无形的战斗在庞大的数据世界里已然打响。那些威胁到数据安全的行为，越来越难以辨认，国家行为与黑客自发组织的界限变得模糊。可以预见的是：保护数据安全，在未来必将会是一个频繁被讨论的话题。

道创宇，就是其中之一。从国家重大活动的网络保障，到打击网络诈骗，再到保护企业数据安全，近年来知道创宇在应对数据安全威胁中积累出自己的“心得”。

从早年互联网普及开始，网络病毒与黑客攻击对于中国的网友已经不是什么新鲜事。不过在如今大数据时代，黑客的攻击手段不断升级，而大数据安全企业的应对同样在不停地更迭。接受《新民周刊》采访时，知道创宇防御产品线总经理张永波提到一个显著的变化是：用大数据来保护大数据本身，正在成为常态。

“过去可能是遭受黑客攻击，数据安全受到威胁之后我们去弥补；现在我们会借助大数据监控，提前发现黑客的行为，比如窃取数据，篡改信息，大规模的数据爬取。对此，我们有一套完整的黑客攻击捕获方案，然后建立大数据威胁情报库，最终实现做到提前预知。”张永波说道。

数据安全变得愈发重要，对于掌握大量数据的企业也提出了更高要求。张永波告诉新民周刊：“过去企业发现自己的数据被窃取，会觉得自己是受害者。但现在数据经济如此发达，企业的社会责任也就相应变大。如果不能保护好自己的关键数据，可能还要承担相应的责任。”

2020 年 10 月，在桔视上线 3 周年之后，滴滴地图事业部在中国测绘学会年会上公布了一组数据：滴滴地图基础数据准确率已经超过 95%，而且每天新增轨迹数据超 108TB。此外，5.5 亿乘客，每天还会上报数十万量级的路况事件。1000 多万滴滴车辆，每天通过桔视，成为滴滴的街景实时测绘车，并成为掌握我国城乡高精测绘数据的重要平台。一旦这些数据都被美国拿到，国家安全势必面临极大的危机。

美国 2020 年颁布了外国公司问责法案（HFCA），要求赴美企业必须接受公众公司会计监督委员会的会计底稿审查。这成为美国证监会 SEC 与中国证监会 CRSC 的交锋焦点。审计底稿之所以重要，是因为审计报告里面包含了公司的重要商业秘密。包括客户和用户数据、董事会、中高层之间的会议纪要、内外部重要业务和经营方面的沟通文件、问题汇总、程序表格，甚至包括往来的电子邮件。所以不难理解，为什么企业对于聘请会计师事务所进行审计的时候，会对事务所的声誉有着严格要求。对于赴美上市的中国企业，很多都是各个行业中的领军企业。就像滴滴、boss 直聘、运满满、货车帮等，一旦美方通过 SEC，拿到了这些企业的所有审计底稿，就可以去分析出中国城乡消费能力，进而推导中国的经济实力，更不用说对于重要部门、国家安全产生的影响，因为这些可以利用关联分析，倒推出很多的数据。

作为手握巨大基础数据的互联网公司，怎么保护自身数据安全？出席 2021 世界人工智能大会安全高端对话的相关专家建议：

一是做好数据分类分级管控。互联网公司应该将涉及国家安全、国民经济命脉、重要民生、重大公共利益的重要数据和核心数据；涉及平台业务的公共数据、涉及大量个人隐私的用户数据，进行数据资产分类分级管理。并利用数据标识工具，针对上述数据进行自动化打标，并结合分级保护策略，对于公司的海量数据进行“合法、合规、合理”的自动化、精细化安全管控。

二是管控数据全生命周期安全。针对不同安全级别的数据，明确其在采集、传输、存储、使用、删除等数据生命周期各个环节的安全防护要求。

三是建立完善的数据安全监测预警机制。通过建设数据安全风险监控平台，预警响应数据安全风险。基于敏感数据、策略、数据流转基线等多维度，对数据的生产流转、数据操作进行监控、审计、分析，及时发现异常数据流向、异常数据操作行为，并进行告警，输出报告。对人员、业务、系统、合作伙伴进行全面布控，进行风险识别与预警，有效提高风险预警能力和风险运营能力，以实现数据全生命周期各阶段的数据安全风险防控。

无形的战斗在庞大的数据世界里已然打响。那些威胁到数据安全的行为，越来越难以辨认，国家行为与黑客自发组织的界限变得模糊。可以预见的是：保护数据安全，在未来必将会是一个频繁被讨论的话题。