网络内容生态治理 网络安全态势感知

网络安全应急指挥平台解决方案

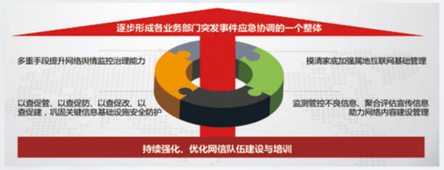
KUAIYE 快页

快页信息技术有限公司
电话： 400-628-1011
官网：www.ky.link
电邮：kefu@ky.link

KUAIYE 快页

平台概述

快页网络安全应急指挥平台是基于大数据、云计算、人工智能技术，根据网信业务特征提供网络舆情、智能网评、传播分析、属地网络违规监管、网络安全态势感知、预警通报及应急指挥等服务，实现业务流程标准化、处理过程智能化、数据分析可视化，构建智慧、协同、科学的网信工作管理体系。



平台架构

平台以业务驱动和整合共享为主线，面向本级互联网信息和网络安全属地化管理需求，建设协作联动的网信管理体系。本平台是以满足日常业务、应急指挥等需求而建设的综合性平台，根据网络安全、内容安全和机构管理等应用功能性要求，采用分层解耦的架构，从下到上依次为：基础设施层、平台服务层、数据服务层、应用服务层以及用户层，辅以安全标准体系和运维管理体系实现长效运转。

基础设施层：

提供大屏系统、视频会议系统、中控系统等基础系统，并按需提供弹性的计算、存储、网络、安全等基础设施服务，满足各类应用的计算能力和存储能力需求,是平台运行的物理基础。

平台服务层：

提供信息处理的能力，以及应用程序的开发和运行环境，为系统接入和开发提供支撑。包括计算服务、存储服务、传输服务等。

数据服务层：

提供数据采集、数据辨识和数据分析能力，集中管理需要交换和共享的数据资源，支撑和反哺各类数字化应用。

应用服务层：

依托基础设施、平台服务及数据服务，融合面向不同用户的多个应用，提供良好的操作界面。应用涵盖舆情监测、属地网络监管、网宣、网评、举报、网络安全等多个方面。

用户层：

支持PC、手机终端以及大屏等进行展示和交互。

平台功能

<table>
<tr><td colspan="4">预警通报</td><td colspan="3">应急指挥</td></tr>
<tr><td colspan="7">预警通报及指挥</td></tr>
<tr><td>账号落查</td><td>属地监管</td><td>举报管理</td><td>网宣管理</td><td>安全采集</td><td>安全分析</td><td>态势感知</td></tr>
<tr><td>舆情监测</td><td>社群监测</td><td>视频监测</td><td>外媒监测</td><td colspan="2">资产测绘</td><td>网站安全监测</td></tr>
<tr><td colspan="4">网络内容生态治理</td><td colspan="3">网络安全态势感知</td></tr>
<tr><td colspan="2">身份认证</td><td colspan="2">工作流引擎</td><td colspan="2">数据整合</td><td>移动网信</td><td>大屏展示</td></tr>
<tr><td colspan="8">统一工作平台</td></tr>
</table>

统一工作平台

身份认证

系统采用统一门户集成技术，构建工作应用。实现基于用户、角色、层级的统一化组织架构管理。利用统一的权限及登录管理，实现用户一次登录，就能轻松处理不同业务系统中的日常工作，实现网络安全应急指挥平台的应用系统集成，包括舆情监测系统、指挥通讯系统、网宣系统、属地网络执法监管系统、网络安全态势感知系统等多个系统的集成，同时也支持第三方系统的集成。

工作流引擎

提供工作流引擎配置工具，支撑网信组织架构的持续成长和工作流程的不断完善。为“横向到边、纵向到底”的网信内外体系建设提供有效支撑。

数据整合

实现基于大数据整合的统一资源管理。对采集落地的数据进行清洗、归集。数据库建设包括基础数据库建设和业务专题数据库建设，业务专题数据库包括网络安全态势感知数据库、互联网舆情监测数据库、网宣员管理业务数据库、应急指挥数据库、其他业务系统数据库。

移动网信

以“安全连接，智慧聚合”为核心理念，实现安全的移动办公平台，支持私有化部署和阅读水印。主要提供基于组织机构的即时消息通信功能，包括支持点对点加密通讯、加密群聊、语音聊天、视频会议、文件传输等功能，同步PC端门户的组织架构。提供联动PC端的工作台，实现移动化办公。

大屏展示

依托网络安全应急指挥平台的建设，整合各类业务系统和基础数据、业务数据、分析数据，实现大数据可视化分析，为研判决策、指挥调度提供单项、并列、对比、聚合、专题、案例等多种类型的统计分析和效果展示。

大屏包括首页综合、内容治理、网络安全、通报指挥四大部分，内容治理涵盖舆情、社群、视频、外媒、属地网络监管、网宣、举报等多个分屏，网络安全涵盖安全综合、资产、攻击、漏洞、内容安全等多个分屏。

网络内容生态治理

舆情监测

舆情监测系统是网络安全应急指挥平台的重要组成部分，舆情监测系统建设实现监测预警、引导调控、综合研判等功能，为负面信息管控、正面引导和舆情态势感知等业务提供支撑。监测预警实现对互联网信息内容、网络重点账号的监测分析，及时发现敏感有害信息和网络舆论热点；综合研判实现网络舆情态势感知与分析，为互联网信息内容管理提供辅助决策支撑。

舆情监测系统支持集成多个舆情数据源，包括舆情秘书、舆情通、云舆情等多个国内主流舆情厂商数据以及微博、微信等API数据。系统实现对多源数据的归并，减少预警数量；利用AI技术，结合规则和模型对舆情事件进行二次研判，减少误报或漏报。

社群监测

社群监测系统包含微信群、QQ群、电报群等国内外主流社群的信息采集、智能分析功能等，实现从信息的获取，分析到服务的全过程管理，支持海量数据分析、处理能力，最终实现对社群的综合分析服务。

视频监测

视频监测系统支持优酷、爱奇艺、腾讯视频、腾讯微视、百度视频、好看视频、快手、抖音、B站等多个专业视频网站，同时支持通用网站、微博号、微信号、自媒体账号发布的文章中包含的音视频和图片内容。

外媒监测

境外媒体监测系统旨在解决境外舆情监测难度大、速度慢的问题，支持针对境外新闻、论坛、博客、脸书、推特、优兔等社交媒体的实时监测。境外监测系统采用先进的境外信息采集技术，能根据用户预定的监控关键词及时发现境外多个国家的社交媒体的相关舆情信息，并对敏感信息及时报警，同时配合专业分析师生成详细的舆情分析报告。

账号落查

账号落查系统提供国内外主流社交网站的虚拟身份识别，包括通过账号查手机号、通过手机号查账号等。（仅限相关执法部门在法律授权范围内使用）

属地网络监管

属地网络监管系统主要用于全面掌握本地媒体动态，正确进行舆论引导，对于加强属地网站监管、整理分析网站信息、应对突发的网络公共事件具有重要作用。实现包含但不限于信息获取、行为监测、执法取证、综合协调等功能，为属地新闻业务和论坛、博客、贴吧、自媒体等具有新闻舆论及社会动员能力的网络平台监管提供支撑。

举报管理

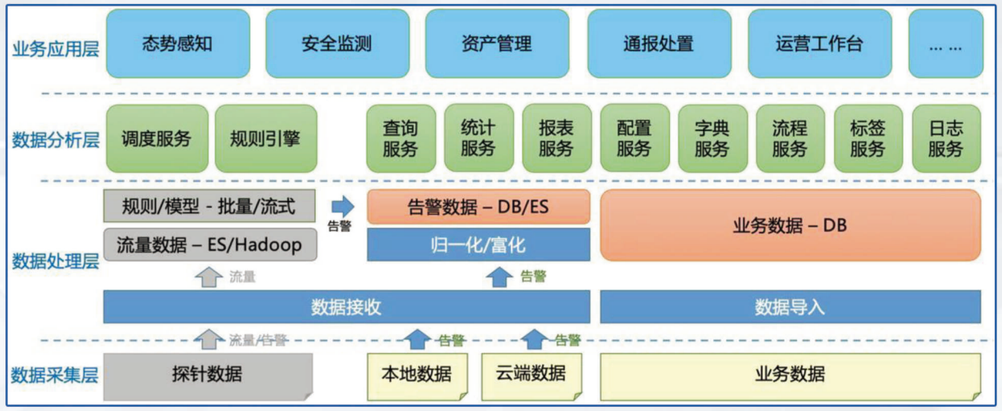
为丰富属地网络监管信息来源，构建清朗互联网空间，建设开通“不良信息举报”平台，体现权威性和有效性。本系统参考12377“违法和不良信息举报”平台的构建标准及构建内容，实现不良信息的及时汇聚、顺畅处理。

网宣管理

网宣管理系统旨在搭建一套信息化、自动化的技术系统，实现网宣工作建立、审批、下发对接媒体及委办部门的工作流程记录，同时能够联系各合作媒体平台，实现一键化、自动化的常用合作平台宣传联动下发。

网络安全态势感知

采用面向服务架构，进行标准化体系接口的设计，采用多层架构，以信息资源库和公共服务为基础进行开发，实现资源和服务的共享，为全方位实现网络空间安全态势感知提供技术支撑。



资产测绘

资产测绘系统针对终端、监控、工控、WEB/在线业务系统等在线网络资产的资产分布、漏洞和指纹信息进行统一管理，摸清辖区资产底数，形成统一的资产立体化监管，针对互联网资产进行深度调查与分类、分级，形成更加细化的信息系统资产数据，包括按所属行业、机关横向分类；按所属地域、行政归属横向分类；按信息系统重要、敏感程度纵向分级；按信息系统脆弱程度、可用程度纵向分级。

网站安全监测

网站安全监测系统支持7*24小时对辖区内的重点网站进行不间断监测，发现网站有被篡改、暗链、敏感词以及挂马、漏洞等安全事件时，及时将安全事件数据同步到应急指挥平台，管理员或者领导在安全应急指挥平台上可以直观的查看与分析本地重点网站的安全风险，并且根据安全事件的分布情况提供领导对安全事件应急指挥的处置的决策依据。

安全大数据采集

安全大数据采集能力建设是平台建设的基础，为大数据安全分析、安全态势呈现、通报预警、应急处置、等保管理、追踪溯源、威胁情报和指挥调度等业务模块提供数据资源。

安全大数据采集能力建设主要包括以下内容：流量采集与分配、高级威胁监测与采集、僵木蠕毒监测与采集、云端威胁情报采集、DDoS攻击监测与采集、网站云安全监测与采集、等级保护数据采集、其他业务系统数据采集等。

系统支持整合安恒、绿盟、天融信、启明星辰、知道创宇、奇安信、奇虎360、深信服、快页等多个厂商探针的数据。

安全大数据分析

安全大数据分析系统采用流式计算引擎、关联分析引擎、智能检索引擎等大数据处理技术，能及时发现、识别网络攻击威胁，监测恐怖组织、黑客组织、不法分子等的攻击活动、攻击行为、攻击方法；监测重点保护对象所受的攻击威胁、破坏、窃密、渗透以及存在的漏洞、隐患等安全情况，并通过报表系统对结果进行分析统计。支持对接入的数据进行导入和导出；支持对数据的基本检索、筛选。

安全态势感知

态势感知系统基于多源数据支持安全威胁监测以及安全威胁突出情况的分析展示。综合利用各种获取的大数据，利用大数据技术进行分析挖掘，实时掌握网络攻击对手情况、攻击手段、攻击目标、攻击结果以及网络自身存在的隐患、问题、风险等情况，对比历史数据，形成趋势性、合理性判断，为通报预警提供重要支撑。该模块支持对网络空间安全态势进行全方位、多层次、多角度、细粒度感知，包括但不限于对重点行业、重点单位、重点网站，重要信息系统、网络基础设施等保护对象的态势进行感知。

态势感知子系统分为两部分：态势分析和态势呈现

态势分析：针对重保单位、网站数据采集分析，通过安全监测子系统对DDos攻击监测、高级威胁攻击检测与APT攻击检测、僵木蠕毒检测、IDS检测等功能，通过恶意代码检测、异常流量分析、威胁分析等技术进行宏观分析后，以监管单位为视角，对本项目监管范围下的单位安全状态进行监测。并且根据系统内置的风险评估算法给出当前被监管单位的整体安全评估。

态势呈现：通过城市安全指数、区域安全指数、单位安全指数、威胁来源、攻击分析、威胁同比、威胁环比、告警详细等呈现整体安全态势。

预警通报

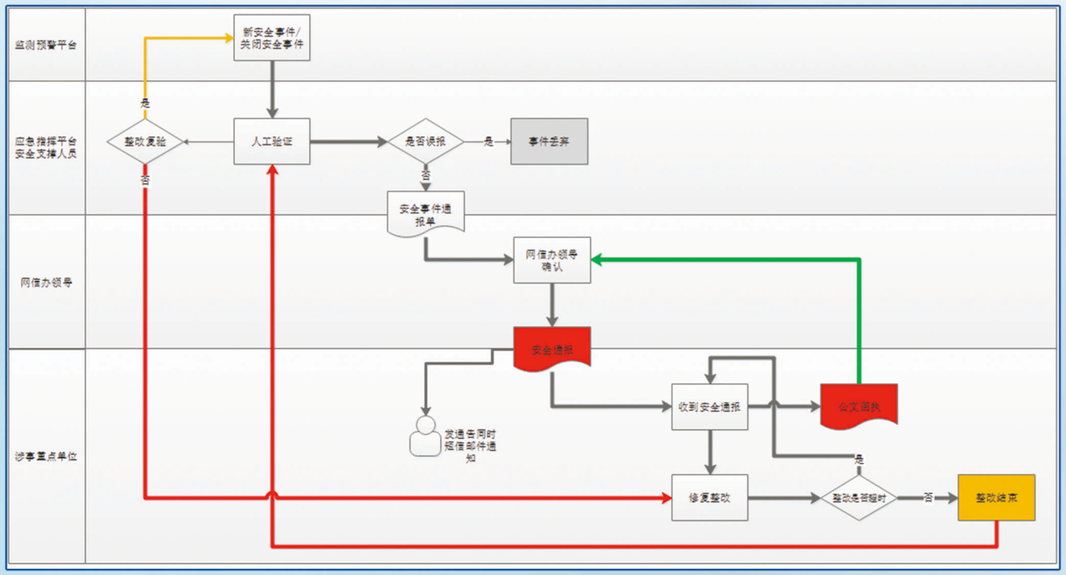
信息通报具备多种通报方式，包括手机APP、短信和微信等。在发生严重情况时，可立即通过短信、电话等方式进行通报；当系统监测到轻微安全隐患时，可进行预警提醒或限期整改，被通报单位须及时反馈处置结果。

信息通报模块对形成的可通报信息进行分类处理，并进行通报业务流转，包括任务看板、通报管理、预警管理、通知管理功能。

应急指挥

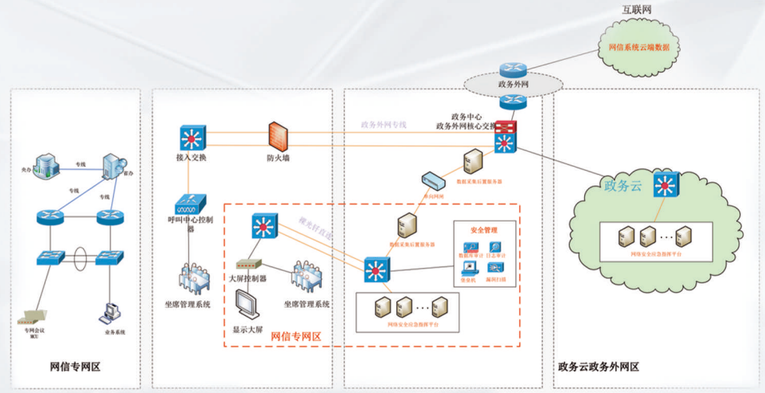
用于在重要会议或活动期间，全方位全天候掌握与活动相关的单位、系统和安全状况，及时通报预警网络安全隐患和网络内容隐患，高效处置网络事件。系统可实现对重保单位/系统、技术支撑单位、安保人员、安保探针、检查小组、驻点排班等静态数据的管理以及对安保检查、通报处置、应急处置、安保巡检、指挥调度等动态业务的支撑。同时，实现对下级网信办、涉网监管单位、重要行业主管单位、技术支撑单位、专家队伍进行综合指挥，从而保障整个重大活动期间的网络安全。

预警通报及指挥



平台部署

网信办业务系统相关的网络主要涉及“三套网络，两条线路”，三套网络分别是网信专网、政务外网、智能化内网，两条线路分别是网信内网线路、政务网线路，整个计算机网络系统三套网络，相互之间物理隔离或逻辑隔离，实现高速有线接入。具体网络架构设计如下图所示：（仅为示例，不同单位的网络架构会有差异）



网络安全应急指挥中心　　政务云中心

平台特点

按照属地化管理要求，建设横向联动、纵向贯通，与上级一体化应急指挥体系相衔接的网信技术体系，其技术构架主要由应急指挥中心物理平台、基础设施和应用系统构成。

平台秉承开放、融合的互联网精神，支持集成第三方系统，融合多厂商的多源异构数据，发挥各自特长，无需重复建设，节约用户投资。

支持二次开发，按需选配子系统及模块，快速自定义工作流程，打造适合自身的网信工作平台。

平台价值

打造成集“网络内容生态治理、网络安全态势感知、预警通报和应急指挥”三大系统于一体的综合应用平台，主要用于执行上级工作指令，督促属地网站落实网上推送、调控管控等工作要求；落实上级网信办要求，执行信息内容管理和网络安全管理的有关工作；做好网络应急值班工作，与上级部门和下级网信办及属地涉网管理部门衔接处置网上突发事件；做好本辖区网络内容和网络安全事件的日常监管工作。