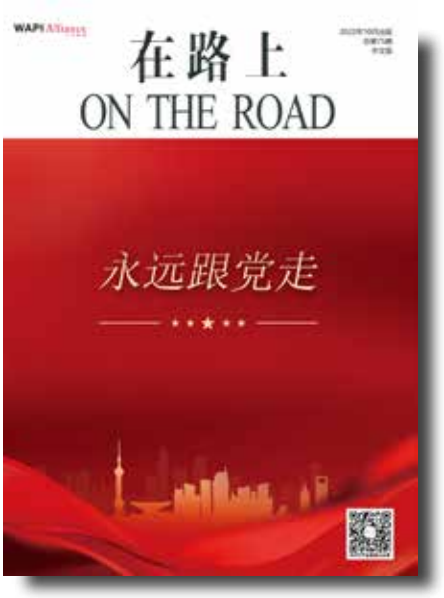
WAPI Alliance
产业|联盟

在路上
ON THE ROAD

2022年10月出版
总第75期
中文版

永远跟党走

WAPI产业联盟公众号



理事成员：

中国移动通信集团公司

中国电信集团有限公司

中国联合网络通信集团有限公司

国家密码管理局商用密码检测中心

国家无线电监测中心检测中心

西电捷通公司

北大方正集团有限公司

北京中电华大电子设计有限责任公司

中电科普天科技股份有限公司

深圳市明华澳汉智能卡有限公司

北京数字认证股份有限公司

WAPI产业联盟

理 事 长：曹　军

秘 书 长：张璐璐

《在路上 On The Road》编辑部

主　　编：张璐璐

编　　辑：周　园　　简　练　　米　东

王立华　　刘剑昕

美术编辑：周　园

WAPI产业联盟秘书处

会员服务部　　标 准 化 部　　市场与产业部

测试实验室　　综合管理部

联络单位

ISO/IEC JTC1/SC6中国对口委员会

工业和信息化部宽带无线IP标准工作组

联系方式

地 址：北京海淀区知春路27号量子芯座1608室

邮 编：100191

电 话：010-82351181

传 真：010-82351181 ext.1901

邮 箱：wapi@wapia.org　zhouy@wapia.org

网 站：http://www.wapia.org.cn

公众号：

WAPI产业联盟公众号

特别报道
Special Report

WAPI 问答
WAPI Q&A

联盟关注
Alliance Concerns

产经要闻
Industrial & Economic News

联盟工作
Alliance Work

新成员
New Member

成员与市场
Member & Marketing

产业技术论坛
Industry & Technology Forum

人民日报：新一代信息技术产业迈上新台阶

《人民日报》（2022年10月06日　第02版）

个人电脑年产量占全球约80%，智能手机和彩电年产量占全球65%以上，电声器件、磁性材料元件等多个门类电子元器件的产量全球第一……

党的十八大以来，我国新一代信息技术产业规模迈上新台阶、质量效益提升，为经济社会发展提供了重要保障。

——电子信息制造业营收10年翻一番。从2012年到2021年，我国电子信息制造业营业收入从7万亿元增长至14.1万亿元，增加值年均增速达11.6%，在工业中的营业收入占比已连续9年保持第一。其中，消费电子产销规模均居世界第一，创造直接就业岗位约400万。

——软件和信息技术服务业快速增长。10年来，软件和信息技术服务业业务收入从2.5万亿元增至9.5万亿元，增长2.8倍。今年1—7月，我国软件和信息技术服务业业务收入达5.4万亿元，同比增长10.3%。

产品创新迭代不断加快

可装入口袋随身携带，展开即可作为外设显示器……日前，维信诺推出业界首款“柔性AMOLED（有源矩阵有机发光二极体）口袋卷曲投幕”。收纳状态时，这款12.3英寸的柔性屏轻巧如一支荧光笔。

“10年来，中国AMOLED产业实现了规模化量产，更在前沿的卷曲拉伸等领域实现突破，诞生了一系列技术创新成果。”维信诺董事长张德强介绍。全球首款消费级可折叠柔性屏手机、全球首款叠屏电视……10年来，诸多“世界首发”消费电子产品问世，我国消费电子产业更是锻造出众多全球驰名品牌。

工业和信息化部电子信息司司长乔跃山介绍，10年来，我国集成电路、新型显示、第五代移动通信等领域技术创新密集涌现，超高清视频、虚拟现实等领域发展步伐进一步加快。基础软件、工业软件等产品创新迭代不断加快，供给能力持续增强。全国软件著作权登记量从2012年的14万件增长至2021年的228万件，年均增长率达36%。

产业结构实现新突破

羚羊工业互联网发布“羚羊工业大脑”、九韶智能发布新一代工业软件内核……9月21日，2022世界制造业大会举办软件、智慧生活专场发布，安徽省在人工智能、工业互联网领域的一批创新成果集中亮相。

“10年来，我国新一代信息技术产业集聚效应凸显，产业结构不断优化。”乔跃山说，2021年，14家中国软件名城软件和信息技术服务业业务收入占全国软件业比重达78.4%。

——集成电路产业规模不断壮大。2021年国内集成电路全行业销售额首次突破万亿元，2018—2021年复合增长率为17%，是同期全球增速的3倍多。产业技术创新能力不断增强，芯片产品水平持续提升，较好地满足了新一代信息技术领域发展需要以及行业应用需求。

——操作系统生态建设加速。国内首家开源基金会——开放原子开源基金会，正加速孵化开放鸿蒙、欧拉等一批开源项目。在服务器操作系统领域，欧拉开源社区用户数量超60万人，合作单位超380家，终端部署量超170万套。在移动操作系统领域，核心技术攻关、应用推广和生态建设加速，鸿蒙操作系统装机量已超3亿台。

融合应用探索新空间

多传感器融合测试、算法优化……黑芝麻智能科技有限公司的技术人员与江淮汽车研发团队，紧锣密鼓地进行全新车型自动驾驶平台实车测试。按照计划，搭载国产车规级大算力自动驾驶芯片的车型，将于年底量产下线。

10年来，以自动驾驶为代表的融合应用层出不穷，我国新一代信息技术产业赋能、赋值、赋智作用深入显现。

——企业上云步伐不断加快，全国累计上云用云企业超过360万家。截至今年6月底，工业互联网应用已覆盖45个国民经济大类，32个重点平台连接设备超7900万台（套），服务工业企业超过160万家。信息消费持续扩大和升级，市场规模由2014年的2.8万亿元增长至2021年的6.8万亿元。今年上半年，我国信息消费规模达到3.24万亿元。

——北斗网络辅助公共服务平台能力建设渐趋完善。今年上半年，平台北斗活跃用户量平均每日4030万，业务量每日3.2亿次。北斗应用规模不断扩大。国内北斗高精度共享单车投放量突破500万辆，货车前装北斗超过百万辆。

10年来，面向教育、金融、能源、医疗、交通等领域典型应用场景的软件产品和解决方案不断涌现。汽车电子、智能安防、智能可穿戴、智慧健康养老等新产品新应用发展取得扎实成效。

许强：把北京打造成世界重要人才中心和创新高地

【编者按】党的二十大报告提出，必须坚持科技是第一生产力、人才是第一资源、创新是第一动力，深入实施科教兴国战略、人才强国战略、创新驱动发展战略，开辟发展新领域新赛道，不断塑造发展新动能新优势。

作为党的二十大代表，北京市科委、中关村管委会主任许强在接受人民日报、北京日报、北京广播电视台等新闻媒体采访时表示，从“国之大者”高度认识和推动国际科技创新中心建设，把北京打造成世界重要人才中心和创新高地，支撑首都高质量发展。


人民日报
RENMIN RIBAO
党的二十大代表热议——
以中国式现代化全面推进中华民族伟大复兴
坚持农业农村优先发展
李克强向科威特首相艾哈迈德致贺电

人民日报

在接受人民日报采访时许强表示，当前北京正加快建设国际科技创新中心，着力释放创新资源要素潜力、激发创新主体活力。


党的二十大
一步一个脚印地走好中国式现代化之路
——党的二十大北京市代表团代表访谈
为奋力谱写全面建设社会主义现代化国家的北京篇章作出昌平贡献
开启全面建设新大兴新国门的崭新篇章
奋力推动怀柔在新时代首都发展中展翅腾飞
“当好密云水库和‘两山理论’守护人
加快建设生态文明幸福的最美冬奥城
把北京打造成世界重要人才中心和创新高地
在加快建设体育强国中勇挑重担
探索深化社区治理现代化的有效模式和工作体系

北京日报

在接受北京日报采访时许强表示，习近平总书记在报告中指出，教育、科技、人才是全面建设社会主义现代化国家的基础性、战略性支撑。北京最大优势是教育、科技和人才。党的十八大以来，习近平总书记和党中央赋予北京科技创新更高的定位、更高的目标，要求我们加快建设科技创新中心。十年来，在市委市政府坚强领导下，我们着力构建国家战略科技力量，持续深化中关村先行先试改革，布局建设“三城一区”主平台，有序推进国际科技交流合作。从成效来看，北京研发经费投入强度保持在6%左右，位居全球创新城市前列，连续5次位居“自然指数—科研城市”榜首，中关村示范区总收入持续保持年均两位数增长。在量子信息、人工智能、区块链、脑科学、基因编辑和细胞治疗等领域产生了一批高水平的成果……从科学中心和创新高地两个维度看，北京已经进入

全球创新型城市前列，为率先建成国际科技创新中心打下了很好的基础。

在向第二个百年奋斗目标进军的新征程中，我们将坚持科技是第一生产力、人才是第一资源、创新是第一动力，更加自觉地从“国之大者”高度认识和推动国际科技创新中心建设，把北京打造成世界重要人才中心和创新高地，支撑首都高质量发展。一是要聚集力量进行原始性、引领性的科技攻关，力争在若干领域突破一批“卡脖子”技术，把核心技术牢牢掌握在自己手中，打赢关键核心技术攻坚战。二是要发挥中关村改革“试验田”作用，不断推进各项先行先试改革，激发创新创业主体活力，构建大企业强、独角兽企业多、中小企业活的创新生态，使中关村创新型企业成为高水平科技自立自强的主力军。三是要围绕世界重要人才中心和创新高地建设，把中关村打造成世界领先的科技园区，培养造就更多的大师、战略科学家和领军人才，为青年人才创造干事创业的机会。四是扩大国际科技交流和合作，努力办好中关村论坛，发挥中关村论坛作为面向全球科技创新交流合作的国家级平台的作用，深化国际人才交流、学术交流、技术交流，参与全球科技创新治理，在加快推进高水平科技自立自强和科技强国建设中当好排头兵、作出北京贡献。

北京广播电视台

在接受北京广播电视台采访时许强表示，我们要依托国家实验室、新型研发机构、一流大学和中关村领军企业，培养人才、引进人才，特别要为青年人才创造良好的环境，为青年人才在学术交流、人才流动、重大科研项目上创造更好的条件。

中国青年报

在接受中国青年报采访时许强表示，从科学中心和创新高地两个维度看，北京已经进入全球创新型城市前列，在量子信息、人工智能、区块链、脑科学、基因编辑和细胞治疗等领域产生了一批高水平的成果，中关村先行先试改革新举措激发创新活力，中关村未来的方向是世界领先科技园区。


党的二十大报告在科技界引发热烈反响

中国高新技术产业导报

在接受中国高新技术产业导报采访时许强表示，报告指出，教育、科技、人才是全面建设社会主义现代化国家的基础性、战略性支撑。建设科技强国、实现中国式现代化，我们既有制度优势和经济实力，还有中华民族优秀传统文化支撑。对于北京来说，最大优势是教育、科技和人才，目前正按照习近平总书记和党中央部署，加快建设国际科技创新中心。

从科学中心和创新高地两个维度看，北京已经进入全球创新型城市前列，在量子信息、人工智能、区块链、脑科学、基因编辑和细胞治疗等领域产生了一批高水平的成果，中关村先行先试改革新举措激发创新活力，正在努力把中关村建设成世界领先科技园区。下一步，将按照党的二十大部署，强化国家战略科技力量，优化配置创新资源，营造良好创新创业生态，扩大国际科技交流合作，加快实现高水平科技自立自强，在科技强国建设中当好排头兵。


新京报客户端

二十大代表许强：北京已经进入全球创新型城市前列

进入 政解焦 阅读更多内容 + 订阅

新京报讯（记者张璐）党的二十大报告中提出，教育、科技、人才是全面建设社会主义现代化国家的基础性、战略性支撑。“建设科技强国、实现中国式现代化，我们既有制度优势和经济实力，还有中华民族优秀传统文化支撑。”二十大代表、北京市科委、中关村管委会主任许强说。

许强表示，对于北京来说，最大的优势是教育、科技和人才，目前北京正按照习近平同志和党中央部署，加快建设国际科技创新中心。从科学中心和创新高地两个维度看，北京已经进入全球创新型城市前列，在量子信息、人工智能、区块链、脑科学、基因编辑和细胞治疗等领域产生了一批高水平的成果，中关村先行先试改革新举措激发创新活力，正在努力把中关村建设成世界领先科技园区。

“下一步，我们将按照党的二十大部署，强化国家战略科技力量，优化配置创新资源，营造良好的创新创业生态，扩大国际科技交流合作，加快实现高水平科技自立自强，在科技强国建设中当好排头兵。”许强说。

新京报

在接受新京报采访时许强表示，建设科技强国、实现中国式现代化，我们既有制度优势和经济实力，还有中华民族优秀传统文化支撑。

对于北京来说，最大的优势是教育、科技和人才，目前北京正按照习近平同志和党中央部署，加快建设国际科技创新中心。从科学中心和创新高地两个维度看，北京已经进入全球创新型城市前列，在量子信息、人工智能、区块链、脑科学、基因编辑和细胞治疗等领域产生了一批高水平的成果，中关村先行先试改革新举措激发创新活力，正在努力把中关村建设成世界领先科技园区。

下一步，我们将按照党的二十大部署，强化国家战略科技力量，优化配置创新资源，营造良好的创新创业生态，扩大国际科技交流合作，加快实现高水平科技自立自强，在科技强国建设中当好排头兵。

世 界 标 准 日

WAPI产业联盟：数字时代的标准化创新与服务

WAPI产业联盟（中关村无线网络安全产业联盟）是我国在无线网络和网络安全领域最具规模的产业联盟，北京市5A级社会组织，国家标准委首批团体标准试点单位，中关村国家自主创新示范区标准化示范单位，科技部A类产业技术创新战略联盟。

16年间，联盟以“专职专业化人员”和“技术标准产业公共服务平台” 为抓手，支持网络安全技术创新和成果转化，打造了百余家全产业链的“网络基础安全技术产业创新联合体”，打通了自主可控的WAPI(无线局域网）和TePA（安全协议基础架构）产业链、创新链、供应链，为我国实现万物安全互联、维护数据安全和信息安全提供保障。

一、联盟标准化工作成果

发布/获发布了 **159项**无线网络和网络领域相关标准。包括国际标准14项、欧洲标准3项、国家标准45项、行业标准7项、团体标准 **90项**。

完成了以太网、电子标签、未来网络、磁域网等 **9个技术领域的国际标准超前布局**。

21项团体标准 获发布成为 **国家标准**，**6项团体标准**获发布成为 **国际标准**。

获ISO/IEC JTC 1/SC 6国内技术对口单位联络组织、工信部宽带无线IP标准工作组联络组织。

二、标准化人才培养

联盟无线网络安全标准化委员会现有81位专家委员；

15位 ISO/IEC国际标准组织注册专家；

10余位 国际标准项目编辑；

1位 WG 召集人；

1位 技术委员会间联络员。

三、无线网络安全标准化委员会

在标准创制和成果转化的机制保障上，联盟严格依循国家标准——GB/T 20004.1《团体标准化 第一部分：良好行为指南》要求，完成建章建制工作，拥有健全的联盟标准化制度规范，形成了包括决策层、协调层和编制层的三层标准化组织结构，按期推进各项工作。目前联盟无线网络安全标准化委员会，由**81位**产业链上下游的标准化工作代表，业界技术专家、标准专家等组成。

四、搭建公共技术服务平台，依标测试产品、服务机构检测能力建设

十余年来联盟测试实验室依标开展WAPI产品和应用测试服务，满足市场和企业需求，目前已完成了**近千款型号产品的测试和整改**，服务市场WAPI产品选型和应用建设。

2022年，WAPI产业联盟发布**《安全无线局域网测评解决方案》**。《方案》包括：与安全无线局域网（WAPI）测评相关的技术标准、工具和服务，覆盖“WAPI产品选型、设计、施工、验收、监督检查”全过程。**一方面满足市场用户依标建设和实施WAPI，另一方面帮助用户和检测机构建设提升WAPI检测能力，支撑实验室资质认定/能力扩项。**

五、获得荣誉

2017年**2项**团体标准入选工信部百项**团体标准应用示范项目**；

2019年**1项**团体标准入选工信部百项**团体标准应用示范项目**；

2020年荣获**中国标准创新贡献三等奖**；

2022年完成**中国标准创新贡献一等奖公示**；

2022年9月，联盟受邀出席由海淀区市场监管局主办的标准创新论坛，并被授予**“海淀区标准创新单位”**。

WAPI 问答（系列连载）

在WAPI服务各行各业关键信息基础设施建设过程中，联盟总结了一些市场用户的常见问题，并结合百度百科、搜狗百科、互动百科、维基百科中文版等对WAPI的解释存在一定不准确乃至错误之处，开辟WAPI问答（系列连载）栏目，帮助大家更加客观准确地了解WAPI。

欢迎您随时和我们交流探讨。

联系方式：010-82351181，staff@wapia.org

第一部分（PART 1）

1. 问：什么是无线局域网？

答：无线局域网（WLAN）是无线高速数据通信两大主流技术之一（另外一个是4G/5G/6G），使用无需授权的ISM频段中的2.4GHz或5GHz射频波段等进行无线连接，具有带宽高、成本低、部署方便等特点，可在局部区域（约100米）内为使用者提供高达数Gbps的高速率数据通信服务。经过二十余年的发展，WLAN已经成为全球宽带信息基础设施的重要组成部分，是目前各国网络用户最主要的宽带接入方式之一。当前最常见的WLAN应用场景主要包括公共接入、个人接入和行业专网等。

2. 问：WLAN、WAPI、Wi-Fi的关系和区别是什么？

答：目前，全球WLAN在数据和管理层面已形成相对统一的技术架构（包括编码调制、数据交换、访问控制、频段分配、切换漫游等），但在安全层面有两条路线：一个是美国主导、Wi-Fi产业联盟主推的IEEE 802.11i（WEP/WPA/WPA2/WPA3）标准，另一个是我国主导发展的WAPI标准。网络安全之外的其他部分是统一的、互通的，产品具备网络安全能力大都采用双模方式，产品可以互连互通。

从技术角度，WAPI和Wi-Fi的区别，大的层面有三个：

（1）安全架构不同。WAPI采用三元对等安全架构（对应全球安全架构演进的第三阶段），Wi-Fi采用二转三元过渡架构（对应全球安全架构演进的第二阶段）。在不同架构下，核心区别是无线接入点（AP）有没有独立身份，这决定了无线局域网终端和接入点的双向鉴别是直接还是间接（三元是直接，二转三元是间

接），也导致Wi-Fi容易遭受中间人攻击（假基站）。

（2）安全协议设计不同。WAPI采用五次传递过程确保安全，Wi-Fi采用的安全协议设计，已被全球业界揭示出容易遭受KRACK、dragonblood等攻击。

（3）使用的密码算法不同。WAPI使用的对称密码算法是中国自主研发的SM4，Wi-Fi则采用美国提出的AES。

3. 问：Wi-Fi技术有什么安全问题？

答：问题主要体现在：Wi-Fi无法实现无线接入点（AP）与终端（STA）的对等双向鉴别和访问控制，STA无法判断AP的合法性，不法分子可以伪造接入点，通过“钓鱼接入”、窃取数据等方式，实施诈骗恐吓、不良信息、造谣传谣等违法犯罪活动，对用户权益、社会稳定等带来严重威胁。特别是，随着无线局域网的应用日益广泛，美国主导发展的Wi-Fi，其安全问题越来越成为威胁我国网络空间安全和国家安全的重大隐患。

4. 问：Wi-Fi安全机制也在不断升级中，它的最高安全机制能否保证安全？

答：Wi-Fi安全技术演进从WEP到WPA、WPA2，再到当前最高等级的WPA3，安全核心架构并未升级，仍然沿用20年前设计的IEEE 802.1x，即二转三元架构模式，无线接入点（AP）没有独立身份，容易导致中间人攻击。并且，密钥需要在AP和鉴别服务器之间传递，而传递密钥的安全通道在Wi-Fi标准中并未明确，而是依赖于厂商自行选择，安全通道存在的漏洞给整个WLAN系统带来非常严重的安全威胁。

WPA3虽然在密码算法和预共享密钥机制等方面，其安全强度有所加强，但因安全架构并未提升，之前业界发现的安全问题未能完全消除，仍然存在安全隐患，因此，目前Wi-Fi最高安全机制并不能保证安全。网络安全等级保护国家标准也明确禁用Wi-Fi的相关模式。

5. 问：什么样的场景下，更适合使用WAPI？

答：在所有应用WLAN的地方，均适合使用WAPI。

符合WAPI标准体系的无线局域网系统，符合国家网络安全法、密码法、标准化法、国家安全法、数据安全法、个人信息保护法等法律，以及网络安全等级保护、密码应用安全性评估、网络安全审查、关键信息基础设施安全保护、商用密码管理等法规，和国家、行业、团体技术标准的要求。

符合WAPI标准体系的无线局域网系统，和Wi-Fi系统相比，建设成本相同。

符合WAPI标准体系的无线局域网系统，保障了无线局域网用户的数据传输安全。

6. 问：建设和使用WAPI的成本比Wi-Fi如何？会不会增加额外成本？

答：WAPI产业成熟度高，市场竞争充分，不会增加用户的采购和建设成本。具体如下：

（1）网络设备方面：所有主流厂商产品全部支持WAPI，大多采用安全能力双模方式，售价与Wi-Fi产品相同。

（2）智能移动终端（Andriod、iOS）方面：全部支持WAPI（双模方式），不仅限于手机和平板电脑，也包括所有使用了类似芯片/操作系统方案的产品，如视频记录仪、移动布控球、智能安全帽等。

（3）非智能终端：绝大部分均可通过软件升级支持WAPI，不增加成本。

7. 问：此前的一些老旧设备（所使用的芯片不支持WAPI功能），怎么支持WAPI？可以升级吗？

答：老旧设备可以通过软件升级，支持WAPI功能。但这类设备已经很少了。

（1）无线局域网（WLAN）是包含调制编码、数据交换、访问控制、天线技术、频段分配和安全协议技术等一系列技术组合而成的。WAPI属于安全协议技术，对WLAN基础通信功能并不做改变，可利用无线MAC芯片连接设备中的中央处理单元（CPU）进行安全协议处理。因此对WAPI功能的支持，完全可以通过纯软件来实现。在芯片全面支持WAPI之前，很多设备厂商均有过实践。

（2）设备通过软件升级支持WAPI，在性能效率方面，不如硬件实现方式高。但对于老旧设备来说，本身支持的都是低速率的通信技术，比如最高理论吞吐量率大致在11Mbps或54Mbps，实际吞吐量也就在8Mbps或20Mbps左右，对于这种老旧低速率设备来说，因其面对的应用场景速率要求不高，纯软件方式实现WAPI对本身的性能影响是满足需求的。

8. 问：前期已经部署的WLAN网络，要达到启用WAPI服务的效果，需要花多少钱？

答：绝大部分WLAN网络设备通过软件升级，均可支持并启用WAPI安全服务，升级的直接费用可以忽略不计。

（1）对于运营商部署的WLAN网络，在采购时即已经要求所有设备必须支持WAPI功能，因此实际上这类网络使用的设备已在功能上支持了WAPI，仅仅是在网络配置上没有启用WAPI服务而已。因此，只需要配置开启WAPI，即可对用户提供WAPI安全服务，这属于网络配置工作，没有成本。

（2）对于非运营商部署的WLAN网络，由于硬件芯片都已在物理上具备了WAPI功能，只需要软件配合启用其服务，而不需要升级任何硬件，具体方式是：设备厂商提供支持启动WAPI服务的升级包对设备进行升级。（而对于网络设备来说，经常在运营中会发现设备存在缺陷或者功能更新需求，因此厂家本身会经常发布

新的升级包，来解决问题和改进，这属于设备厂商对产品生命周期正常管理的范畴。）

（3）为了给用户提供WAPI安全服务，按照标准要求，一个无线局域网需要配置一个具备鉴别服务单元（ASU）功能的实体，ASU单元的形态有如下三种：内置在无线接入点（AP）中，软件升级AP，无硬件成本；内置在现有的其他网络服务器设备中，软件升级设备即可，无硬件成本；在一些关键基础设施中以独立设备——鉴别服务器（AS）方式部署，价格方面，市场会发挥作用，会从支持用户的综合效益考虑，每台几百、几千、几万乃至不要钱都是有可能的。另外，部署鉴别服务设备的投资者也可以通过提供的服务从市场获得收益，这部分的投资可以忽略不计。

9. 如何判断一款产品是否已经支持了WAPI?

答：对于无线电发射设备，如无线接入点（AP）、终端（STA）等产品，依据国家法律法规，上市前应取得《无线电发射设备型号核准证》。如果厂商在型号核准阶段申请测试了WAPI功能，则《型号核准证》“设备名称”一栏上会标注“WAPI”。相关信息可在工信部网站公开查询：https://zwfw.miit.gov.cn/miit/resultSearch?wd=WAPI&categoryTreePid=&categoryTreeId=313

对于产品的标准符合性，以及多厂商间产品的互操作最优化性能，行业用户通常采用委托WAPI产业联盟测试或采信联盟测试报告的方式；值得关注的是，联盟接受行业用户委托进行测试通常是免费的。

此外，国内多家检测机构均具备WAPI相关测试能力，也可采信这些机构出具的报告。他们包括但不限于：国家无线电监测中心检测中心、上海无委无线电检测实验室有限公司、广州广电计量检测股份有限公司、辽宁信鼎检测认证有限公司、江苏省电子信息产品质量监督检验研究院、广州通导信息技术服务有限公司、国家无线电频谱管理研究所有限公司、工业和信息化部电子第五研究所、国家信息技术安全研究中心。

10. 问：在行业无线网络部署中，选WLAN还是选5G?

答：这两者之间不是非此即彼的关系。但WLAN较之5G专用网络，更适合行业应用工程“大带宽、大连接、移动性”的应用需求。

（1）WLAN是现有行业专网的自然延伸，自建自营，独占网络资源，数据自己掌握，完全自主可控。

（2）在已部署有线网络/光纤的区域使用WLAN完成“最后一公里”覆盖，性价比高。一次建成后，可以不断承载新增业务。例如，电网变电站等应用场景的场地特性基本排除了外部同频干扰的可能，可在局部区域实现“饱和式”覆盖，网络连续性、安全性、性能冗余等目标可自主设计实现。

（3）相对而言，5G专用网络无论是设备物理专用，或者是切片逻辑专用，仍都是行业租用了运营商的服

务，运维和数据将通过运营商，应用行业难以自主可控。行业5G专用网络中设备由运营商所有，由运营商运维；数据通过运营商，运营商做数据分析（注：原则上不查看用户数据内容，只看数据头用于分析业务质量，但存在非法获知用户数据内容的可能）。

（4）目前阶段，WLAN产业链成熟度高于5G专网，而且建设费用和运维成本较低。我国5G正式商用还不到半年，尚未经受大流量、大连接、高可靠、低时延的充分考验，网络切片等大规模组网技术尚未验证（来源：中国工程院邬贺铨院士）。相比而言，WLAN自1997年发展至今，最新一代速率可达数9.6Gbps，技术不断演进、产业成熟、成本更低。

人工智能背景下全球关键信息基础设施安全挑战与对策

信息安全与通信保密杂志

【摘要】随着算力提升、数据积累等因素的共同作用，人工智能技术的应用门槛逐步降低，在网络安全领域的应用快速拓展，加剧现实安全威胁的同时也催生了新型安全威胁，全球关键信息基础设施安全受到挑战。从人工智能在网络安全领域的应用出发，以网络安全威胁为视角进行分析，得出关键信息基础设施防护面临着攻击模式自动演化、攻击手段自动化、攻击者分工专业化等挑战。结合当前全球关键信息基础设施防护的普遍实践，提出智能化防护体系、缩短发起响应的时间、培养AI+网络安全人才等对策，为保障关键信息基础设施安全提供科学参考。

自20世纪50年代首次提出人工智能这一概念后，随着计算机技术的不断进步，人工智能概念的范围也逐渐扩大，计算机图像识别、数据挖掘、深度学习等技术也相继被纳入人工智能的范畴。近些年，在算力提升、数据积累等因素的共同作用下，人工智能技术的应用范围不断扩大，应用门槛也逐步降低，引起了世界主要国家和集团的高度重视。2017年，中国印发了《新一代人工智能发展规划》，提出要在2030年使“中国人工智能理论、技术与应用总体达到世界领先水平，成为世界主要人工智能创新中心”。2019年，美国发布《2018国防部人工智能战略概要》，提出要将人工智能作为未来关键的军事技术进行研究，并于同年发布了新的《国家人工智能研究与发展战略规划》。欧盟、俄罗斯、日本、印度等国也相继发布其在人工智能领域的规划和目标。人工智能已经成为大国竞争的新领域，各国政府都在积极推动人工智能技术在各领域的应用。与此同时，人工智能的各类问题也引起了研究者们的重视，特别是人工智能伦理、人工智能军事化、人工智能对政府治理的影响等议题尤为突出，已经有研究者将人工智能列为未来几十年中人类面临的最大挑战之一。随着人工智能在网络安全领域应用的逐步加深，越来越多的研究者也开始重视人工智能对于网络安全的影响。

关键信息基础设施作为网络空间的基础组成部分，其安全关乎网络空间的稳定与秩序。近年来，全球范围内针对关键信息基础设施的攻击呈快速增长和危害增强的趋势：2019年，委内瑞拉国家电网干线遭到攻击，造成全国大面积停电；2021年，美国最大燃油管道公司被黑客勒索，导致美国东海岸能源供应出现问题；2022年俄乌战争期间，乌克兰的黑客支持者对白俄罗斯铁路网络进行攻击，导致正常的铁路调度无法完成。随着数字经济在国家发展中的重要性不断增强，关键信息基础设施在网络攻击目标中的重要性明显提升，攻击关键信息基础设施成为各类组织获取非法经济利益、推进政治主张的重要手段。人工智能在网络安全领域的应用也强烈地影响着关键信息基础设施的安全，特别是由于人工智能的“赋能”效应对各类网络安全威胁的赋能使现有的关键信息基础设施安全防护体系面临挑战。

本文将对当前人工智能在网络安全领域的应用情况进行梳理分析，在此基础上根据关键信息基础设施防护现状，从网络安全威胁的角度分析关键信息基础设施面临的挑战，最后提出应对挑战的对策与建议，以期为关键信息基础设施安全防护工作提供理论参考。

1 人工智能在网络安全领域的应用现状和特点

人工智能技术在网络安全领域得到应用的时间并不长，但因其应用前景使得越来越多的研究者投入其中，如今，人工智能已经是网络安全领域中一个无法忽视的应用方向并形成了在其他应用领域所没有的特点。

1.1 人工智能在网络安全领域的应用现状

人工智能技术在网络安全领域中的应用最早可以追溯到 2000 年左右，当时有国外的研究人员提出在入侵检测中采用机器学习算法来提高检测效率，为人工智能在网络安全领域的应用提供了初始方向。得益于过去20年来计算机算力水平的提高、网络安全数据的积累以及各类算法的进步，人工智能在网络安全领域的应用越来越多，从现有的情况来看，人工智能在网络安全领域的应用主要集中在威胁检测、漏洞挖掘与修复、组织和发现僵尸网络、威胁情报识别以及绕过安全防护等方向。

威胁检测是人工智能在网络安全领域最早应用的方向之一，应用也最为成熟。传统的流量分析检测技术对流经检测节点的每个数据包进行检测分析，存在资源开销大、溯源表现弱等客观问题。美国“棱镜计划”曝光后，国内外网络安全研究机构和厂商加快了将人工智能技术引入威胁检测中的步伐。美国的FireEye公司、以色列的Deep Instinct公司以及国内的360政企安全、启明星辰、安天等公司均在自己的产品中引入了人工智能技术，融合日志、流量、资产等信息，提高了威胁检出效率。

漏洞挖掘与修复一直都是网络安全领域最受重视的方向之一。长期以来，漏洞挖掘和修复工作都要依赖人工进行，这限制了网络安全人员对漏洞的发现和修正速度，给黑客及黑客组织使用漏洞进行攻击提供了机会。2016年，美国国防部高级研究计划局资助的第一届机器自动攻防大赛（Cyber Grand Challenge，CGC）揭示了人工智能加持下漏洞自动化挖掘和修复的未来。近年来，已经有大量研究者提出将深度学习应用到漏洞挖掘中，并取得了一定的成果。僵尸网络一直隐藏攻击者、开展大规模分布式拒绝服务攻击（Distributed Denial of Service，DDoS）方面扮演着重要角色。人工智能给僵尸网络带来的最大变化就是以大量物联网（Internet of Things，IoT）设备为基础，通过蜂巢网络（Hivenets）和机器人集群（Swarmbots）使僵尸网络中的设备从“奴隶”变为可以在一定监督下进行自主行动的机器人，极大地提高了僵尸网络拥有者能够维护的网络规模以及僵尸网络的扩张速度。网络安全研究者也尝试通过使用人工智能技术来实现为僵尸网络发起的DDoS攻击提供早期检测 。

威胁情报识别与利用对于现在的网络安全愈发重要。攻击者数量的快速增长，迫使网络安全防护体系尝试在攻击发起之前就形成阻断，这就是威胁情报的核心作用。然而传统的威胁情报生成方法识别精度不高，普遍需要人工分析确认。人工智能能够通过算法和模型提高人工分析的速度和准确度，进而提高威胁情报的产

出。已有研究者提出使用神经网络来进行威胁实体的识别，并在大规模网络安全数据集上取得了较好的实验结果。绕过攻击对象的安全防护一直是网络攻击者的目标，人工智能通过威胁模型算法提高安全防护的同时，也给攻击者提供了新的安全敞口和攻击思路。例如，人工智能模型的训练需要不断的数据积累，攻击者可以通过构造错误的数据来干扰人工智能模型的学习，从而使模型失效，也就是“中毒攻击”。也有直接通过构造数据对算法本身脆弱性进行攻击的例子。也有攻击者尝试通过人工智能来发现现有防御体系的弱点或隐藏具体攻击行为。目前已有研究提出通过对抗神经网络来实现对现有流量监测技术的绕过。

除此之外，人工智能在网络测绘、事件响应、风险评估等方面的应用也在持续深入。

1.2 人工智能在网络安全领域的特点

通过对人工智能在网络安全领域的应用情况进行梳理，本文认为当前人工智能在网络安全领域的应用相比其他领域的应用存在技术服务化、伦理顾虑少、对抗性强等特点。

（1）技术服务化。人工智能经过多年的发展，即使已经比最初诞生时大幅度降低了学习和使用的门槛，但其所要求的算力、知识和数据的绝对数量依然是大部分个人开发者难以负担得起的。在人工智能应用的几个主要领域中，人工智能作为产品进行售卖时往往需要进行较多的定制才能够贴合实际业务场景的需要。网络安全领域高度单一的对抗需求使得人工智能产品能够形成聚焦精准方向的应用。专注于攻击的比通用型的人工智能应用开发更加简单、场景更加单一，不再需要终端用户的大量适配，可以轻松封装成为产品，从而使开发者和使用者分离开来，也就是技术服务化。

（2）伦理顾虑少。人工智能的伦理问题一直是社会关切的话题，已有学者指出人工智能本身具有的特征可能在基本人权、社会秩序和国家安全上产生伦理风险。在网络安全领域中，已经有学者考虑到人工智能在个人信息保护中的伦理问题。但基于网络安全领域本身的安全属性，使得研究者们在新技术应用时受到的制约相对较少且缺少监督。在自动化攻击手段使用场景和影响、自动化渗透测试方面对从业人员的影响等相关伦理问题的顾虑和讨论较少。

（3）对抗性强。网络安全领域的诞生与发展是网络中对抗行为的结果。当越来越多的人涌入网络空间时，网络空间受到的攻击也呈指数增长。相较于人工智能在其他领域的应用，网络安全领域的人工智能的根本目的在于帮助使用者在对抗中取得优势：众多研究者的研究目的在于提高安全性，而攻击者们希望突破安全防护。可以说，网络安全领域的人工智能由于领域的特性，在表现上呈现出了远超其他领域的对抗性。

2 人工智能与关键信息基础设施安全

威胁分析关键信息基础设施安全一直是世界各国政府网络安全工作关注的焦点。美国作为网络技术的发源地，联邦政府高度重视信息化建设工作。早在 1996 年 7 月 15 日就发布第 13010 号行政命令《关键基础设施保护》，并于次年对关键信息基础设施进行定义。1996 年，中国开始实行的网络和信息系统等级保护制度

也可以被认为是一种具有中国特色的关键信息基础设施保护制度；2021 年 9 月 1 日起施行的《关键信息基础设施安全保护条例》从法规上进一步完善了中国关键信息基础设施安全防护体系。关键信息基础设施安全防护的具体制度和措施在不同国家存在差别，但从全球主要国家的相关举措上也可以看到，当前全球关键信息基础设施安全存在着安全组织制度建设强于技术体系、基础组件供应链高度同质化、容易成为网络攻击目标等共同点。

（1）安全组织制度建设强于技术体系。由于关键信息基础设施涵盖种类多，部署地域分散等特点，建立统一的关键信息基础设施防护体系存在技术上的难度，很少有国家形成系统性的关键信息基础设施安全防护技术体系。更多国家是将关键信息基础设施运营者组织起来形成制度化的威胁情报共享机制、事件响应协同机制，如日本的网络安全信息共享、脱欧以来的英国网络安全新体制等都是在组织和制度角度提高关键信息基础设施的安全水平，像是美国爱因斯坦工程那样覆盖全国关键信息基础设施的安全技术体系还是少数。

（2）基础组件供应链高度同质化。关键信息基础设施大多结构复杂，但在全球关键信息基础设施建设过程中可供选择的软件却高度同质化。特别是自 Web2.0 时代以来，越来越多的信息系统采用B/S架构，关键信息基础设施采用的开源组件高度同质。2021年末爆发的Apache Log4j远程代码执行漏洞以及2014的Heartbleed漏洞在全网范围内造成了重大影响，大量关键信息基础设施在漏洞爆发期安全承压，甚至产生了应急人员不足的情况。关键信息基础设施基础组件供应链高度同质化的情况可见一斑。

（3）容易成为网络攻击目标。从近年来的重要网络安全事件来看，针对关键信息基础设施的攻击数量急剧增长。一方面，关键信息基础设施承载国民经济正常运行，一旦被攻击成功往往能让攻击者快速达到金钱、政治等方面的攻击目的。另一方面，随着网络在社会中的渗透，特别是物联网、工业互联网的发展使得大量设备接入网络空间，攻击者能够访问到关键信息基础设施的机会也越来越多。收益预期和攻击敞口的变化使得关键信息基础设施越来越容易成为网络攻击的目标。

当前网络空间人工智能化的网络攻防趋势已经形成，关键信息基础设施安全进一步受到全面挑战 。关键信息基础设施长期面对有国家背景的APT组织、随时爆发的高等级脆弱性以及APT水平的勒索软件等威胁，人工智能在网络安全领域的应用又加速了传统网络安全威胁的进化。结合全球关键信息基础设施安全的共同点，可以认为全球关键信息基础设施面临攻击模式自动演化、攻击手段自动化以及攻击者分工专业化等安全挑战。

2.1 攻击模式自动演化挑战

传统关键信息基础设施安全主要是从边界防护的角度对整体防护体系进行设计，从理念上来看缺少对抗性。现有渗透测试方法中通过构造包含大量无效数据的请求包来绕过防火墙正是防护体系缺乏对抗性的表现。在人工智能的背景下，攻击者将通过人工智能快速提高对抗的次数并进行分析，实现攻击模式的自动演化。现在已经有攻击者尝试通过生成对抗网络（Generative Adversarial Networks，GAN）来模拟关键信息基础设施防

护体系的威胁检测系统，从而让自己的恶意代码能够绕过防护体系。类似的情况也发生在恶意文件检测的绕过上。攻击模式自动演化是人工智能给关键信息基础设施带来的最为严重的挑战，长期来看将使关键信息基础设施的安全防护体系的建设理念发生重大转变。

2.2 攻击手段自动化挑战

随着人工智能应用门槛的进一步降低，越来越多的攻击者开始通过人工智能技术开发自动化的攻击手段或为原有的攻击手段进行智能化升级。这一点在勒索软件即服务（Ransomware as-a-Service，RaaS）和组织僵尸网络上体现得尤为明显。越来越多的勒索软件和僵尸病毒通过预先设定的机器人（bot）程序在网络内自动搜索并感染设备，从而快速扩大感染规模。攻击者只需将恶意病毒载荷进行一次有效投放，就可以自动化实现阶段性的攻击目的。也有攻击者为各个攻击节点通过人工智能增强其自主性，实现去中心化的自动攻击。总的来看，攻击手段自动化一方面加快了攻击成功后扩大影响的速度，另一方面延后了攻击暴露的时间节点，对关键信息基础设施安全响应的速度提出了更高要求。

2.3 攻击者分工专业化挑战

早年的网络攻击者进行网络攻击的目的较为多样，以炫技、出名为主要目的的攻击者并不在少数，往往一个人承担了网络攻击的全部环节。随着数字经济的发展，越来越多的攻击者开始专注于非法利润的获取，对于攻击工具更高的要求以及突破越来越多的安全防护策略使攻击者逐渐产生分工。人工智能在网络安全领域技术服务化的特点进一步加速了这一进程。网络攻击者中的研发人员可以更快地将更高级的工具封装好提供给购买供给服务的人，关键信息基础设施安全则受限于产业中人才的缺乏等因素，无法实现同样速度的防护技术更新。

3 关键信息基础设施应对挑战建议

有效应对人工智能对全球关键信息基础设施安全形成的挑战，需要从系统角度全面考虑。现有研究大多集中于技术层面，对人工智能带来的全方位挑战的重视度不够。通过上文的分析，本研究认为全球关键信息基础设施应对人工智能带来的安全挑战需要从构建智能化防护体系、缩短发起响应的时间以及培养 AI+ 网络安全人才等方面做起。

3.1 构建智能化防护体系

建设关键信息基础设施安全防护体系一直是保障关键信息基础设施安全的重要举措。面对自动演化的攻击模式，需要对关键信息基础设施的安全防护体系进行全面的智能化改造。

除当前已经广泛采用的基于人工智能的流量检测外，关键信息基础设施安全防护体系智能化还可以从以下几个方面进行。一是加强人工智能在辅助决策方面的应用，将有限的安全运营人员从快速增长的大量攻击中解放出来，专注于处理真实、高等级的攻击，提高防护效率。二是采用多元化的威胁分析算法及模型，形成现有防护体系的联动，如通过建设智能化的网络安全运营中心，为低智能的安全设备赋能，整体提升防护体系的

智能化水平。三是主动采取生成对抗网络、遗传算法等人工智能技术对现有防护体系进行测试，从而智能化地补充防护体系的安全策略。

3.2 缩短发起响应的时间

在网络安全领域，包以德循环（OODA）是由Observation（观察）、Orientation（判断）、Decision（决策）、Action（执行）4 个单词的首字母组合得名，常用于描述对从发现到响应网络攻击的过程。应对自动化的网络安全攻击手段，关键是缩短 OODA 中各环节的时间。当前较为有效的方法是大量部署基于云端数据的终端检测 与 响 应（Endpoint Detection and Response，EDR）系统并提高威胁情报的作用。

一方面，EDR 系统作用于网络攻击的控制、利用阶段效果显著，能够帮助关键信息基础设施的安全运营者及时发现存在异常行为的终端，加快发现已经成功的网络安全攻击的速度。另一方面，准确迅速的威胁情报能够帮助关键信息基础设施安全防护体系及时启动并完成有关研判，能够大幅度提高安全策略的修改速度，缩短安全运营人员针对特定网络安全攻击发起响应的时间。

3.3 培养AI+网络安全人才

关键信息基础设施安全离不开专业人才的支持。面对越来越多的封装好的人工智能攻击工具，需要有更多具有人工智能学科背景的研究人员进行人工智能攻防技术的研究，从而研发出更有效的网络安全防护产品。关键信息基础设施运营者应该积极参与AI+网络安全人才的培养，提高人才数量和质量，加快网络安全相关人工智能技术的研发和应用，赋能关键信息基础设施安全防护。特别是关键信息基础设施每天面临着数量众多的网络攻击，运营者掌握着大量宝贵的真实攻击数据，通过和研究院所、企业等人才培养实体的合作，这些攻击数据可以在培养 AI+ 网络安全人才的过程中发真实场景构建、威胁数据建模等作用，提高人才培养效率。

4 结语

关键信息基础设施对于全球各国的社会经济稳定与发展都有着重要意义，关键信息基础设施安全也因此受到越来越多的重视。人工智能对于当前全球关键信息基础设施形成的挑战是普遍且深刻的。面对人工智能带来的攻击模式自动演化、攻击手段自动化、攻击者分工专业化等挑战，需要加快构建智能化防护体系、缩短发起响应的时间并积极参与培养AI+网络安全人才，持续保障关键信息基础设施安全。

作者简介：

宋　钊，男，硕士，助理工程师，主要研究方向为网络安全、应急管理；

孙　骞，男，博士，高级工程师，主要研究方向为网络安全。

选自《信息安全与通信保密》2022年第 6 期

美国新版《国家安全战略》的九大网络议题看点

奇安网情局

美国政府10月12日发布新版《国家安全战略》，重申了加强国家数字防御和打击网络犯罪分子的承诺。

该战略详细说明了为加强国家网络安全所采取的一系列措施，并粗略提到了外国对手所构成的网络威胁挑战。该战略提出：一是美国正在与盟友和合作伙伴密切合作，为关键基础设施制定标准，以快速提高网络弹性，并建立集体能力以快速响应攻击；二是建立了创新的合作伙伴关系，以扩大执法合作，打击网络犯罪分子和及其网络洗钱活动，以应对来自犯罪分子的破坏性网络攻击；三是致力于加强规范以减轻网络威胁并增强网络空间的稳定性，目标是阻止来自国家和非国家行为者的网络攻击，并将使用所有适当的国家力量工具果断地应对网络空间中的敌对行为，包括破坏或削弱重要国家职能或关键基础设施的行为；四是将继续推动遵守联合国大会批准的负责任国家网络空间行为框架；五是通过跟踪、归因和防御网络空间中恶意行为者的活动来保护投资并增强弹性；六是在军事方面投资于一系列先进技术，包括在网络和太空领域、导弹打击能力、可信人工智能和量子系统的应用，同时及时向战场部署新能力；七是将跨包括网络空间在内的军事领域和包括信息和技术在内的非军事领域进行整合，以实施综合威慑；八是将制定道路规则，包括迫切需要更新技术、网络空间、贸易和经济的道路规则；九是将磨砺治国之道，包括强化网络外交、对新兴技术的关注和网络安全服务。

奇安网情局编译有关情况，供读者参考。

美国政府10月12日发布了《国家安全战略》，重申了加强该国数字防御和打击网络犯罪分子的承诺，但未提供新的细节。

该期待已久的文件最初预计会在今年早些时候发布，但俄乌战争和其他世界事件促使美国白宫重新审视其优先事项。根据法律，美国总统必须每年提交一份国家安全战略，但政府往往不这样做。美国总统拜登2021年并未提出国家安全战略。

美国国家安全顾问杰克·沙利文在新闻发布会上表示，“这一战略并没有详细说明美国面临的每个挑战和机遇。它涉及我们在世界每个地区的计划，但它试图更广泛地讨论我们打算如何抓住这个决定性的十年来推进美国的切身利益。”

此份48页的文件是在白宫发布情况说明书的第二天发布的，该文件详细说明了它为加强国家网络安全所采取的一系列措施，粗略提到了与俄罗斯等外国对手所构成的总体挑战有关的网络问题。该战略只在一个简短的部分来讨论该主题，题为“保护网络空间”，内容本质上是对以前政府声明和承诺的翻版。

保护网络空间

我们的社会，以及支持它们的关键基础设施，从电力到管道，越来越数字化，容易受到网络攻击的干扰或破坏。此类攻击已被俄罗斯等国家用来破坏国家向公民提供服务的能力并胁迫民众。我们正在与‘四方安全对话机制’等盟友和合作伙伴密切合作，为关键基础设施制定标准，以快速提高我们的网络弹性，并建立集体能力以快速响应攻击。面对来自犯罪分子的破坏性网络攻击，我们建立了创新的合作伙伴关系，以扩大执法合作，拒绝为网络犯罪分子提供庇护，并打击非法使用加密货币清洗网络犯罪所得。作为一个开放的社会，美国显然有兴趣加强规范以减轻网络威胁并增强网络空间的稳定性。我们的目标是阻止来自国家和非国家行为者的网络攻击，并将使用所有适当的国家力量工具果断地应对网络空间中的敌对行为，包括破坏或削弱重要国家职能或关键基础设施的行为。我们将继续推动遵守联合国大会批准的负责任国家网络空间行为框架，该框架承认国际法在线适用，就像离线一样。

同时，该战略在其他部分也提出与网络相关的问题和措施。

合作应对竞争时代的共同挑战

邪恶的行为者（国家支持的及非国家支持的）正在利用数字经济筹集和转移资金，以支持非法武器计划、恐怖袭击、助长冲突，并勒索被勒索软件或网络攻击袭击的国家卫生系统、金融机构和关键基础设施。

实施现代产业和创新战略

我们还通过跟踪、归因和防御网络空间中恶意行为者的活动来保护我们的投资并增强其弹性。

现代化和加强我们的军队

随着新兴技术改变战争并对美国及其盟国和合作伙伴构成新威胁，我们正在投资一系列先进技术，包括在网络和太空领域、导弹打击能力、可信人工智能和量子系统的应用，同时及时向战场部署新能力。

综合威慑

我们的国防战略依赖于综合威慑：能力的无缝结合，让潜在对手相信他们的敌对活动的成本超过了他们的收益。

它需要：跨领域整合，认识到我们竞争对手的战略跨越军事（陆地、空中、海上、网络和太空）和非军事（经济、技术和信息）领域——我们也必须这样做。

打击跨国有组织犯罪

跨国有组织犯罪影响了越来越多的受害者，同时扩大了从移民到网络攻击等其他相应的全球挑战。跨国犯罪组织参与的活动包括贩运毒品和其他非法商品、洗钱、盗窃、人口走私和贩运、网络犯罪、欺诈、腐败以及非法捕鱼和采矿。

制定道路规则

最迫切需要更新技术、网络空间、贸易和经济的道路规则。

磨砺我们的治国之道

我们的国家安全机构和劳动力支撑着美国的全球领导地位以及美国人民的安全、繁荣和自由。为了实现我们雄心勃勃的目标，我们必须现代化和调整我们的治国之道，以应对当今的挑战。例如，我们正在：

通过使国务院现代化来加强美国外交，包括最近成立了一个新的网络空间和数字政策局以及关键和新兴技术特使。

重组负责政策的国防部副部长办公室，以加强对新兴技术的关注，并提高高级领导人对关键地区的关注。通过重新构想国土安全部如何雇用、培养和留住顶级和多样化的网络人才，加强国土安全部（DHS）的网络安全服务。

预计美国政府将在推迟发布的《国家网络安全战略》提供关于网络议题的新细节信息。

习近平：

坚持科技是第一生产力 人才是第一资源 创新是第一动力

习近平在二十大报告中强调，必须坚持科技是第一生产力、人才是第一资源、创新是第一动力，深入实施科教兴国战略、人才强国战略、创新驱动发展战略，开辟发展新领域新赛道，不断塑造发展新动能新优势。

他说，要坚持教育优先发展、科技自立自强、人才引领驱动，加快建设教育强国、科技强国、人才强国，坚持为党育人、为国育才，全面提高人才自主培养质量，着力造就拔尖创新人才，聚天下英才而用之。推进教育数字化，建设全民终身学习的学习型社会、学习型大国。完善科技创新体系。坚持创新在我国现代化建设全局中的核心地位。完善党中央对科技工作统一领导的体制，健全新型举国体制，强化国家战略科技力量，优化配置创新资源，提升国家创新体系整体效能。扩大国际科技交流合作，加强国际化科研环境建设，形成具有全球竞争力的开放创新生态。加快实施创新驱动发展战略。加快实现高水平科技自立自强。以国家战略需求为导向，集聚力量进行原创性引领性科技攻关，坚决打赢关键核心技术攻坚战。加快实施一批具有战略性全局性前瞻性的国家重大科技项目，增强自主创新能力。营造有利于科技型中小微企业成长的良好环境，推动创新链产业链资金链人才链深度融合。深入实施人才强国战略。

习近平：

健全关键核心技术攻关新型举国体制

2022年9月6日，习近平主持召开中央全面深化改革委员会第二十七次会议，审议通过了《关于健全社会主义市场经济条件下关键核心技术攻关新型举国体制的意见》。

习近平强调，要发挥我国社会主义制度能够集中力量办大事的显著优势，强化党和国家对重大科技创新的领导，充分发挥市场机制作用，围绕国家战略需求，优化配置创新资源，强化国家战略科技力量，大幅提升科技攻关体系化能力，在若干重要领域形成竞争优势、赢得战略主动。

会议指出，健全关键核心技术攻关新型举国体制，要把政府、市场、社会有机结合起来，科学统筹、集中力量、优化机制、协同攻关。要加强战略谋划和系统布局，坚持国家战略目标导向，瞄准事关我国产业、经济和国家安全的若干重点领域及重大任务，明确主攻方向和核心技术突破口，重点研发具有先发优势的关键技术和引领未来发展的基础前沿技术。要加强党中央集中统一领导，建立权威的决策指挥体系。要构建协同攻关的组织运行机制，高效配置科技力量和创新资源，强化跨领域跨学科协同攻关，形成关键核心技术攻关强大合力。要推动有效市场和有为政府更好结合，强化企业技术创新主体地位，加快转变政府科技管理职能，营造良好创新生态，激发创新主体活力。

外交部：

越来越多的事实一再证明 美国是全球网络安全的最大威胁

2022年9月28日，外交部发言人汪文斌在主持例行记者会时表示，中国相关机构针对美国家安全局对西北工业大学进行恶意网络攻击第三次发布调查报告，向外界公布了更多美方安全机构对中方实施大规模网络攻击的证据。中方已通过不同渠道要求美方对恶意网络攻击作出解释并立即停止不法行为。但到目前为止，美方一直保持沉默。美方在编造散播所谓“中国黑客”的谎言时高调积极，对中国相关机构公布的实锤铁证却视而不见，避而不谈。人们不禁要问这背后到底隐藏着什么见不得人的秘密？

汪文斌指出，长期以来作为公认的“黑客帝国”“窃密大户”，美国凭借在互联网领域的绝对优势在全球范围实施无差别网络控制和窃密，借以谋求政治、军事、外交和商业利益。美国的网络“黑手”越伸越长，这已经成为国际社会日益强烈的共同关切。越来越多的事实一再证明，美国是全球网络安全的最大威胁。我们呼吁各国团结起来，共同抵制侵犯网络主权，破坏国际规则的霸权行径，共同营造和平、安全、开放、合作的网络空间。

民政部：

坚持安全可控 全面加强民政领域数字政府建设

2022年9月26日，民政部办公厅印发《民政部贯彻落实〈国务院关于加强数字政府建设的指导意见〉的实施方案》，明确了民政领域加强数字政府建设的总体要求、主要任务与保障措施，对进一步推动民政数字化转型作出系统部署。《方案》提出，要坚持安全可控，全面落实总体国家安全观，全面构建制度、管理和技术衔接配套的安全防护体系，切实守住网络安全底线。《方案》强调，要加强关键信息基础设施安全保护和网络安全等级保护，定期开展网络安全、保密和密码应用检查。

国标委：

开展国家标准化创新发展试点率先实现“四个转变”

2022年8月22日，国家标准委印发《关于开展国家标准化创新发展试点率先实现“四个转变”的指导意见》，将在标准化工作基础好、区域代表性强、带动作用明显的部分省（自治区、直辖市）开展国家标准化创新发展试点，探索率先实现“四个转变”，即：标准供给由政府主导向政府与市场并重转变，标准运用由产业与贸易为主向经济社会全域转变，标准化工作由国内驱动向国内国际相互促进转变，标准化发展由数量规模型向质量效益型转变。

《意见》明确，要通过国家标准化创新发展试点，切实优化标准化治理结构，增强标准化治理效能，提升标准国际化水平，形成一批可复制、可推广的新机制、新路径、新举措，推动全国形成以高标准助力高技术创新、促进高水平开放、引领高质量发展的良好局面。

田世宏：

以标准化推动数字时代发展

2022年10月14日，市场监管总局党组成员、副局长，国家标准委主任田世宏在2022年世界标准日主题活动中指出：党的十八大以来，以习近平同志为核心的党中央高度重视标准化工作，习近平总书记对标准化工作多次作出重要指示批示，为做好新形势下标准化工作指明了前进方向、提供了根本遵循。

田世宏强调，世界标准日国际主题“美好世界的共同愿景”，与我国推进高质量发展、更好满足人民对美好生活的向往高度契合。要用标准化推动产业升级，夯实美好生活的经济基础；要用标准化守护绿色家园，筑牢美好生活的生态屏障；要用标准化优化公共服务，增强美好生活的保障能力；要用标准化助力乡村振兴，提升美好生活的质量成色。

田世宏指出，高质量发展需要数字化支撑，美好世界的共同愿景离不开数字化赋能。国家标准委将今年世界标准日的中国主题确定为“数字时代的标准化”，旨在以标准化推动数字信息更安全、数字联通更高效、数字产品更可靠、数字环境更优越。

市场监管总局：

具有先进性、引领性、实施效果良好的团体标准可制定为国家标准

2022年9月9日，国家市场监督管理总局发布的《国家标准管理办法》规定：对具有先进性、引领性，实施效果良好，需要在全国范围推广实施的团体标准，可以按程序制定为国家标准。对技术尚在发展中，需要引导其发展或者具有标准化价值的项目，可以制定为国家标准化指导性技术文件。

中国连任国际电信联盟理事国

2022年10月3日，国际电信联盟2022年全权代表大会选举理事国和无线电规则委员会委员，中国成功连任理事国，中国候选人、国家无线电监测中心主任程建军成功当选无线电规则委员会委员。

国际电信联盟理事会由48个理事国组成，负责在两次全权代表大会之间履行管理机构职责。无线电规则委员会由12名专家组成，负责解释无线电规则、补充完善规则程序，并协调解决成员国之间无线电频率干扰等问题。

北京市委市政府：

标准引领高质量发展

2022年10月14日，中共北京市委、北京市人民政府印发《首都标准化发展纲要2035》，旨在更好地落实首都城市战略定位、建设国际一流的和谐宜居之都，以标准化助力高技术创新、促进高水平开放、引领高质量发展。

《纲要》提出，到2025年，标准化服务“四个中心”功能建设的能力充分提升，以标准化助力首都经济社会高质量发展的作用更加显著。到2035年，标准化全面服务“四个中心”功能建设。结构优化、先进合理、国际兼容的首都标准体系更加健全，标准化在推进首都治理体系和治理能力现代化中的基础性、引领性作用得到充分体现，科技标准创新、治理标准示范、生态标准引领和标准化领域国际交往活跃的目标全面实现。

《纲要》指出，将加强“四个中心”功能建设标准化支撑、推动标准化助力京津冀协同发展服务国家重大战略、提升产业标准化水平引领现代化经济体系建设、提升产业标准化水平引领现代化经济体系建设、提升产业标准化水平引领现代化经济体系建设、深化平安北京标准化建设筑牢首都安全防线、提升标准化对外开放水平形成全面开放新格局、夯实标准化发展基础提升支撑能力。

王小云：

坚持总体国家安全观 推进网络空间安全学科建设与人才培养

2022年10月，中国科学院王小云院士在中国网信杂志发表文章中表示，要坚持总体国家安全观，促进网络空间安全学科建设。网络安全作为新时代国家安全体系的重要组成部分，与其他安全领域密切相关。2014年4月15日，习近平总书记在中央国家安全委员会第一次会议上首次提出总体国家安全观。总体国家安全观的内涵是以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系。新时代国家安全体系包括政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、网络安全、太空安全、海洋安全等16种安全。其中，网络安全具有技术体系要求高、科技创新依赖性强等特点，因而在保障国家网络安全高水平发展过程中，科技创新与高层次人才是重要的支撑力量。网络空间安全学科建设应当坚持以总体国家安全观为指导，面向国家重大需求，树立安全大理念，注重学科建设内涵。

她提出，要把握网络空间安全发展态势，构建网络空间安全防护体系。随着大数据、云计算、人工智能的迅速发展，网络入侵、信息恶意窃取、数据篡改以及伪造攻击等严重影响国家安全，也损害公民、法人及其他组织的合法权益。近年来，网络防御技术已不再局限于防火墙、入侵检测、反病毒等技术范畴，而是发展到涉及计算机操作系统整体安全、网络信息系统安全、计算环境安全（人工智能安全、区块链）、硬件系统安全（如可信执行环境和密码芯片安全等）以及应用软件安全等。得益于密码学的发展，网络信息系统以及信息基础设施安全防护体系的理论支撑体系日益清晰，密码系统建设呈现出全面可证明的安全发展趋势。所谓可证明安全，是信息系统预达到的理想安全形态，使得信息系统能够抵御潜在攻击，从而达到高安全和高可信的要求。

在技术层面，只有具备深厚的网络空间安全基础理论与创新能力，才能深刻把握网络空间安全态势与内涵。深入把握网络安全和系统安全攻击形态，分析评估其安全威胁，制定有效的防范措施，构建系统化的网络安全态势感知平台将是一个重要而长期的任务。随着密码技术应用到网络空间的细分领域，密码体系的设计安全、实现安全、运营安全、管理安全的评估与检测将成为密码态势感知的核心内容，并逐步发展成为网络态势感知的核心内容。在密码态势感知的基础上，进行迭代升级，构建基于以密码安全为支撑的网络安全防御体系，从而实现“密码安全即服务”的工作模式，真正实现“信息系统+数据安全+计算安全”的融合发展。

高 林：

网络安全标准化要发挥基础性、规范性、引领性作用

2022年9月6日，中央网信办网络安全协调局副局长、一级巡视员高林在2022年国家网络安全宣传周——网络安全标准与产业装备发展论坛致辞中指出，网络安全标准化作为网络安全保障体系建设的重要组成部分，发挥着基础性、规范性、引领性作用。

一是要强化标准的规范性作用，贯彻落实《网络安全法》《数据安全法》《关键信息基础设施安全保护条例》等法律法规提出的标准化要求，加强法律法规配套标准的研究制定；

二是要提升标准的引领性作用，将先进适用的科技创新成果融入标准，通过标准规范指导新技术应用模式；

三是要加强标准对产业的基础支撑作用，强化网络安全产品互联互通等标准与产业的互动；四是要加大标准落地实施力度，政府和行业共同发力，加强政策引导，倡导行业自律，依托团体组织积极开展标准试点与产业示范。

陕西人大：

保障数据安全，统筹推进信息基础设施建设

2022年9月29日，陕西省第十三届人民代表大会常务委员会第三十六次会议通过了《陕西省大数据条例》，自2023年1月1日起施行。《条例》规定，要统筹推进信息基础设施建设，完善基础通信网络，推动信息基础设施共建共享、互联互通；要依照有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施。

至周科技无线接入点系列产品通过WAPI产业联盟测试

WAPI产业联盟　王立华

2022年9月22日，北京至周科技有限公司（以下简称至科技）的无线接入点系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性、功能及性能测试。联盟为上述产品出具了测试报告。本次通过测试的产品，将服务于智能制造、仓储物流、煤矿、管廊等工业互联网场景。

本次测试通过的无线接入点型号为WAP4221-I和WAP6222-I，无线控制器型号为ECG3006。两款无线接入点均支持瘦架构组网方式，与无线控制配合组网，实现数据的集中/本地转发模式，支持2.4/5GHz双频接入，通信速率支持802.11ac协议，可满足行业应用中对大宽带传输、数据集中管理的应用需求。

WAPI产业联盟测试实验室依据GB/T 32420—2015《无线局域网测试规范》和T/WAPIA 037.2—2021《无线局域网测试 第2部分：设备测试规范》，对上述设备进行了协议互通性、完整性、功能及性能测试，对首轮测试未通过项进行了精准定位并提出整改建议，至周科技依据建议完成了整改。

据至周科技介绍，公司多年来专注工业级、企业级无线局域网产品的研发，具有室内吸顶式、室内面板式和室外多形态的无线接入点产品，同时具有与之配套的无线控制器系列产品。至周科技也希望能通过联盟和更多厂商达成WAPI产品市场合作，服务自主可控工业互联网建设。

博洛米首款鉴别服务器通过WAPI产业联盟测试

WAPI产业联盟　王立华

2022年10月10日，南京博洛米通信技术有限公司首款鉴别服务器（AS）发布，目前已通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及功能测试，联盟为上述产品出具了测试报告。

该鉴别服务器型号为B0882，具备漫游功能，方便用户使用同一张数字证书在不同区域内接入WAPI网络，能满足行业市场WAPI大规模部署中对漫游的需求。联盟测试实验室依据GB/T 32420—2015《无线局域网测试规范》和T/WAPIA 037.2—2021《无线局域网测试 第2部分：设备测试规范》，对上述设备进行了协议互通性、完整性及功能测试，对首轮测试未通过项进行了精准定位并提出整改建议，博洛米已依据联盟建议完成了产品整改。

鉴别服务器（AS）是WAPI网络的重要组成部分，用以实现对用户证书的管理和用户身份的鉴别等。伴随WAPI安全无线局域网广泛应用，行业用户在设备选型中比较青睐设备厂商能够提供“从接入到鉴别的整体解决方案”，因此越来越多的设备厂商投入了鉴别服务器的开发制造。

据博洛米介绍，目前WAPI是该公司最重要的产品线之一。近几年公司持续加大了WAPI安全无线局域网系统的研发投入。这款鉴别服务器，填补了公司在WAPI接入认证管理产品上的空白，丰富了WAPI鉴别服务器市场供货环境。

博洛米表示，公司将继续丰富和完善WAPI产品线，提供模组、终端设备、无线接入点、接入控制器和鉴别服务器等产品。目前推出的二十多款产品，已相继通过了WAPI产业联盟测试，正服务于国防、能源、交通等行业。

WAPI产业联盟获第二届北京社会组织推介活动肯定

WAPI产业联盟　周　园

2022年9月28日，中关村无线网络安全产业联盟（以下简称：WAPI产业联盟）受邀参加北京市民政局社会组织管理中心主办的第二届北京社会组织推介活动开幕式。联盟因各项工作成果突出，获活动重点推介。

活动以线上线下相结合的方式，围绕市委、市政府中心工作，以“社会治理，社会组织在行动”为主题，宣传推介优秀社会组织，动员引导各社会组织大力弘扬公益文化，培育公益理念，有效整合社会资源，广泛参与社会治理，推动社会组织健康有序发展，以实际行动迎接党的二十大胜利召开。

北京市委社会工委委员、市民政局副局长赵学刚出席发布会并致辞，北京市社会组织管理中心主任温育梁介绍了《十八大以来北京社会组织发展简况》，中心党委副书记刘卫社通报了市级社会组织“党建强发展强”品牌项目及“党建标杆”创建示范单位，中心副主任庞庆涛通报了2021年以来受到表彰的市级优秀社会组织，中心副主任雷承佐通报了2022年为企业减负成效突出的市级行业协会商会，中心纪委书记宋传强通报了发挥“四个服务”作用突出的社会组织。

庞庆涛表示：近年来市级社会组织积极参与国家建设发展，不断提升社会影响力，在各项工作任务

中发挥了重要作用。作为本次受表彰的优秀市级社会组织，WAPI产业联盟2021年已累计开展了180余项标准制修订，获得了中国标准创新贡献奖；WAPI全球累计出货量达220亿颗，正广泛服务海关、能源、政务、公安、交通等命脉行业关基建设。

多年来，WAPI产业联盟通过“联盟专职专业化的人员”和“公共服务平台等抓手”，支持网络安全科技成果创新和转化，打造了百余家覆盖全产业链的“网络基础安全技术产业创新联合体”，打通了自主可控WAPI(无线局域网）和TePA（安全协议基础架构）技术产业的创新链和供应链，基本实现了网络安全协议等产业链上游的基础安全技术的自主可控，为我国万物安全互联、维护数据安全和信息安全提供保障。在技术产业协同创新和服务的过程中，WAPI产业联盟也成长为我国在无线网络和网络安全领域最具规模的产业联盟，是北京市5A级社会组织，科技部A类产业技术创新战略联盟、国家标准委首批团体标准试点单位，中关村国家自主创新示范区标准化示范单位。

WAPI产业联盟认为，荣誉是肯定更是激励。我们将继续砥砺奋进，坚持党建引领，坚持规范治理，坚持服务大局，坚持科技创新初心，以“时不我待，只争朝夕”的使命担当，推动我国无线网络和网络安全发展，以实际行动迎接党的二十大。

科技部产业技术创新战略联盟协发网调研WAPI产业联盟

WAPI产业联盟　刘剑昕

2022年9月21日，科技部产业技术创新战略联盟协同发展网秘书长程学忠、副秘书长王聆燕、杨丹泽，以及半导体照明联盟、存储联盟、烟气治理联盟等领导到WAPI产业联盟调研座谈。

张璐璐秘书长分享了WAPI产业联盟在无线网络安全产业领域标准制定、产业服务、市场拓展、国际超前布局等方面取得的成绩与经验。双方就联盟专职化运行、标准平台建设及我国无线网络安全领域现状与卡脖子问题、联盟间跨行业跨产业发展合作进行了深入讨论，并达成多项共识。

WAPI产业联盟于2006年成立，2010年1月8日入选为科技部首批产业技术创新战略联盟试点单位，并在历年评估中持续获得A级评价。联盟现有112家会员单位，包括三大电信运营商、行业用户单位和ICT领域骨干企业等，覆盖完整产业链、供应链。联盟自成立以来，以组织推动我国自主可控无线网络和网络安全技术创新和产业应用为目标，以“整合协调产业和社会资源，提升联盟会员在无线网络和网络安全相关领域的研究、开发、制造、服务水平，促进产业健康发展”为宗旨，以“立足产业、标准引领、技术标准研制与产品验证同步进行、产业与市场互为促进和谐发展”为工作指导思路，发挥了专职化秘书处和专业化服务平台作用。通过国际领先基础共性技术TePA和WAPI的协同创新，带动了我国无线网络和网络安全产业健康高效发展，提升了产业群体综合竞争力。

截至2022年9月，在联盟及成员单位的共同努力下，已开展了180余项标准制修订，其中获发布159项，包括：国际标准（ISO/IEC）14项、欧洲标准3项、国家标准41项、国家军用标准4项、行业标准7项、团体标准90项；全球支持WAPI的无线局域网芯片已达500多个型号，累计出货量已超过220亿颗，支持WAPI的移动终端和网络侧设备19000余款。随着各行业领域自主可控无线局域网建设成为刚需，WAPI因其产业成熟度高、不增加采购成本、能对行业信息通道安全和数据资产安全形成有效保护，受到用户青睐，已在全国海关的信息化系统、重要仓储物流管理信息系统、公安重要部位和重大活动智能监控管理系统、电力综合数据网接入系统等行业，以及北京大兴国际机场、重庆机场海关口岸、新疆地铁、城市地下综合管廊等国家地方重点项目中广泛应用。联盟研发并推出的安全无线局域网（WAPI）测评技术标准、工具和服务，覆盖“WAPI产品选型、设计、施工、验收、监督检查”全过程，为市场用户依标建设和实施WAPI提供有效支撑。

WAPI产业联盟团体标准《无线局域网证书鉴别漫游应用扩展技术规范》即将进入征求意见阶段

WAPI产业联盟　米　东

2022年10月，WAPI产业联盟团体标准《无线局域网证书鉴别漫游应用扩展技术规范》草案稿经项目组充分讨论并达成一致意见，即将进入征求意见阶段。

在各行业大规模开展的WAPI安全无线局域网建设中，亟需研究多AS鉴别服务器组网架构及相关业务流程，包括用户本地接入鉴别、跨AS接入的漫游用户鉴别、根AS之间的互通等技术内容及制定相应的组网规范。

本标准在T WAPIA 010.2—2010《补篇2 无线局域网证书鉴别漫游规范》的基础上，扩展定义了规模WAPI组网中多AS组网架构，详细说明了在漫游接入情况下根AS之间的证书鉴别协议流程、协议处理和帧格式等技术内容，适用于指导符合GB15629.11系列国家标准的无线局域网鉴别服务器产品的开发，服务公共热点和各行业的WAPI网络建设。

该标准于2021年12月正式立项，由中国电信集团公司、WAPI产业联盟（中关村无线网络安全产业联盟）、无线网络安全技术国家工程研究中心、新华三技术有限公司、西安芯语慧联信息科技有限公司、北京数字认证股份有限公司等单位共同编制。标准立项以来召开了多次项目组会议，对AS组网技术进行研究磋商，并结合标准内容及发展，将名称定义为《无线局域网证书鉴别漫游应用扩展技术规范》。目前标准草案稿及编制说明已在项目组内达成一致意见。根据联盟团体标准制修订程序，即将进入征求意见阶段。

北京联盛德微电子有限责任公司加入WAPI产业联盟

WAPI产业联盟　周　园

2022年10月14日，经联盟理事会批准，北京联盛德微电子有限责任公司（以下简称联盛德）正式加入WAPI产业联盟，联盟会员单位增至113家。

联盛德成立于2013年11月，是一家基于AIOT芯片的物联网技术服务提供商，国家高新技术企业。总部位于北京，在深圳、苏州均设有分支机构。旗下产品主要应用于智能家电、智能家居、行车定位、智能玩具、医疗监护、无线音视频、工业控制等物联网领域。

联盛德WLAN SOC芯片符合GB15629.11系列国家标准，今年6月相继推出多款支持WAPI协议的芯片、模组、网络端相关产品和解决方案。联盛德表示，加入联盟后将在WAPI领域不断增加产品品类，并面向电力、能源、军队、政务等多方面提供从芯片到整机产品，从终端到网络端的完整解决方案。

联盛德人才资源雄厚，拥有一批海外归国学者以及来自北大、清华、中科院等国内一流院校的高素质人才，拥有十年以上的无线通信芯片设计研发经验、行业方案应用开发经验。联盛德秉承以“同芯、同德、同梦想，创新、创业、创未来”的精神，坚持以客户为中心，市场为导向，价值创造为核心，争做同领域中技术最全面、应用领域最广泛的公司之一，做行业的先行者和领导者。

“创”出新活力 “转”出新局面
民营企业“数智化”发展观察

新华社

2022年9月28日，新华社记者采访了西电捷通公司等多家民营企业，记者采访发现，多家民营企业通过聚焦“数智化”实践，推动企业不断跑出加速度，实现效益持续增长。对越来越多民营企业而言，创新已不再是“可选题”，而是实现持续快速发展的“必答题”。面对国内外市场日新月异的变化，“数智化”转型成为许多企业变中寻机、难中求进的最优选择。民营企业能够踏踏实实搞研发、实实在在促转型，离不开政策环境的持续优化。

作为一家长期致力于科技创新的民营企业，西电捷通公司申请或授权的专利数量目前总计突破1000项。“近年来我国的知识产权保护力度不断提升，让我们可以更安心投入技术研发，促进技术成果转化。”西电捷通董事长曹军接受采访时说。

近年来，一系列政策举措陆续出台，支持民营企业创新发展：“十四五”期间，中央财政计划安排100亿元以上奖补资金，再培育1万家专精特新“小巨人”企业；持续加强产权保护，着力解决影响创新创业创造的体制机制问题；面对复杂严峻的国内外环境，围绕减税降费、金融支持等出台一系列纾困举措，让企业创新力充分涌动……

在创新支持政策引导下，民营企业加大研发投入力度，提高研发产出率，切实发挥创新在企业高质量发展中的引领作用。

全国工商联日前发布的《2022研发投入前1000家民营企业创新状况报告》显示，上年度研发投入前1000家民营企业的研发费用总额1.08万亿元，占全国研发经费投入的38.58%，占全国企业研发经费支出的50.16%；同比增长23.14%，增速比全国高8.5个百分点，比全国企业高7.9个百分点。54.7%的企业具备高技术、高成长、高价值属性。

“一系列护航民营企业创新发展的政策制度持续出台，激励企业在复杂环境下，提升技术研发积极性，增强自主创新能力，向高质量发展不断迈进。”曹军说。

世界标准日之访谈西电捷通

长治久安

西电捷通2000年9月在西安创立，面向全球产业提供领先的网络安全协议技术、装备及解决方案。

网络的本质在于连接和互联，标准化是西电捷通推动技术创新成果向全球产业转化的重要途径，也是实现通信行业产品互联互通的重要依据。西电捷通研发的三元对等虎符TePA技术架构及其体系，已成为全球互联网四层协议演进的必要组成部分。自主技术创新成果已被14项国际标准、3项欧洲地区标准、43项国家标准，近百项行业及团体标准所采纳。目前，在标准的支撑下，全球至少16个国家和地区实施了我们的虎符创新技术。

西电捷通是首个国家标准必要专利贡献者，也是中国在国际标准组织ISO的首个国际标准必要专利的贡献者，西电捷通所拥有的ISO标准必要专利数量位列全球第20位，中国第一。

西电捷通做了什么?

（1）按照纲要要求“要深化标准化交流合作”：2022年，西电捷通按照ISO工作计划，继续推动RFID安全国际标准提案，完善以我国为主导的物联网安全国际标准体系；同时以物联网基础安全标准发布和体系形成为契机，积极推动和东盟、一带一路国家的对接合作。

（2）纲要明确提出要“优化标准供给结构，大力发展团体标准，推进团体标准应用示范”。西电捷通贡献了我国在计算机网络通信领域的第一个自主的国家标准——无线局域网国家标准，采纳了我国自主创新的WAPI安全协议技术。国家在2006年成立了全球性的产业联盟，推进标准体系完善和应用落地。目前在西电捷通参与下，已经形成了90项团体标准，并成为第一批团体标准试点单位。2022年在能源、海关、国防、铁路等领域推进标准应用，促进团体标准服务于国家关键信息基础设施安全。

关于科技、专利、标准一体化西电捷通怎么做?

基于过去22年的创新及标准化实践，西电捷通认为标准必要专利就是引领标准高质量发展的一个重要指标，是标准技术的核心竞争力。专利技术被标准采纳，也是证明技术创新性和高价值的重要指标。

过去，在推动技术成果被标准采纳的同时，西电捷通也积极开展标准专利政策研究，成为我国国家成员体参与国际标准组织ISO专利政策研究组的政策研究支撑团队，在国际标准组织专利政策制定过程中为我国技术创新“走出去”争取必要的发展空间及话语权。

MTK发布天玑1080移动平台 支持WAPI

MediaTek

2022年10月11日，MediaTek天玑系列 5G 移动平台再添新成员——天玑1080。天玑1080支持802.11ax连接速率，支持WAPI，提供了多项关键技术升级，可为用户提供更加安全流畅的移动网络，性能和影像功能也将更为出色。

天玑1080采用八核CPU架构设计，包括两个主频为2.6GHz的Arm Cortex-A78大核，搭配Arm Mali-G68 GPU，在游戏、流媒体播放、网页阅览等应用中提供更为顺畅的体验；搭载了MediaTek Imagiq ISP影像处理器，最高可支持2亿像素主摄，先进影像功能助力用户拍摄高品质的照片和视频；采用6nm制程，拥有优秀的能效表现，可延长智能手机的电池续航时间。

据悉，搭载MediaTek天玑1080 5G移动平台的智能手机预计将于2022年第四季度上市。

高通推出全新中端骁龙平台 支持WAPI

高 通

2022年9月6日，高通技术公司宣布推出第一代骁龙6移动平台和第一代骁龙4移动平台，上述平台均支持WAPI，面向中端和海量智能手机市场，提供先进的技术解决方案。

第一代骁龙6移动平台提供出色的影像能力、强劲的游戏体验和直观的AI辅助，让更多用户能够全面体验覆盖广泛的连接以及持续稳定的高能效和性能。该平台采用高通FastConnect 6700移动连接系统，搭载该平台的商用终端预计将于2023年第一季度面市。

第一代骁龙4移动平台的优秀性能和多天电池续航，让用户随时捕捉喜爱的精彩瞬间。该平台具有优秀的性能和AI特性，支持无缝、直观的交互体验，先进的影像特性带来出色的拍摄能力，更佳的连接体验让用户能够尽情分享。该平台采用高通FastConnect 6200移动连接系统，搭载该平台的商用终端预计将于2022年第三季度面市。

数字认证：以人为本，构建数字政府数字信任体系

数字认证

近日，北京数字认证股份有限公司（简称：数字认证）东北大区总经理高洋在“推动数字政府建设 赋能龙江营商环境”企业家沙龙中表示：社会信任主要靠人际信任和制度信任维系，而在数字政府建设中，数字信任是人际信任和制度信任的拓展。

数字信任并非新名词，多年来在全球得到广泛应用。聚焦我国数字政府业务场景，数字政府信任体系的概念内涵可概述为业务主体身份可信、业务内容可信、业务行为可信三个方面。

一是着力建设以可信身份互联互通为核心的数字信任基础设施，筑牢数字信任体系构建基石。可信的业务主体身份是构建数字政府数字信任体系的关键，而密码技术是解决身份问题的核心技术。建议政府一方面推动建立统一的主体身份标识、主体识别认证和相关的安全策略机制，促进数字政府不同领域和层级业务主体身份的互信互认；另一方面加强对数字信任基础设施形态、服务模式的创新突破，满足区块链、物联网等新技术、新业态、新领域加速发展背景下数字政府的数字信任体系建设需求。

二是推动建立以政府为主导的可信监管，实现业务主体行为追溯与责任判定。建议构建面向多业务主体的统一开放的可信监管平台，对应用、服务以及数据的可信性实施有效监管，促进市场良性发展，为网络空间治理提供支撑。

三是适时开展典型业务场景下的数字信任体系建设落地试点，打造示范标杆。坚持全面部署和试点带动相促进的原则，围绕数字政府业务的重点领域、关键环节、共性需求等优先开展数字信任建设的试点示范工作。以个人信息保护为例，建议开展以下三个方面的工作：重点研究和突破个人信息保护的关键技术；紧密结合相关法律法规要求，推动配套标准制定实施；增强对个人信息滥用等行为的监管力度。

近年来，我国数字政府建设进入快车道。数字信任是数字政府的安全基石，在数字政府业务场景下，多样的主体身份、海量异构的数据流动、复杂的业务交互催生出新型信任体系的概念内涵，以业务主体身份可信、业务内容可信和业务行为可信为核心要义的数字信任体系构建已迫在眉睫。

黑客改装无人机
飞到金融公司楼顶通过Wi-Fi入侵内部系统

安全内参

日前，美国一家金融公司的工作人员发现其内部页面出现反常现象。查找原因的过程中，发现两架无人机。据海外媒体theregister报道，两架无人机都经过了改装，黑客利用两台无人机搭载电子设备，通过Wi-Fi入侵了公司的内部网络。

其中一台无人机装有一个改进过的Wi-Fi设备，用于网络渗透测试。另一台无人机携带着一个箱子，里面装着一台GPD迷你笔记本电脑，一个4G调制解调器和另一个Wi-Fi设备。其中一台无人机搭载的设备最初是在几天前被用来拦截一名工作人员的凭证和Wi-Fi信息的。”随后，这些数据后来被硬编码到另一台无人机的部署工具中。登入Wi-Fi后，无人机上的工具被用来瞄准该公司内部的Confluence页面，以便利用存储在那里的凭证连接到其他内部设备。

拜登再次强调关键基础设施安全要“锁紧数字大门”

安全内参

2022年10月，在亲俄黑客组织KillNet的攻击导致14个美国机场网站瘫痪后第二天，美国总统拜登在白宫发布加强美国关键基础设施网络安全的情况说明书，并宣布将“不懈关注”国家关键基础设施防御的改善，建立一个全面的方法来“锁定美国的数字大门”。

“情况说明书”强调的六项重点工作包括：

- 发布关键基础设施安全绩效考核指标
- 实施产品安全标签，帮助美国消费者了解他们购买的产品是否（网络）安全
- 大力培养国家网络安全人才并加强网络安全教育
- 扩大反勒索软件倡议联盟
- 推进联邦零信任架构实施战略

通过国家量子倡议和发布国家安全备忘录10(NSM−10)来开发抗量子加密，建立美国技术优势，从而保护从在线商务到国家机密的未来。

关键基础设施安全方面，由于美国的许多关键基础设施由私营部门拥有和运营，因此美国政府与交通、银行、水和医疗保健等各个部门密切合作，以帮助利益相关者了解关键系统的网络威胁并采用最低限度的网络安全标准。其中一些网络安全措施包括运输安全管理局(TSA)提出的多项基于性能的指令，以提高管道和铁路部门的网络安全弹性，并衡量航空部门的网络要求。

白宫的情况说明书指出：“我们正在发布网络安全绩效考核目标，这些目标将为推动投资朝着最重要的安全成果提供基准。我们将继续与关键基础设施所有者和运营商逐个部门合作，以加快网络安全和弹性的快速改进以及落实积极措施。”

拜登通过其2021年5月颁布的第14028号总统行政命令，要求相关部门采取有效的网络安全措施，例如多因素身份验证，提高联邦政府系统的安全性。白宫还发布了联邦零信任架构实施战略，并提供了预算指导，以确保联邦机构将资源与国家的网络安全目标保持一致。

去年，美国政府还发起了30多个国家和欧盟之间的“反勒索软件倡议”，目标是加快合作以应对严重威胁关键基础设施、基础服务、公共安全、消费者保护的勒索软件和隐私问题。

情况说明书称，白宫将于10月31日至11月1日接待国际合作伙伴，以加速和扩大“反勒索软件倡议”合作项目。目标是提高集体弹性，让私营部门参与进来，并破坏网络犯罪的基础设施。美国还加大了犯罪分子转移非法资金的难度，同时制裁了勒索软件犯罪分子经常使用的一系列加密货币混合器，以收缴和“清理”其非法收入。

除了反勒索软件倡议之外，拜登政府在北约建立一个新的虚拟快速反应机制，以确保美国的盟国能够高效地相互提供支持，以应对网络攻击事件。

根据情况说明书，白宫重点强调了培养国家网络安全人才和加强网络教育，为此举办了全国网络劳动力和教育峰会。在峰会上，拜登政府宣布了为期120天的网络安全学徒冲刺计划，以帮助增加网络安全就业机会。在峰会的推动下，美国政府将继续与合作伙伴合作，培养网络安全人才，改善以技能为基础的高薪网络安全就业路径，教育美国人掌握必要的安全技能，并在网络安全领域提高多样性、公平性、包容性和可及性。（DEIA）

拜登政府还计划通过开发抗量子加密来保护未来的数字社会。美国国家标准与技术研究院(NIST)宣布了四种新的后量子加密算法，这些算法将成为NIST后量子加密标准的一部分，预计将在大约两年内完成。这些算法是首批抵御未来量子计算机攻击的加密工具，保护在线银行和电子邮件等日常数字系统不受量子计算的威胁。

8月，美国网络安全和基础设施局(CISA)指出将ICS（工业控制系统）升级到后量子密码将是一个挑战，因为部署相关ICS硬件成本高昂，并且相关设备通常在地理上较为分散。但CISA仍然呼吁ICS组织确保其硬件更换周期和网络安全风险管理策略能够应对量子计算带来的风险。

拜登于5月发布了NSM−10，旨在发展美国在量子计算方面的技术优势，同时降低易受攻击的密码系统的风险。该措施使政府对量子技术的研发（R&D）投资增加了一倍以上，在全国范围内建立了新的研究中心和劳动力发展计划。

此外，NSM−10优先考虑“通过推进研发工作、建立关键合作伙伴关系、扩大劳动力和投资关键基础设施，确立美国在量子技术方面的领导地位，同时确保关键基础设施的加密升级到抗量子加密。”

拜登签署涉及芯片、AI、量子计算等领域的新行政令

网络空间国际法前沿公众号

9月15日，美国总统拜登签署一项行政命令，要求美国外国投资委员会（Committee on Foreign Investment in the United States，简称CFIUS）确保美国对不断变化的国家安全风险进行强有力的审查。这是自CFIUS1975年成立以来，美国总统围绕外国投资事项签署的首个总统指令。

该行政令表面上并未针对特定外国国家，但白宫提供的事实清单中提到来自“竞争对手或敌对国家（competitor or adversarial nations）”的外国投资者所带来的风险，并具体解释了未来将加强审查的领域，其中包括半导体、人工智能、生物技术、量子计算和先进清洁能源等技术领域。

该行政令提出五项因素供CFIUS在其投资审查过程中着重考虑，包括事关供应链和美国技术领先地位的两项既有法定因素，以及事关行业投资趋势、网络安全风险和个人数据隐私安全的三项新增因素。

美国政府一位高级行政官员声称，一些国家利用美国的开放投资生态系统，以直接违背美国价值观和利益的方式推进其相关事项，而这项新的行政命令是美国政府为维护美国经济和技术领导地位、保护美国国家安全所做的努力的关键部分。

欧盟委员会提出《网络弹性法案》要求在数字产品全生命周期引入强制性网络安全要求

网络空间国际法前沿公众号

9月15日，欧盟委员会发布《网络弹性法案》（Cyber Resilience Act）草案，旨在保护消费者和企业免受安全功能不足的产品的侵害。这是欧盟范围内的首个此类立法，它在具有数字元素的产品的整个生命周期内引入了强制性的网络安全要求。法案将适用于除医疗设备、航空和汽车外，直接或间接连接到另一个设备或网络的所有产品。

该法案提出的措施基于欧盟产品立法的新框架，将规定：

（1）将带有数字元素的产品投放市场以确保其网络安全的规则；

（2）设计、开发和生产具有数字元素的产品的基本要求，以及与这些产品相关的经济运营商（economic operators）的义务；

（3）制造商为确保具有数字元素的产品在整个生命周期内的网络安全而制定的漏洞处理流程的基本要求，以及与这些流程相关的经济运营商的义务；

（4）市场监督和执法规则。这将使消费者和公民以及使用数字产品的企业受益，提高安全属性的透明度，促进对具有数字元素产品的信任，并确保更好地保护他们的隐私和数据保护等基本权利。

虽然世界各地的其他司法管辖区都在考虑解决这些问题，但《网络弹性法案》可能会成为欧盟内部市场之外的国际参考标准。《网络弹性法案》草案目前还在由欧洲议会和理事会审查中，一旦通过，经济运营商和成员国将有两年时间来适应新的要求。

基于WAPI技术的架空特高压输电线路在线监测系统解决方案

本文由西安芯语慧联信息科技有限公司供稿

一、方案背景

在电力系统中，架空特高压输电线路是连接发电厂、变电站和用户之间的重要纽带，具有地域分布广阔、运行条件复杂、巡检和维护工作繁重及易受自然环境影响和外力破坏等特点，其作为电力系统重要基础设施，对于电网的安全 、可靠 、经济运行极为关键。但是架空特高压输电线路不但要承受正常的导线等自身重量和内部电压电流的不断变化，由于长期暴露于野外，还要经受大气污秽的污染、绝缘老化、以及覆冰、雷击、强风、鸟害等外界因素的侵害，存在着巨大的安全隐患，因此对输电线路的安全运行进行在线监测显得尤为重要。

图：架空特高压输电线路

特高压输电线路在线监测技术是基于物联网技术原理，利用分布在高压输电线路不同地点的传感器，对输电线路运行环境和运行状态进行实时监测、隐患评估、事故诊断、风险预警等。系统将采集的相关数据信息进行收集、汇总，并通过数据采集终端上传到主站监控管理平台处理。供电企业监测人员通过对传感器回传的数据信息进行研究分析，对高压输电线路中可能存在的隐患和故障进行识别，精准确定隐患和故障发生的位置和原因并及时解除隐患和故障，从而为高压输电线路维护人员的工作提供针对性的数据支持，保障特高压输电线路的运行安全。

图：输电线路运行安全保障

二、监测对象

特高压输电线路在线监测系统的监测对象主要包括以下几个方面：

（一）绝缘子状态

高压输电线路的漏电和短路故障，多数都来自绝缘子的附着物的积累，这些附着物一部分来自各种降水带来的杂质沉积，一部分来自动物的排泄物，一部分来自非法空飘物的缠绕。如果绝缘子出现污浊和破损，输电线路监测系统应第一时间上报数据并预警。

（二）设备状态完好性

输电线路的完好与否，是否出现螺丝脱落、是否出现电缆的破损断丝、是否出现塔架的破坏性故障、是否出现输电杆塔倾斜、是否出现人为破坏等，都是输电线路在线监测系统的基本监测数据，需要第一时间上报数据并预警。

（三）气象数据

输电线路沿途的气象数据，特别是降水量、降雪量、蒸发量、气温、相对湿度、风向、风力、积雪程度、覆冰程度、导线舞动等数据对于输电线路的运维调度工作有着重要的意义。输电线路在线监测系统必须将沿途的气象数据作出汇总分析，并及时完整地上报。

（四）输电线路运行状态数据

利用传感器进行输电线路运行状态检测量的周期性采集工作，对输电线路状态数据进行实时采集、传输、统计和分析，及时获悉输电线路运行状态及预警信息，及时消除安全隐患，确保输电线路的安全稳定性。

图：在线监测系统大数据平台

三、解决方案

在设计架空特高压输电线路在线监测系统时，除了上述的应用需求外，还应结合国家“新基建”战略需求和网络安全法规的相关要求，深化和规范在线监测技术在架空特高压输电线路中的应用。在线监测系统应满足以下基本要求：

（一）可靠性、稳定性

鉴于特高压输电线路的特殊性和重要性，在线监测系统及装置自身应该非常可靠和稳定，避免因自身隐患或故障对输电线路造成影响，其设计需求应满足特高压输电线路使用场景的可靠性和稳定性要求。例如在线监测装置与输电线路之间应设计缓冲区域，避免在线监测装置对输电线路造成物理伤害，例如在线监测装置应具备一定的抗干扰能力，从而保证其数据传输的准确性与全面性，等等。

（二）安装部署的便捷性

在线监测系统及装置的安装部署方式应较为便捷，从而降低高空环境下安装人员的工作难度。

（三）可维护性

在线监测系统部署后，其本身的可运维性、可管理性也是系统是否可用的重要指标，与该系统的可靠性密切相关。

（四）与特高压输电线路环境的适配性

在线监测系统及装置，应充分考虑特高压输电线路使用环境的实际情况，应能适应输电线路的现场情况。例如：

在线监测系统装置常需用到较低电压的稳定电源，耗电量不大，但在特高压输电线路上提供这样的低电

压电源供给却很不方便，所以要求在线监测系统装置要具备较严格的低功耗能力。目前特高压输电线路上这类电源供给一般有以下几种方法：

1、太阳能电池板供电

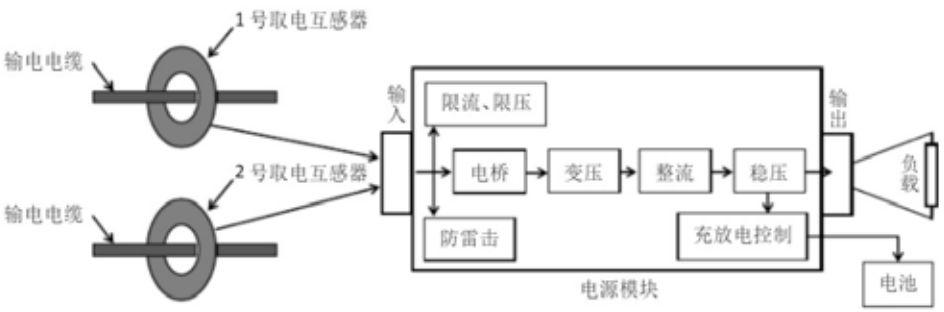
太阳能电池板受天气因素影响较大，且在长久工作一段时间后，就需要保护或改换，这在重要的输电线路上就需要停电，所以此方法并不可靠。

2、经过光纤进行激光供电

这个方法存在供电量小的弊端，且因为激光发射器、光纤、光电变换器易老化，极易影响供电质量，所以此方法也不可靠。

3、利用高压输电线的电流进行电磁感应取电

即利用电流互感器从高压输电线的负荷电流所产生的磁场进行电磁感应取电。随着智能电网的发展，这种取电方法目前在特高压输电线路上应用比较广泛，也是目前最适合特高压输电线路在线监测系统的取电技术，但由于这种方式所取电量十分有限，所以对供电对象设备有较为严格的功耗要求，若供电对象设备功耗太高，则无法使用。



图：电流互感器取电原理示意图

（五）网络安全技术合规性

在线监测系统及装置应满足“新基建”战略背后自主、安全、可控的需求，符合国家相关的网络安全法规要求，其网络安全技术应符合电网行业要求，保障电力行业重点基础设施的安全性。

目前在特高压输电线路场景中应用的无线网络通信技术主要包括：蓝牙、LoRa、卫星通信、LTE230、5G等技术，其中：

1、蓝牙和LoRa技术不符合国家和电网行业相关的网络安全法规要求，从网络安全技术合规性角度，应首先排除，不在长期考虑范围内；

2、卫星通信覆盖范围广，但发送有延迟，且易受太阳活动及气候影响，终端功率也偏大，并不适合特高

压输电线路实际应用场景；

3、LTE230和5G均利用运营商网络，监测范围广，其中230MHz是电网专用频段，目前得到了广泛应用，但网络建设及维护成本高，如与无线局域网技术结合使用，效果更佳；

除上述在用技术外，作为中国无线局域网国家标准的WAPI技术也非常适用于架空特高压输电线路在线监测场景。

图：中国无线局域网国家标准

WAPI是中国无线局域网国家标准GB 15629.11中规定的无线网络安全技术，具有完全自主知识产权及产业配套体系，满足“自主、安全、可控”的战略需求，WAPI作为无线局域网技术，其网络建设方便快捷，建设成本低且无需后续投入，数据传输速率高、实时性强、部署灵活、产业配套完善，已在电力、海关、国防、公安、交通等多个行业规模化应用，近年来已被电网行业采纳为合规的无线网络通信技术标准，为变电站、配电房等配输电应用场景提供安全、稳定、可靠的无线网络通信服务，获得了行业的一致认可。

图：方电网变电站WAPI应用现场

四、方案特点

综合上述因素考虑，我们设计了一种“基于WAPI技术的架空特高压输电线路在线监测系统解决方案”，该方案具有高可靠、高安全、全国产、低功耗、高性能、适配性强、部署灵活、成本低、网络安全合规等特点，无需网络侧AP设备投入，仅以芯语慧联自主研发的全国产WAPI MCU低功耗无线数传模组TH6180为载体，借助高压输电线路电磁场取电方式，通过WAPI多级无线级联技术就可以沿输电线路实现分段式远距离数据实时传输，从而实现架空高压输电线路的全天候实时在线监测，并且能够在不改变杆塔结构和现有线路走径的前提下，降低线路遭受内、外部破坏的可能性，保障特高压输电线路的安全、稳定运行。

图：基于WAPI技术的架空特高压输电线路在线监测系统构成示意图

另外，该系统解决方案还具备很强的应急拓展能力，例如在遇到自然灾害导致系统原有通信被迫中断的紧急情况下，可以通过无人机等手段构筑天地一体化应急通信保障系统，第一时间精确定位故障发生地点，保障电网运行安全。

图：全国产高安全低功耗WAPI MCU无线数传模组——TH6180

WAPI 产业联盟成员单位名录

中国移动通信集团公司
中国电信集团公司
中国联合网络通信集团有限公司
国家密码管理局商用密码检测中心
国家无线电监测中心检测中心
北大方正集团有限公司
西安西电捷通无线网络通信股份有限公司
北京中电华大电子设计有限责任公司
北京数字认证股份有限公司
中电科普天科技股份有限公司
深圳市明华澳汉智能卡有限公司
北京六合万通微电子技术股份有限公司
无锡中太数据通信有限公司
青岛海尔科技有限公司
海信集团有限公司
联想（北京）有限公司
华为技术有限公司
大唐移动通信设备有限公司
北京朗波芯微技术有限公司
大唐微电子技术有限公司
上海鼎芯科技有限公司
北京天一集成科技有限公司
北京联信永益信息技术有限公司
深圳鑫金浪电子有限公司
深圳市普天宜通科技有限公司
北京汉铭信通科技有限公司
西安大唐电信有限公司
深圳共进电子股份有限公司
北京华安广通科技发展有限公司
深圳国人通信有限公司
东蓝数码有限公司
美国安移通网络公司北京代表处
北京五龙电信技术公司
北京同耀通电科技有限公司
北京登合科技有限公司
宇龙计算机通信科技（深圳）有限公司
上海润欣科技有限公司
弘浩明传科技股份有限公司
京信通信技术（广州）有限公司
北京城市热点资讯有限公司
优比无线技术（深圳）有限公司
南京智达康无线通信科技股份有限公司
上海欣民通信技术有限公司
福建三元达通讯股份有限公司
新华三技术有限公司
北京傲天动联技术股份有限公司
中兴通讯股份有限公司
武汉虹信通信技术有限责任公司
广州市卓纪思网络科技有限公司
赛芯电子技术（上海）有限公司
雷凌科技股份有限公司
瑞晟微电子（苏州）有限公司
联发科技股份有限公司
四川天邑信息科技股份有限公司
湖南城市热点无线通信有限公司
珠海市魅族科技有限公司
深圳市雄脉科技有限公司
奥泰尔科技（深圳）有限公司
北京网贝合创科技有限公司
网件（北京）网络技术有限公司
上海市数字证书认证中心有限公司
北京创原天地科技有限公司
阿德利亚科技（北京）有限责任公司
深圳市华讯方舟软件信息有限公司
迈创智慧供应链股份有限公司
科通宽带技术(深圳)有限公司
邦讯技术股份有限公司
惠州市宝丰信息科技有限公司
晨星软件研发（深圳）有限公司
卓望数码技术（深圳）有限公司
迈普通信技术股份有限公司
北京汇通融业科技发展有限公司
上海寰创通信科技有限公司
吉翁电子（深圳）有限公司
北京汇为永兴科技有限公司
福建星网锐捷网络有限公司
北京新岸线移动多媒体技术有限公司
广东欧珀移动通信有限公司
上海贝尔股份有限公司
成都鼎桥通信技术有限公司
飞天联合（北京）系统技术有限公司
中国电力科学研究院
锐迪科微电子（上海）有限公司
苏州汉明科技有限公司
神州数码网络(北京)有限公司
北京必虎科技股份有限公司
北京市政务信息安全保障中心
天津赞普科技股份有限公司
上海连尚网络科技有限公司
深圳市瑞科慧联科技有限公司
深圳市信锐网科技术有限公司
福建新大陆通信科技股份有限公司
北京比邻科技有限公司
天津市电子机电产品检测中心
高通无线通信技术（中国）有限公司
中科开创（广州）智能科技发展有限公司
北京华信傲天网络技术有限公司
南京博洛米通信技术有限公司
广西新海通信科技有限公司
上海麓慧科技有限公司
深圳市智开科技有限公司
南方电网数字电网研究院有限公司
深圳航天科创实业有限公司
南方电网深圳数字电网研究院有限公司
广西电力线路器材厂有限责任公司
广西通量能源技术有限公司
恩智浦（中国）管理有限公司
南方电网科学研究院有限责任公司
山东华辰泰尔信息科技股份有限公司
山东思极科技有限公司
深圳市国电科技通信有限公司
北京至周科技有限公司
北京联盛德微电子有限责任公司

【注：截至2022年10月，联盟正式成员已达113家，以加入联盟的时间先后排序。】

WAPI Alliance

地　址：北京市海淀区知春路27号量子芯座1608室
邮　编：100191
电　话：010-82351181
传　真：010-82351181 ext. 1901
邮　箱：wapi@wapia.org
网　址：http://www.wapia.org.cn