际委员会立场文件》（以下简称《立场文件》）中，ICRC呼吁各国和国际组织在UNGEE和OEWG的框架内，对国际人道法规则在网络行动中如何适用以及现有规则是否完善进行政府间讨论。

综上，应当由ICRC主导包括比例原则在内的国际人道法规则适用方面的网络空间国际合作从而促进国际社会形成有关规则解释与适用方面的普遍共识的达成，以解决比例原则等国际人道法规则在网络空间的适用困境与难题。

3.2 协商确定相关IHL术语和适用规则

ICRC已经意识到，目前在网络空间中的专业术语一直缺乏明确性，故呼吁各国致力于形成一部“关于网络军事行动的共享辞典”。因此，ICRC可以在联合国大会上利用UNGEE和OEWG的平台，提出初步构想和内容框架以供各国协商、沟通和交流，呼吁各国家和国际组织尽快就国际人道法相关规则在网络空间的适用达成共识。

在内容上，这一共享辞典不仅应当包括网络空间的技术性术语，还应当包括国际人道法中的相关术语和规则在网络空间中的内涵与适用范式等。

在形式上，这一共享辞典可以以日内瓦公约及其附加议定书的官方解释文本形式呈现，对比例原则、区分原则等关键规则的适用不允许提出保留。如此形式既可以避免国际人道法规则适用于网络军事行动时超出原有的规则框架，又能够在技术更新发展需要时，对有关规则进行增补、修改时更为简单、快捷。

对于比例原则，该辞典应当对诸项问题做出回应和解释：首先，网络军事行动是否构成网络攻击的标准如何确定；其次，如何对网络攻击的间接损害效果进行合理预期，从而保证比例性分析的确定性；最后，“过分”是否应当有明确的外部边界，能否允许那些预期取得足够大的具体和直接的军事利益但也造成大范围附带性损害的攻击。各国和国际组织在上述问题上的国际合作与共识的缺位，直接导致了比例原则在适用上的模糊性困境，如不能对上述问题进行明确界定，适用比例原则进行比例性分析将沦为一纸空谈，在网络军事行动中通过比例原则保护平民和民用物体的目标将难以实现。

4 结束语

网络空间并不是法外之地，作为新型作战方法和手段的网络攻击，必须受到国际人道法规则的约束。比例原则理解和适用的核心是比例性分析的进行，即确保没有造成“过分”的附带性损害。

在网络空间中，比例原则的适用面临两大困境：一是国际社会并未对网络攻击的概念达成共识；二是难以对网络攻击可能造成的附带性间接损害进行合理预期。为了确保比例原则等国际人道法规则能够在网络攻击中实际适用，应当由ICRC发挥主导作用，就国际人道法规则在网络空间的适用等问题，呼吁各国家和国际组织开展国际合作，以条约官方解释文件的形式，明确网络军事行动的技术性术语和规则性术语的具体内涵，为国际人道法规则在网络空间的适用奠定制度基础。

应当再次重申的是，鼓励开展网络空间国际合作以明确国际人道法在武装冲突中的网络行动，以及网络攻击中的具体适用规则，并不意味着鼓励网络空间的军事化，也不能证明网络战争的合法性，而是为了能够确保国际人道法规则，能够适应现代新型作战技术和作战手段发展的需要，在作战手段和方法不断创新和发展的过程中，更好地为平民和民用物体提供保护。网络空间安全的实现，离不开网络空间国际法治。网络空间国际法治的实现，需要世界各国以及国际组织的积极协商与合作。ICRC应当积极发挥作用，爱好和平的国家与人民也义不容辞。

参考文献：

[1] 朱文奇.何谓“国际人道法”[J].武大国际法评论,2003(00).

[2] Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons,ICJ Report,July 8,1996.

[3] Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report, A/AC.290/2021/CRP.2, 2021.

[4] 郎平.互联网如何改变国际关系[J].国际政治科学,2021,6(02):90-121.

[5] International Humanitarian Law and Cyber Operations during Armed Conflicts, ICRC Position Paper, November 2019.

[6] 郭小伟.新时代总体国家安全观中信息安全的法理基础[J].网络空间安全,2021,12(Z4):1-7.

[7] 洛朗·吉塞勒,蒂尔曼·罗登霍伊泽,克努特·德曼.二十年回顾：国际人道法与武装冲突中保护平民免受网络行动影响的工作[C].2021.

[8] 黄志雄,应瑶慧.论区分原则在网络武装冲突中的适用——兼评《塔林手册2.0版》相关内容[J].云南民族大学学（哲学社会科学版）2019,36(05):135-149.

[10] Additional Protocols 1987 Commentary, ICRC.

[11] International Expert Meeting Report: The Principle of Proportionality, ICRC, 2016

[12] 迈克尔·施密特.网络行动国际法塔林手册2.0版[M].社会科学文献出版社, 2017.

[13] Eric Talbot Jensen, Cyber Attacks. Proportionality and Precautions in Attack[J]. International Law Studies Series, US Naval War College,89, 198 (2013).

[14] 迈克尔·施密特,朱利江.重新布线的战争：有关网络攻击之法律的再思考[C].2016:97-116.

[15] 人道的力量——第32届红十字与红新月国际大会报告：国际人道法及其在当代武装冲突中面临的挑战[R].2015:37-56.

[16] 黄志雄.网络空间国际规则制定的新趋向——基于《塔林手册2.0版》的考察[J].厦门大学学报（哲学社会科学版）,2018(01):1-11.

[17] 屈冠群.网络空间治理国际合作面临的难题及其应对策略[J].科技传播,2019,11(11):125-126.

[18] Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts, The ICRC Report, 2021.

[19] 国际人道法与武装冲突期间的网络行动[C].红十字国际委员会,2021:2-14.

[20] Eric Talbot Jensen.Cyber Warfare and Precautions against the Effects of Attacks[J]. Texas Law Review, 2010, 88(7), 1533-1570.

[21] Hensey A.Fenton II.,Proportionality and Its Applicability in the Realm of Cyber-Attacks[J].Duke Journal of Comparative and International Law,2019, 29(2), 335-359.

[22] 王赫.总体国家安全观下关键信息基础设施安全研究[J].网络空间安全,2022,13(06):1-6.

作者简介：

焦雪晴（1999-），**女，汉族，山东淄博人，中国人民公安大学法学院，在读硕士；主要研究方向和关注领域：国际公法学、网络法学和网络安全。**

（上接第28页）

通信技术与政策,2021,47(09):65-71.

[5] 曲忠芳,李正豪.个人信息保护上了“安全锁” 企业合规面临大考[N].中国经营报,2021-08-30(C01).

[6] 中华人民共和国个人信息保护法[N].人民日报,2021-08-23(014).

[7] 王磊.大数据视域下个人信息民法保护研究[D].哈尔滨:黑龙江大学,2022.

[8] 戴聪.基于国密算法和模糊提取的多因素身份认证方案[J].计算机应用,2021,41(S2):139-145.

[9] 张德强.浅析智慧城市建设中个人信息的保护[J].网络安全技术与应用,2023,No.268(04):111-113.

作者简介：

张德强（1977-），**男，汉族，重庆人，东北石油大学，本科；成都市住房和城乡建设信息档案中心，高级工程师；主要研究方向和关注领域：信息系统建设、网络与信息安全、数据安全治理。**

基于PDCERF的高校校园信息系统漏洞处置实践

张毅
（广东医科大学，广东湛江 524023）

摘要：

［目的/意义］ 近年来，高校校园信息系统受到漏洞攻击导致瘫痪的安全事件时有发生，为降低漏洞带来的安全风险，探寻问题的有效解决措施，保障校园信息系统安全运行。

［方法/过程］ 将PDCERF方法学运用在日常对高校校园信息系统的漏洞处置工作中，通过理顺漏洞处置的阶段、顺序和流程等完成漏洞处理。

［结果/结论］ 经过实践应用，形成了规范合理的漏洞处置机制，降低了高校校园信息系统安全风险，提升了高校校园网的安全管理水平。

关键词： 网络安全；PDCERF方法学；高校；信息系统；漏洞处置

中图分类号： TP393 **文献标识码：** A

Vulnerability disposal of university campus information system based on PDCERF methodology

Zhang Yi
(*Guangdong Medical University, Guangdong Zhanjiang 524023*)

Abstract:

[Purpose/Significance] In recent years, the campus information system of colleges and universities is attacked by loopholes resulting in the paralysis of security events happen from time to time. In order to reduce the security risks brought by loopholes, to explore effective solutions to the problem, to ensure the safe operation of campus information system.

[Method/Process] This paper discusses the application of PDCERF methodology in the daily vulnerability disposal of campus information system, and completes the vulnerability disposal by straightening out the stage, sequence and process of vulnerability disposal.

[Results/Conclusion] Through the practical application in the school, a standardized and reasonable vulnerability disposal mechanism has been formed, which reduces the security risks of campus information system and improves the security management level of campus network.

Keywords: network security;PDCERF methodology;university;information system;vulnerability disposal

0 引言

近年来，网络安全漏洞威胁持续加剧，高校校园信息系统受到漏洞攻击导致瘫痪的安全事件时有发生。如何降低漏洞带来的安全风险，保障校园信息系统安全运行，已经成为高校网络管理人员迫切要解决的重要问题。

为了有效地提升高校校园信息系统的安全性，将广为接受的PDCERF方法学运用在日常对校园信息系统的漏洞处置工作中。通过建立漏洞响应处置机制，理顺漏洞处置的阶段、顺序和流程，协调各方人员合作完成漏洞处理，从而提升校园信息系统的安全防护能力，防止因漏洞而造成的安全隐患。

1 网络安全漏洞

网络安全漏洞是指信息系统在设计、实现、运维等过程中产生的某类问题或缺陷，使攻击者能够在未授权的情况下访问或破坏系统，对系统的安全（机密性、完整性和可用性）造成不利影响。如果漏洞造成敏感信息泄露，就会导致系统的机密性被破坏；如果使系统中的信息被非法篡改，就会导致系统的完整性被破坏；如果使服务器的进程崩溃，就会导致系统可用性的丧失[1]。

常见的网络安全漏洞类型包括操作系统类（Windows主机、类Unix主机、云平台、虚拟化、国产操作系统、Apple类等）、网络设备类（路由器、交换机、防火墙等）、应用程序类（Web服务组件、中间件、API漏洞、开源组件类、容器类、信息类等）、数据库类（Oracle、SQLServer、MySQL等）、弱口令类等。基于漏洞的触发攻击包括缓冲区错误、跨站脚本、操作系统命令注入、参数注入、代码注入、SQL注入、路径遍历、跨站请求伪造、权限许可和访问控制不当、默认配置错误、信息失窃泄露等问题。漏洞对信息系统的危害极大，可被不法者安装恶意程序、传播病毒以及植入木马，导致信息系统受攻击瘫痪，或者导致重要的数据和信息被窃取，严重者会导致操作系统被破坏，信息系统数据全部丢失，给学校带来不可挽回的损失。

2 PDCERF方法学的应用

PDCERF方法学最早是由1987年美国宾夕法尼亚匹兹堡软件工程研究所在关于应急响应的邀请工作会议上提出。它将应急响应分成准备（Preparation）、检测（Detection）、抑制（Containment）、根除（Eradication）、恢复（Recovery）、跟踪（Follow-up）等6个阶段的工作；按照网络安全应急响应总体策略来对每个阶段定义适当的目的，明确事件响应的顺序和过程，使得能快速、科学、合理和有序地处置网络安全事件。PDCERF方法学有助于网络管理者在事件发生前做好各种可能的准备，以及在事件发生后采取有效措施，减少损失并尽快恢复正常运行[2]。

PDCERF方法学如图1所示。

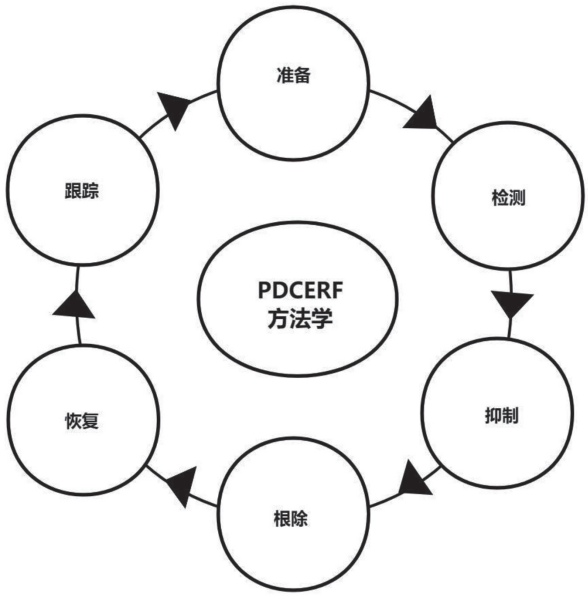

图1 PDCERF方法学

2.1 准备

准备阶段是在信息系统漏洞未出现或攻击未发生前尽可能做好各种准备。

首先，梳理出所有信息系统的情况总清单，掌握信息系统（网站名、网址、IP地址、开放端口）、中间件、数据库、主机操作系统等相关软件的部署情况，以及信息系统的业务描述、服务范围（校内、校外、教工、学生、全体师生）、备案定级等信息，并根据信息系统的重要性、应用范

围、影响程度评估其安全漏洞风险等级。

Ⅰ级：可能造成面向校外互联网访问的信息系统运行受到重大影响或者数据丢失、被窃取、被篡改的，4小时处理完毕。

Ⅱ级：可能造成校内使用、服务全体师生的信息系统运行受到重大影响或者数据丢失、被窃取、被篡改的，8小时处理完毕。

Ⅲ级：可能造成校内使用、仅服务教工或学生的信息系统运行受到重大影响或者数据丢失、被窃取、被篡改的，12小时处理完毕。

Ⅳ级：除上述情形外，对信息系统运行构成一定威胁、造成一定影响的，24小时处理完毕[3]。

其次，明确相关人员及其联系方式，包括信息系统所属单位责任人及联系人、信息系统开发公司联系人及技术人员、安全运维人员、安全处置公司联系人和技术人员等。

再者，根据信息系统风险等级情况和人员安排制定漏洞处置顺序和程序，选定漏洞扫描工具、设置漏洞扫描策略、扫描时间周期、漏洞处理方式和事件响应流程等。

2.2 检测

检测阶段是由安全运维人员运用技术手段，主动对信息系统开展漏洞检测。一般通过漏洞检测工具进行，检测工具通过扫描、弱口令猜测、漏洞验证等手段，对信息系统的安全脆弱性进行检测和发现可利用的漏洞，具有速度快、漏洞情报库实时更新、检测项覆盖广和检测成本低的特点。安全运维人员设置好要检测的信息系统并在工具中选用合适的扫描策略执行。其中的策略主要包括常规安全扫描、完全扫描、Windows主机扫描、类Unix主机扫描、中高危漏洞扫描、Web服务组件扫描、云平台漏洞扫描、数据库扫描、中间件扫描、大数据相关漏洞扫描、病毒相关漏洞和后门扫描、方程式黑客工具相关漏洞扫描等，扫描周期一般为2个月一次[4]。

漏洞扫描工具扫描策略如图2所示。

漏洞检测工具执行完成后会生成信息系统漏洞扫描情况报表，安全运维人员从中筛选出存在“高危漏洞”“中危漏洞”“信息类漏洞”等的信息系统与学校信息系统总清单比对整理，按风险等级程度排序，形成本次信息系统漏洞扫描报告。

漏洞扫描工具扫描执行结果如图3所示。

安全运维人员及时将有问题的信息系统向信息系统单位责任人通报，涉及Ⅰ级、Ⅱ级信息系统的还要上报学校相关部门，并与所属单位、公司等相关人员沟通研判，确认漏洞是否存在、是否已被利用及威胁的程度，评估漏洞对信息系统的影响程度、覆盖范围、处理的优先次序和应采取什么样的处置措施等。

2.3 抑制

抑制阶段主要是要限制漏洞影响信息系统（主机操作系统、数据库、中间件、应用组件等）的范围和恶化的趋势，防止出现扩散和突发攻击事件，主要包括拒绝服务攻击、僵尸木马蠕虫爆发传播、域名安全事件、数据泄露和网站遭恶意篡改等。具体处理是按照安全漏洞风险等级（Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级）依次对存在问题的信息系统，按不同时限要求采取相应的处置措施降低影响范围，包括且不限于断网隔离、网络封堵、收缩安全防护策略、关闭主机、关闭信息系统和关闭涉及的服务等[5]。

2.4 根除

根除阶段是通过分析漏洞找出问题根源，查明漏洞的危害方式，确定漏洞修复优先级，制定解决方案并彻底修复，以避免攻击者利用漏洞攻击系统，引发安全事件。处置措施包括且不限于软件升级、密码重置、病毒木马清除、补丁修复加固、限制系统（网络隔离、行为管理等）、升级安全设备和完善安全策略等。为了防止漏洞修复对信息系统可能造成影响，漏洞修复时应选在非业务高峰期，除安全运维人员外，信息系统所属单位联系人、公司技术人员等应全程共同参与，做好详细记录，必要时还需有专业的安全处置公司技术人员配合支持，保障漏洞修复完成。

2.5 恢复

恢复阶段的过程是把受影响系统、主机设

图2 漏洞扫描工具扫描策略

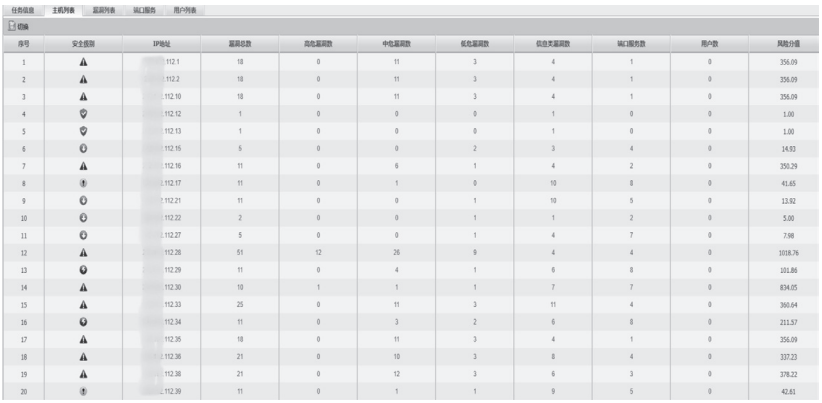

图3 漏洞扫描工具扫描执行结果

备、软件和应用服务还原到正常的工作状态。首先是评估漏洞修复后的信息系统数据是否丢失被破坏、应用服务是否正常、确定使系统恢复正常的需求和时间表，接着采取相应的技术手段将被破坏的信息彻底地还原到正常运作状态，主要包括系统恢复、网络恢复、用户恢复、数据恢复、重新部署和系统全面安全加固等，最后观察确认信息系统业务恢复正常。

2.6 跟踪

跟踪阶段是对信息系统的漏洞情况进行复查验证，确认漏洞处置已完成，并向相关单位、部门报告处置情况。同时，回顾和整理本次处理安全漏洞的类型、影响范围、处置时间、检测方法、抑制方法、根除方法、恢复情况等相关信息，分析存在问题、经验教训、改进措施等形成总结报告，并据此对前面准备阶段的信息系统清单、安全漏洞风险等级、安全漏洞处置程序等做更进一步的修改完善，以促进下次信息系统安全漏洞处置更好的开展[6]。

3 实践成效

就广东医科大学信息化建设而言，经过二十多年的快速发展，校园信息系统部署超过300个，

为全校2万多名师生提供了网站群、网办、邮箱、教务、OA办公、精品课程、教学在线等种类丰富的线上服务，已成为师生日常教学、办公、生活不可或缺的工具，安全性也越来越受到重视。为此，学校借鉴PDCERF方法学中定义各个阶段明确任务、顺序和过程的指导思想，将日常对校园信息系统的安全漏洞处置过程按阶段进行合理划分，并运用在每一次对信息系统安全漏洞的处置当中，取得了一定的成效。通过各阶段循环的积累完善，形成了规范性的防护工作处置机制，使得校园网络管理人员能持续掌握信息系统安全状况，化被动响应为主动发现，及时处理问题，有效地降低校园信息系统安全风险，提高了校园网安全管理水平。

4 结束语

高校校园信息系统的安全漏洞处置是网络安全事件响应的重要部分，PDCERF方法学的运用只是规范了漏洞处置的流程，不能确保处置成功。为了缓解和降低漏洞攻击的危害，在日常运维中还应做好及时更新补丁、升级系统软件、合理配置系统访问权限、信息系统的实时备份与快速恢复、加强安全设备部署和策略优化、强化网络安全实时监测、定期开展网络安全渗透测试与应急演练、定期组织网络安全培训等工作。

参考文献：

[1] 顾绵雪,孙鸿宇,韩丹,等.基于深度学习的软件安全漏洞挖掘[J].计算机研究与发展,2021,58(10):2140-2162.

[2] 段海新.计算机网络安全的应急响应[J].电信技术,2002,12:10.

[3] 查德平,季千惠,赵泽宇.高校网络安全漏洞治理探索与实践[J].网络空间安全,2022,12(01):47-54.

[4] 张昊贺,江敏,屈晔.网络安全漏洞检测技术研究及应用[J].网络空间安全,2020,11(09):84-89.

[5] 刘俊芳,谷利国,陈存田,等.网络设备漏洞及防范措施[J].网络安全技术与应用,2023,(03):20-22.

[6] 冯涛.网络安全事件应急响应联动系统研究[D].西安:西安电子科技大学,2004,(03):7-11.

作者简介：

张毅（1976-），**男**，**汉族**，**广东阳江人**，**华南理工大学**，**硕士**；**广东医科大学教育技术与信息中心**，**高级工程师**；**主要研究方向和关注领域**：**校园网管理和网络信息安全**。

智能化医疗业务的信息安全管理策略研究

黄文犀
（百色市人民医院，广西百色533000）

摘要：

［目的/意义］提高医院医疗数据信息、业务信息的安全防护水平，建立医疗业务信息安全管理系统。

［方法/过程］在Windows2008服务器操作系统支持下，建构涵盖用户访问控制、网络攻击防范、数据完整性保护的智能化医疗信息业务管理系统（Hospital Business Information System，HBIS)。

［结果/结论］对患者挂号、检查预约、医疗分诊和医疗报告等业务数据信息，做出收集、加密传输与安全存储，实现医疗访问用户认证和医疗业务信息的安全管理。

关键词：智能化；医疗信息业务；信息安全管理；系统；网络安全

中图分类号：TP393.0 **文献标识码：**A

Research on information security management strategies for intelligent medical information business

Huang Wenxi
(*Baise People's Hospital, Guangxi Baise 533000*)

Abstract:

[Purpose/Significance] To improve the security protection level of medical data and business information in hospitals, establish a medical business information security management system.

[Method/Process] With the support of the Windows 2008 server operating system, an intelligent medical information business management system (HBIS) covering user access control, network attack prevention, and data integrity protection has been constructed.

[Results/Conclusion] Collect, encrypt, transmit, and securely store business data information such as patient registration, examination appointments, medical triage, and medical reports to achieve medical access user authentication and secure management of medical business information.

Keywords: intelligence;medical information business;information security management;system;network security

0 引言

为了提高医院医疗数据信息、业务信息的安全防护水平，需依托Web服务器、Data Base服务器、Switch核心交换机和Windows2008服务器操作系统等软硬件，建立医疗业务信息安全管理系统，设置基础硬件层、数据采集层、关联挖掘分析层、数据存储层和数据分析运算层等安全管理层级，针对网络安全攻击、报警事件，使用关联规则挖掘技术进行智能化关联规则分析计算，并针对外部用户访问使用网络安全防御拓扑结构进行身份认证，使用数据加密技术和分布文件系统，对采集到的结构化、非结构化医疗业务信息资源，做出加密传输和分布式管理，以便于后台管理系统的任务响应和数据调用。

1 医疗信息、业务的安全管理需求

1.1 用户访问的身份鉴权认证

用户访问认证也被称为身份鉴权认证，是根据外部访问者输入的用户名和密码进行身份验证，防止黑客攻击者冒充正常用户访问系统。医院医疗业务信息安全管理系统的身份鉴权认证，是通常医务人员用户和患者用户的身份识别认证。基于Web服务器的用户名密码认证机制，使用“auth-user-pass /etc/openvpn/server/user.txtauth-nocache”执行命令、“auth-user-pass-verify”验证脚本，用于从环境变量中验证“$1:用户名”和“$2:密码”参数的合法性。结合医院医疗业务信息管理的实际需求，使用Web Server服务器内置的用户验证机制，做出用户名密码中字母、数字、下划线（'_'）、破折号（'-'）、点（'.'）或a（'@'）的字符串数据认证[1]。

1.2 网络攻击安全防范

网络攻击包括外部入侵用户攻击和内部管理人员攻击。对于外部入侵用户攻击的网络安全防范，通常需要利用入侵检测系统，例如借助于Apache Hadoop调度、机器学习、流处理和关联分析等大数据技术，确认非法用户的数据源地址IP、目的地址IP、访问时间和访问端口，掌握网络攻击、安全报警事件的序列模板，通过数字签名和数据序列匹配完成攻击防范。内部网络攻击的安全防范，是针对医院职工和开发/运维人员的非法入侵攻击，采取身份认证和人机交互验证的方式予以防范[2]。

1.3 数据传输和存储安全保护

对于医院医疗病患、挂号、检查预约、医疗分诊和医疗报告等基本信息的安全管理，是数据传输和存储防护的重要方面。特别是面对网络医疗管理系统的海量数据资源，可能会由于外部用户非法攻击、医务人员操作不当，导致输入和传输的病患登记、医疗检查、医疗报告、采集图像和患者随访等信息，出现数据信息泄露、误删和丢失的问题，这就需要采用数据加密和分布式存储技术做出数据安全防护。

1.4 人机交互验证的安全管理

人机交互验证是指对用户输入和系统输出信息的验证流程，在这一过程中，应用系统可能存在着跨站脚本攻击、SQL注入漏洞和文件上传漏洞的问题。外部用户可通过在医疗网站链接中插入恶意代码方式，发起针对医务人员和患者访问的跨站脚本攻击，盗取用户名密码书籍、链接网页信息[3]。在将SQL语句输入至POST接口、URL网页链接请求接口时，可使后台数据库被动执行SQL恶意攻击语句，SQL注入攻击绕过用户登录权限，可直接访问与盗取数据库信息，或者利用网站漏洞上传可执行文件至Web Server服务器端，上传文件中包含病毒、木马和恶意代码等，WebShell执行。因而需要采用用户访问、数据输入/输出的交互验证方式，降低应用系统恶意攻击、高危漏洞的安全风险。

2 智能化医疗业务系统的组成架构

基于大数据挖掘、关联规则分析和分布式存储等技术，可以建构起医疗业务信息安全管理的多层级系统平台。其中，包括基础硬件层、数据

采集层、关联挖掘分析层、数据存储层和数据分析运算层等安全管理层级，各层级间由网络安全防护墙、TCP/IP协议和API接口等形成设备的连接。

2.1 基础硬件层

基础硬件层为医疗信息和业务信息安全管理的底层硬件支持层，由Web服务器、DataBase服务器、数据库、Switch核心交换机和Client PC等硬件组成，负责为医疗业务信息的访问控制、数据资源传输和数据存储提供支持。

2.2 数据采集层

利用爬虫、爬虫引擎、调度器、和下载器等信息爬取组件，批量采集网络医疗平台的病患、挂号、检查预约、医疗分诊、医疗报告等信息，按照医疗业务信息的结构化格式和非结构化格式做出分类。

2.3 关联挖掘分析层

关联挖掘分析层为医疗业务信息的预处理层，通常由大数据挖掘、批处理、流处理、数据加密、身份鉴权认证、关联规则分析等组成模块，不同模块分别负责数据处理、数据加密、用户访问身份认证和安全攻击溯源操作。同时，对某一时间窗口内的静态、动态医疗业务数据信息，分别使用批处理方式和流处理方式进行计算，以便及时响应突发事件的数据处理请求。使用ECC共识算法的认证方式，做出医疗业务信息的密钥生成、加解和解密；使用网络安全防御拓扑结构，进行访问用户的身份鉴权认证；使用关联规则分析技术对已发生的网络安全攻击、报警事件作出判断和溯源，包括多源多点数据传输的深度关联分析，针对不同网络节点的安全隐患提出应对措施。

2.4 数据存储层

数据存储层包含分布式文件系统、关系数据库、NoSQL（Not only SQL，NoSQL）数据库等组成模块，负责将接收到的医疗业务数据日志、数据表结构信息作出分类与存储。按照不同医疗业务信息的类别，利用分布文件系统的去中心化数据存储方案，将病患登记信息、挂号信息、检查预约信息、疗分诊信息、医疗报告信息、采集图像信息、患者随访信息等隐私数据，设置为多个数据块分配至不同的网络节点，识别与剔除可能存在安全隐患的医疗诊疗信息、业务数据集合，将网络安全数据分布存储至NoSQL 分布式数据库、关系数据库之中[4]。

3 医疗业务系统的防护服务功能实现

3.1 用户访问身份认证

网络云计算环境下的医疗用户访问、业务信息传输，通常单位时间内需抓取海量（100GB+）的数据日志，因而应在局域网部署多台核心交换机、Web服务器、DataBase服务器，进行分布式医疗数据信息采集、批量任务处理。首先借助于核心交换机的沙箱检测引擎、沙箱分析模块，抓取局域网内医疗业务信息管理系统的数据流量，使用沙箱分析模块作出Linux文件、Office文档、HTML文件、PDF文件、URL网页链接、Python或Javascript脚本的安全威胁分析，识别危险行为的API接口、数据文件节点，替换或删除包含隐藏木马、恶意病毒的数据文件信息。

随后，依托核心交换机、路由器、Web服务器、WFilter主机（超级嗅探狗）等软硬件，由WFilter网管组件在交换机、路由器中配置“镜像端口”，形成与监控主机之间的“镜像端口”连接，来实现VLAN路由执行命令、用户访问的监控控制。依照网络业务信息安全管理系统的基础硬件层结构，设置Cisco 3550双层交换机2个VLAN路由分别为Vlan1-192.168.0.1/24和Vlan2-192.168. 0.2/24，将与Cisco 3550交换机形成连接的WFilter镜像端口IP地址设置为192.168.1.1和192.168.2.1，并配置网络安全访问的VLAN路由规则，即可完成用户访问身份鉴权、医疗业务信息传输安全管理。

3.2 数据传输加密控制

分布式医疗业务信息传输的去中心化属性，要求对不同网络节点的数据信息做出加密、解密与共享操作，这时采用ECC椭圆曲线加密算法，完成各网络节点数据的非对称加密运算[5]。假定椭圆曲线Ep(a,b)中的点P满足$nP=P_1+P_2+...+P_n=O$，点P的阶数为ord(P)、O为椭圆曲线的无穷远点。随后定义G为椭圆曲线Ep(a,b)的循环子群、P为G的生成元，引入发送明文m对椭圆曲线上的点P编码得到$mP=(x_m, y_m)$。设定G的生成元P阶数为n(n为大素数)的，使用网络加密的私钥k(1<k<n)、公钥Q对明文mP作加密变换，得到加密完成后密文C可表示为C1=kP、C2=Pm+kQ、$C=(C_1,C_2)$。对密文$C=(C_1,C_2)$的解密时，需根据以上私钥k(1<k<n)、公钥Q，计算$C_2-xC_1=P_m+kQ-xkP=P_m+kxP-xkP=P_m$。网络攻击者若要解密计算出明文mP,则必须求取基于椭圆曲线密钥加密的C=(C1,C2)离散对数问题。

3.3 网络攻击安全防范

本文采用卡尔·皮尔逊相关系数，面向海量的外部用户访问、数据信息传输，展开网络安全事件、安全隐患的关联程度计算，通过正相关/负相关分析计算公式反映二者的线性相关强弱程度：

$$Pearson\ r=\frac{\sum_{i=1}^{n}\left(x_i-\bar{x}\right)\left(y_i-\bar{y}\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i-\bar{x}\right)^2\sum_{i=1}^{n}\left(y_i-\bar{y}\right)^2}}$$

其中$X=(x_1,x_2,...,x_i)$、$Y=(y_1,y_2,...,y_i)$分别表示各网络节点的网络安全事件、网络安全隐患数据变量，r > 0、r < 0分别表示两变量存在正相关或负相关，r=0表示两变量不存在相关关系。

特别对于多源网络节点的传输数据关联分析过程中，例如针对Web跨站访问请求、跨站脚本攻击，做出报警事件逻辑关系的正确响应、分析安全威胁，可辅助网络平台开发人员和安全管理人员，及时发现网络安全攻击问题、处理安全报警事件，根据网络安全事件的节点溯源结果采取适宜的多点防护方案。

3.4 数据分类存储实现

HDFS分布式文件系统为主从式结构，包括NameNode、DataNodes和Client等组成构件，分别用于医疗业务元数据信息的分割、存储与访问控制。在文件系统命名空间NameSpace中，将医疗数据文件信息f分为δ和1-δ两部分，δ部分文件采用等份分割方式分为i个子数据块，1-δ部分文件采用交叉分割、存储方式，将多个分割后的子数据块文件缓存至相应网络节点、存储至后台数据库，记录数据文件创建、读取、删除与存储操作执行的目录路径，并由客户端Client控制外部用户访问、DataNode存储交互操作。

4 结束语

医疗业务信息安全管理系统通常针对用户身份鉴权认证、访问控制、数据统计、数据传输保护、日志审计和人机交互验证等功能需求，建立起完善的业务管理、医疗信息管理系统，使用智能化网络拓扑结构、ECC共识算法、关联规则分析技术和分布式文件系统，检测与发现网络节点的高危安全漏洞、数据传输攻击问题，以提升医院医疗业务信息管理的智能化水平。

参考文献：

[1] 张晨.医院信息系统信息安全等级保护的实施探讨[J].电脑知识与技术,2021(32):53-54.

[2] 李铮,魏星,佟明泽,王悦.基于网络安全的医院信息安全设计改造与分析[J].微型电脑应用,2021(03):10-12.

[3] 范翔,陶贤,戴冰.医院信息安全与系统监控管理平台的建设分析[J].信息与电脑（理论版）,2019(19)：202-203.

[4] 陈金木,陈峰,郑少朋.高校计算机网络信息安全问题及其防范措施研究[J].网络空间安全, 2023(1): 85-90.

[5] 魏智.医院虚拟服务器实施管理及网络安全研究[J].网络空间安全, 2022,(02): 58-60.

作者简介：

黄文犀（1988-），**男**，**壮族**，**广西来宾人**，**广西师范学院**，**本科**；**百色市人民医院**，**助理工程师**；**主要研究方向和关注领域**：**医院信息系统应用、信息化和智慧化**。

高校图书馆信息安全防护体系构建研究

王大阜[1]，石宇凯[2]
（1.中国矿业大学，江苏徐州21116；2.诸暨市融媒体中心，浙江诸暨311800）

摘要：

［目的/意义］针对高校图书馆信息系统面临的安全风险，提出可行的安全防护体系，从而实现信息系统全方位的安全防护。

［方法/过程］以高校图书馆信息系统安全为切入点，依据等级保护的要求，从物理安全、网络安全、主机安全、数据安全、安全管理5个维度提出有效的安全防护策略。

［结果/结论］为高校图书馆构建网络安全防护体系提供参考依据，从而有效地提升网络安全保障水平。

关键词：等级保护；信息系统；安全防护；网络安全

中图分类号：G250 **文献标识码：**A

Research on the construction of information security protection system in university library

Wang Dafu[1], Shi Yukai[2]
(*1.China University of Mining and Technogy, Jiangsu Xuzhou 221116; 2. Zhuji Integrated Media Center, Zhejiang Zhuji 311800*)

Abstract:

[Purpose/Significance] In view of the security risks faced by the information system of university library, this paper puts forward a feasible security protection system, so as to realize the all-round security protection of the information system.

[Method/Process] Based on the security of university library information system and the requirements of hierarchical protection, this paper proposes effective security protection strategies from five dimensions of physical security, network security, host security, data security and security management.

[Results/Conclusion] It provides a reference for the construction of network security protection system in university libraries, so as to effectively improve the level of network security.

Keywords: university library; information system; security protection; network security

0 引言

随着高校数字图书馆和智慧图书馆的建设发展，图书馆信息系统的规模逐渐庞大，图书编目、读者借阅等业务数据，以及电子书、期刊、学位论文等数字资源呈爆炸式增长。与此同时，图书馆信息系统面临网络攻击、拒绝服务和病毒传播等各种传统的已知威胁，以及零日漏洞、高级可持续攻击（Advanced Persistent Threat，APT）等未知威胁。在漏洞风险方面，据教育行业漏洞报告平台的数据显示，自2017年2月至2022年11月，某高校发现漏洞总数237个，在全国高校排名第67位[1]。图书馆作为高校重要的知识资源储藏中心，潜在的隐患也不容小觑。以高校图书馆广泛使用的图书管理系统“江苏汇文”为例，国家信息安全漏洞共享平台于2015年6月公布手机联机公共目录检索系统（Online Public Access Catalog，OPAC）存在SQL注入漏洞，允许攻击者获取数据库敏感信息。2014年教育部出台《教育行业信息系统等级保护定级工作指南（试行）》，根据高校图书馆管理系统受到破坏时所侵害客体及侵害程度，判定至少应符合二级等级保护的定级要求。2019年12月1日我国开始实施等级保护2.0标准，为了适应新技术的发展趋势和安全要求，等级保护2.0在等级保护1.0的基础上做了优化和调整，对云计算、物联网、移动物联网和大数据等新领域的保护对象进行了扩展覆盖。

面对如此严峻的网络安全形势和潜在的风险隐患，驱使高校图书馆必须采取有效的应对策略，从而提升网络安全防护水平，为读者用户提供安全和可靠的网络服务。网络安全具有“木桶效应”，任何一个薄弱的环节都会影响整体安全防护效果，图书馆应当全方位地做到总体布局、防患于未然。

1 信息安全防护体系

1.1 物理安全

机房环境条件直接影响服务器和存储及网络设备等硬件设施的运行状态。国家颁布的GB50174～2008《电子信息系统机房设计规范》，对机房的电力、温湿度、电磁防护、防水、防火、防静电和安防等均有详细的规定。其中，供电系统和空调系统是两个最为关键的物理安全要素。为了保障供电系统的稳定性和可靠性，采取双路市电输入、双模块化UPS系统的供电模式。机房要尽量使用精密空调，保证温度控制在23℃±1℃，湿度控制在40%RH～55%RH[2]。机柜采用“背靠背、面对面”的布局结构，同时建立冷热通道，提高机房冷却效果。目前，国内高校都在致力建设绿色节能的数据中心，如何降低数据中心能耗，降低电源使用效率（PUE）值，也是亟需关注的问题。

1.2 网络安全

1.2.1 基础设施

图书馆的关键网络设备（例如核心交换机），一旦出现故障会导致全网瘫痪，为此有必要进行冗余配置，避免形成单点故障。常用的冗余技术手段是采用VRRP协议，结合MSTP生成树协议，避免网络形成环路。当前，交换机虚拟化技术非常流行，例如思科公司的VSS与华为公司的IRF，可以将2台以上的物理设备虚拟成1台可管理设备，更便于网络管理，同时还实现了双活数据交换处理。对于汇聚层和接入层交换机可采用端口聚合技术，与上联设备进行双链路互联，既能增加互联带宽，又能提高设备的冗余性[3]。图书馆的接入层交换机通常采用虚拟局域网（VLAN）技术，将办公PC、电子阅览室、公共检索机和服务器等多个逻辑区域划分不同的VLAN，抑制广播风暴造成的网络拥塞，同时配置三层交换机访问控制ACL，对不同VLAN的服务器之间的通信进行限制。此外，私有VLAN（Private VLAN，PVLAN）采用上下两层VLAN隔离技术，实现同一个VLAN下的所有端口二层隔离，只允许与网关通信，避免同网段中感染病毒或木马计算机，被黑客利用作为跳板，危害其他正常计算机，从而进一步提升接入网络通信安全。

1.2.2 安全防御体系

在传统模式下，数据中心采取的安全架构是在网络边界“串联”部署入侵防御系统、Web应用防火墙和防毒网关等安全设备，有针对性地对攻击行为实现阻断。但是，这种做法的不足是逐一追加设备投资成本高，不同的设备无法实现集中管控。下一代防火墙（NGFW）在传统防火墙的包过滤、NAT和VPN等功能基础上，通过对数据包进行捕获、解析以及特征分析检测[4]，能够有效地防御Web攻击、暴力破解、缓冲区溢出和DDoS等网络层与应用层的攻击行为[5]。中国矿业大学图书馆的网络拓扑，防火墙划分3个隔离区：外网区、DMZ区和内网区。外网区上联图书馆核心交换机，与校园网互联，DMZ区部署诸如OPAC、数据库镜像等信息系统，内网区部署汇文Oracle数据库及采编、流通、检索等业务工作机。此外，通过旁路部署入侵检测系统（IDS），对关键交换机的镜像端口进行抓包分析，判断网络中是否有违反安全策略的行为和遭受攻击的迹象[6]，从而进一步保障网络安全。如图所示。

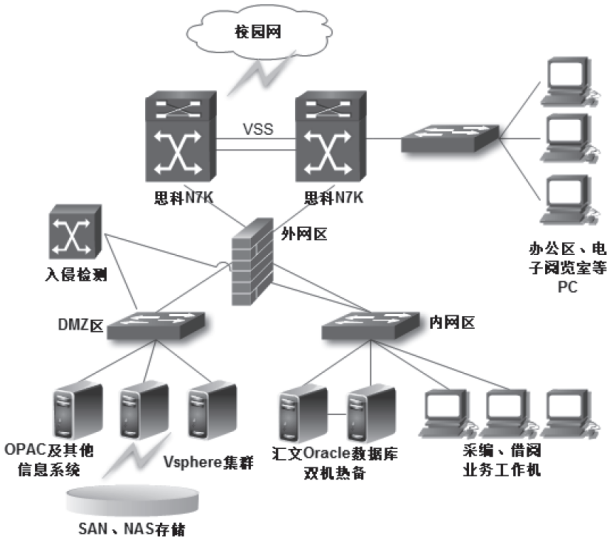

图 中国矿业大学图书馆网络拓扑图

网络态势感知（Cyberspace Situational Awareness,CSA）是安全防护技术体系中进行网络安全预警的新技术，CSA通过大数据分析技术，将网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络的当前状态数据和变化趋势进行提取、理解（评估）、预测、显示。安全态势感知是对系统进行全面的漏洞、篡改、敏感词等监控，并将下一代防火墙、上网行为审计、IDS等安全设备的日志数据进行融合，结合威胁情报、大数据等技术，全方位发现网络空间的安全威胁，同时能与安全设备进行联动，当检测到威胁时给相关安全设备下发阻断访问策略，避免威胁进一步渗透发展。

1.3 主机安全

1.3.1 操作系统安全

Windows操作系统因操作简便而得到多数人的青睐。Linux操作系统因为完全开源，漏洞相对较少，安全性远优于Windows操作系统，因此重要信息系统应尽量选用Linux操作系统。为了降低感染病毒的风险，同时避免产生知识产权法律纠纷，应尽量使用正版化软件。在病毒防范方面，可以采用360公司、火绒公司等网络版杀毒软件进行集中管控。通过本地或云端的控制中心平台对所有服务器进行统一病毒查杀、病毒库升级以及打补丁操作，从宏观上掌握单位病毒感染和漏洞威胁的全貌。在访问限制方面，应按照“最小服务”原则，采用白名单机制只允许开放特定的业务必要端口（例如Web服务的80端口），对于其他无用端口，尤其类似WannaCry勒索病毒传播利用的SMB端口坚决关闭。此外，软硬件供应商的运维工程师仅允许通过堡垒机进行远程访问，一切操作记录要留痕，从而有效地封堵黑客攻击的隐患入口。

1.3.2 应用程序安全

（1）统一平台及身份认证

图书馆的网站包括门户网站和各类专题子网站，以往网站采用开源内容管理系统或自主开发建设，程序的安全性没有保障，而且采用“烟囱式”建设模式，为每个网站独立分配服务器、存储资源，这样会造成资源浪费，维护成本增加。按照统一平台建设原则，图书馆应采用学校统一采购、安全系数高的网站群平台，实现建站、管理和安全防护。此外，诸如各单位用于会议预约和参观预约等业务审批的流程引擎，以及发布学者研

究成果的学者库，均应该通过校级平台统一建设。

图书馆信息系统众多，用户访问每个系统都需要单独登录，这样的体验不友好，而且各个信息系统具有独立的身份认证模块，如果认证强度不够，容易出现弱口令风险。为此，可以考虑将各个系统与学校统一身份认证平台的API接口集成，提高身份认证的安全性。借助单点登录（SSO）功能模块，可以进一步地达到一次认证、多处访问的目的。

（2）合理部署架构

图书馆信息系统可以按照重要程度决定部署模式。以图书馆最为核心的OPAC系统为例，会涉及到针对图书的编目、典藏、流通和检索等重要业务。考虑到“不将鸡蛋放在一个篮子里”，采用解耦方式，将系统的Oracle数据库和OPAC的前端Web服务分离部署。高校读者用户数庞大，为了避免出现高并发访问导致OPAC系统过载，可以通过负载均衡设备将用户的访问请求分流到真实服务器。此外，为了保障系统的高可用性，采用双击热备方式部署，工作机和备用机通过心跳监测各自运行状态，当监测到工作机出现故障时，备用机自动接管工作机的应用服务[7]。

很多高校图书馆出于经济、可靠和安全因素的考虑，将系统迁移至云端，采用软件即服务（SasS）架构模式部署图书管理系统，安全性和稳定性由软件提供商负责。在云计算环境下，图书馆对于软件供应商的信任和监管问题有待探索，鉴于此，国内大部分对安全性需求高图书馆采用公有云和私有云两种混合模式运行[8]。公有云服务商一般提供了服务等级协议（SLA）协议，在公有云服务不可用时间段内，为了不中断读者借阅图书和归还图书等重要服务，则需要定制离线方案。

1.4 数据安全

1.4.1 数据容错与备份

服务器采取RAID磁盘冗余方式保护数据安全，常用的RAID级别有RAID1、RAID5和RAID10。当磁盘发生故障时，采取热备份机制，RAID控制器自动启用热备盘替换故障盘，并在热备盘上进行数据重建。近年来，分布式存储较为流行，分布式存储由多节点集群组成，采取纠删码和多副本技术，允许同时多个节点或磁盘发生故障，相较于传统的集中式存储，读写性能更高，容错级别更高。

RAID、多副本等机制可以解决磁盘或节点硬件故障问题。由于数据一旦因感染病毒或网络攻击遭受损坏是无法恢复的，因此需要采用自动化备份软件对重要系统的整机系统、数据库和文件等各种粒度数据进行选择性地备份。备份策略要考虑恢复点目标（RPO）和恢复时间目标（RTO）两个指标，根据数据重要性、数据量大小、变化频率合理制定备份计划任务，设定备份周期，数据一旦遭受损坏，快速利用备份数据进行恢复。

1.4.2 数据加密保护

高校图书馆信息系统会涉及到个人信息，包括身份证号、手机号码等个人隐私信息，以及图书借阅、预约和检索等用户行为信息[9]。这些个人信息如果以HTTP协议进行明文传输，存在被“嗅探”窃取的隐患，因此应采用HTTPS协议进行数据加密传输，由数字证书认证机构（CA）签发数字证书，客户端和服务器端通过对称和非对称密码机制对数据进行加密、解密。此外，考虑到数据加密带来的计算开销，要以尽可能小的开销实现可靠的数据保密性，同时兼顾了安全和效能。对于不同安全级别的数据可采取分级加密手段，例如对身份证号、手机号码以及特色文献等与作者和资源相关的核心数据，加密强度要高；对于用户行为的重要数据，加密强度可略低。

1.4.3 数据合理收集使用

在智慧图书馆时代，图书馆正在积极探索如何有效搜集和利用用户身份和阅读行为等大数据信息，为读者进行用户画像以实现个性化服务。近年来，我国相继颁布关于网络安全、数据安全、个人信息保护等方面的法律法规，图书馆信息系统或移动APP应以最少侵犯隐私的原则收集信息，并公开收集信息的范围、目的，强化用户对个人信息处理的知情权和决定权[10]。同时，有

力地保障用户个人信息、借阅信息等数据的安全，以避免遭受破坏和泄露，从而在为读者提供服务和尊重、保护读者隐私数据之间找到平衡点。

2 网络安全管理

俗话说“三分技术，七分管理”。网络安全是依靠顶层设计的一把手工程，校领导、馆领导应高度重视，可以从5个方面着手：（1）加强经费的投入，保障网络安全建设工作可持续性开展；（2）加快推进完善的管理制度体系的建立，包括人员管理、资产管理、数据备份和应急预案等；（3）建立信息化与网络安全同步规划、同步建设的机制，落实信息资产全生命周期管理[11]，信息系统确保符合等级保护测评要求；（4）加强应急技术队伍的建设，定期组织开展应急演练；（5）加强对图书馆员工的网络安全培训，提高馆员安全意识和责任素养。

3 结束语

网络安全建设是一项巨大、复杂的系统工程，本研究从5个维度提出了高校图书馆信息安全防护体系架构，在网络安全工作实践中起着重要的指导作用，并证实了体系架构的可行性。随着大数据、云计算、物联网等新兴技术在高校图书馆的应用，鉴于新兴技术的高复杂性、馆员技术水平普遍较弱、安全设备误报率较高等局限，使图书馆网络安全工作面临巨大的挑战，因此说网络安全永远在路上。

做好高校图书馆的网络安全工作，是当代高校图书馆和学校信息化主管部门共同肩负的重要责任，应当以等级保护为抓手，采取管理和技术并重的举措，加强信息安全防护，通过态势感知平台全方位感知图书馆整体安全概况，提升安全监测预警能力和安全处置效率。网络攻击行为检测是网络安全防御的重要基础，网络安全设备采用的硬件配置和底层算法模型的优劣影响着检测的性能和精度，未来可以借助分布式计算架构和深度学习先进技术进行优化，以满足高效攻击行为检测，满足降低漏报率与误报率的需求。在数据安全治理方面，利用区块链技术的“去中心化、不可篡改、可追溯”的优势特性，进一步保障数据存储、传输安全。

基金项目：

江苏省高校哲学社会科学研究项目“数据驱动下学术资源个性化推荐与主题发现研究”阶段性成果（项目编号：2022SJYB1129）。

参考文献：

[1] 全国高校漏洞排行榜,教育行业漏洞报告平台[EB/OL].[2023-01-13.]https://src.sjtu.edu.cn/rank/firm/0/.

[2] 孙戈.公共图书馆网络信息安全风险与防范策略[J].图书馆理论与理论,2018(11):19-22.

[3] 陈思义.图书馆应对网络系统危机探讨[J].图书馆学研究,2016,(21):16-19.

[4] 余其明.下一代防火墙在高校图书馆的应用[J].情报探索,2017,(03):78-81.

[5] 鲍旭华,洪海,曹志华.破坏之王：DDoS攻击与防范深度剖析[M].北京:机械工业出版社,2004.

[6] 王欣,王传清.图书馆网络信息系统安全危机管理[[J].图书情报工作,2009,53(23):40-43,90.

[7] 王传清,王欣,刘伟,等.数字时代图书馆网络系统危机及应对策略[J].图书馆,2012,(02):39-43.

[8] 周纲,孙宇.开创性的下一代图书馆服务平台解决方案——FOLIO[J].中国图书馆学报,2020,46(01):79-91.

[9] 马晓婷.大数据环境下图书馆敏感数据的识别与保护[J].图书馆论坛,2017,37(04）:129-136.

[10] 张冉.个人信息保护之目的限制原则的适用与反思[J].网络空间安全,2023,14(02):22-27.

[11] 查德平,季千惠,赵泽宇.高校网络安全漏洞治理探索与实践[J].网络空间安全,2022,13(01):47-54.

作者简介：

王大阜（1981-），**男**，**汉族**，**江苏盐城人**，**贵州大学**，**硕士**；**中国矿业大学图书馆**，**馆员**；**主要研究方向和关注领域**：**知识图谱、推荐系统和网络安全**。

石宇凯（1980-），**男**，**汉族**，**浙江诸暨人**，**西南交通大学**，**本科**；**诸暨市融媒体中心**，**工程师**；**主要研究方向和关注领域**：**网络安全、数据治理**。

智慧校园高校网络安全应急管理体系研究与实践

杨阳
（南开大学，天津300071）

摘要：

［目的/意义］高校是我国信息化高速发展的前沿领域，也是网络安全防御的重要阵地，高校亟需建立完善的网络安全应急管理体系。

［方法/过程］分析高校网络安全应急管理体系的构成要素，阐述监测预警、应急演练、应急响应环节的实施步骤和工作重点。

［结果/结论］建立完善的网络安全应急管理体系，在应急预案的指导下，通过现场处置方案将各要素有机结合，组织开展应急管理工作，对高校网络安全工作意义重大。

关键词：网络安全；应急预案；应急响应；安全管理；监控预警

中图分类号：TP **文献标识码：**A

Research and practice on the emergency management system for cyber security in the smart campus

Yang Yang
(*Nankai University, Tianjin 300071*)

Abstract:

[Purpose/Significance] Universities are not only frontiers of information technology, but also important areas of cyber security. It is important to establish a comprehensive of cyber security in universities.

[Method/Process] The paper analyses the factors of cyber security emergency management system, and introduces the procedures of monitoring, emergency drilling and emergency response.

[Results/Conclusion] Establishing a comprehensive network security emergency management system and organically combining various elements through on-site disposal plans under the guidance of emergency plans is of great significance for the development of emergency management work in universities.

Keywords: cyber security; emergency plan; emergency response; security management; monitoring and early warning

0 引言

网络信息技术迅猛发展，使得经济和社会活动高度依赖网络和信息系统的支持。随着智慧校园时代的来临，互联网+、大数据、云计算和人工智能等先进技术纷纷被引入高校。这些技术催生出的应用，在为高校发展提供驱动力的同时，也给网络安全形势带来了极大的冲击[1]。数量庞大的物联网设备、访问便捷的互联网服务和生成的海量数据，都成为网络安全攻击的重要目标[2]。在此背景下，被动和零散的防御已不能满足高校网络安全工作的要求。

我国于2016年发布的《国家网络空间安全战略》提出“完善网络安全监测预警和网络安全重大事件应急处置机制”，为我国网络安全应急管理工作指明了方向[3]。在“应急预案-应急体系-应急机制-应急法规”相协调的网络安全应急管理体系的指导下，高校应依照战略层面的总体性应急预案[4]——《国家网络安全事件应急预案》的大框架，结合实际工作，建成一套行之有效的网络安全应急管理体系。

1 体系构成要素

网络安全应急管理体系由防护主体（机构和人员）、防护客体、应急预案、现场处置方案要素构成。如图1所示。

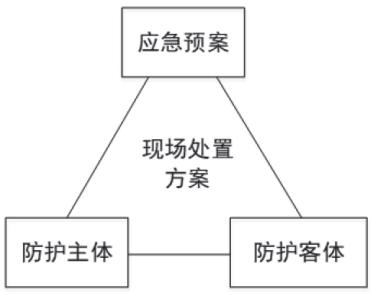

图1 网络安全应急管理体系的构成

1.1 防护主体

科学合理的机构设置和协调有序的人员机制，构成了网络安全应急管理的防护主体，是应急工作高效开展的基础保障。

1.1.1 机构设置

应急管理机构可按所属不同分为校内机构和校外机构两部分。校内机构由网络安全和信息化领导小组（以下简称网信领导小组）、网络安全和信息化管理部门（以下简称网信主管单位）、各二级机构构成；校外机构由教育主管单位、公安部门、网络安全和信息化办公室（以下简称网信办）、安全厂商构成。如图2所示。

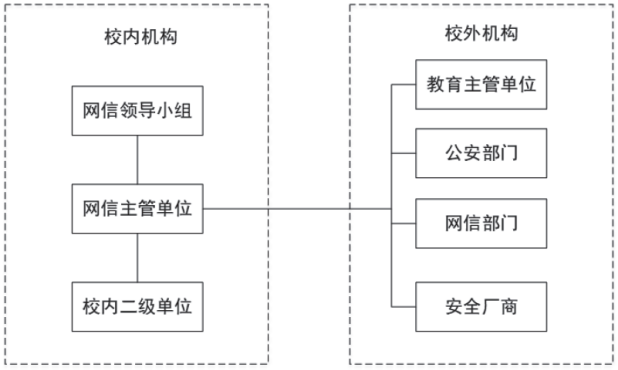

图2 应急管理机构示意图

网信领导小组作为高校网络安全工作的决策层，应充分发挥其领导作用，从全局把控网络安全应急工作的方向和原则[5]。网信主管单位负责统筹协调日常监控预警和网络安全事件的应对，建立校内各部门联动处置机制，向网信领导小组汇报工作动态，并与上级主管部门、公安部门、网信办保持信息联络。校内各部门负责本部门所运行网络信息系统的安全运维工作，依据网信主管单位的指导对预警和事件进行处理，并向其汇报安全状态。

在校外机构中，教育主管单位、公安部门、网信办为管理部门，与高校建立日常沟通机制，向高校通报预警信息，接收高校关于安全事件的报告，并在非常时期指导高校进行应急处置工作。安全支撑厂商为与高校签约的网络安全服务商，根据网信主管单位的具体安排进行日常监控预警、安全加固、事件处理等工作。

1.1.2 人员队伍

在明确机构职责的基础上，应建立一支安全应急管理人员队伍，并明确人员职责。队伍分4个

层次：第一层为学校网信领导小组成员，小组指定一名校领导任组长，担任网络安全应急工作的总指挥；第二层为学校网信办工作人员组成的安全运维团队，执行安全应急管理的具体工作；第三层为学校各部门网络安全责任人和联系人，负责与本部门有关的应急响应工作；第四层为各网络信息系统的安全管理员，负责各系统的安全运维和应急处理具体操作。

1.2 防护客体

应急管理的防护客体是高校的网络信息资产，新技术的应用促使防护客体向多样和复杂的方向发展。除了传统的信息系统，防护客体还应包含基础网络、云平台、大数据、物联网应用等。全校各责任部门在网信主管单位的组织下结合《信息安全技术网络安全等级保护基本要求》，确定资产的等级保护级别。对网络信息资产相关信息进行全生命周期维护时，应特别注意资产边界的确定，以便于在监测预警和应急响应环节快速定位受影响的客体范围。

针对全部网络信息资产，归纳可能面临的网络安全风险。依照信息资产的等保级别，确定事件的应急响应级别，并在此基础上形成可能发生的安全事件列表。

1.3 应急预案

根据《国家网络安全事件应急预案》和《教育系统网络安全事件应急预案》的指导精神，结合实际工作情况，高校应出台适合本校环境的网络安全事件应急预案。预案是应急工作的纲领性文件，包含机构设置、安全事件分级、监控预警、应急响应、应急演练等内容，并对每个环节流程做出明确规定。预案和机构与人员体系、防护客体紧密结合，覆盖应急处置工作的全部环节，指导网络安全应急管理工作的开展。

1.4 现场处置方案

在总体应急预案的指导下，高校应将应急管理工作进一步细化，制定网络安全事件现场处置方案。与应急预案相比，现场处置方案强调具体性、完备性、可操作性。处置方案以学校资产列表和事件列表作为基础，根据事件类型、响应级别进行分类，针对每一具体事件给出有针对性的处置流程。处置方案可以流程图的形式制定，每一环节都应具备人员、对象、动作三个要素，明确所处环节和下一环节指向，将主体、客体和应急预案有机整合，以保证高效、准确地完成应急处置工作。

2 日常监测预警

日常监测预警作为事前防范措施，是应急体系中非常重要的环节。网络安全等级保护2.0明确提出相关要求，应通过多种渠道和技术实现网络安全监测预警[6]。在应急预案的指导下做好监控预警工作，可以最大程度地避免网络安全事件真正发生，是保障应急管理体系坚不可摧的重要基础。依据信息来源划分，监测预警包括自主监控和外来信息预警。

2.1 自主监控

在技术上，自主监控依赖于安全防护中心的建立。将流量监控、机房动力监控、环境系统监控、安防监控等监控设备有机整合，结合防火墙、WAF、病毒防护、漏洞扫描等安全设备信息，将各种安全信息汇总分析，可建成网络安全大数据分析平台，为学校提供及时、有效的监控告警信息。

在管理上，高校可通过定期网络安全检查工作，及时发现管理上的风险；并在安全保护对象上线、升级、改造等环节做好风险评估工作。

2.2 外来信息预警

由于对网络安全工作的高度重视，国家网信部门、公安部门、教育行业管理部门已以多渠道建立安全监测预警信息共享机制。高校应充分利用现有的监测预警渠道，快速完成预警信息的接收、评估、处理和反馈。

除此之外，通过与安全厂商、安全机构建立

协同机制，高校可最大程度地增加安全情报收集渠道，及时发现可能发生的安全威胁。

3 应急演练

除日常监测预警之外，应急演练是应急管理体系中又一重要的事前防范手段。定期开展应急演练，可验证应急预案和处置方案的合理性，规范事件处理流程，健全应急工作机制[7]。

3.1 演练类型

依据演练的组织形式，应急演练一般可分为桌面推演、模拟演练和实操演练[8]。

桌面推演一般由应急演练小组假设安全事件发生的场景，根据应急预案、现场处置方案规定的处置过程，利用通讯、视频等辅助手段模拟完成处置工作。桌面推演可检验预案、方案的有效性和可操作性，使相关人员熟悉处置流程和自身职责，以提高网络安全应急处置能力。桌面推演是普通高校最为常用的应急演练形式。

模拟演练的进行需要预先搭建演练环境，用于模拟网络安全事件发生的场景。参演人员依根据应急预案、现场处置方案内容，在演练环境中进行应急处置工作。相对桌面推演，模拟演练的优势在于可检验相关人员对情况的判断能力和实际操作能力，但需要网络安全专业人员的指导，并且演练环境的搭建需要一定成本。

实操演练是依托真实网络环境进行的应急演练，学校自行开展有一定困难。学校可依托公安系统、教育系统组织开展的实战演练提高自身的应急处置能力。

3.2 演练流程

高校应每年至少开展一次网络安全应急演练。

在演练准备阶段，高校应制定演练计划、制定演练方案、落实演练保障。演练计划应包含演练目的、演练原则、演练时间、演练形式、演练预算等要素。演练方案则应明确参演的部门人员和演练场景，编写演练脚本，制定演练评估标准。演练保障则包括落实人员、场地、工具、经费等一系列工作，为演练顺利进行起保障作用。演练正式开始前，应组织所有参演人员参加演练培训，明确每个人在演练中的工作与职责。如有条件可进行预演。如果演练形式为模拟演练，还需要在演练前完成演练环境的搭建和测试工作。

指挥组宣布演练开始后，参演人员依照演练脚本进行预警信息收集、研判、报告、处置和恢复等环节的工作，评估人员按标准对演练各环节进行评估。演练过程全程录像。

演练结束后，全体参演人员召开会议总结演练过程，形成演练总结报告。针对演练中发现的问题，修订应急预案和现场处置方案。

4 应急响应

应急响应是网络安全应急管理体系中的核心内容。在数据激增、万物互联的当代，严密的防护措施无法彻底杜绝网络安全事件的发生。因此，应急响应环节是检验应急管理体系是否有效的关键一步。应急响应一般分为初步处置、事中响应、事后总结三步。

4.1 初步处置

初步处置包含入侵发现、入侵抑制、资源保护等工作[9]。监测到事件发生后，应急预案启动。首先，应采取紧急措施防止事件的进一步恶化，如重置网络、隔离系统等。根据事件的客体、影响范围、严重程度确定事件级别，依据现场处置方案上报上级管理部门。初步处置环节中应特别注意将事件现场的快照、服务器或安全设备的日志进行备份。

4.2 事中响应

事件责任单位和网信主管单位根据现场处置方案对安全事件进行处理。在有效的现场处置方案的指导下，处置工作专注于事件的根除与恢复，二者是同时进行的，目标是通过消除网络安全事件的不良因素恢复网络安全状态[10]。事中响

（下转第93页）

面向物流电子证据的区块链存证方法研究

钱晓雨，任俊玲，李军
（北京信息科技大学，北京100192）

摘要：

［目的/意义］ 条形码和二维码作为物流电子证据的关键要素，对促进商品流通和溯源发挥着重要作用。如何保证海量电子证据的数据安全和快速发现是当前研究的热点之一。

［方法/过程］ 基于深度学习的目标检测模型，提出“区块链+YOLOv5”的识别触发算法，设计物流电子证据摘要存证方案，构建摘要生成模型。

［结果/结论］ 实现从海量物流数据源中，对潜在问题证据精准识别，保证精准发现真实的潜在问题证据，同时为物流电子证据关键要素溯源，提供可信存证依据。

关键词： 区块链；存证技术；物流电子证据；深度学习；关键要素提取

中图分类号： TP311 **文献标识码：** A

Research on blockchain deposition methods for logistics electronic evidence

Qian Xiaoyu, Ren Junling, Li Jun
(*Beijing Information Science and Technology University, Beijing 100192*)

Abstract:

[Purpose/Significance] Barcodes and QR codes, as key elements of logistics electronic evidence, play an important role in promoting commodity circulation and traceability, and how to ensure data security and rapid discovery of massive electronic evidence is at the same time one of the hot spots of current research.

[Method/Process] In this paper, we propose a blockchain+YOLOv5 recognition trigger algorithm based on a deep learning target detection model, design a logistics electronic evidence abstract deposition scheme, and construct an abstract generation model.

[Results/Conclusion] To achieve accurate identification of potential problematic evidence from massive logistics data sources, ensure accurate discovery of real potential problematic evidence, and at the same time provide a credible deposition basis for the traceability of key elements of logistics electronic evidence.

Keywords: blockchain;deposition technology;electronic evidence in logistics;deep learning;extraction of key elements

0 引言

随着物流行业信息化进程的飞速发展，文件形式呈现出多元化发展趋势，电子文件已经成为传递信息、记录事实的重要载体。物流电子证据容易在多节点流通过程中被破坏，导致信息不完整，难以快速发现并实时存证，且物流信息具有海量性，无法全部保存和快速追溯。另外，相比于大量传统形式的货物流与信息流，物流电子证据也容易被人为篡改和伪造，同时在存储和传输的过程中，存在着关键信息破损和数据丢失的可能性，对取证和查验带来不真实性和不确定性。

区块链在物流行业中的应用，已经成为各种区块链应用中极具落地价值的实际应用场景[1]。区块链技术在物流领域的应用主要可以分成两个层面[2]：一是帮助用户通过区块链技术实现权利保障，通过区块链技术存证和取证能够使用户即时发现，保护自身权益；二是物流单位应用区块链技术管理货物流和信息流，做到精准溯源，避免发生纠纷，通过区块链技术确认、保存相关信息，确保存证数据的真实性和不可篡改性，更加有效地保护用户与物流单位的信息安全。

1 物流电子证据信息识别研究现状

深度学习在物流电子证据关键要素提取方面已有大量研究，条码和二维码作为物流电子证据的关键要素已被广泛研究并应用于各类物流场景。文献[3]最早开始使用深度学习的模型对文字区域进行检测，开创文字识别的新思路；文献[4]使用深度学习的光学字符识别算法（Optical Character Recognition，OCR），实现物流单据上的数字号码快速识别；文献[5]使用深度学习图像识别模型卷积循环神经网络（Convolutional Recurrent Neural Network，CRNN），针对复杂背景下的文本识别模型改进优化取得了较好的效果；文献[6]使用轻量级目标检测（Single Shot Multibox Detector，SSD）单卷积神经网络检测条形码位置，但是在实验中发现效果较差；文献[7]和文献[8]使用优化的SSD深度学习检测器检测复杂背景下的条码数据获得了较好的效果；文献[9]使用Faster R-CNN（Region-CNN）网络检测条码，提升了检测的准确度，但是速度较慢。

因此，针对电子证据数据量大且关键要素易被破坏的关键问题，为避免潜在问题证据引起纠纷，亟需建立基于区块链的电子证据全生命周期的可信管理模式，结合区块链和深度学习模型，实现从海量电子证据中快速发现潜在问题证据并实时上传，提出新的存证方案，实现物流电子证据的可信数据安全管理。

2 物流电子证据存证方案

二维码与条形码作为物流电子证据的溯源的关键要素，不仅包含有关用户与商家个人隐私信息，而且还涉及到商品流通的实时状态。在终端经过可信身份认证后产生的存证交易，仍存在被用户质疑源证据真实性的疑问，或在流通过程中出现溯源码破损等情况，导致无法真实溯源引发经济纠纷。为了从海量物流源数据中把潜在问题证据进行精准识别、摘要生成、存证上链，构建物流电子证据的存证记录与源文件不可篡改的真实证据存档十分关键，进而实现物流电子证据的存证安全和权限可控查询。

2.1 物流电子证据存证方案的实现功能

提出基于区块链的物流电子证据存证流程。基于区块链的物流电子证据安全存证方案，需要实现电子证据的是证据识别、摘要生成、自动存证、溯源和下载等功能，其中物流电子证据存证是指将可能产生纠纷的证据源数据与电子摘要的详细信息存储到存证链的过程。

基于区块链的物流电子证据存证模型如图1所示。

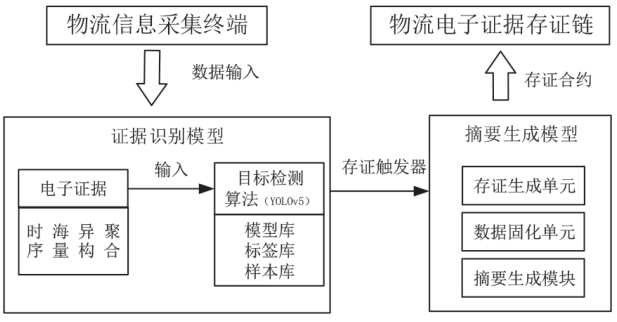

图1 基于区块链的物流电子证据存证模型方案

2.2 物流电子证据识别模型

主要针对物流活动中产生的溯源码证据作为存证依据，存证之前的预处理步骤，识别电子证据图像类文件。YOLOv5是目前理想的目标检测模型之一，在精确度、检测速度和所需存储空间上表现优异，适用于物流电子证据中的溯源码识别。

YOLOv5检测网络包含输入端、骨干网络（Backbone）、特征融合网络（Neck）和预测网络（Prediction）。在YOLOv5检测流程中，以YOLOv5s为例，网络首先将训练集中的每幅图像分成个网格，每个网格通过自适应锚框计算后都有不同大小的候选框，由物体中心所在的网格负责检测物体；然后，通过骨干网络的卷积层提取特征；最后，预测层用于多尺度预测，负责预测的特征图有多个尺度，可以预测大小不同的物体，由特征金字塔结构进行多尺度特征图融合而得，每个网格预测B个锚框、置信度得分以及C类。

YOLOv5结构图如图2所示。

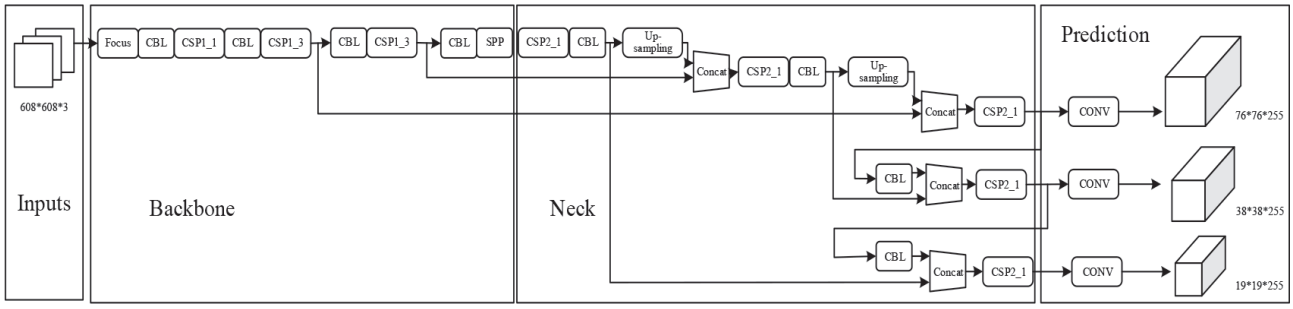

图2 YOLOv5结构图

2.3 物流电子证据摘要生成模型

针对上节模型检测后输出置信率低于（γ＜0.85）的可疑溯源码，导入摘要生成模型，生成可进行查证和溯源的存证摘要。

摘要生成模型结构流程如图3所示。

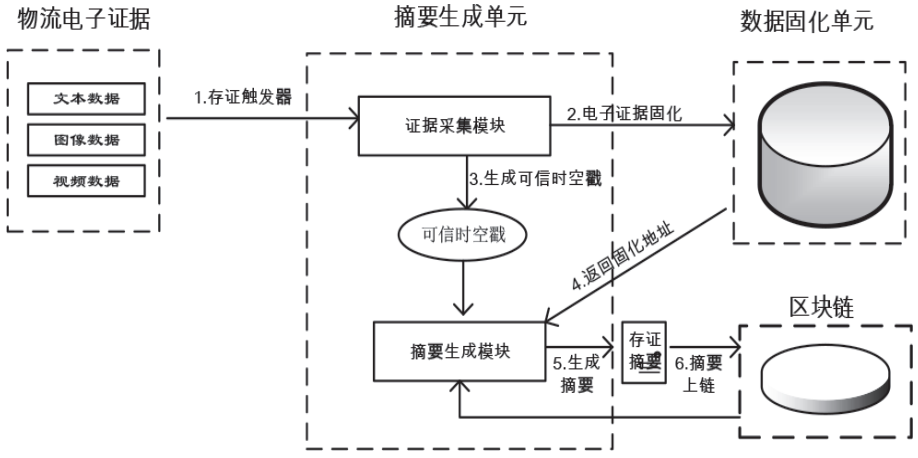

图3 摘要生成模型结构流程

摘要生成网络主要由摘要生成单元、数据固化单元以及电子证据存证区块链三部分组成。摘要生成单元由摘要采集模块和摘要生成模块组成。证据采集模块根据物流电子证据的存证条目名称采集具体的电子存证，同时生成可信时空戳。可信时空戳是由6位数字组成的证据编号、14位时空戳以及上传用户的6位数字签名编号组成，用来唯一标注这个存证。摘要生成模块负责生成存证摘要结构体，并将可信时空戳添加至存证摘要的摘要头，将每个条目电子证据生成对应的SHA256哈希指纹，并将其以键值对形式对应添加至存证摘要的摘要体中。之后将具体的电子存

证送入数据固化单元进行保存，返回数据固化地址，存证摘要模块将数据固化地址添加至摘要尾部，最终形成完整存证摘要。

3 结束语

通过对基于区块链的电子证据安全存证方案做出总结，结合深度学习的目标识别算法，提取物流电子证据中的关键要素条形码和二维码。深度学习模型的引入，保证了从海量电子证据源数据中，实现潜在存证目标的精准识别和发现，提出了物流电子证据提取的摘要生成模型，形成了摘要与证据原文件一同上链的存证方案以便检索。依据分析，方案适用于物流背景下的电子证据记录安全存证，为后续的存证实验实现和验证夯实基础。

基金项目：

1.国家自然科学基金“ 基于集成模型的网络行为数据流敏感目标挖掘与检测技术研究”（项目编号： U1936111）；

2.北京信息科技大学2021“勤信拔尖人才”项目资助（项目编号：5112211107）；

3.2023年“慧眼行动”——基于集成学习的目标跟踪和情报关联挖掘技术（项目编号：F2B6A194）；

4.2023年第一批国防基础预研项目。

参考文献：

[1] 王君宇,吴清烈,曹卉宇.国内区块链典型应用研究综述[J].科技与经济,2019,32(05):1-6.

[2] 饶东宁,王军星,蒋志华.等.区块链技术在物流供应链领域应用综述[J].软件导刊,2018,17(09):1-3+8.

[3] Wang T,Wu D J.Coates A, et al. End-to-End Text Recognition with Convolutional Neural Networks.2012 International Conference on Pattern Recognition,2012.

[4] 李毅荣,郭磊,张漫杨.基于Tesseract-OCR的快递单中手机号码识别应用实 现[J].电子测试,2018(22):8-10.

[5] Tong G, Li Y, Gao H,et al. MA-CRNN: a multi-scale attention CRNN for Chinese text line recognition in natural scenes. IJDAR 23,103–114 (2020)

[6] Kolekar A, Dalal V. Barcode detection and classification using SSD (single shot multibox detector) deep learning algorithm[C]//Proceedings of the 3rdInternational Conference on Advances in Science & Technology (ICAST).2020.

[7] Ren Y,Liu Z.Barcode detection and decoding method based on deep learning[C]/2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE).IEEE,2019:393-396.

[8] Li J,Zhao Q,Tan X,et al.Using deep ConvNet for robust 1D barcode detection[C]/International Conference on Intelligent and Interactive Systemsand Applications. Springer, Cham,2017:261-267.

[9] Carion N,Massa F,Synnaeve G,et al.End-to-end object detection with transformers[C]//European conference on computer vision.Springer,Cham,2020:213-229.

[10] 任俊玲,王兴芬,王承权.面向电子商务的新一代验证码系统分析[J].网络空间安全,2017,8(12):34-39.

[11] 李军,于灵凡,田斌,等.数据流安全查询技术综述[J].网络空间安全,2019,10(09):62-72.

[12] 钱雪,李军,唐球,等.基于YOLOV5的药品表面缺陷实时检测方法[J].信息技术与网络安全,2021,40(12):45-50.

作者简介：

钱晓雨（1997-），女，汉族，山东烟台人，北京信息科技大学，在读硕士；主要研究方向和关注领域：区块链和信息系统安全。

任俊玲（1979-），女，汉族，山西平遥人，北京邮电大学，博士；北京信息科技大学，副教授；主要研究方向和关注领域：网络空间安全和智能信息处理。

李军（1983-），男，汉族，山东滕州人，北京邮电大学，博士；北京信息科技大学，副教授；主要研究方向和关注领域：人工智能和信息安全。

入侵检测技术在网络安全中的应用探讨

王娜，狄秋燕
（中国联合网络通信集团有限公司，北京100033）

摘要：

［目的/意义］ 近几年，随着互联网的普及和推广，互联网技术在各个行业中应用广泛，在一定程度上加快了我国社会改革的发展步伐，但是也引发了一系列网络安全问题。

［方法/过程］ 以入侵检测技术为探究重点，分析入侵计算机网络的常见方式，并在此基础上着重探讨了一种基于神经网络的入侵检测系统，以及入侵检测技术在网络安全中的应用。

［结果/结论］ 入侵检测技术的使用，可以更好加强网络安全技术的开发和设计，在网络安全中应用效果比较理想，使得相关网络技术人员提供了一个安全的网络环境。

关键词： 入侵检测；网络安全；系统设计；入侵信息；数据挖掘

中图分类号： TP393.0 **文献标识码：** A

Discussion on the application of intrusion detection technology in network security

Wang Na, Di Qiuyan
(*China United Network Communications Group Co., Ltd., Beijing 100033*)

Abstract:

[Purpose/Significance] In recent years, the popularization and promotion of internet technology have been widely applied in various industries, accelerating the pace of social reform and development in China to a certain extent, but it has also triggered a series of network security issues.

[Method/Process] Currently, hackers, viruses, and other threats pose to people's network security. In order to provide a secure network environment for people, relevant network technicians have strengthened the development and design of network security technology. The application effect of intrusion detection technology in network security is relatively ideal.

[Results/Conclusion] The use of intrusion detection technology can better strengthen the development and design of network security technology, and its application effect in network security is relatively ideal. It provides relevant network technicians with a secure network environment for people.

Keywords: intrusion detection; network security; system design; intrusion information; data mining

0 引言

互联网展现出较强的易开发性特点，能够促进各项资源的传递和共享。同时，计算机自身展现出较强计算能力，容量比较大，满足了人们日常工作和生活要求，得到了各个行业的推广和普及。随着网络时代快速发展，非法入侵、盗取等现象比较普遍，通过调查得知，2022年6月，境内被篡改网站的数量为3 644个，与上月的5 279个相比减少31.0%；境内被植入后门的网站数量为1 939个，与上月的1 838个相比增加5.5%；与上月的11 638件相比增长48.7%。数量最多的分别是网页仿冒类事件8 482件、漏洞类事件4 077件和恶意程序类事件3 679件。由此可见，在新形势下，做好网络安全管理工作是非常必要的[1]。

1 入侵计算机网络的常见方式

1.1 网络病毒攻击

计算机病毒是一种具备自我复制功能的计算机程序，会直接影响系统的正常运行，造成系统中重要信息的泄露。从网络病毒角度分析，展现出较强的传染性和隐蔽性，是造成网络安全受到维修的主要因素[2]。

1.2 拒绝服务攻击

因为存在磁盘操作系统（Disk Operating System，DOS），会造成计算机死机或者瘫痪，让用户面临严重影响。为了降低影响，需要把一定序列或者数量的报文传递到网络系统中，这样整个网络服务器中的数量将随之增加，会造成网络资源的浪费，不能保证计算机网络系统运行的稳定性和安全性。

1.3 身份攻击

在网络使用中，应该对用户身份提前确定，设有一定访问权限。尽管如此，依然会有部分人员通过各种不法方式盗取网络中重要信息，进入到网络中，引发严重的网络攻击问题。如果是身份攻击，破坏者会通过网络漏洞对其扫描，如果发现漏洞，可能会导致合法用户重要信息泄露，威胁系统运行安全[3]。

2 基于神经网络的入侵检测系统设计

2.1 神经网络

神经网络（Back Propagation，BP）是一种通过误差逆传播方式形成多层次前馈神经网络，这也是当前计算机网络中广泛使用的神经网络模型。在网络中，设有不同阶段，只能接受上层输出，对于相同层面节点之间不会出现交互作用，相邻两层的节点主要采用全连接模式。在结构层面上，神经网络中包含了输出层、输入层和隐含层，其中隐含层是一种多层次，在数据传入以后，由隐含层进入到输出层。在神经网络中，通过形成神经网络信号，实现正向传递或者误差函数的反向传递。在执行算法过程中，需要重新设计网络结构，对输出结果和期望结果之间误差精准计算，在误差满足预期要求以后，结束算法。

神经网络结构如图1所示[4]。

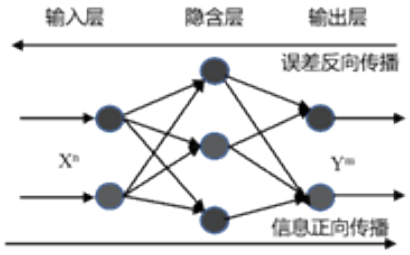

图1 神经网络结构

在具体实践中，对于影响计算机运行的各种活动，都可以认定为计算机网络入侵。这种入侵行为不但能够获得操作系统各项运行信息，也能实现网络侦察，通过植入相关安全程序的方式，实现对主机系统的远程监控，获取计算机中各种敏感的信息，因而无法保证计算机系统运行安全。在通常情况下，网络入侵行为和用户正常使用系统资源各不相同，虽然在入侵过程中比较隐蔽，但是无法确保不会在计算机网络系统中留下痕迹，这些痕迹是检测入侵行为的重点因素。对于入侵检测技术来说，通过建立入侵检测模型，确定入侵检测要求，对入侵行为进行追踪，抽象

表达，从中获得和入侵行为相关的各项信息，制定详细的入侵检测计划，从而起到预防、检测和监管网络的效果。通过收集和整理各种新型入侵行为，入侵检测可以对用户行为进行核查。如果用户行为不满足网络安全要求，则会被定义为入侵，从而系统自动提示入侵，便于管理人及时采取相关措施进行处理。

2.2 系统网络结构

在网络结构设计中，隐含层层数和节点数量的确定作为重点内容，需要适当地增加隐含层数量，让检测结果更加准确，从而减少网络误差。但是，在神经网络中，隐含层数量的增加，使得训练时间相对偏长。如果是单隐层神经网络，隐含层神经元数量随之减少，可能会造成网络学习能力的下降；如果神经元数量增多，网络学习能力将明显增长，但是也会让网络泛化能力下降，导致网络呈现出过拟合状态。

在网络结构设计方面，应从两方面落实：第一，神经网络检测精度明显提高，尽可能减少神经元数量；第二，通过仿真实验方式从中寻找隐含层节点数量。在探究中，网络结构中设有多层前馈神经网络，结构简单，处理流程比较复杂，同时模式识别能力和分类能力远远大于反馈网络。在神经网络结构设计中，一般采用生长法，也就是提前确定一个相对简单的网络结构，之后通过隐含层、节点增加等方式获得其他网络结构。

2.3 移除层

在神经网络中，可能会呈现过拟合状态，使得计算准确性明显下降。通过移除层（Dropout），能够将这种问题科学处理。Dropout也就是在神经网络训练过程中，按照对应流程，暂时把网络中神经元从网络中抽离，以确保每个Dropout中部分隐含层节点保持在0状态。由于这种丢弃属于随机的，因此每个Dropout在训练中网络结构各不相同，由此影响到神经元之间的相互作用。Dropout主要是把概率P中部分神经元丢弃，其他神经元则可以通过1-P进行保存，确保输入层和输出层的神经元不会发生改变，通过对网络结构进行调整，实现网络结构的反向传递，实现科学操作，重新设定权重，直到完成训练。

2.4 神经网络算法优化

对于神经网络来说，展现出自主学习能力和自适应能力等。但是，随着信息技术发展水平不断提高，在具体应用中将会面临各种问题，具体表现在两个方面。

第一，可能会陷入局部最优。神经网络是一种局部搜索的方式，处理的问题以一般复杂非线性问题为主，网络权值调整则是根据局部梯度来完成。如果操作不当，可能会陷入局部最优中，并且神经网络对网络权值的初始值有着一定的敏感度，如果网络全资初始不同，产生的结果也会各不相同。

第二，神经网络预测能力和训练能力之间存在矛盾。在通常情况下，神经网络预测能力会随着训练能力提高而增强。但是，在训练达到一定强度以后，预测能力不断降低，从而发生过拟合现象。在当前时代发展中，通过采用线性整流函数（Rectified Linear Unit, ReLU）神经元网络，实现高斯分布权值初始化设定，通过加入动量项，神经网络在训练中对权值适当调整，知识则是根据当前迭代梯度下调方向调整，通过把动量项应用在权值调整公式中，稳定结构[5]。

3 入侵检测系统在网络安全中的应用

3.1 数据挖掘技术和智能分布技术

对于数据挖掘技术来说，需要深入到互联网中，做好各项数据信息的采集、整理工作，及时检测存在的错误问题，并采取相关措行处理。通过使用数据挖掘技术，能够将技术的应用价值充分发挥，对于网络中存在的异常运行流程科学划分，并具备较强的数据分辨能力，让数据保持在一个正常任务程序中，更好地保证网络运行安全。

对于智能分布技术来说，也是入侵检测技术中比较重要的组成部分，展现出了智能化和适应能力强等特点，是网络安全检测中不可或缺的一部分。通过使用智能分布技术可以维护网络系统

安全，把网络划分成多个领域，适合应用在校园网络环境中。通过在各个检测区域中设置监测点，并对监测点检测数据信息科学管控，找到网络安全系统中存在的入侵行为，以保证网络运行安全。

3.2 信息响应与防火墙系统

通过信息响应及时找到入侵检测系统中信息攻击行为，对信息实际情况和运行状态实时检测与记录，并把信息反馈到控制台。在计算机系统中，对于各种控制技术而言，可以对用户计算机系统中各项资源进行保护，以防止网络入侵产生严重的攻击行为。随着科技发展水平的不断提高，在传统防火墙应用和用户自身需求之间有着明显差别，所以在使用入侵检测技术时，需要把入侵检测技术和防火墙进行结合，相互作用和影响。通过把入侵检测技术中的攻击性数据及时初拉力，提供比较准确和完整的计算机网络信息，形成一个比较全面的防火体系。同时，通过入侵检测技术和防火墙技术的结合，可以将防火墙的过滤功能充分发挥，更好地保证网络信息安全。

3.3 协议技术和移动代理技术

协议分析作为一项全新的网络入侵检测技术，在使用方面更加便利，信息处理效率和水平相对偏高，不会造成资源的严重消耗与浪费，可以及时找到网络攻击行为，做出相应反应。在使用分析协议过程中，需要对协议和获得的攻击碎片进行整理，深入分析各种协议内容。如果包含IP碎片设置，需要对数据包重新处理，让系统可以及时检测其中存在的攻击行为，保证协议的完整性。在使用模式匹配入侵检测系统过程中，可以降低分析协议的错误率，通过命令分析器，了解各种特征串内涵，找到其中存在的攻击性元素。移动代理技术能够取代客户或者其他检测流程进行安全检测，实现主机之间科学转换，不会受到时间或者空间方面的影响，向用户传递准确的信息结果。在使用移动代理技术过程中，展现出的应用价值就是具备强大的离线计算功能，在网络资源比较匮乏的环境下，可以更好地保证网络运行安全，不会受到不法行为影响，同时能够在不同主机中运行，无需终止其他正常运行的程序，在不同主机中自由转换。

3.4 主机的入侵检测系统

主机入侵检测系统也就是HIDS（Host-based Intrusion Detection System，HIDS）。对于主机入侵检测系统安装代理来说，HIDS保持在系统安全保护范畴中，把操作系统内核和服务进行结合，了解主机系统审计日志和网络链接情况，对各个系统进行全面监控与管理。例如，启动系统内核和API，防止系统受到不法攻击，对系统中重要文件动态监管，通过主机入侵检测系统，可以及时找到系统中存在的入侵行为，并提前做好防范和控制工作。但是，对于主机入侵检测系统来说，在运行中也会存在一些不足，例如成本投放量大，以及操作系统、主机代理之间有着明显差别，主机代理会随着系统的升级改造而改变，从而给系统维护和安装工作开展带来一定的影响。

3.5 入侵信息的收集与处理

入侵检测技术通常通过整理各项数据信息，实现对网络运行情况的安全状态判断，系统日志和网络日志都会展现出较强的保密性，在执行程序上有一定的限制要求，需要及时做好网络检测数据的整理工作。在计算机网络运行中，需要在网段中安装入侵检测系统（Intrusion Detection System，IDS）代理，数量不得小于1个，以完成各项信息的采集和整理。在入侵检测系统中，需要设置交换机构或者防火墙，为核心数据传递提供安全环境。除此之外，在计算机系统中入侵行为不断下降的情况下，应建立一个比较集中的数据群，展现出入侵行为检测的科学性和准确性。在入侵信息收集完成以后，需要在对应模型和系统作用下完成信息处理，之后由管理器统一分析。入侵检测技术可以及时找到计算机系统中存在的安全问题，并将其传递到控制器中，为计算机系统安全运行提供良好条件。

4 结束语

计算机网络安全维护对于网络信息安全来说有着现实意义，而入侵检测技术的使用，可以更好地保证网络运行安全。结合当前情况，入侵检测技术在计算机网络安全维护方面的应用广泛，逐渐朝着完善化的趋势发展。但是，依然存在一些问题和不足，需要相关技术人员加强对入侵检测技术的检查与探索，提高技术水平，严格按照操作流程，为计算机网络安全维护工作正常进行提供技术支持。

参考文献：

[1] 徐梦萍.探究入侵检测技术在计算机网络安全中的应用[J].电脑知识与技术,2022,18(36):75-77.

[2] 王业.入侵检测技术在计算机网络安全中的应用分析[J].无线互联科技,2022,19(14):99-101.

[3] 刘玉娜.基于签名的网络安全入侵检测技术研究[J].现代工业经济和信息化,2022,12(06):113-114+117.

[4] 尤少雄,雷钊.计算机网络安全存在的问题及其应对措施分析[J].网络空间安全,2021,12(Z3),83-86.

[5] 徐慧.校园网网络病毒的入侵途径和防范策略[J].网络空间安全,2021,12(Z1),54-57.

作者简介：

王娜（1978-），**女，汉族，上海人，北京邮电大学，本科；中国联合网络通信集团有限公司，高级工程师；主要研究方向和关注领域：网络安全、网络运营管理。**

狄秋燕（1978-），**女，汉族，山西运城人，北京邮电大学，硕士；中国联合网络通信集团有限公司，高级工程师；主要研究方向和关注领域：数据治理。**

（上接第84页）

应也应依据现场处置方案规范进行处置工作，合理调动人力物力高效完成，最大程度争取宝贵时间。现场处置过程中全部操作应进行详细记录，并按照现场处置方案进行总结和汇报工作。

4.3 事后总结

事后总结是应急响应工作的收尾步骤，也是确保应急管理体系有效性的关键环节。确认事件处理完毕后，应对事件发生原因进行分析，找出监控预警等工作中的疏漏，改善日常工作流程。总结应急响应过程，分析流程中不合理的部分，优化应急管理体系。

5 结束语

智慧校园时代对高校网络安全工作提出了新的要求，被动防御、零散处置的工作方式已无法应对复杂多变的网络安全形势。在高校中建立科学完善的应急管理体系，并在其自身元素的作用下不断地自我更新和迭代，提高面对威胁和事件的实际应对能力，是网络安全工作顺利开展的重要保障。

参考文献：

[1] 廖海生.基于大数据技术的智慧校园安全管控[J].计算机测量与控制,2021.29(10):133-138.

[2] 张彬,范佳伟,李志国,孙威.智慧校园下的网络安全防护[J].网络安全技术与应用,2022,(04):93-95.

[3] 胡俊,严寒冰.从《国家网络安全时间应急预案》看我国网络安全事件应急体系[J].中国信息安全，2021(03):68-72.

[4] 李明.美国网络安全时间响应预案制度研究[J].电子政务，2017(08): 32-40.

[5] 王士贤.刘洪.于俊清.高校信息化体制机制研究与探索[J].大学教育,2022(04):24-27.

[6] 朱圣才.等保2.0框架下高校网络安全体系建设[J].网络空间安全,2020,11(04):14-18.

[7] 刘璀.基于多链路出口访问技术的高校网络安全管理研究[J].网络空间安全,2018,9(08):54-58.

[8] 朱贤斌.探讨网络安全应急演练和实战攻防演练[J].网络安全和信息化,2021(04):134-141.

[9] 牛晓博.方群.邵晓.基于威胁评估的网络安全应急响应[J].网络安全技术与应用,2022,(11):3-4.

[10] 陈美华.张明亮.王延飞.美国重大网络安全事件应急响应的情报解析[J].情报理论与实践.2023.

作者简介：

杨阳（1984-），**女，汉族，天津人，南开大学，硕士;南开大学，工程师；主要研究方向和关注领域：智慧校园、信息化建设和网络安全。**

高校网络安全课程实验教学平台的设计与研究

亢立明
（长春职工大学，吉林长春135100）

摘要：

［目的/意义］ 网络信息安全与国家安全密切相关，若想不断提升网络安全性能，就需要更多的高层次人才，所以高等院校在教育工作中应注重培养网络安全人才。

［方法/过程］ 国内很多高校先后开设了网络安全课程，并创建了网络安全课程实验教学平台。平台主要是基于网络安全课程展开设计与开发，能够对与网络安全课程有关的实验教学信息进行实时发布，实现实验教学资源的共享机制。

［结果/结论］ 基于系统需求，对高等院校网络安全课程教学现状展开分析，设计网络安全课程实验教学平台，以期能够促进高校网络安全课程教学改革。

关键词： 网络安全；实验教学；平台设计；高校；仿真实验

中图分类号： TP393.08-4 **文献标识码：** A

Research on the design of experimental teaching platform for network security courses in colleges and universities

Kang Liming
(*Changchun Workers' University ,Jilin Changchun 135100*)

Abstract:

[Purpose/Significance] Network information security is closely related to national security. Especially in recent years, network information security has occupied an important position in more and more industries in China, and the government's attention to network information security has reached an unprecedented level.

[Method/Process] To this end, many universities in China have successively opened network security courses and created an experimental teaching platform for network security courses. This platform is mainly designed and developed based on network security courses, capable of real-time publishing of experimental teaching information related to network security courses, and achieving a sharing mechanism for experimental teaching resources.

[Results/Conclusion] Based on the system requirements, this article analyzes the current situation of network security course teaching in colleges and universities, and designs an experimental teaching platform for network security courses in order to promote the teaching reform of network security courses in colleges and universities.

Keywords: network security; experimental teaching; platform design; colleges and universities; simulation experiment

0 引言

通过研究高校网络安全课程教学模式，提出实验教学选择网络与线下面对面相结合的教学模式。同时，通过对高校网络安全课程实验教学平台的开发，构建网络安全课程实验教学网站。平台以高校师生互动为核心，通过校园网结合线下教学，充分发挥教师与学生交互作用，从而为教务管理、学生以及教师，提供“管、学、教”三合一的开放式教学环境，共享高校教学资源，同时实现师生的跨时空互动[1]。基于系统需求，对高等院校网络安全课程教学现状展开分析，设计网络安全课程实验教学平台，以期促进高校网络安全课程教学改革。

1 系统需求分析

高校网络安全课程实验教学平台是一种教学网站，主要是为网络安全课程的开发设计提供一个平台。教学平台可以实时发布网络安全课程实验教学信息，共享实验教学资源，学生上传课程实验信息，这样不仅方便、快捷，而且不会受到空间和时间限制，同时可满足4项要求。

1.1 功能完整，个性化构建

高校网络安全课程实验教学平台主要从管理员与学生两个角度划分功能，其中学生属于普通用户，能够在线观看实验教学信息与教学视频，其中包括实验教学计划、课程简介以及教学大纲等，学生也可上传实验报告或者下载实验软件、学习资料等。教师属于管理员，主要是借助公告模块向学生发布相关信息，也可实时更新课程信息，或者上传教学视频、实验软件等，教师与学生可借助实验教学平台沟通交流学习问题，对学生实验报告进行在线批阅等[2]。

1.2 一体化建设方案，防止信息孤岛

根据高校网络安全课程特性，平台基于计算机教务系统，为高校师生创建一体化教学支撑环境，以形成考、学、练三方并重的实验架构。

1.3 符合规范，可持续发展

网络安全课程实验教学平台与国内数字化校园建设规范相符合，无缝衔接教务管理系统，实现数字化校园应用系统的有机构建。

1.4 主流技术，稳定且安全

高校网络安全课程实验教学平台中的数据库，会对高校师生敏感数据进行存储，因此具有较高的平台安全性要求，此为网络安全实验教学平台的建设重点。

2 课程实验教学平台现状

作为优秀网络安全人才培养基地，高等院校若要突出学科特色，为国家输出更多的优秀网络安全人才，关键在于创建国内领先且特色鲜明的网络安全课程实验教学平台。但是，在实验教学平台建设过程中，却面临着诸多挑战。

课程实验教学平台不能满足网络安全课程实践教学要求。作为网络安全课程教学重点，实践教学一方面帮助学生正确理解与应用理论知识，另一方面也有助学生应用知识能力与动手实践能力的提升。网络安全是具有较高实践要求的一门学科，比较注重培养学生的实践能力[3]。然而，高校普遍存在重理论轻实践的问题，高校生也将更多的精力花费在理论知识学习上，却忽略了提升实践能力。为此，高校不断创新培养方案，进一步延长了网络安全课程课时，网络安全课程的实验学分也有所提高。当前，高校所创建的信息安全实验室与网络安全仿真教学平台，很难满足创新优化后的高校网络安全实践教学需求。

课程实验教学平台并没有创建统一的关联共享机制。现有平台未进行整体规划设计，仅仅在实验教学过程中适用，无法为学生提供科研创新、学科竞赛等多元化服务。

课程实验教学平台内的实验项目与软硬件资源很难满足教学需求，甚至很多实验项目较为落后，和网络安全、智能化以及信息安全等技术发展相脱节。

3 课程实验教学平台设计

3.1 设计网络安全实验教学体系

高校网络安全课程实验教学体系借助先进的实验装备，选择最新实验设备与技术，展开网络安全实验教学，培养高校生的逻辑思维与创新能力。为与网络安全课程发展需求相适应，同时满足宽口径、厚基础优秀人才培养目标，高校应创建独立设置学分课程、培养学生创新能力、平台实践实验-综合创新实践-专业实践实验的网络安全课程实验教学体系[4]。如图1所示。

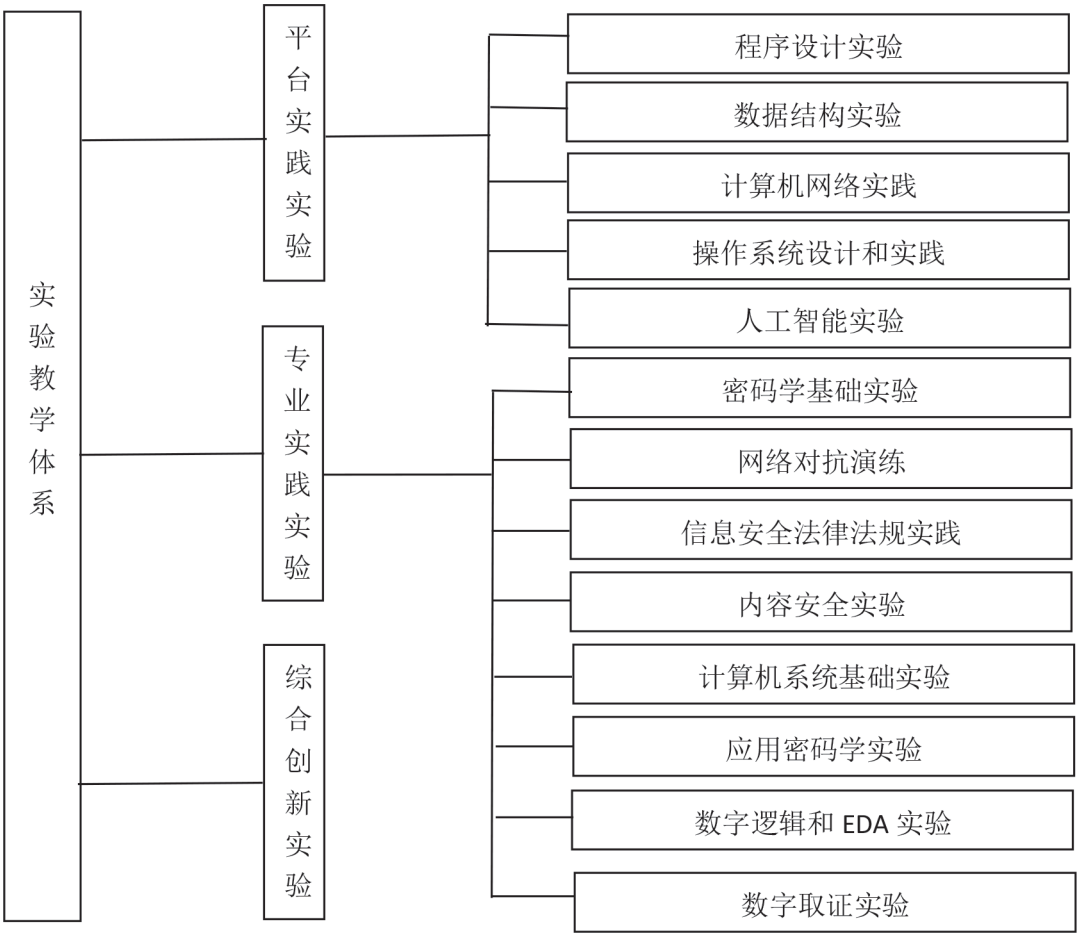

图1 高校网络安全课程实验教学体系

高校网络安全课程实验教学体系主要涵盖网络空间安全和信息安全两大核心知识点，同时也包括网络安全课程的实践内容。网络安全课程教学体系一方面看重的是学生对理论知识的掌握，另一方面对学生实践能力的培养也非常重视。尤其是近些年来，高校不断优化网络安全课程，同时也完善了相应的教学体系，以培养更多优秀、高素质的网络安全人才。

3.2 需求特色

从根本上说，高校网络安全实验教学主要是基于实验教学体系，将相关实践环境提供给网络安全专业学生。但是，由于网络安全课程本身比较特殊，对比其他专业课程，网络安全实验平台的设计，既要综合考虑实验性能、可扩展性和功能等需求，又要考虑到网络安全课程的特殊需求。

3.2.1 实践内容多样性

网络安全课程本身是集通信、教育、计算机、电子和数学等多门课程于一体的特殊学科。由于这一课程存在着交叉特色，所以高校在网络安全人才培养方案中，对实践课程的设计既要包含密码学基础实

验、网络安全实验以及网络对抗演练等网络安全实践内容，又要包含程序设计实验、操作系统设计实践、计算机系统基础实验以及数据结构实验等实践内容，同时也包括信息安全法律实践等法律学科内容。在设计实验教学平台过程中，必须包含各个学科内容，从而达到内容、数据融合共享的目的。

3.2.2 实验环境复杂性

通常网络安全实验必须有一个复杂的拓扑结构且规格比较庞大的互联网环境，如果仅仅靠硬件设备搭建网络安全物理环境，往往难以达到目标。

3.2.3 专业实验特殊性和破坏性

通常网络安全课程技术会有特殊性、破坏性，这就需要在实验项目中进行网络安全漏洞的人为设置，但是这样就会存有潜在的网络安全风险，若将病毒注入真实网络环境，则会引发严重的后果。

3.2.4 实验资源共享性

作为交叉性较强的一门学科，网络安全课程中的各种教学实验数据与内容间有很大的关联性，这就需要共享实验资源。

3.3 设计思路

网络安全实验教学平台的需求相对特殊，这就要在设计教学平台中做好三项工作：（1）通过云计算、虚拟现实和大数据等技术，在计算平台和高性能数据中心建设云计算平台，通过虚拟技术实现网络安全实验教学系统集成化，最终达到数据和应用的融合共享目标；（2）对网络安全实验教学平台进行统一的云平台管理，包括数据管理、用户认证、资源管理和访问控制等内容；（3）网络安全课程实验教学平台系统，依照不同实验场景与环境实现定制化创建，例如密码系统安全实验平台、网络靶场实验平台、网络安全仿真实验平台和云安全实验平台等，选择虚拟仿真技术对真实的互联网环境进行模拟。此外，人工智能安全实验平台与工业控制安全实验平台必须结合工业设备、软件系统等进行部署和搭建。

3.4 架构

网络安全课程实验教学平台主要采用服务层、数据中心和应用层三层架构。如图2所示。

3.5 组成内容

数据中心、实验平台系统联合构建形成网络安全实验教学平台，功能主要体现在8个方面。

3.5.1 平台数据中心

平台数据中心是高校网络安全实验教学支撑平台，内含组网设备、专业服务器和万兆光纤网络等设备，将云平台软件、虚拟化软件和数据库管理系统等部署在服务器中，以此构建多元化和智能化实验教学支撑中心。网络安全实验教学系统中含有网络人工实验、网络协议仿真实验、网络安全虚拟实验、人工智能安全实验、可信身份与行为分析实验等平台。

3.5.2 网络安全仿真

虚拟仿真实验平台其实就是具有开放特征的一种实验云平台架构。平台所涉内容有运维安全实训、数据库安全实训、网络安全实训、信息安全实训和密码安全实训等，可以根据平台架构开展网络安全知识的学习。

3.5.3 网络靶场

基于竞赛靶场实验平台的构建，展开网络安全防御技术、防御策略和防御产品的验证，建立应用研究成果向工程技术转化的网络安全课程支撑平台。网络靶场实验平台通过安全信息对抗、攻防竞赛，充分发挥网络攻防演练、技能学习、日常训练和安全培训等作用，为信息系统安全课程提供虚拟仿真的实践氛围。

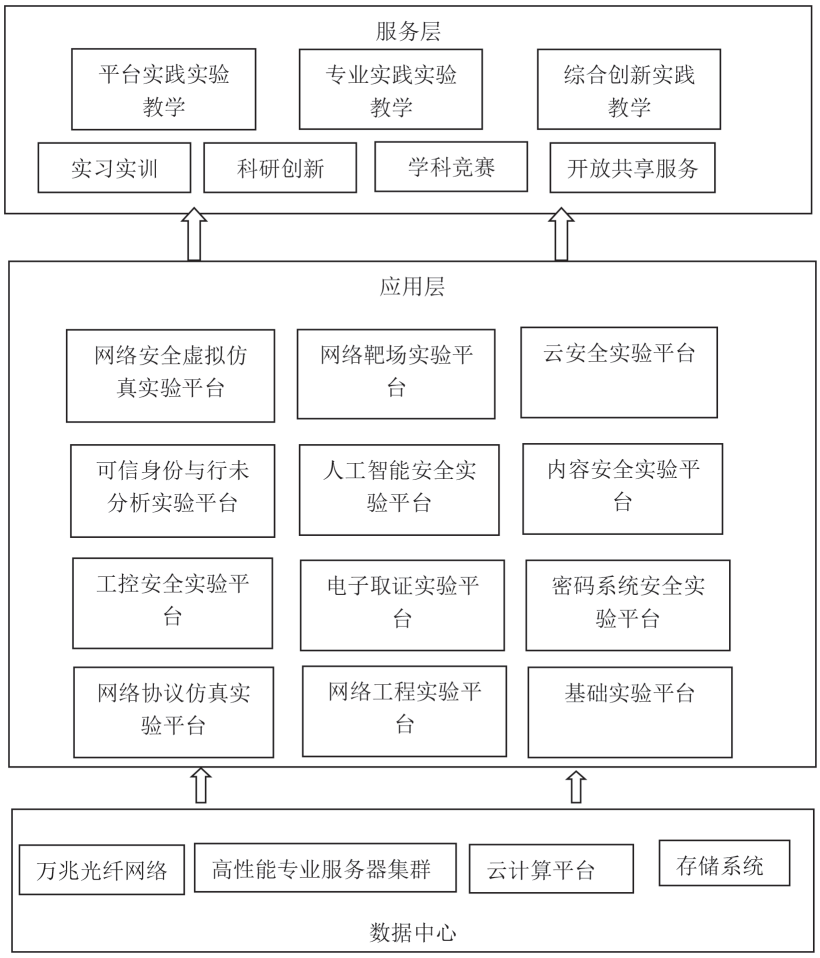

图2 高校网络安全课程实验教学平台架构

3.5.4 云安全

云安全实验平台的创建，打造以第三方为主体的云计算安全测评机制、云计算网络安全研究和云计算安全监督平台，不仅能够为计算机网络前沿技术、网络安全、网络空间安全等提供云平台支撑，同时也能够将更为智能化的安全保障与测评服务，提供给当地企业或政府，保证当地企业或政府可以安全、有效地应用云计算技术。

3.5.5 可信行为与身份分析

可信行为与身份分析实验平台，通常在可信行为与身份技术研究、人才培训、基础理论和相关应用技术研究等环节应用，也是网络安全实验平台的重要组成内容。

3.5.6 人工智能安全

人工智能安全实验平台主要是对高质量的智能化人才进行系统性培养。实验平台主要提供自然语言处理、深度学习、人工智能算法、神经网络、GPU应用技术和计算机视觉等内容，而且涵盖了人工智能知识点的应用方向。

3.5.7 工业控制安全

实验教学中工业控制安全实验平台是基于仿真工业生产流程、仿真工业控制网络，将安全检测、攻防技术验证、风险评估和攻防演练等多样化功能提供给高校师生，可以展现出恶意软件攻击与部署网络安全防护方案所导致的影响，同时有效地验证新防护和互联网攻击技术，最终实现检测验证和人才培养目标。

（下转第110页）

网络犯罪的治理现状和疏解路径

刘洋
（江西理工大学，江西赣州341000）

摘要：

［目的/意义］ 由于互联网在人们日常生活中扮演着日益重要的角色，网络犯罪也因此而伴生和持续扩大，成为网络社会的犯罪新类型。当前，我国的网络犯罪活动日渐猖獗，给国民经济带来了严重损失，并且对国家和人民重要法益构成了极大威胁，这对稳定网络空间秩序，维护网络空间安全，推进网络空间命运共同体建设而研究治理网络犯罪问题，具有十分重要的现实意义。

［方法/过程］ 为了有效地应对网络犯罪，应当在坚持罪刑法定原则和国家宽严并济基本犯罪政策相互联系的基础上,积极探索防范良策，合理拓展网络犯罪圈,严格规范互联网的刑事司法活动，赋予网络服务商对网络犯罪管理刑事法义务。

［结果/结论］ 加强对网络犯罪的治理，构建中国特色社会主义法治社会建设的网络空间命运共同体，必将在治理网络空间中实现跨越式发展。

关键词： 网络犯罪；立法现状；治理现状；网络安全；疏解路径

中图分类号： D914 **文献标识码：** A

The current situation of cybercrime management and the way to solve it

Liu Yang
(*Jiangxi University of Science and Technology,Jiangxi Ganzhou 341000*)

Abstract:

[Purpose/Significance] As the Internet plays an increasingly huge role in the daily life of the society, the Internet crime is accompanied and continuously expanded, becoming a new type of crime in the network society. Currently, information network crimes grow rapidly, which brings serious losses to the national economy and poses great danger to the important legal interests of the country and people. It is of great practical significance to stabilize the order of cyberspace, maintain cyberspace security, promote the building of a community of shared future in cyberspace, and study and control cyber crimes.

[Method/Process] In order to effectively deal with information cyber crimes, we should, on the basis of adhering to the principle of legality and punishment and the interrelation between the national basic crime policy of leniency and justice, actively explore good prevention measures, reasonably expand the Internet crime circle, strictly regulate the Internet criminal judicial activities, and give Internet service providers the obligation to manage the criminal law of Internet crimes.

[Results/Conclusion] To strengthen the governance of cyber crimes and build a community of shared future in cyberspace for building a socialist society under the rule of law with Chinese characteristics will surely achieve leapfrog development in the governance of cyberspace.

Keywords: cyber crime; legislation status; governance status; network security; dredging path

0 引言

伴随着全球大数据信息化网络新型化的产生和发展，人类赖以生存的生活环境和生存状态发生了翻天覆地的变化，成功地开创了人类新纪元时代。随着万物互联的大数据时代的来临,我国网络经济日益繁荣、网络社交日益频繁,网络已成为公众参与经济、社会活动及日常交流的重要载体。同时，网络犯罪随之不断滋生、蔓延且形态各异,网络犯罪案件总量以及在全部犯罪案例总数中的占比都呈现逐渐增加态势。网络犯罪既扰乱公共秩序的共性也有自身特性，例如犯罪手段的特殊性及行为人的不在场性等。

有效预防和控制网络犯罪，是进一步提升我国网络安全范围内防范机制和防护能力现代化的需要。着眼于全球网络环境综合整治，积极构建世界网络环境发展命运共同体，推进“境内全球双循环互动新增长布局”。应当密切注视网络犯罪的发展状况，总结并厘清发展脉络，以寻求防范良策。

1 我国网络犯罪立法现状

网络犯罪是针对或者利用网络方式进行的犯罪行为活动，触犯的罪名高达47种，特别是在2015 年 11 月《中华人民共和国刑法修正案(九)》施行后，随着刑事立法新罪名的实施，网络犯罪触犯的罪名明显增多，主要可分为两部分进行修改。

1.1 新增网络犯罪罪名

通过《中华人民共和国刑法修正案(九)》〔以下简称《刑法修正案(九)》〕第286条之一拒不履行网络安全管理义务罪、第287条之一非法利用信息网络罪、第287条之二帮助信息网络犯罪活动罪，对网络犯罪罪名进行了扩大化。

1.2 对传统网络犯罪纠偏

对与网络行为相关的传统犯罪的网络化等犯罪进行纠偏，包括《刑法》第246条侮辱、诽谤罪，第253条侵犯公民个人信息罪，第285条非法侵入计算机信息系统罪，第286条破坏计算机信息系统罪，第288条扰乱无线电通讯秩序罪，第291条之一的编造、故意传播虚假信息罪等。

总的来看，我国对于预防和惩治网络犯罪的力度在不断加大，根据当前网络犯罪发展趋势逐步扩大化的情况下，对于网络刑事犯罪的行为主体、行为方式、罪名体系以及刑罚处罚幅度等，我国在刑事立法方面也是逐步呈现扩张化的趋势。但是，面对信息化网络时代日益复杂多变的情况，我国在刑事立法方面也是在《刑法修正案(九)》的基础上，扩大了网络犯罪的罪名形式，加重了对违反网络犯罪的惩治力度。尽管如此，国家司法机关在防范和惩治信息化网络犯罪的进程中，依然阻力很大，呈现出的特点是多样化、复杂化和智能化。与此同时网络犯罪的行为手段也在日新月异。因此，仍需正视当前司法实践阶段网络违法犯罪的治理现状，剖析相关网络违法犯罪的具体情况，有效地预防和控制网络违法犯罪的肆意滋生。

2 我国网络犯罪的治理现状

网络犯罪活动有着集群化、专业性、智能化和隐秘化等特征,而由于信息科技的发展更是不断地迭代改造,且不受地区、国别局限，对社会危害将明显地高于普通的传统犯罪行为，对社会带来了重大损失,更是危及国家安全，广大人民群众对此犯罪行为也是深恶痛绝、在社会上反响强烈。所以，对当前网络犯罪的刑法政策，在总体上仍以“严打”为基础，并在规定、司法的各环节和教育领域中持续保持着高压态势，从而构成对公共信息网络中犯罪活动的有效震慑。

在传统网络犯罪不断涌现、技术手段日益翻新的今天，新兴网络犯罪手段已呈现出了智能化、复杂化、多样化的趋势。具体而言，既包括传统的木马控制、黑客渗透、病毒操纵、挂黑链、DNS劫持、DDoS攻击等，还包括新型的撞库盗取数据、预置静默插件、VPN 翻墙等，甚至出现了网络型集资诈骗、非法吸收公众存款以及网络黑恶势力犯罪。与此同时，网络犯罪还呈现出产业化和组织化的倾向，上下游犯罪关联紧密。上游犯罪有技术手段、设施、平台做保障，下游犯罪分子可以运用上游犯罪所提供的程序、工具、技术手段，进行诈骗、制造、故意传递虚假恐怖消息、侵害公民的个

人信息，并利用互联网对他人实施威胁、敲诈勒索或破坏社会秩序，从而产生极其不良的社会危害。

犯罪行为人将网络科技与犯罪手段相结合，不断更新行为方式，致使新型网络犯罪呈现出混杂、异化趋势，危害后果具有严重的多元性和复杂性。具体来说，危害后果主要包括4点。

一是对国家的危害。犯罪行为人利用互联网进行针对国家机关的危险活动。例如，发布破坏我国政权的言论、泄露和传播国家机密等，在不断激化社会矛盾的同时，通过网络号召不特定的行为人加入其中，宣扬并传播危害国家安全的价值理念、意识形态。

其二，对企业的危害。主要表现在对企业商业秘密、著作权等的侵犯，犯罪行为人通过网络对经济活动进行破坏、对企业商业秘密进行盗取、对著作权进行剽窃等。

其三，对个人的危害。例如，以人肉搜索的形式对当事人进行骚扰，尤其是集体网络暴力行为，对被害人的身心健康造成极为严重的侵害。

其四，对公共利益的侵害。鉴于网络犯罪具有对象的不特定性、快捷性、虚拟性、跨区域性，致使其侵害的法益超越个体，逐渐转变为对公共利益的侵害，危害后果具有持续性、频繁性和难以惩治性。

在我国网络犯罪立法初期，由于上网人数少、网络基础设置建设不足、网络普及率极低、计算机等设备多由国家、企业等管理、使用、经营，当时的犯罪行为多是针对计算机设备的犯罪行为，侵害的法益主要是国家对网络的管理秩序。随着我国经济的发展，网络设备不断更新、网络技术不断进步、网络使用者数量与日俱增，个人逐渐成为网络活动的主体。此时，网络犯罪法益侵害对象由秩序类法益向公民个人法益转变，且犯罪行为侵害对象多系不特定的被害人，并波及公共利益及网络秩序，致使法益侵害兼具公共性、秩序性。

3 预防和惩治网络犯罪的疏解路径

3.1 贯彻宽严相济的刑事原则

由于互联网空间的高速增长，犯罪活动方式也越来越多样化，而刑事犯罪观念也需要伴随互联网氛围的增长而不断更新。罪刑法定原则特点是“法无明文规定不为罪,法无明文规定不处罚”。

我国在刑事立法方面增加了网络刑事犯罪的相应刑罚，司法机关在解释网络犯罪等条文时，注重对网络服务提供者的预设行为、辅助行为、制定适当的监管义务等方面的延伸性解释，不仅有利于规范网络犯罪行为，而且可以避免犯罪的刑期被打破，填补我国在这一领域原有的刑事理念的空缺，给立法者指点了迷津，让司法人员有“法”可依。但是，宽严相济也是现行中国刑事犯罪的基本方针，贯穿于刑事立法、审判和刑事执行的始终。在各类以网络犯罪活动为典型的新型违法犯罪活动中，不是简单地按照新的刑事法制构建的现实需要和社会能动作用，从犯罪行为反映出的客观事实和客观规律出发，走过去一味“严打”和一概“严打”的套路，而是必须抓住宽严并济的基本原则，对服务的社会领域进行严厉打击。

总之，实施信息技术网络犯罪的基本刑事法律制度，正是要紧紧围绕宽严相济这一基本刑法政策，坚持和掌握“宽”与“严”两个字中间需要动态平衡的“济”字的真正内涵，建立起良性互动、优势互补的机制，才能使宽严相济这一基本刑法政策真正落到实处。

3.2 合理扩张网络犯罪圈

随着信息网络技术的迅速发展和不断更新，网络越轨与犯罪行为相应地实现“迭代更新”。由于刑法现行的信息技术犯罪圈并不能有效合理地限制新型网络犯罪活动,因而刑事法律规制和惩罚性滞后于网络犯罪活动也是客观存在的现象。这样，就迫切要求我国的立法工作适时推进，以扩大网络与犯罪圈，进而有效地堵住刑立法制度的漏洞。由于信息网络科技的迅猛发展，又一茬的网络犯罪开始和正在出现，其隐蔽性、高发性以及危害范围都将进一步扩大，因此公共领域信息网络犯罪态势依然严重。

维护网络空间安全，对刑事立法也必须适时反应，合理拓展网络的犯罪圈。这种从严管理的扩张型立法，具体可能呈现为三种类型：第一种是根据新类型的网络危害情况，适时创设与之相

呼应的刑罚惩治措施；第二种是在犯罪实施条件的设定上，可通过对准备犯罪正实施犯化和对辅助手段正犯化的主动扩展措施，提早对个罪的打击时间和拓展个罪的打击领域，以实现“打早打小”；第三种是在犯罪配置上，可以设置限制甚至剥夺行为人参与网络安全犯罪行为备案记录机会的禁止性条件，这样可以更有针对性地提高网络安全犯罪行为的违法效率。可以预料的是，网络犯罪活动必将成为今后中国犯案管理中的重症和顽疾。

加强网络空间安全治理，在未来对于网络犯罪的刑事立法，也必须及时有效且积极主动，以严为先，合理扩大网络犯罪活动圈。根据当前网络犯罪的严峻形势，积极合理地拓展公共网络犯罪圈，是对贯彻国家宽严相济基本犯罪政策“严厉”的实际要求，而严厉打击并不是简单粗暴地直接运用于刑事司法活动。刑事司法也有自己的基本规则，必须坚持与程序合法、罪刑合法、罪责刑相适应的基本司法为准则。

从这种意义上说，对于网络犯罪的刑事司法工作必须小心为之，切忌以从严打击为由运动式地执行，以至产生出大量的冤假错案，进而破坏国家法治与司法的公信力。合理地规定网络犯罪的刑事审判行为，要从程序规定上严格按照程序的合法原则行事。针对特殊、复杂的公共网络犯罪案件，特别需要注意程序规定的必要性，以避免因事、因案而突破法律程序规定。针对特定情况、没有明确具体流程规定的特定刑事案件，通过研究具体办案流程中的各种疑难问题，提炼调整和创设某些制度上的原则，从而促进刑事案件司法程序的立法改进。在确定刑罚的过程中，也要严格遵循罪刑法定的原则。

面对新型网络偏差犯罪，妥当地使用扩张理解方式，正确掌握已有犯罪的构成要素内涵，不能以相似性为判定基础而类推入罪。对确有重大社会危害的网络行为，如果无法依据已有罪名进行规制的，也就无法单纯套用一些含有法律兜底规定的新罪名，进行强行定罪或惩罚。司法机构只能在坚持罪刑法定原则的基础上，选择从宽政策予以出罪，并在总结犯罪行为的类型性和社会危险性后，进行犯罪立法或修订的工作。

3.3 赋予网络犯罪控制刑事法义务

对于网络服务提供者的刑事责任，主要是通过司法解释的形式来完成，此前已经确立了《刑法修正案(九)》。其中，对于“管理责任”的规定，主要是“两高”解释(二)第3条关于办理利用互联网、移动通信终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的规定。该条款被视为正式使用的“从犯罪”。有学者在反思“从犯”思维后认为，网络服务提供者的管理责任应直接通过立法形式确立，对服务提供者的行为规范应予以明确。《刑法修正案(九)》第28条实际上就是以立法的形式，对互联网服务提供者明确内部控制义务这一思想的直接反映。

网络空间是一种信息内容迅速扩散、使用者群体规模巨大的空间，管辖对象非常复杂。互联网服务的管理工作范围必须在立法时作出明确规定，才能对网络平台空间的管理服务作出合理、恰当的规范。但是，也缺乏立法中明确、具体化的管理服务规范，这是目前立法中尚未明确划分网络平台服务提供者的标准所致。《刑法》关于网络服务提供者义务的规定，既要有区别性，又要有适用范围，网络服务提供者的义务应当具有区别性。在美国和欧洲，把要求所有包含网络平台内容的各种主体“分担责任”，作为互联网管理的基本准则之一。

针对不同互联网服务提供者的管理义务，需要政府根据服务领域的不同做出明确的规定。

一是对涉及个人隐私的信息或内容进行审查，互联网服务提供者不应尽到主动审查的义务。因为这类对信息内容的审查可能会损害信息内容发布者的保护利益，与维护公众隐私权理念相对立。

其二，必须强化第三方交易平台作为互联网服务提供者的监管义务，从而降低互联网欺诈以及其他互联网金融类犯罪行为的风险。

其三，必须全面保护消费者的信息权益，确定需要使用消费者个人信息的行为与途径，设立消费者主动的途径，享受救济权利，不滥用管理义务。《关于办理非法利用信息网络犯罪活动、

帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》2019年10月25日，最高人民法院、最高人民检察院联合发布，明确了拒不履行网络安全管理义务犯罪的主体范围、犯罪的前置条件、入罪标准和客观行为方式，同时做到了入罪有据。

国家刑法必须对这些义务作出合理的规定，在不过分依赖某一方面的监督，让各个监督机关相互协调的情况下，找到政府、社会和网络服务供应商三方对网络监督管理的平衡点，才能更好地对网络空间进行监督和管理，这不仅是为了履行管理义务。

4 结束语

随着信息技术和信息产业的不断发展，网络犯罪行为将趋于多样化而更具争议，网络犯罪的司法认定问题也将更为复杂，惩治网络犯罪更加富有挑战。网络犯罪直接关系到国家安全、经济发展、社会稳定及个人权益。正如总书记所言，“网络空间不是‘法外之地’。”国家刑事司法机关对互联网犯罪惩治十分重视，强调加大对网络犯罪活动的严厉打击力度。对于纷乱芜杂的新兴网络犯罪，应结合典型特征和突出问题，有针对性地提前预防、加以规制，在惩治网络犯罪的同时，营造和谐、规范的网络创新环境，促进网络经济、网络生态的健康和有序发展。

参考文献：

[1] 习近平.习近平谈治国理政（第二卷）[M].北京:外文出版社,2017年版,第534页.

[2] 皮勇.新型网络犯罪独立性的教义学分析及司法实证[J].政治与法律,2021(10):91-106.

[3] 单奕铭.我国网络犯罪立法现状及其应然方向[J].河北法学,2018(06):141-149.

[4] 赵靓.论信息网络犯罪发展态势与刑事政策完善[J].中国应用法学,2022(01):122-134.

[5] 李源粒.网络安全与平台服务商的刑事责任[J].法学论坛,2014(06):25-34.

[6] 悦洋,魏东.网络平台犯罪的政策调适与刑法应对[J].河南社会科学,2019(05):88-95.

[7] 张佳华.大数据时代新型网络犯罪的惩治困境及进路[J].学习与实践,2022,(05):85-95.

[8] 王志杰.网络恐怖犯罪分析与防控对策研究[J].网络空间安全,2023,14(01):40-44.

[9] 常晨曦.网络空间治理视角下网络暴力问题研究[J].网络空间安全,2022,13(03):6-10.

[10] 马朝霞.网络安全治理体系建设对策研究[J].网络空间安全,2021,12(Z5):6-10.

[11] 刘霜,陈佳玉.论网络空间刑事理念面临的挑战、应对与重塑[J].河南社会科学,2020(08):63-71.

作者简介：

刘洋（1998-），**男**，**汉族**，**湖南衡阳人**，**江西理工大学法学院**，**在读硕士**；**主要研究方向和关注领域**：**刑法学和网络安全**。

网络越轨行为治理困境与对策研究

李政轩
（中国人民公安大学，北京100038）

摘要：

［目的/意义］ 随着经济社会持续发展，网络技术极大地丰富了人们的日常生活。但是，由于精神世界的空虚和制度规范的滞后等因素，导致文化堕距形成，并由此不断诱发出网络越轨行为，成为当下网络空间治理无法回避的问题。

［方法/过程］ 通过对网络越轨行为进行分析，网络越轨行为包括悖德行为、网络一般违法行为和网络犯罪行为。根据文化堕距理论，目前仍存在“网络空间的治理规范不足”“物质文化的发展引发结构性紧张”“信息技术使用能力有待提升”的治理困境。

［结果/结论］ 需要从“加快网络空间法治化”“回归社会源头治理”和“深化公安技术治网水平”方面缩小文化堕距，实现网络越轨行为的治理。

关键词： 文化堕距；网络空间；越轨；治理；犯罪预防

中图分类号： D917.3 **文献标识码：** A

Research on the dilemma and countermeasures of network deviant behavior

Li Zhengxuan
(*People's Public Security University of China,Beijing 100038*)

Abstract:

[Purpose/Significance] With the continuous development of economy and society, network technology has greatly enriched People's Daily life. However, due to the emptiness of the spiritual world and the lag of system and norms, cultural lag has been formed, and thus constantly induces network deviant behavior, which has become an unavoidable problem in the current cyberspace governance.

[Method/Process] Through the analysis of the network deviant behavior, the network deviant behavior includes the unethical behavior, the network general illegal behavior and the network crime. According to the perspective of cultural lag theory, there are still governance dilemmas such as "insufficient governance norms in cyberspace", "structural tension caused by the development of material culture" and "the ability to use information technology needs to be improved".

[Results/Conclusion] Therefore, it is necessary to narrow the cultural lag from three aspects: "speeding up the rule of law in cyberspace", "returning to the source of social governance" and "deepening the level of public security technology governing the Internet", so as to realize the governance of network deviant behaviors.

Keywords: cultural lag; cyberspace; deviant behavior; governance; crime prevention

0 引言

在物质文化迅猛发展的今天，人们的生活越来越依赖于网络，衣食住行、商务办公、社会治理等已经从物理空间延伸至虚拟网络。根据中国互联网络信息中心发布的第51次《中国互联网络发展状况统计报告》，截至2022年12月，我国网民规模达到10.67亿，互联网普及率达到75.6%。在互联网为人们的生活带来便捷的同时，也滋生出利用互联网进行谩骂、网络骚扰、传播淫秽视频、电信诈骗等网络越轨行为[1]。同时，由于网络犯罪存在于数字世界，取证固证的难度大，而且公安机关传统的侦察模式协作程序繁琐、信息不畅通，因此很难抓住罪犯并对其进行惩罚[2]。

网络越轨行为产生自经济社会的发展，并危害社会，需要从社会的宏观视角剖析。虽然当前人们物质生活条件得到了极大改善，但是与之并存的精神文化的空虚、有关规范的滞后，文化堕距由此形成，并成为网络越轨行为愈演愈烈的重要因素。通过文化堕距理论的视角，在社会大力发展物质文化的同时，也要重视丰富人们的精神文化，提高内在辨别意识，加强制度建设，筑牢外部规范，在缩小文化堕距的同时，实现网络空间的长效治理。

1 网络越轨行为的定义和分类

西方国家最早对越轨行为进行了系统的社会学研究，并产生了相应的学派，分别代表着越轨概念界定的不同视角。在19世纪末，迪尔凯姆以自杀现象为典型展开了对越轨问题的研究。他认为，失范是所有道德的对立面，社会失范在宏观层面表现为社会制度体系的不稳定，在微观层面指的就是失范行为，即越轨行为[3]。

我国古代用越轨喻指不按常规抑或违反制度，例如《北史·魏纪三·孝文帝》载:“乃者人渐奢尚,婚葬越轨”。《大百科全书·社会学卷》中对“越轨”所做的定义是指违反重要的社会规范的行为，又称为离轨行为或偏离行为[4]。

此外，我国学者皮艺军认为，越轨是社会生活中的越轨，超越了社会生活中的规则，这些规则包含了人的价值观、道德观、法治观念和基本行为准则。它是个体对于主导文化的不适应，同时也是寻求一种新的适应，只不过新的适应所归顺的是另一套与主导文化相分离的亚文化规范体系[5]。为了使得越轨概念得以操作化，本文界定的网络越轨行为，系行为人在使用网络过程中违反有关法律规范或对现有法治观念造成损害的行为，包括悖德行为、网络一般违法行为与网络犯罪行为[6]。

1.1 网络悖德行为

2019年10月，在中共中央、国务院印发的《新时代公民道德建设实施纲要》中，从新时代公民道德建设的战略高度出发，强调要抓好网络空间道德建设。网络空间的匿名性和非物理性在一定程度上导致了秩序与自由之间的紧张张力，产生出大量网络越轨行为。近年来，追星乱象屡禁不止甚至愈演愈烈，在群体极化的心理效应下，饭圈一昧夸赞偶像和维护偶像形象，在盲目吹捧中颠倒到黑白。此外，网络暴力频繁发生。注重“实事求是”的唯物主义辩证法在部分网民的网络生活中遭到忽略，事情变得非黑即白，参与事件的网民盲目支持某一方过于绝对化的观点，披着道德的外衣做着违反道德的事，抑或站在道德的制高点对他人进行批判。这表现出一种扭曲的价值观，坚决不承认错误，抑或在对别人的批判中产生了一种“变态”的优越感。

1.2 网络一般违法行为

互联网并不是法外之地，网络空间中的一言一行都需要在法律规定的范围内进行。在新型冠状疫情爆发时期，有些别有用心的人唯恐天下不乱，造谣传谣，导致人心惶惶、扰乱疫情防控秩序。《中华人民共和国治安管理处罚法》（以下简称《治安管理处罚法》）第25条对网民散播谣言的行为规定了相关处罚。违法行为人利用网络技术将涉及警情、疫情和险情等谣言[7]推送至公众面前，抑或发表过激言论，既扰乱了舆论生态，同时也违背了主流意识形态理念灌输，通过公共危机事件误导群众，对政府社会治理体系造成极大威胁[8]。

此外，根据学者的实证研究，目前黄色污染

已经成为网路上最大的污染问题。有七成大学生为满足精神上的好奇和生理上的需求选择浏览色情网站，极有可能演变出严重的社会问题[9]。《计算机信息网络国际联网管理暂行规定》第13条规定，不得浏览有关淫秽信息，若涉及复制、传播、牟利等行为，将触及《治安管理处罚法》乃至《中华人民共和国刑法》。

1.3 网络犯罪行为

随着计算机和信息技术的发展，网络犯罪现在正成为执法组织面临的最重大挑战之一，是指利用计算机或网络的犯罪活动。根据网络在犯罪中扮演的主要角色，网络犯罪可以划分为不同的类型，即可以是侵犯版权等将网络用作工具的犯罪、散播病毒等将网络作为目标的犯罪和电信诈骗等将网络作为场所的犯罪，其中包括了通过网络促成的传统犯罪和网络新型犯罪[10]。通过对中国知网（CNKI）中文总库中设置主题词为“网络犯罪”进行检索并进行可视化分析，首先可以看出学者对这一领域的关注总体上呈现递增趋势，如图1所示；其次从主题分布来看，学者们除了聚焦电信网络诈骗犯罪、“帮信罪”等网络新型犯罪，还关注到赌博、传销等传统犯罪在网络空间中的新态势；最后主要侧重于公安机关和司法认定、司法适用等打击主体、法律制定主体层面的事中控制以及事后对策研究，缺乏对于事前预防的相关研究，如图2所示。

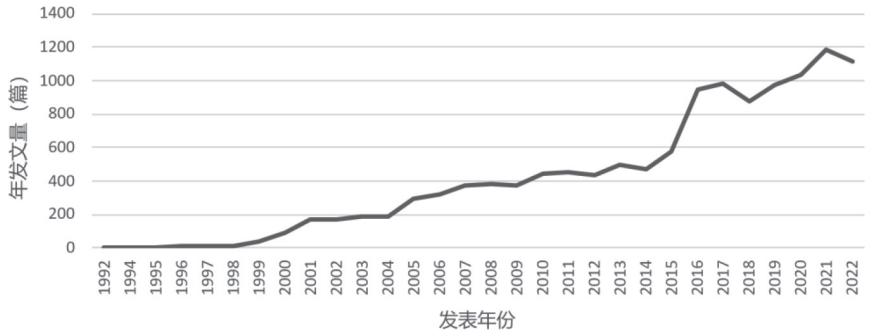

图1 “网络犯罪”主题词的年发文量趋势图

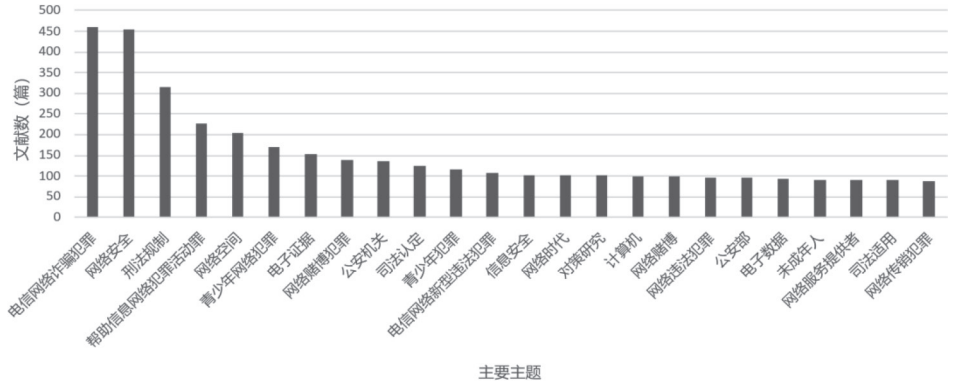

图2 文献主要主题分布图

2 诱发网络越轨行为的文化堕距

文化堕距理论由美国社会学家奥格本于1922年发表的《社会变迁》一书中提出。所谓的“文化堕距”指的是相互联系的各部分，各自独立地率先变化或滞后，其中自变量包括科技、经济、意识形态等，当变化的时间和程度不平衡而引起相互联系的各部分关系紧张就叫文化堕距[11]。在社会变迁中，物质文化变化的速度往往较快，而与之适应的制度和观念等非物质文化扩散得则较慢，这种滞后的时间倘若持续较长，会成为重大的社会问题[11]。目前，我国处于社会转型期，在经济快速发展、科技日益崛起的今天，人们过于追求效率，实用主义、工具理性逐渐占据人们的生活世界，于此同时人文

精神的培养以及相应的行为规范出现滞后。

2.1 物质生活改善是文化堕距产生的客观基础

改革开放以来，我国在人口红利的基础上不断发展经济，经过数十年的努力，我国已然成为世界第二大经济体，从“中国制造”到“中国智造”的转变、新发展格局的提出和对于“两山论”的贯彻等，都彰显出我国经济行稳致远的发展前景。与此同时，当今世界正在经历百年未有之大变局，国际形势深刻复杂、瞬息万变，在我国社会转型过程中，各类社会矛盾纠纷凸显，在社会分工不断细化、市场经济竞争机制运作以及多元文化共同作用下，人与人差异增大，分化出不同利益主体，随之形成某些“角落里”，不但包括通常意义上的“弱势群体”，还包括 “弱势特征”，比如抑郁、过劳、焦虑和失眠等[12]。与此而来的便是相对剥夺感：相对剥夺是与绝对剥夺对应的两个概念，后者涉及社会成员的生存条件，前者涉及社会成员的发展条件。

当前，我国已全面实现小康社会，社会成员产生绝对剥夺感的可能性较小，但是在日常生活的各种群体压力下，相对剥夺感时常出现。因此，虽然人们的物质生活水平得到极大改善，但是随之而来的还有各种各样的压力和冲突，在相对剥夺感产生的无奈情绪下，人们迫切地想要寻求安慰和摆脱现实困境。例如，具有交往受挫、性格敏感、人际交往能力较弱等性格特点的青年，由于无法从现实的人际交往中获得满足，于是转向网络寻求宽慰，但是随着上网时间的增加，反而会体验到更多孤独感等不良情绪，导致形成恶性循环，长期以往会形成沉溺型、发泄型或悖德型等人格障碍[13]，越轨行为因此愈演愈烈。

2.2 工具理性成为思维定式是主观条件

在我国进行现代化建设时期，市场经济高速发展、世界文化交流互鉴，“西方高度工业化过程带来的人文精神失落、生活世界萎缩的消极后果，也清晰地展示在我们眼前。工具理性过于膨胀，人与人之间关系物化、心理扭曲”[14]，由此带来的是交往沟通出现障碍。工具理性也系“效率理性”，以“实现目的”为导向，无论此目的正当与否，旨在通过精确计算功力的方式来最有效地达成目的。以此，人际交往的主体间性降格成为主客体关系，人与人之间的关系越来越趋于物化导向的合理化，缺乏共情与信赖，人与人之间的情感沟通弱化，这些不但增加的矛盾冲突产生的可能性，同时缺乏个人的情感宣泄，加剧了相对剥夺感。

人文精神的追求在经济发展的同时遭到淡忘，缺乏对于身边不良亚文化的警惕。西方国家通过文学作品、影视剧等方式，强调西方文化价值观优越性的同时向我国大肆宣扬和渗透，企图在经济全球化的今天实现政治和文化的一体化。西方的拜金主义和享乐主义等思潮在网络中涌现，一方面削弱了社会主义核心价值观的影响力，另一方面使得人们无法作出正确的价值判断。此外，由于网络的非物理性和便捷性，促使侵害人身安全的传统犯罪数量下降，利用互联网侵害他人财产的犯罪案件层出不穷，以诈骗罪和盗窃罪最为显著[15]。因此，利用网络的逐利型犯罪因隐蔽性、损失大和分布广等特点而成为众矢之的。在市场经济激烈竞争的催化下，人们“不患寡而患不均”，部分人群过于追求“有钱就是成功”的成功观，不断扩大的欲望模糊了人们心中的道德底线，因此转向得以快速致富且治理有待完善的网络空间。

3 网络越轨行为的治理困境

物质文化和非物质文化发展不平衡所引发的文化堕距诱发了网络越轨行为。与此同时，当前对于网络越轨行为的治理还存在与两者相关的困境，包括非物质文化层面相关法律规范的不健全，以及在物质文化层面，社会宏观侧的结构性紧张和公安微观侧对先进网络技术使用的不充分。

3.1 网络空间的治理规范不足

当前，利用网络犯罪越来越猖獗的原因，在于我们在“思想认识”监督体系“立法”执法等防范对策上的严重滞后性与犯罪的快速超前性，这种“文化堕距”现象，给违法分子以可乘之机[16]。法律规范作为规制网络越轨行为的依据，仍亟需进一步完善。为了回应数字社会中的犯罪，大型互联网平台成为了承担网络治理责任的“看门人”[17]。但

是，尚存常态化监管机制不足、数据共享缺乏法律依据，以及对使用数据行为的外部法律规制不健全等问题[18]，因此非物质文化的滞后与网络技术高速的发展形成了紧张张力。例如，通过各种便携智能设备的APP，就能进入各种短视频和音视频平台。自媒体时代互联网平台的准入门槛低，受众广泛，在人工审核标准有待考证和监督处罚机制不完善的情况下，色情擦边视频、涉毒音视频等亚文化产品屡禁不止，因此为了营造风清气正的网络空间环境，首当其冲的就是要整治网络文化市场中的歪风邪气，创新网络文化内容[19]。

3.2 物质文化的发展引发结构性紧张

最早提出“结构紧张”概念的是美国社会学家默顿。他通过这个概念，试图解释社会结构在什么情况下会导致社会问题的发生。他认为，“结构紧张”系社会文化所营造出来的成功价值观，与社会结构所能提供实现成功手段之间的一种失衡状态。比如，我国的社会矛盾已经转变为“人民日益增长的美好生活需要和不平衡不充分发展之间的矛盾”。目前，我国的基尼系数已经超过0.4，这就是“结构紧张”的客观证明[20]。在这种状态之下默顿认为，社会矛盾和犯罪等就会激增。

当前，某些价值观认为物质财富的富有才是成功。但是，贫富差距大、社会分层明显，同时不同阶层之间流动的途径有限，因此可以通过各种越轨行为实现向上的社会流动来缓解结构紧张[21]。与此同时，高校的专业设置和人才培养模式，需要一定的周期来调整转换。这种滞后性就激化了“人岗失落”、供需失配的结构性矛盾[22]。在学生在毕业后面临失业的压力下，实施越轨行为成为了满足生存需求的选择。

3.3 信息技术使用能力有待提升

随着网络社会的到来，传统的违法犯罪，例如贩卖毒品、拐卖人口、黑恶势力等借助新技术不断向网络空间蔓延，互联网甚至成为某些违法犯罪的主要平台和渠道，严重地危害了社会秩序，影响到了公众安全感[23]。与此同时，在大数据改变了人们生活方式的同时，也导致了电信诈骗、网络骚扰、和病毒攻击等一系列违法犯罪频发[24]，而公安机关的人力物力有限，传统的汗水警务模式已经无法适应信息化环境下现代警务工作的需要[25]。在使用大数据技术进行防控的过程中，公安机关的数据利用和警务机制仍存在滞后现象，情报信息和指挥分立等问题使得数据无法发挥出蕴含的价值。对此，必须以减少中间环节的流转、实现应用最大化为目标，对现有的警务机制进行改革和完善[26]。通过数字赋能实现治理创新是推进政府治理体系和治理能力现代化的必要途径，公安机关应该坚定信心、向数据借力，以机制改革不断提升自身治理能力。

4 提升网络空间治理能力

4.1 加快网络空间法治化

一方面针对日新月异的网络安全威胁，加快《未成年人网络保护条例》《网络数据安全管理条例》征求意见稿的修改完善以及立法进程，对不同法律规定之间冲突、衔接不畅之处，建立常态性法律内容审查机制，及时进行整合、删改，确保法律规范之间的协同性[27]。通过及时约谈、责令整改、下架停更、通报罚款等一系列惩罚手段，依法查办有关网络越轨行为，形成威慑效应。与此同时，深入开展“八五”普法规划，数字平台、学校社区、公安机关等主体分别以不同的形式，做好全国网络的普法工作。

另一方面要重视网络多元主体的自制规范。如今，以微博为代表的信息即时获取平台、微信和QQ为代表的信息交流平台，以及以抖音、快手为代表的短视频直播平台，以社会公众喜闻乐见的形式散播海量信息，对此有必要积极引导各互联网企业实事求是地制定平台准入、运营、退出规则体系以及信息管理机制[28]，从而履行好“看门人”的义务，以超大数字平台的治理回应治理能力危机，推进犯罪治理转型[29]。

4.2 回归社会源头治理

首先，宏观层面落实各项社会政策。社会政策的作用在于“润滑”各种社会关系，调和多种社会问题，而这些社会问题往往就是犯罪诱因。虽然社会政策不是对付犯罪的专门手段，但是对于犯罪却

具有治本之效[30]。因此，通过调整社会保障政策、教育政策、分配政策等，为潜在犯罪人提供良好生存发展条件，减轻结构紧张。

其次，中观层面借助新媒体弘扬社会主旋律。中华民族优良道德传统重视道德实践，强调“修身”，例如儒家倡导以追求崇高理想人格为追求，这些价值观需要我们结合当今的时代特色加以继承弘扬，同时要从多元文化中“取其精华、去其糟粕”，将优秀的人类文化其融入社会主义核心价值观话语中，并运用网络媒体新平台来加强宣传。

最后，微观层面要做好亲职教育以及学校教育。开发出“线上+线下”模式的亲职课程，按照每个家庭的不同情况有针对性地设置不同课程。例如，根据孩子所处的不同年龄阶段、不同家庭结构等设计有针对性的教育内容，尤其要关注留守家庭、单亲家庭等特殊家庭[31]。同时，学校老师不能忽视一些非考试课程的重要性，例如性启蒙课、心理健康课等，要培养“德、智、体、美、劳”全面发展的学生。

4.3 深化公安技术治网水平

公安机关要通过警务机制改革实现“公安信息化”“智慧公安”，以数据赋能逾越部门鸿沟，实现“条线”串联的一体化运作，充分调动资源，助力网络综合治理体系的构建。

一是充分利用数据。整合资源和查询权限，对全局范围内的情报、信息资源和查询权限实行集中管理。同时，最大限度统筹警种有关案件预警、数据分析、收集情报等重复性情报工作，提高警务效能。

二是完善数据建模。情报分析系统是以关联分析、统计分析和预测等模型为基础建立起来的，如果缺少相应的数据模型，则说明情报系统的分析能力不足，为此要将业务流程转化为业务模型，再转化为数据模型，最终转化为应用程序，以便开展科学预测、趋势分析、跟踪监测、犯罪模式发现等应用[32]。

三是构建对外信息共享平台，公安机关在情报获取和侦查破案中也需要与其它政府部门或者有关社会机构交流信息，例如推进与其它政法机关，金融、电信等机构的信息共享工作。共享平台建设要与边界接入平台建设紧密结合，采用安全隔离设备和身份认证及访问控制来确保公安内、外网数据交换共享的安全[32]。

5 结束语

孔子最早主张人应该在满足基本物质生活的基础上关注精神需求，而且要以关注精神需求作为人们幸福生活的依据。在经济持续向好、网络技术不断发展的今天，网络越轨行为敲响了治理的警钟，物质生活水平的进步是人民幸福、国家发展的基石，同时我们也不能忽视非物质文化的滞后带来的不良社会问题。因此以缩小文化堕距作为治理目标，才能更好地理解把握网络越轨行为，并提出有效的事前治理对策。

参考文献：

[1] 白淑英,邵力.社会存在还是意义建构?——为青少年网络越轨行为辩护[J].青少年犯罪问题,2010(03):70-74.

[2] 梁朕.总体国家安全观下电信网络诈骗研究[J].网络空间安全,2023,14(01):16-20.

[3] 朱力.失范范畴的理论演化[J].南京大学学报（哲学.人文科学.社会科学版）,2007,(04):131-144.

[4] 刘晓善,洪晓楠.越轨的界定与划分研究[J].大连理工大学学报（社会科学版）,2012,33(02):99-104.

[5] 皮艺军.越轨社会学概论[M].北京:中国政法大学出版社,2004:2.

[6] 皮艺军.人类性越轨探源[M].北京:长征出版社,2000:34.

[7] 姚福生.依法行政视野下网络谣言的治理研究——基于2021年以来公安机关行政处罚案件的分析[J].西北民族大学学报（哲学社会科学版）,2023(02):87-96.

[8] 武峥.网络谣言对主流意识形态的危害及其治理[J].长白学刊,2023(02):49-57.

[9] 李志,李龙.网络色情信息对大学生的影响及治理[J].青年记者,2015,(23):11-12.

[10] Zhang Y, Xiao Y, Ghaboosi K, et al. A survey of cyber crimes[J]. Security and Communication Networks, 2012,5(4): 422-437.

[11] [美]奥格本.王晓毅,等;译.社会变迁[M].浙江:浙江人民出版社,1989:144,269.

[12] 冯仕政.社会治理与公共生活:从连结到团结[J].社会学研究,2021,36(01):1-22+226.

[13] 王珑玲.网络对青年心理健康的负面影响及对策[J].中国青年研究,2011(03):82-86.

[14] 韩红.交往的合理化与现代性的重建——哈贝马斯交往行动理论的深层解读.[M].北京;人民出版社,2005:279.

[15] 张智辉,姜娇.网络犯罪新样态与刑法应对[J].学术探索,2023,(03):61-68.
[16] 肖爱兰.高科技工具——网络技术犯罪的主要特点及预防对策[J].科技进步与对策,2003,20(08):156-157.
[17] 单勇.数字看门人与超大平台的犯罪治理[J].法律科学（西北政法大学学报）,2022,40(02):74-88.
[18] 孟凡新.双循环视角下提升数字平台治理水平的机制研究[J].商业经济研究,2023,(06):105-109.
[19] 马朝霞.网络安全治理体系建设对策研究[J].网络空间安全,2021,12(Z5):6-10.
[20] 刘仁春,徐连明.社会结构紧张之下的网络怨恨及其纾解[J].广西师范大学学报（哲学社会科学版）,2019,55(05):16-25.
[21] 陈晓明.引发犯罪的社会结构因素分析[J].甘肃政法学院学报,2007(01):98-104.
[22] 许涛.共同富裕与高校大学生高质量就业:社会分层结构变迁的审视[J].黑龙江高教研究,2022,40(12):132-137.
[23] 宫志刚.历史交汇期社会风险防控与警务战略转型[J].公安学研究,2018,1(01):55-77+123.
[24] 刘志勇.大数据战略视角下警务合成作战指挥机制创新研究[J].公安学研究,2021,4(02):51-73+123-124.
[25] 原庆.大数据背景下合成作战平台建设思路及其应用[J].警察技术,2021(04):37-40.
[26] 张应立.大数据背景下的盗抢犯罪防控研究——以宁波市为例[J].河南警察学院学报,2018,27(04):71-81.
[27] 陈荣昌.网络信息内容治理法治化路径探析[J].云南行政学院学报,2020,22(05):48-53.
[28] 崔聪.论网络空间道德秩序构建的法治保障[J].思想理论教育,2021,(01):21-27.
[29] 单勇.数字平台与犯罪治理转型[J].社会学研究,2022,37(04):45-68+227.
[30] 蔡应明著.犯罪预防学[M].上海:上海三联书店,2010:198.
[31] 于阳,周丽宁.青少年弑亲行为的主要特征、成因分析与防治对策——基于2010-2019年的31起典型案件分析[J].青少年犯罪问题,2020,No.226(01):68-79.
[32] 张兆端.智慧公安[M].北京:中国人民公安大学出版社,2015:90,159.

作者简介：

李政轩（1999-），**男**，**汉族**，**福建泉州人**，**中国人民公安大学犯罪学学院**，**在读硕士**；**主要研究方向和关注领域**：**犯罪社会学和网络安全**。

（上接第98页）

3.5.8 内容安全

实验教学体系中的内容安全实验平台，主要涵盖数据挖掘深度学习、信息处理架构、信息内容识别、网络编程、信息挖掘和分析、融合安全监测防护、网络安全响应和网络信息舆情技术等内容。

4 结束语

高等院校网络安全课程实验教学平台的优势主要在于便捷灵活，而且能够实现网络信息资源共享，所需实验设备成本比较低，能够在短时间内进行课程实验平台的构建。在网络安全人才培养方面，实验教学平台的亮点和特色非常突出，比方设计实施一体化、实验项目内容开放共享和项目分阶段实施等。高校网络安全课程实验教学平台既满足“网络安全”“计算机网络”等课程教学需求，而且又注重绿色创新实验教学理念。为此，高校应与自身人才培养目标和办学定位相结合，遵循绿色发展理念，重视综合型人才的培养，加大设施设备投入力度，通过虚拟化、大数据和云计算等技术，逐渐向智慧化实验教学方向转型。

参考文献：

[1] 史建焘,李秀坤,张宏莉.虚拟仿真云平台下信息内容安全实验课建设[J].实验技术与管理,2019,34(04):9-13.
[2] 尚涛,刘建伟.网络安全课程探究型实验教学模式构建[J].工业和信息化教育,2020(05):6-9+5.
[3] 崔玉礼,黄丽君.网络安全分析中的大数据技术应用[J].网络空间安全, 2016:15-16.
[4] 杨钰琳,杨翠翠.大学生网络安全教育现状及对策研究[J].网络空间安全, 2020, 11(3)85-89.

作者简介：

亢立明（1993-），**男**，**汉族**，**吉林通化人**，**长春理工大学**，**硕士**；**长春职工大学**，**助教**；**主要研究方向和关注领域**：**计算机软件及应用、网络安全教学**。

网络暴力入罪之批判与治理路径探析

陆林炜
（南京师范大学，江苏南京210046）

摘要：

[目的/意义] 在互联网技术飞速发展的同时，亦导致了网络暴力的横行。网络暴力对公民的人身和财产权益造成了严重威胁，妥善的刑事规制值得关注。

[方法/过程] 厘清网络暴力概念，提出言论犯罪有违自由主义刑法理念。网络暴力造成行为人法益损害的结果与行为之间的因果性难以确定。

[结果/结论] “网络不是法外之地”，维护平等、自由的网络言论空间是保障民众网络合法权益的前提。在选择网络治理工具时，要警惕“刑法万能主义”观念。

关键词： 网络暴力；立法；名誉；法益；网络安全治理

中图分类号： D924.3 **文献标识码：** A

Analysis of criticism and governance pathways of cyber violence criminalization

Lu Linwei
(*Nanjing Normal University, Jiangsu Nanjing 210046*)

Abstract:

[Purpose/Significance] The issue of harm caused by online infringement has gained attention from legal scholars, yet the creation of a standalone criminal charge runs counter to the prudence principle of criminal law and lacks necessity. Proper regulation of online infringement can be achieved through the utilization of alternative governance tools.

[Method/Process] To tackle online violence effectively, it is essential to have a clear understanding of its concept. However, criminalizing speech crimes may not align with the liberal philosophy of criminal law. Furthermore, ascertaining causality between online violence and the legal harm suffered by the perpetrator is difficult.

[Results/Conclusion] "The internet is not exempt from the law". Preserving an equitable and liberal atmosphere for online expression is essential for upholding the lawful rights and interests of citizens. While selecting means for online regulation, we should be mindful of the concept of "The omnipotence of criminal law".

Keywords: online violence;legislation;reputation;legal interests;network secutity governance

0 引言

当前，互联网技术的飞速发展给公民的生活带来了诸多便利。众多网络社交平台的出现拓展了公民沟通交流的渠道，使得人与人之间的沟通不再受到时间、空间的限制。而在互联网技术带来诸多便利的同时，也带来了网络暴力的横行，对公民的人身和财产权益造成了严重威胁。具体而言，网络施暴者在虚拟空间中利用网络技术传输文字、图像和视频等信息，并对被网暴者施加侮辱和诽谤行为，被网暴者因负面评价信息导致心理创伤甚至发生自残、自杀的悲剧。

例如，四川德阳安医生与其丈夫在游泳时受到男孩骚扰，丈夫将男孩头按入水中。在这段视频被爆出后，安医生受到持续网络暴力侵害，最终选择服药自杀[1]。考研成功后的女生郑某某拿着录取通知书与病床上的爷爷拍照，这段情景在上传到网络后，只因一头粉红色的头发便受到诸多恶评，最终郑某某选择结束了自己的生命[2]。网络暴力的法益侵害性日益受到刑法学界的关注，不少学者提出有必要将网络暴力单独设立为一条罪名予以规制。但是，“法律万能论”的修法理念是否妥当？刑法的堤坝是否能止住网络暴力的洪流？除运用刑法规制网络暴力之外，网络安全治理方案应当是一套多层次和多角度的网络安全治理体系。

1 网络暴力概念

“网络暴力”并不是一个规范意义上的刑法概念，是对利用网络实施侮辱、诽谤、造谣和侵犯个人信息等一系列行为的形象表达。讨论网络暴力入罪与否，离不开对网络暴力概念的准确把握。

1.1 观点陈列与分析

关于何谓网络暴力，不同学者从不同角度给出了不同解释。有学者将网络暴力视为网络言语暴力，认为网络暴力是指网民利用网络手段营造舆论，对他人进行道德审判和语言攻击、辱骂，甚至通过“人肉搜索”暴露他人隐私，从而严重影响他人生活的行为[3]。这种观点可谓网络言语暴力说。

另有观点着眼于网络暴力的实施手段，将网络暴力定义为网民对当事人或者组织所实施的以制造心理压力为手段，以迫使当事人或组织屈服的网络攻击性行为的总称[4]。这种观点可谓暴力手段说。

还有学者将网络暴力行为与传统暴力行为相对比，认为网络暴力行为是指网络行为的实施方主体利用黑客技术、网络诽谤和网络造谣等网络攻击手段，侵犯他人人身权利、财产权利、危害国家公共安全和社会管理秩序，具有社会危害性的行为[5]。这种观点可谓特殊暴力说。

各论者虽然从不同的角度阐述了网络暴力的内涵，但是都不足以将网络暴力全面、规范地评价为一个刑法概念。网络言语暴力说指出了网络暴力的行为特征，即利用语言对他人实施攻击、辱骂，但其无法涵盖网络上利用图片、视频和语音等诸多其他手段对他人实施的网络暴力行为。暴力手段说认识到了网络暴力行为的独特性，但是论者无意中预设了网络暴力的目的要素，即“迫使他人屈服”，实施网络暴力者的内心起因是多方面的，其中不乏盲目跟风者和哗众取宠者。论者所说的目的要素将网络暴力实施者限缩在了一个很小的范围内，无法解释其他无目的的网络暴力行为。

特殊暴力说指出了网络暴力行为与传统暴力行为相比具有的独有特征，即黑客技术、网络诽谤和网络造谣等网络攻击手段，也认识到了网络暴力行为对诸多法益的侵害性，相比以上几种定义更佳，但是论者使用“黑客技术”这一表达并不严谨。众多周知，“黑客”一词源于英文“Hacker”，最初的含义为利用网络实施网络攻击者。黑客技术本身是中立无害的，但是实施黑客技术的目的和造成的结果，决定了黑客技术是否值得处罚。所以，技术作为中立的概念，不宜与诽谤和造谣等负面评价概念相并列。

因此，在总体认同特殊暴力说的基础上，综合多种学说的观点认为：刑法上所谓的网络暴力（行为）是指行为人利用网络，以网络侮辱、网络诽谤和网络造谣等为手段，实施的侵犯他人人身权利、财产权利、危害国家公共安全和社会管理秩序，具有社会危害性，值得刑法处罚的行为。

1.2 网络暴力特征

从上述定义出发，结合网络暴力的现实情况，从刑法视角总结出了网络暴力具有4个特征。

1.2.1 实施场域的特定性

虽然网络暴力所造成的结果是现实性的，可能对人身、财产和秩序等法益造成一定的侵害，但是网络暴力行为的实施场域只能限于公开的互联网。如果行为人在现实场景中针对网络上的话题，对相关人员实施侮辱和诽谤等行为不能称之为网络暴力，否则会含混网络暴力与现实暴力的边界，亦会造成网络暴力的外延不明。

1.2.2 侵害法益的多重性

网络暴力所侵害的法益是多方面的，包括人身权利、财产权利、国家公共安全和社会管理秩序等多重法益。也许有人会指出，将网络暴力造成的法益侵害拓展致国家公共安全和社会管理秩序，是否会造成保护法益的泛化。对此，需要说明的是，目前学术界和实务界已经达成了共识，即网络空间可以被解释为刑法意义上的公共场所。因此，在公共场所针对安全、秩序法益造成的侵害结果便不足为奇。

1.2.3 行为手段的多样性

因网络信息技术发展迅猛，目前利用互联网实施的网暴行为是多种多样的。行为人不仅可以在网络上以文字的形式发表言论，亦可发布图片和视频等多种信息载体，而这些载体都能够反映对他人的侮辱、诽谤。因此，网络暴力的行为手段不限于网络言语暴力，只要行为人发布的信息具有一定的法益侵害性，都可被评价为网络暴力。

1.2.4 影响扩散的广泛性

互联网信息具有弥散性的特点，通过网络散播的信息能够在短时间内扩散至较为广阔的范围。同时，信息传播的弥散性决定了网络暴力能够在短时间内形成广泛的影响，信息散播的群体数量亦会在短时间内呈指数级上升。因此，网络暴力通常造成的影响是广泛的，不受地域、时间和空间的限制。

2 网络暴力入罪理由检视

正是因为网络暴力具有较强的法益侵害性，且网络空间中不断发生的热点事件不断挑逗着民众正义的神经，故近年来不断有学者呼吁将网络暴力入刑。网络暴力入罪论者的理由有三点。

2.1 网络暴力侵害客体的特殊性

网络语言暴力行为的特点是以网络作为平台，以语言作为暴力犯罪的工具，对现实中的人进行精神上的恐吓与摧残。网络语言暴力侵犯的客体和传统犯罪是有区别的，应该以专项罪名加入刑法[6]。网络言语暴力说认为，网络言语暴力会使得受害人人格受到侮辱，心理受到摧残，严重者可能会导致受害者自杀，因此网络言语暴力行为与传统民事侵权行为所涉及的名誉权和隐私权不同。论者言下之意，正是因为网络暴力造成的侵权结果，以民法手段不足以全面保护，故侵害的客体特殊，值得突破刑法的谦抑性，从而设立专门罪名予以规制。

2.2 网络暴力社会危害性较大

有学者指出，网络暴力的社会危害性表现在三个方面：一是语言暴力会对他人名誉权（包括人格尊严）造成显著侵害；二是当语言暴力与某些违背传统道德观念的事件相联系时，尤其是被错误地强加于网络语言暴力的对象时，会造成他人社会评价的降低；三是“网络语言暴力”可能致使他人的人身权与财产权受损。因此，“网络语言暴力”不仅直接对他人名誉造成侵害，而且还可能造成他人人身和财产等其他权益的损害，有将其入刑的必要[7]。而从目前的司法实践来看，民事和行政法律只能对轻微的网络暴力行为进行法律规制，对于严重的网络暴力行为规制是

有心无力。赔偿财产损失、消除影响和道歉等民事侵权的责任承担方式，与网络暴力造成严重的社会危害性是不相符合的[8]。

2.3 刑法及司法解释规定存在疏漏

除了上述两种入罪理由外，网络暴力入罪论者还有一种较为有力的观点，认为目前的刑法与司法解释，对于网络暴力行为规制存在一定程度的疏漏。

2.3.1 司法解释不当限缩了诽谤范围

《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》（以下简称《解释》）中对“网络诽谤”的行为方式作出部分列举，同时对网络诽谤在何种情形下达到情节严重的程度也进行了列举。《解释》针对网络诽谤行为作出相关规定，将其纳入“诽谤罪”中进行规范。《解释》并没有扩大诽谤罪的处罚范围，相反，明显缩小了诽谤罪的处罚范围。在此意义上说，《解释》关于情节严重的解释缺陷，不是客观归罪与扩大处罚范围，也不是所谓“他人助罪”，而是不当缩小了网络诽谤的处罚范围[9]。

2.3.2 寻衅滋事的适用过于笼统

《解释》第5条将“网络侮辱”纳入了“寻衅滋事罪”范围。这项条款对网络侮辱行为做出的规定，也基本套用了“寻衅滋事罪”相关规定。但是，这样的规定在现实中缺乏震慑性，且过于笼统和宽泛。网络语言暴力行为并不能简单地用传统刑法上的侮辱诽谤来描述，它有自己的行为特征与犯罪形式，所造成的后果严重程度，也与传统刑法上的侮辱诽谤有很大不同，因为借助互联网络平台，伤害会被无限放大，甚至难以控制[10]。

2.3.3 现有罪名规制不足

《中华人民共和国刑法修正案（九）》分别规定了出售和非法提供公民个人信息罪和非法获取公民个人信息罪。但是，结合司法实践案例会发现，对于实践中的人肉搜索类网络暴力，并不能进行有效的规制。人肉搜索既是对被搜索人个人信息的披露，也是对被搜索人行为的惩罚[11]。在刑法的规范视域中，网络暴力带来的精神压迫（伤害）既没有直接造成死亡结果，也不能一概排除被害人的认知与判断能力，达不到教唆未成年人、无责任能力人自杀者，或教唆邪教组织人员自杀者对被害人具备的精神控制力，难以评价为故意杀人罪的实行犯或间接正犯[12]。

3 网络暴力入罪论之批判

针对网络暴力入罪论者的诸多理由，认为网络暴力并不适宜被设立为一条独立的刑法罪名，具体理由有三项。

3.1 违背自由主义刑法理念

网络暴力入罪即通过衡量行为人的言语判断其是否具有入罪的前提，也即是一种言语犯罪。实际上，有关言论犯罪的讨论早已有之。长久以来，言论犯罪作为自由主义刑法理念的对立面，历来就受到了批判。

孟德斯鸠指出，言辞绝不是构成罪的实体，而是仅仅停留在思想里。在大多数情况下，言辞本身并不说明任何东西，倒是说话时的口气能说明某些东西。重复同样的言辞，意思往往不相同，言辞的意思取决于与其思想相关的其他东西。沉默所表明的东西有时候比任何言辞更多，含混不清莫过于此。那么，怎么可以把言辞以大逆罪论处呢？凡是有这种法律的地方，连自由的影子都没有，遑论自由[13]。之所以孟德斯鸠认为言论犯罪剥夺了人的自由，是因为言论的对错只有通过事后检验才可得知，作为社会普罗大众，不能苛责文化教育水平一般的民众以学者的严谨探究言论背后的真伪。申言之：禁止一种意见的表达，其独有的罪恶之处在于，它是对包括当代人与后代人在内的全人类自由的剥夺[14]。因为如果言论是正确的，那么错误的言论会失去被纠正的机会，只有真理与谬误相碰撞才能无限靠近客观真相。

从近年来发生的网络热点事件来看，“网络暴力”与“网络正义”往往仅存一线之差，面对生活中现实发生的恶，广大网友朴素的正义感被瞬间激发，现实生活中“沉默的大多数”因为网络匿名性的包裹，选择站出来为正义发声，增强了社会的正义力量。其中，比较有代表性的有“唐山烧烤店打人事件”。正是因为网友针对施暴者进行广泛、有力的谴责，渐入尾声的扫黑除恶运动重新进入了大众的视线，全国范围内又开展了一批针对黑恶实力的打击活动，民众的安全感在一定程度上得到了提升。再如，“丰县生育八孩女子事件”的曝光，在网络上激起一波千层浪，如果不是该事件的曝光和广大网友的持续关注，普通民众难以想象正在大踏步迈入现代化的中华大地上竟还有如此荒诞、残暴的悲剧存在。试想如果不是网络力量的介入，已失去发声能力的“小花梅”断然没有可能依靠自己的力量重见天日，最终可能成为隐秘在角落的一粒尘埃，淹没在无人问津的事实深处。

所以，从事实结果上考量，所谓“网络暴力”是一把双刃剑，“网络暴力”入刑论者往往只看到了网络言论造成的悲剧，而忽略了其带来的正义之光。如果将网络言论套上刑法的枷锁，则无异于扼住了民众正义的喉舌，在衡量利弊后原本愿意为正义发声的民众，会因忌惮刑罚惩罚而选择缄默，最终损害的不仅是民众的言论自由，更会使得正义不彰、人性冷漠。

3.2 社会危害性虚幻难测

网络暴力“入刑论”者认为，网络暴力入刑的重要目的之一，即为保护人的名誉。但是，名誉本身就是一个虚无缥缈的概念，以刑法保障名誉权的思想值得警惕。18世纪的贝卡利亚提醒：名誉这个词是一个被用作高谈阔论的基础，却不带有任何稳定确切含义的辞藻。

贝卡利亚关于名誉权的否定不无道理，名誉权作为一种模糊的概念并不具有明确性，行为人对他人作出的负面评价是否会造成对其名誉权的损害，不取决于评论本身，而取决于听众的判断，只有虚假的事实被听众信以为真并形成内心负面的内心确认，才有可能降低他人的社会评价。另一方面，在多大程度上才能够评价为社会评价的降低？即有多少人因网络暴力产生了对他人的负面评价难以查明，将一个不明确的概念作为保护的对象，会损害刑法的明确性，违背罪刑法定原则。

网络暴力“入刑论”者的另一项理由认为：网络暴力不仅直接对他人名誉造成侵害，而且还可能造成他人人身和财产等其他权益的损害，言下之意，网络暴力应当作为结果犯予以考量。但是，网络暴力对他人造成的人身、财产损害结果，能否作为行为结果考量，让人值得怀疑。首先，网络暴力造成行为人法益损害的结果，与行为之间的因果性难以确定。结果是由行为造成的，行为是因，结果是果。条件说是因果关系判断中出现最早的学说，其中又以相当因果关系的折中说最为学术界认可。相当因果关系的折中说认为：如果行为时一般人知道或行为人特别知道被侵害人的特殊体质，应当肯定行为人与被侵害人死亡结果之间的因果关系。反之，则应当否定行为与结果的因果关系。

在网暴事件中，很多被网暴者先前具有心理疾病，作为网络暴力的实施者，以一般人的判断能力难以知晓其特殊体质，因此难以确定行为与结果之间具有因果关系。或许有人会从客观归责理论的角度提出反对意见。客观归责对因果关系的判断思路为：“制造不被允许的危险——实现不被允许的危险——结果没有超出构成要件的保护范围”。在制造不被允许的危险层面，如果行为人没有减少法益损害的危险，但也没有以法律上的重要方式提高法益损害的危险时，不能将结果归责于行为。

例如，行为人向快要决堤的河里倒了一盆水，由于不能肯定一盆水增加了决堤的危险，故不能将决堤的结果归责于行为人[16]。与上述例子类似的是，网暴行为可能是“压死骆驼的最后一根稻草”，但是在大规模的网暴事件中，没有一句恶评是无辜的，刑法如果惩罚“最后一根稻草”，那在此之前规模巨大的网暴者群体该如何处理？更何况网络上的数据可以被删除、修改，准确认定“最后一根稻草”在现实侦查活动中几无可能。更何况，在网络上发表言论本就是公民的言论自由权利，无法想象网络上只能允许正面

评价而不能有负面评价，网友的负面评价本就具有社会相当性。

3.3 相关法律、司法解释完备

关于网络暴力行为的治理，我国各部门的司法解释已全方面进行了规定，形成了一张层次丰富、内容全面的司法保护网。依据相关法律和司法解释等规范性文件，足以规制不同程度、不同方式的网络暴力行为，再设计一条单独的罪名违背了刑法谦抑性，更无必要性。

例如，《治安管理处罚法》第42条规定，对侮辱、诽谤行为公安机关可予以行政处罚。上述条款还列举了4种较为常见了网络暴力行为：（1）公开辱骂、无中生有，诽谤他人；（2）捏造事实，诬告陷害他人，企图使他人受到刑事追究，或者受到行政处罚；（3）屡次发送淫秽、侮辱、恐吓等信息，扰乱他人正常生活的；（4）偷窥，偷拍，窃听，传播他人隐私的。

再者，《中华人民共和国刑法》（以下简称《刑法》）第246条规定了侮辱、诽谤罪。2013年9月出台的《解释》对办理利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等刑事案件适用法律的若干问题作了相应解释。司法解释将网络暴力、网络谣言纳入“诽谤罪、寻衅滋事罪”两项罪名中进行规范，并对其应认定为严重情节的情况作了相应规定。从我国对寻衅滋事等暴力犯罪的规定来看，立法已经照顾到了网络暴力的特殊性。虽然罪名中的暴力都要求能够对法益产生物理性的作用力，但是罪名中的威胁行为并非都一定要求其所威胁的内容马上在当场付诸实行[17]。这一点与网络暴力侵害法益的特殊形式相符。

至于“入罪论”者所言该司法解释不当，缩小了网络诽谤的处罚范围的观点，并不认可。该《解释》不过是将常见的网络诽谤行为进行了进一步列举，对各级法院审理网络诽谤案件提供了切实可行的指导，这并不意味着新出现的网络诽谤方式被排除在了《解释》所列举的情形之外。无论是司法工作人员抑或是学者，对法律进行合理解释后进行适用，应是理所应当的使命和任务。而事实上，“法律不经解释无法适用”；“解释者对法律的理解可能比创立者对法律的理解更好，法律也可能比起草者更聪明——甚至必须比它的起草者更聪明”[18]。不应当机械地依赖司法解释的规定，而是要将司法解释、学理解释相结合适用法律，利用特定的解释方法求得合理的裁判理由。至于适用寻衅滋事罪过于笼统并不是一个立法上的问题，而是由于随着信息网络技术的飞速发展，网络暴力不断出现新情况、新形式，即使设立专门的网暴罪名也并不能一一列举正在出现或尚未出现的网络暴力新形式。

法律的滞后性是与生俱来的，通过妥善的解释不会出现处罚上的漏洞。事实证明，为了进一步严密刑事法网，立法机关并不是无所作为的。2015年11月1日生效的《刑法修正案（九）》新增291条第2款，规定了编造、故意传播虚假信息罪。这项条款的有关规定进一步明确限制了4类严重散播网络谣言、扰乱社会秩序的行为。除《刑法》的相关规定外，我国《民法典》第1194-1198条也明确规定了网络用户、网络服务提供者的网络侵权责任，以及网络服务提供者防止损害扩大采取必要措施的义务。

令人感到欣慰的是，近年来我国政府部门对网暴的治理更为积极，态度更为坚决。2021年，国家互联网信息办公室发布了《关于进一步压实网站平台信息内容主体责任的意见》。2022年，中共中央网络安全和信息化委员会办公室印发了《关于切实加强网络暴力治理的通知》，进一步压实了网络平台和网络监管者的主体责任，建立了切实可行的工作机制。

4 网络暴力的多维治理路径

基于网络暴力现实存在的社会危害性，为了更好地治理网络暴力，还网络空间一方净土，除了立法论方式外，其实还有更多的治理工具。

4.1 开展网络安全治理专项打击整治行动

开展专项打击、整治活动是我国整治违法犯罪的有效方式。近年来，我国开展了形式各样、规模各异的多项专项打击、整治工作，取得的成效是明显的。以“扫黑除恶”专项行动为例：

2018年至2022年，检察机关起诉涉黑涉恶犯罪26.5万人，其中组织、领导和参加黑社会性质组织犯罪6.4万人；人民法院依法审结涉黑涉恶案件3.9万件26.1万人[19]。所谓“利莫大于治，害莫大于乱”，开展对违法犯罪的专项整治活动，有利于结合有限的力量在一定时间内形成合力，对特定违法犯罪群体、特定种类的违法犯罪活动进行有针对性的打击，有利于发挥刑罚的积极预防效果。2022年，中央网信办部署开展了“清朗·网络暴力专项治理行动”，主要针对有影响的网络媒体建立监测、预警、溯源和曝光机制，这项行动迈出了有关部门从被动应对到积极治理的关键一步。为了进一步加大打击网络暴力的力度，司法机关应当主动参与到网络暴力的打击和治理专项行动中，对网络暴力重拳出击。

4.2 应用网络暴力信息治理技术

网络暴力的发展具有扩散速度快、隐秘性强等特点，一旦网络暴力受到网络群体的关注，便极易在较短的时间内、在众多网络平台上散播并形成燎原之势。在网络暴力形成的初期，对涉暴言论进行一定的控制，可以有效地防止网络暴力事件的形成，目前在技术层面上也是完全可以实现的。例如，可以根据留言内容识别违规评论，首先将文本信息向量化，再利用自己提出的文本分类模型来提取特征并进行分类工作[20]。以此，将网络暴力语言进行一定识别，然后再运用Deffuant 模型与 CODA（Continuous Opinions and Discrete Actions）模型中个体的行为选择机制，探索从底层揭示个体观点的决策行为。

通过对网络个体观点变化的定性分析，考虑网络环境中个体认知所带来偏差与无界信任的特性，建立舆情反转模型，用来探索网络中突发事件舆情演化时，网络个体观点交互的特点对其影响，从而解释舆情演化过程中的反转现象，提出相应的避免机制与控制策略[21]。对于平台的运营者而言，可以将侮辱性的词语予以过滤，并设置网络提示语提醒网友谨言慎行。为了将新兴技术进行广泛、深入和有效的运用，有必要将新技术进行更大规模的推广，并在网络平台上加以运用，早日实现对网络暴力的自动预警、防控和治理机制。

4.3 建立网络暴力多方合作治理机制

网络暴力的治理除了政府和司法机关需要主动担当外，社会的各方主体应当围绕暴力暴力进行广泛和深入的合作，形成社会共治的合力。具体而言，国家网信部门作为网络治理的主管部门应当切实履行自身职能，在“清朗·网络暴力专项治理行动”的开展基础上总结经验，对网络经营者实施常态化监督，督促网络经营者运用新兴技术、设立预警弹窗控制网络不当言论，防止网络暴力的形成。

网络经营者需要在自身经营范围内，配合国家网信部门主动建立起针对网络暴力的管控、防范系统。具体而言，网络经营者可以在建立内部合规和审核机制，对网络不当言论进行实施监控，一旦出现网络暴力风险，应当以特定形式引导正面舆论，并控制负面言论，对涉嫌违法犯罪的网络暴力活动，开展有针对性的人工识别，并提供后台数据供司法机关依法处理。作为网络活动最广泛的参与者，广大网民应当在政府、网络平台的号召下对网络言论进行适当识别，避免成为网络暴力的“帮凶”。

4.4 制定《反网络暴力法》

目前，用以规制网络暴力的法律规范多散见于民法、行政法、刑法等领域，诸多法律之间缺少必要的衔接，网络暴力治理缺少权责明细的职权划分。为了解决网络暴力治理出现的问题，有必要制定专门的反网络暴力法律。具体而言，首先，在《反网络暴力法》的总则部分，应该明确立法目的，为保护法益奠定价值基础，协调具体的规范内容，构建具体的立法体系。其次，在《反网络暴力法》中应该规定全链闭环治理过程中的各项具体内容作为法律文本的基干。再次，在《反网络暴力法》中应该压实政府监管责任、平台主体责任，协调政府与平台之间的关系和定位，通过专门的赋权条款划分两者在处理网络暴力信息时的权责边界。最后，《反网络暴力法》应该明确实施网络暴力者的民事责任、行政责任和刑事责任，设置专门的衔接性条款，通过既定的衔接通道将损害实质法益的情况交由刑法处理[22]。

5 结束语

网络信息技术的发展，让民众获得了平等发表意见的平台，民众的言论自由在网络空间中得到了极大的拓展。与此同时，朴素的正义与盲目的激愤相叠加，增加了网络空间的戾气。“网络不是法外之地”，维护平等、自由的网络言论空间是保障民众网络合法权益的前提。在选择网络治理工具时，要警惕“刑法万能主义”的观念，动辄以刑制暴反而会矫枉过正，使得正义的言论变得畏畏缩缩。社会不仅需要歌功颂德式的赞歌，也需要横眉冷对式的批判，能交给技术处理的网络安全治理无须动用刑法规制。

参考文献：

[1] 一点咨询网.德阳安医生自杀事件 “正义”不应成为暴力的挡箭牌.[EB/OL].https://www. yidianzixun.com/article/0JvIFqoi.

[2] 腾讯网.因染粉色头发遭网暴的24岁女孩走了，我看到最不堪一幕.[EB/OL].https://new.qq.com/rain/a/20230221A03EHT00.

[3] 陈代波.关于网络暴力概念的辨析[J].湖北社会科学,2013(6):61.

[4] 陈代波.关于网络暴力概念的辨析[J].湖北社会科学,2013(6):63.

[5] 施鑫.犯罪场视域下网络暴力行为的控制路径[J].哈尔滨工业大学学报,2018(1):33.

[6] 陈纯柱,马少盈.网络语言暴力的治理困境及路径选择[J].中国人民公安大学学报,2019(2)144.

[7] 蔡荣.“网络语言暴力”入刑正当性及教义学分析[J].西南政法大学学报,2018(2):66.

[8] 姜军.网络暴力的界定及刑法规制[J].网络空间安全,2022(5):24.

[9] 张明楷.网络诽谤的争议问题探究[J].中国法学,2015(3):75.

[10] 陈纯柱,马少盈.网络语言暴力的治理困境及路径选择[J].中国人民公安大学学报,2019(2)144.

[11] 姜军.网络暴力的界定及刑法规制[J].网络空间安全,2022(5):23.

[12] 敬力嘉,胡隽.网络暴力法律规制的完善路径[J].中国人民公安大学学报（社会科学版）,2021(5):148.

[13] 孟德斯鸠;许明龙,译.论法的精神[M].北京:商务印书馆,2012:233-234.

[14] 约翰·穆勒;孟凡礼,译.论自由[M].上海:上海三联书店,2019:18.

[15] 切萨雷·贝卡利亚;黄风,译.论犯罪与刑罚[M].北京:北京大学出版社,2008:24-25.

[16] 张明楷.刑法学（第六版）[M].北京:法律出版社,2021:228.

[17] 郭旨龙.网络暴力刑法治理的解释原理[J].江淮论坛,2023(5):122.

[18] G.拉德布鲁赫;王朴,译.法哲学[M].北京:法律出版社,2005:115.

[19] 中华人民共和国公安部官方网站.扫黑除恶在法治轨道上行稳致远.[EB/OL].https:// www.mps.gov.cn/n2255079/n4242954/n4841045/n4841050/c8920673/content.html.

[20] 吴浩,潘善亮.基于BERT-RCNN的中文违规评论识别研究[J].中文信息学报,2022(1):122.

[21] 黄传超,胡斌,闫钰炜,赵旭.网络暴力下突发事件中观点决策与舆情反转[J].管理工程学报,2019(1):253.

[22] 刘艳红.理念、逻辑与路径：网络暴力法治化治理研究[J].江淮论坛,2022(6):28.

作者简介：

陆林炜（1994-），**男，汉族，江苏扬州人，江苏警官学院，本科；南京师范大学法学院，在读硕士；主要研究方向和关注领域：刑法学、网络犯罪和网络安全。**

网络软暴力犯罪侦查对策研究

王一轩
（中国人民公安大学，北京100038）

摘要：

[目的/意义] 网络软暴力犯罪是软暴力犯罪通过网络媒介的进一步软性升级，会对社会秩序和人民群众的日常生活造成恶劣影响。研究网络软暴力犯罪的侦查对策，是打击网络犯罪和维护网络安全的重要保障手段之一。

[方法/过程] 分析现阶段侦查人员应对网络软暴力犯罪所面临的困境，针对侦查过程中存在的行为认定模糊、取证难度大和网络监管缺位难等难点进行研究和总结。

[结果/结论] 紧跟互联网技术的更新换代，采取措施加强取证工作、强化网络侦查能力、扩大线索来源和促进侦查协作，以规范互联网行业和净化网络空间，实现对网络软暴力犯罪的有效治理。

关键词： 网络软暴力；侦查难点；网络安全；网络犯罪；侦查对策

中图分类号： D918 **文献标识码：** A

Research on the investigation countermeasures of the crime of online soft violence

Wang Yixuan
(*People's Public Security University of China,Beijing 100038*)

Abstract:

[Purpose/Significance] Online soft violence crime is a further soft upgrade of soft violence crime through online media, causing adverse effects on social order and the daily lives of the people. Researching investigation countermeasures for online soft violence crimes is one of the important means to combat cybercrime and maintain cybersecurity.

[Method/Process] Analyze the current difficulties faced by investigators in dealing with online soft violence crimes, and conduct research and summary on many difficulties in the investigation process, such as vague behavior identification, high difficulty in obtaining evidence, and difficulty in network supervision.

[Results/Conclusion] Following the updates and upgrades of internet technology, measures should be taken to strengthen forensic work, enhance online investigation capabilities, expand sources of clues, and promote investigation cooperation, in order to standardize the internet industry and purify the online community space, and achieve effective governance of online soft violence crimes.

Keywords: online soft violence; difficulties in investigation; cybersecurity; cybercrime; investigation countermeasures

0 引言

现阶段的网络软暴力犯罪大多集中在黑恶势力犯罪范畴和债务催收方面，实际上单单就网络软暴力本身而言，已不止是黑恶势力范畴内的概念，它是犯罪分子危害行为和手段的又一次进化，对网络空间安全形成严重威胁。

网络软暴力行为通过网络攫取非法利益，已经具备与传统暴力和威胁手段对等的危害性可能，表现形式多变、手段不断翻新。现阶段，虽然对犯罪趋势虽有所遏制，但是许多网络软暴力犯罪行为，不仅没有被报警立案，更不用说进入诉讼程序。加强对网络软暴力犯罪的打击，对实现我国网络空间安全的有效治理有着现实意义。

1 概述

1.1 对网络软暴力犯罪案件的理解

软暴力是近年来黑恶势力常见的行为特征[1]，网络软暴力则是软暴力嫁接到互联网的产物。2019年出台的《关于办理实施“软暴力”的刑事案件若干问题的意见》（以下简称《意见》），对软暴力的性质内容有了明确规定。据此，网络软暴力就是行为人为谋取不法利益或形成非法影响，通过网络或通信工具实施的，对他人或者在有关场所进行滋扰、纠缠、哄闹和聚众造势等，足以使他人产生恐惧、恐慌进而形成心理强制，或者足以影响、限制人身自由、危及人身财产安全，影响正常生活、工作、生产和经营的违法犯罪手段。

《意见》的实质，依然是承接往年打击黑恶势力的刑事政策，主要是限定在黑恶犯罪的范畴，但是网络软暴力犯罪的实际内容部分超出了现有规定的边界。个人实施的网络软暴力行为能否具备心理强制性而入罪，规范文件留有一定空间，不是只有在主体是团伙、集团时才能定罪。网络软暴力手段依然可以作为黑恶势力的行为特征和具体犯罪的行为要件进行认定，同时非黑恶势力实施的网络软暴力，如果达到规范文件的标准，也应依法予以定罪惩处，这两者并不矛盾。

网络软暴力犯罪往往涉及多种罪名，例如寻衅滋事罪、敲诈勒索罪、非法经营罪和催收非法债务罪等，在实践中多表现为贷款行业中的讨债行为。除涉网黑恶实施的及其他非法借贷之外，一些网贷公司也存在网络软暴力犯罪行为，比如在放贷时要求借贷人提供个人信息，违法获取其手机号码和通讯录，并未经第三人同意而任由借贷人将第三人手机号登记为紧急联系人。然后，对无关第三人、通讯录内人员实施网络软暴力催收，又或者将催债业务委托给中介公司，以规避法律制裁。内容与一般意义上的网络暴力也有所交叉[2]，比如纠集网络水军对他人进行人身攻击、恐吓，或网上捏造事实诽谤他人[3]，要求被害人交纳金额才予以删除内容，或者利用水军营造恶性舆论、带偏公众言论，以实现不法目的等。

1.2 网络软暴力的常见类型

网络软暴力分为胁迫型网络软暴力和滋扰型网络软暴力[4]，前者的法益侵害程度要高于后者。

胁迫型网络软暴力是通过使用网络以威胁、恐吓的方式，致被害人形成心理恐惧或心理强制的状态。其多以组织形象或硬暴力为基座，进行现实空间肉体暴力的预告，通过电话、短信、微信、QQ等发送含暴力威胁内容的言语信息，或是以拍摄不雅照、寄送花圈、冒充身份骗取个人信息等非暴力方式威胁受害者，对人格权利进行侵犯[5]。这些都会产生与肉体暴力对等的心理控制或者恐惧效果。

滋扰型网络软暴力在司法认定上存在更多分歧，具体内容更加丰富多变。例如，主要表现为以电话、短信、视频和网络社交媒体等方式进行滋扰、通信骚扰、辱骂等，包括对欠债人的通讯录进行信息轰炸。在社交媒体上，以多种途径发布经过PS的淫秽、丧葬、造谣和涉及个人隐私等的图片视频，又或是使用网络水军破坏网络秩序、操纵舆论、起哄闹事、恶性市场竞争等。

2 网络软暴力犯罪的侦查难点

网络软暴力的出现，产生了一种可以完全不

依托线下的犯罪可能，有没有黑恶势力的存在，有没有现实中暴力的实施，又或者是否通过网络软暴力来达到剥离先前暴力惯常手段，实现犯罪升级的目的，这些是侦查人员面临的首要问题。

2.1 行为认定和案件定性难

网络软暴力犯罪涉及罪名多，案件定性困难，往往作案手段形似。但是，侵犯的法益却有差别，伤害内容属于心理层次，危害结果难以量化[6]。对于受害者却有着等同于现实暴力的危害，尤其是在行为外观上，没有对受害者造成明显伤害，往往达不到刑事标准而难以纳入侦查范畴，仅作民间借贷纠纷的简单处理。由于民间借贷领域存在监管漏洞，非法借贷业务不受监管，公安机关也不负责摸排调查和风险监控，导致若以贷款名义作包装，外观是债务纠纷，那么如何对其进行评价则不易下手，甚至可能忽略其刑事责任。公安机关在接到报警后，案件实际情况能不能构成犯罪都是存疑的。一些网络软暴力行为没有造成法定后果的，往往只有在黑恶势力的范畴内才能予以刑事处理。而若没有直接发现黑恶势力的踪迹或是情节较轻者，最后大多不予立案或作为普通治安案件处理。但是，轻易将其从侦查视野中移除、不深入挖掘线索，而实际上背后牵连的是黑恶势力，那么这样的个案处理很可能会影响到对一些网络软暴力行为的整体打击。在这种黑恶势力寻求网络伪装，不断更新犯罪手段、逐渐脱暴力化，并且隐藏在幕后进行反侦查的现实背景下，网络软暴力犯罪的侦查工作对侦查人员的线索敏感性、线索渠道把握、串并案和研判分析能力等要求很高。

2.2 犯罪行为隐蔽，侦查取证难

互联网的高效性、虚拟性带来的是犯罪具备更强的伪装性和隐蔽性，导致网络犯罪安全性高、成本低，侦查人员难以发现关键线索和证据。在网络软暴力犯罪中，嫌疑人与被害者无现实接触，实施过程隐蔽、技术含量高，很难遗留痕迹记录，而且大多造成精神伤害，没有明显的肉体损伤或财产损失。案件取证只能依靠电子证据和言辞证据，这样的证据证明力低又往往需要实物证据辅助，能否达到全面且合法的标准将直接影响证据认定的质量[7]。其中，电子证据易损毁缺失，而且数据量多且面广，取证工作成本高、难度大和效率低。案件如果定性不准，从处警所获证据不足，在后续补充调查取证时，网络证据灭失的可能性极大。此外，有些办案人员证据能力弱，缺乏相关办案经验，不熟悉电子证据取证或是取证不规范，应对事实复杂、流水账目繁多的情况很吃力。对于涉黑恶的网络软暴力犯罪，网络媒介则进一步促进团伙关系的疏离，无视时空障碍的特性，让犯罪成员可以轻松掩盖行踪、分散在全国各地。组织机构的公司化层级结构松散、人数众多，下设的催收部门与其他部门割裂，实施者也多是雇佣的外围闲散人士。组织人员之间无现实接头、互不了解，无法提供组织内部情况，侦查时根本触及不到幕后的核心人员，通过一般审讯也难以获得有用信息。

2.3 互联网监管缺位，线索深挖困难

面对互联网衍生产品的产业化所带来的市场份额争夺战，互联网企业的商业化运营模式决定了总是会放宽一定的监管，以换取更多的用户、流量和利益，能否做到有效监管难以确定。在现阶段，互联网几乎是天然的犯罪场所，网络软暴力犯罪对直接的财力和物力投入需求较小，嫌疑人可以通过互联网以擦边球的方式和极低的犯罪成本来实现目的，很难迅速得到法律的惩罚。同时，现阶段网络从业人员能力素质不高，互联网各行业的实名登记信息工作存在缺口，需要侦查人员逐一溯源核查，却容易引起犯罪分子的警觉而躲避侦查。互联网黑灰产业的完备链条，也为网络软暴力犯罪提供原始数据，包含可以被任意购买的个人信息，例如手机号码、IP地址、账户等，被害者无法通过简单的界面内容来辨别伪装后的犯罪者。若要对互联网尤其是社交网络的聊天内容进行实时监控与分析，不仅需要技术、设备和资金支撑，还涉及到个人权益保护的敏感问题，从而无论是哪方主体，即使是公安机关也无力做到完全遏制其蔓延，监管职能存在着一定的局限性。

在办案实践中，刑事、行政和民事三者衔接不畅，当事人多存在顾虑不予民事起诉，去行政立案又对基层派出所要求过高，意味着外观上未达到处罚标准的网络软暴力行为大多不会被处理。由于案件中的债务性质需要准确界定，套路贷、高利贷、非法债务和合法贷款在接触伊始都有相似的债权关系的外观，但是实际触犯的罪名完全不同，再加上犯罪分子使用虚假身份开设第三方支付平台账号、银行账户，以匿名访问、IP欺骗等方式实施网络软暴力，民警难以直接识破。往往由于行为危害未达严重程度，付出成本却十分高昂，最终导致基层派出所难以独自承担复杂的网络侦查工作的多环节展开，仅凭派出所来深挖扩线、进行网络追踪是不现实的。种种因素导致后续的深挖扩线几无可能。

3 网络软暴力犯罪的侦查对策

3.1 强化证据收集

首先要加强取证工作，从基本的个人手机号、手机软件登录信息，到社交媒体上的聊天记录、视频图片、转账记录等，侦查过程中要采取有效措施防止这类电子证据被破坏灭失。要客观评估造成的危害，准确判断是否足以与硬暴力相对等，尤其是要注意涉黑恶案件中与硬暴力关联的证据。要严格把握取证的时效性，迅速固定证据，灵活进行讯问询问，要关注案件中造成的精神强制来源，是否是出自一些组织的非法控制力和社会影响力。通过证明心理强制的伤害存在，来理清网络软暴力行为与危害结果的因果联系[8]。重视固定医院诊疗记录、病例情况说明、司法鉴定等，能够客观反映网络软暴力造成精神伤害的证据材料，让抽象的案件事实落地。

在案件涉及放贷问题时，可以从贷款的源头切入，搜集涉案公司的经营状况、账户和财务信息，结合网银平台、第三方支付平台等的交易记录，追踪涉案资金流向，进一步摸清犯罪组织的层级结构。要强化网络追踪、电子数据提取固定和数据恢复技术能力，扩大网络预警与监测的范围，对一些关键词、重点领域要实时监管，利用云数据即时对网络软暴力行为中的网络舆情、水军发帖、账户交易等作出反应，迅速进行IP定位和服务器数据调取，追溯信息来源，确定嫌疑人员，配合线下控制实现精准打击。

3.2 增强办案能力，规范认定与取证

侦查人员应熟练掌握案件的分辨与认定规则，强化自身理论学习，明确认识网络软暴力犯罪的认定边界和证明标准，准确界分黑恶势力与普通刑事案件。随着打击的深入，犯罪形式与手段也在不断变换升级，所以要努力突破物理暴力定罪的固定模式，避免产生认知偏差。要加强基层民警网络侦查思维的培养，提高对网络软暴力案件的行刑衔接特点的敏感性。对于涉黑恶的网络软暴力案件，黑社会性质组织要么以现实暴力作支撑或存在随时付诸实施的可能，要么存在先前的暴力行为而以网络软暴力作为后续控制手段或转型升级的替代模式。恶势力团伙的行为和组织特征较前者稍弱，侦查过程中只需对网络软暴力行为事实进行取证。

此外，要严格处理好法律与政策在实践工作中的关系，提高办案责任意识，摈弃错误的指标考核化倾向。同时，树立正确的证据意识，拓宽取证思路，利用好网络智能迭代带来的技术革新，对网络软暴力犯罪的行为本身及其背后可能隐藏的组织都要给予关注。网络软暴力行为明确认定为黑恶势力实施的，可以相对于非黑恶案件采取较低的入罪标准[9]，或是在后续侦查中发现其他犯罪行为的，可以作为黑恶势力的认定条件。不涉及黑恶势力的个案处理要结合具体情况，按照符合的具体罪名要件加以处置，做到“不放过”“不凑数”。

3.3 广辟线索来源渠道

网络软暴力行为的隐蔽性，让传统的从案到人的侦查模式逐渐疲软，公安机关不能仅仅依靠报案信息，而要拓宽侦查视野，扩大线索来源。基层所队要提高警惕，重视网络软暴力讨债类警情，重点摸排辖区债务纠纷类问题，排查社区内是否存在逃债放债讨债以及涉及网络软暴力的事项，鼓励群众积极举报提供线索。涉黑恶的网络

软暴力大多通过有预谋的集体活动，对不特定的公众造成心理强制和威慑。人民群众是网络软暴力犯罪最直接的见证者，所以要加强对不同区域人民群众的调查访问，发动群众积极检举揭发[10]，消除人们的恐惧心理。

公安机关要与社区组织密切联络，通过居委会、村委会等组织单位，及时把握网络软暴力犯罪的情况，构建警民合作渠道，实现及时沟通与信息反馈。同时，在网上平台专设举报版块，经常进行基层走访和区域性排查，做好宣传教育工作。要立即核查收集到的线索，并进行初步判断、分类筛选，把握重要线索来深入调查。此外，还可以定期汇总各部门的经济纠纷报警记录，梳理排查串并案件。

3.4 加强侦查协作与行业整治

侦查机关要与治安部门加强协同作战，建立刑侦、网安等警种的预警防范、联合打击机制，避免网络软暴力犯罪线索因受理主体对治安刑事的界定不同而被切断。运用大数据技术进行网络阵地控制[11]，要对借贷、互联网金融和网络舆论等领域进行重点管控，强化对网络黑灰产业的综合打击，共同对重点人员进行全面摸排。要善于梳理已发案件，结合其他渠道获得的犯罪人信息、犯罪手段特征等，逐步通过案件对比串并、信息数据碰撞来挖掘网络软暴力犯罪新线索，以及背后可能存在的黑恶势力。同时，加强公安机关与其他部门的协作，建立以打击犯罪为中心的信息传递、案件通报和执法衔接机制，压实互联网公司主体责任，成立涉网黑恶数据共享平台，整合资源渠道，确保信息数据准全。最后，加强对易侵害群体的普法宣传工作，健全网络软暴力源头防范治理机制，以案促改、以案促治，以强大的打击惩治攻势来实现网络空间的精准化与智能化治理[12]。

4 结束语

网络软暴力犯罪的认定，依然是一个存在较大政策弹性空间的法律适用过程[13]，侦查人员面临的困难会继续存在。对网络软暴力催债行为的打击，不是保护老赖，而是要规范合法合理的债权关系。坚决遏制网络软暴力案件多发高发势头，要正确遵循法律与政策的引导，加大惩治力度，规范借贷市场，引导网民自觉遵规守纪，推动扫黑除恶斗争在互联网空间持续纵深展开。

参考文献：

[1] 董雪米.黑恶势力“软暴力”犯罪的司法认定[D].成都:西南财经大学,2020.

[2] 张晓慧.网络软暴力犯罪预防研究[D].重庆:西南政法大学,2021.

[3] 张猛.打击网络软暴力犯罪的对策[J].网络空间安全,2019,10(03):111-117.

[4] 张力.网络软暴力行为的司法认定[J].中国人民公安大学学报（社会科学版）,2021,37(02):42-48.

[5] 王秀梅,李采薇.网络软暴力入罪的客观分析[J].河南警察学院学报,2022,31(01):43-52.

[6] 洪晨露.网络软暴力型寻衅滋事罪之分析[J].湖北工业职业技术学院学报,2021,34(02):51-56.

[7] 李白冰.软暴力型黑恶势力犯罪侦查研究[D].北京:中国人民公安大学,2021.

[8] 胡玉明,冒伟.黑恶势力软暴力行为的侦查取证策略[J].辽宁警察学院学报,2023,25(01):26-32.

[9] 石魏.黑恶势力“软暴力”之实证分析及规制路径——以2016-2020年1726件涉“软暴力”刑事案件为样本[J].北方论丛,2021,(04):85-93+168.

[10] 涂晓晗.公安机关打击软暴力犯罪策略初探[J].中国防伪报道,2021,(05):84-89.

[11] 刘东瓒.网络黑恶犯罪侦查难点与打击对策[J].网络空间安全,2022,13(02):8-13.

[12] 李威翰.新型网络有组织犯罪情报分析方法研究[J].网络空间安全,2022,13(06):24-29.

[13] 黄京平.软暴力的刑事法律意涵和刑事政策调控——以滋扰性软暴力为基点的分析[J].新疆师范大学学报（哲学社会科学版）,2019,40(06):103-121+2.

作者简介：

王一轩（1996-），**男**，**汉族**，**江苏徐州人**，**中国人民公安大学研究生院**，**在读硕士**；**主要研究方向和关注领域**：**犯罪学和网络安全**。

网络贩毒侦查的技术挑战与对策研究

兰钰超
（中国人民公安大学，北京100038）

摘要：

[目的/意义] 随着互联网技术的不断发展，网络贩毒已经成为一个全球性问题，如何有效地侦查和打击网络贩毒活动成为一项重要挑战。

[方法/过程] 通过分析网络贩毒现状，指出其特点与危害，探讨网络贩毒侦查的技术挑战和当前侦查工作的困境，从而提出相应对策。

[结果/结论] 采取多种网络技术手段相结合的策略，例如建立网络安全技术平台、加强国际合作和完善法律法规等，可以有效地打击网络贩毒活动。

关键词： 网络贩毒侦查；网络技术；隐蔽性、匿名性；数据治理；网络空间安全

中图分类号： D918.2；DF793.2 **文献标识码：** A

Technological challenges and countermeasures in network drug trafficking investigation

Lan Yuchao
(*People's Public Security University of China, Beijing 100038*)

Abstract:

[Purpose/Significance] With the continuous development of Internet technology, online drug trafficking has become a global problem, and how to effectively investigate and combat online drug trafficking has become an important challenge.

[Method/Process] By analyzing the current situation of online drug trafficking, pointing out its characteristics and harms, exploring the technical challenges of online drug trafficking investigation and the difficulties of current investigation work, corresponding countermeasures are proposed.

[Results/Conclusion] A combination of various network technology approaches should be adopted to effectively combat online drug trafficking. These approaches include establishing a network security technology platform, strengthening international cooperation, and improving legal regulations.

Keywords: online drug trafficking investigation; network technology; concealment, anonymity; data governance; cybersecurity

0 引言

网络贩毒是指通过互联网或其他电子通讯工具，从事购买毒品、销售毒品、收取毒资等活动[1]。它具有隐蔽性和跨境性，为毒品走私和销售活动提供技术支持，给打击毒品犯罪带来极大挑战。随着互联网技术的发展，网络贩毒已成为全球性问题[2]，严重地威胁到了网络安全、社会治安和公共秩序。

研究网络贩毒侦查，可以更好地了解网络贩毒的形式和特点，制定出有效的打击策略和预防措施。但是，网络贩毒的隐蔽性和匿名性对传统打击方式提出了挑战，需研究新技术和新方法，以提高网络贩毒的侦查效率和精准度。

此外，研究网络贩毒侦查，还可以为相关部门和机构提供科学依据和指导，促进国际间合作和信息共享，从而加强对网络贩毒的全球性打击力度。因此，本文旨在探讨网络贩毒的形式与特点、侦查技术的困境与挑战和应对措施，促进开展打击网络贩毒侦查工作。

1 网络贩毒的形式和特点

1.1 网络贩毒的常见形式

互联网平台和网络工具的发展，为网络贩毒活动提供了诸多的隐蔽和便利。常见的网络贩毒形式有4种。

一是暗网，即基于匿名性的加密网络，用户可以通过特定的软件和技术在暗网上匿名访问各种内容。暗网上存在着大量的非法市场，例如“公民个人信息市场”“宣扬恐怖主义市场”等，其中就包括贩卖毒品的非法市场。

二是社交媒体，贩毒者通过创建虚拟账户来销售毒品，使用私人信息与潜在买家联系，双方可轻松地在社交媒体平台完成交易。

三是电子商务网站，即允许企业和个人在网上交易的平台，贩毒者可在此类网站销售毒品，通过在网站发布广告或建立虚假的店铺进行交易。

四是即时通讯应用，即允许用户通过网络进行即时沟通的应用程序，例如WhatsApp和Telegram等。以Telegram为例，客户端是自由及开放源代码软件，但是服务器端是专有软件，用户可以相互交换加密并自毁消息，类似于“阅后即焚”。贩毒者使用此类即时通讯应用与潜在买家交易，可明显地提高交易隐蔽性。这些网络平台和工具的使用，使贩毒者更容易地销售毒品，也让打击贩毒活动变得更加困难。因此，深入了解网络贩毒的特点和形式，对于制定有效的打击网络贩毒策略和技术具有重要意义。

1.2 网络贩毒的特点

网络贩毒的特点主要包括隐蔽性、匿名性和跨境性。这些特点使网络贩毒具有更高的危害性且更难以被侦查和打击。一是隐蔽性，网络贩毒往往采取隐蔽的手段，例如使用加密通信和隐藏身份等技术手段，使其更难以被发现和侦查[3]。同时，网络贩毒行为也常隐藏在普通的交易或通信活动中，侦查人员难以识别。二是匿名性，网络贩毒往往采用匿名的方式进行，例如使用虚拟货币、暗网等手段实现交易，难以追溯和确认网络贩毒者身份，同时匿名性也增加了网络贩毒者逃避法律惩罚的可能性。三是跨境性，网络贩毒通常跨越国家和地区进行，使其行为的管辖权变得复杂，同时也给侦查工作带来了更大难度。此外，不同国家和地区法律法规的差异与执法水平的不同也会影响对网络贩毒的侦查和打击。结合以上特点分析，为有效应对网络贩毒相关问题，需要不断加强侦查技术手段和国际合作，以提高侦查和打击效率，同时也需完善相关法律法规并加强公众反毒意识教育。

1.3 网络贩毒对社会的危害

网络贩毒对社会造成了许多严重的危害。首先，网络贩毒难以被检测，通过互联网进行交易，买家和卖家在虚拟世界中相互联系，实现匿名性交易。这种交易模式使网络贩毒行为不受地理限制。同时，网络贩毒的信息传播速度快，消息可在瞬间传至全球各地，实现毒品市场全球化，从而导致网络贩毒活动的广泛性和难以监测性。执法部门在监测时，需要面对海量的数据、复杂的网络结构和难以追踪的交易路径，难以快

速准确地确定犯罪行为和相关人员。其次，网络贩毒逃避打击能力强。相对于传统的贩毒方式，网络贩毒具有匿名性、隐蔽性和迅速传播的特点。网络贩毒分子利用互联网的高度开放性和信息传输的便捷性，通过加密技术[4]、虚拟货币等手段来隐藏身份和资金流动，使执法部门在网络空间中追踪和定位犯罪分子变得异常复杂，加大了打击网络贩毒的难度。再次，网络贩毒的存在也加剧了毒品滥用问题。由于网络贩毒便捷且隐蔽，容易引诱更多人参与毒品交易和毒品滥用，给青少年和弱势群体带来更大的危险，不利于其身心健康发展。总而言之，网络贩毒的存在和发展给社会带来了极大的危害，必须采取有效的措施和方法来防止和打击网络贩毒。

2 网络贩毒侦查的困境

随着互联网技术的发展和普及，网络贩毒已成为严重的社会问题。网络贩毒的存在给社会带来了极大的危害，因此打击网络贩毒已成为国家的重要工作之一。然而，网络贩毒侦查工作也面临着诸多困难和挑战。

2.1 技术壁垒的限制

在网络贩毒侦查中，技术手段是非常关键的。侦查人员需要利用网络技术、数据分析技术等手段对网上贩毒的活动进行调查和追踪。但网络贩毒分子也在不断地升级技术，采用各种反侦查手段，例如利用虚拟机、翻墙软件和暗网等，侦查人员难以获取大量有效线索。同时，一些犯罪分子会利用各种加密手段来保护自己的交易记录，避免警方追踪。由于这些技术手段，侦查人员在追踪网络贩毒时会受到技术壁垒和隐私权保护等多方面的限制[5]。

2.2 跨境合作难度大

由于国家法律体系的不同和贩毒集团的组织分布，网络贩毒往往是一种跨国性犯罪活动[6]，网络贩毒侦查工作面临着跨境合作难度大的挑战。不同国家法律制度和执法机构不同，跨国合作需协调各国执法资源，法律程序也需协调解决。同时，涉案信息和资金可能涉及多个国家，需各国协作共享情报和证据，这需要一定的信任和安全机制。此类问题会大幅增加打击网络贩毒的难度。

2.3法律法规不完善

由于网络贩毒的特殊性质，当前相关的法律法规并不完善，导致警方在网络贩毒侦查中面临着诸多的困境和挑战。比如，一些国家和地方并未将网络贩毒罪纳入刑法体系，警方的侦查和打击行动缺乏相关法律条文的支撑。此外，网络贩毒跨境性质强，需要多国协作打击，但国际间的协作和合作在法律上仍有待加强，这也限制了侦查人员的行动空间。

3 网络贩毒侦查的技术挑战

3.1 网络贩毒侦查技术的应用现状

网络贩毒侦查技术是指针对互联网上的贩毒活动进行监测、追踪和打击的一系列技术手段。随着网络的发展和贩毒活动的转移到互联网上，各国执法机构和安全机构积极采用各种技术手段，以侦破和打击网络贩毒活动。现行的网络贩毒侦查技术主要包括三种。

3.1.1 一是数据挖掘和分析

数据挖掘技术主要用于从海量的网络数据中发现模式、趋势和关联。随着数字化时代的到来，人们每天都会产生大量的网络数据，这些数据包括交易记录、通讯记录、行为模式等。执法机构通过数据挖掘、网络追踪等技术手段分析社交媒体、在线论坛和暗网等平台上的信息，从海量的数据中筛选出与毒品交易相关的信息，帮助警方锁定犯罪嫌疑人的身份和活动轨迹，从而提高了打击网络贩毒的效率。同时，在侦查过程中，需要对大量的数据进行分析和应用，这可以帮助警方更好地了解毒品交易的规律和特点，提高打击犯罪的准确性和效率。例如，数据分析可

以揭示毒品交易的地点、时间、方式、参与者以及交易量等关键信息，为警方制定打击策略提供科学依据。同时，数据应用也可以为警方提供更加准确的预测模型[7]，预测未来毒品交易的可能发生地点和时间，为警方加强巡逻和监控提供更好的指导。这些技术的应用可以帮助警方识别和定位犯罪嫌疑人，找出交易的路线和时间，以及了解犯罪组织的架构和运作方式，从而为警方的打击工作提供更好的保障。

3.1.2 网络监控和过滤

网络监视和过滤分析可以帮助警方分析和监视犯罪分子的网络活动，提高网络贩毒侦查的效率和精度。执法机构会设置监控系统，对互联网上的流量进行实时监测和过滤。这些系统可以识别和拦截包含贩毒内容或相关信息的通信，从而快速发现并打击贩毒活动。此外，人工智能技术的发展也为网络贩毒的侦查提供了新的可能，例如，自然语言处理技术可以自动分析和理解网络中的文本内容，从而快速地发现和识别犯罪嫌疑人的信息和活动轨迹。

3.1.3 数字取证技术

数字取证技术用于从电子设备、计算机系统和网络中收集、保护和分析与贩毒活动相关的证据。可以帮助侦查人员恢复已删除的数据。当涉案设备中的数据被删除或隐藏时，数字取证技术可以通过专业的软件和技术手段对存储介质进行扫描和分析，以找回被隐藏或删除的数据。这些数据可能包含有关贩毒交易、联系人和交流的重要信息，有助于揭示犯罪嫌疑人的身份和活动。此外，数字取证技术还能够分析电子邮件和通信记录。网络贩毒活动往往涉及大量的电子邮件、即时通讯和社交媒体等通信方式。通过数字取证技术，侦查人员可以获取和分析这些通信记录，寻找涉案人员之间的联系、交易细节以及隐藏的指令和计划。这为打击网络贩毒提供了重要的线索和证据。

3.2 网络贩毒侦查技术的不足

从侦查技术的应用现状中，可以看出网络贩毒侦查技术的重要性和潜力，但是也必须正视其所面临的挑战和不足。

首先，相较于网络贩毒手段，网络贩毒侦查技术的更新迭代速度较慢且准确性和可靠性存疑。网络贩毒分子不断利用新技术、新平台和新手段来规避侦查，而现有的网络贩毒侦查技术往往滞后于这些变化。这导致侦查人员难以及时了解最新的网络贩毒活动和交易方式，影响了打击效果。此外，网络贩毒侦查技术的准确可靠性也存在问题，可能会导致误判或遗漏重要线索，给侦查工作带来困扰。

其次，网络贩毒侦查技术在追踪和打击层面具有延迟性。由于网络空间的匿名性和跨境性，犯罪嫌疑人在贩毒后可能会暂时逃脱警方追捕[8]，甚至将贩毒行为转移到其他地方或国家进行。这使侦查人员不得不花费更多的时间和精力来追踪和定位犯罪嫌疑人，延缓了打击行动的进行。网络贩毒的快速转移和遮蔽性给侦查工作带来了巨大的挑战，需要加强与其他国家的合作，共同打击网络贩毒活动。

此外，使用网络贩毒侦查技术也存在法律和道德风险[9]。在使用侦查技术的过程中，可能涉及侵犯个人隐私和信息安全的问题，给个人权益带来潜在的威胁。因此，需要完善相关的法律法规和监管机制，确保侦查行为的合法性和合规性。

综上所述，结合网络贩毒侦查技术的应用现状和不足，侦查机关应采取一系列措施来提高侦查技术的应用效果和合法性。例如，加强技术创新和国际合作，完善法律法规和监管机制，以确保网络贩毒侦查工作的准确性、及时性和合法性。只有如此，才能更好地应对网络贩毒的威胁，维护社会的安全和稳定。

4 应对网络贩毒的对策

网络贩毒作为一种新型犯罪行为，其隐蔽性和匿名性增加了侦查工作的困难程度。为应对网络贩毒的

威胁，侦查工作需要采取一系列对策，包括建立网络安全技术平台、加强国际合作和完善法律法规等。

4.1 建立网络安全技术平台

随着计算机技术的不断发展，网络贩毒的侦查技术也在不断提升。现如今，越来越多的数据被存储在云端，网络贩毒犯罪也逐渐向着智能化和自动化方向发展。因此，建立网络安全技术平台逐渐成为应对网络贩毒的重要手段之一。在技术方面，可以采用人工智能、机器学习等技术手段，对海量数据进行分析，并不断研发更新、更加高效和精准的网络贩毒侦查技术，建立起跨平台的网络安全技术平台，为网络贩毒侦查提供技术支持和保障。也可通过加强与互联网企业和平台的合作，建立多方合作机制，提高技术水平和共同应对网络贩毒威胁的能力。例如，可以建立网络安全技术平台，通过数据挖掘、监测和分析技术，实现对涉毒信息的筛选和监测、对涉毒人员的追踪和定位和对网络贩毒行为的及时打击。

4.2 加强国际合作

网络贩毒是一种跨地区、跨国家的犯罪行为，因此需各国之间加强合作、促进侦查工作的协调配合，共同打击网络贩毒。在国际合作方面，应建立信息共享机制，加强跨国警务合作，加强不同国家、地区的侦查机构之间的协作。与其他国家和地区的执法机构建立联合机制，共同开展网络贩毒犯罪打击行动。加强国际刑警组织和相关国际组织的协调合作，共同制定打击网络贩毒犯罪的国际法律法规，推动全球范围内的打击网络贩毒犯罪的合作与协调，防止出现“气球效应”。同时，加强相关部门间的配合，例如公安、海关、边防等，建立跨国打击网络贩毒的法律和政策体系。

4.3 完善法律法规

在打击网络贩毒犯罪的过程中，需要有针对性的法律法规支持，才能更好地保障打击工作的顺利进行。因此，需要加强网络安全体系建设，建立完善的网络安全法律法规和标准，加强对网络贩毒犯罪的监管，明确网络贩毒的行为界定和惩处标准，加大对网络贩毒犯罪的打击力度，规范网络贩毒行为，从源头上遏制网络贩毒犯罪的发生。

5 结束语

随着互联网技术的发展，网络贩毒犯罪对公民和社会都产生了极大负面影响。同时，传统网络贩毒侦查也面临诸多挑战。为保护人民的身心健康，维护网络空间的安全和社会的稳定，公安机关应掌握最新发展动态并搭建网络安全技术平台、深化国际合作、完善法律法规、建立健全的侦查体系，从而提高网络贩毒的打击力度和预防能力。

参考文献：

[1] 徐才淇.网络贩毒犯罪发展原因及对策探讨[J].东岳论丛,2016,37(05):180-187.

[2] 田圣斌.互联网刑事案件管辖制度研究[J].政法论坛,2021,39(03):36-48.

[3] 赵微,郝冬婕.刑事诉讼法修正后毒品犯罪案件证据制度的完善[J].辽宁大学学报（哲学社会科学版）,2012,40(03):112-117.

[4] 何文海,信佳佳.网络信息安全中存在的问题及数据加密技术研究[J].网络空间安全,2019,10(01):24-26.

[5] 王文华.互连网上侦查权与隐私权的冲突及其刑事政策——以加拿大为视角[J].比较法研究,2003(06):75-84.

[6] Drug—Free ASEAN 2015: Status and Recommendations, United Nation Office on Drugs and Crime Regional Center for East Asia and the Pacific, 2008.

[7] 吕雪梅.美国预测警务中基于大数据的犯罪情报分析[J].情报杂志,2015,34(12):16-20.

[8] 韩关锋.公安学视角下网络犯罪匿名性论述[J].网络空间安全,2022,13(05):97-103.

[9] 彭俊磊,周长军.大数据时代技术侦查的法律规制——以合理隐私期待理论为视角[J].山东社会科学,2022,No.328(12):170-177.

作者简介：

兰钰超（1999-），女，汉族，山东德州人，中国人民公安大学，在读硕士；主要研究方向和关注领域：刑事侦查学、禁毒学和网络安全。

让我们携手努力
营造网络空间治理与安全生态环境
夯实网络空间安全共同体学术基石

网络空间安全

Cyberspace Security

（Wangluo Kongjian Anquan）
（双月刊）
2023年10月

主管单位：中华人民共和国工业和信息化部
主办单位：中国电子信息产业发展研究院
赛迪工业和信息化研究院（集团）有限公司
出版单位：北京赛迪出版传媒有限公司

主　　编：仝培杰
美术编辑：高思帅
编辑电话：010-88559466
Q Q 咨 询：1466817369
电子信箱：tongpeijie@ccidmedia.com
infost@126.com
订阅热线：010-88558777
通信地址：北京市海淀区紫竹院路66号中国赛迪大厦17层
邮政编码：100048

期刊主页：www.aqjs.cbpt.cnki.net
出版日期：2023年10月25日
本期售价：60元/册

承印单位：廊坊市纸颜印刷有限公司

国际标准连续出版物号：ISSN 2096-2282
国内统一连续出版物号：CN 10-1421/TP
广告发布登记：京海工商广登字 20170178 号
邮发代号：80-893