一、互联网的发展趋势

计算机网络诞生于冷战时期，最早是为了应对核战争中对指挥信息网络的打击而开发出来的技术。随着冷战的结束，如今的互联网已经演变成为全球经济体系的基础架构，成为了全人类各种社会活动都不可或缺的“神经系统”。

未来互联网在移动应用、物联网应用、AI 智能等领域还有广阔的应用，同时也会从单一的信息网络扩展成可深入控制实体系统的智能化控制网络。到那时，互联网的一举一动对社会运转都将起到最核心作用。

由于互联网已经在经济和政治中起到了不可替代的作用，当前，全球互联网已经逐步根据国家政治体系演化出带有主权特性的网络空间。各个主权网络基于自身的地域条件、社会条件和网络技术条件，逐步形成带有技术边界的国家级网络区域。

一个国家主权必须在自己的网络区域内实施特定的管理模式和防御手段，保护主权网络的健壮性，从而保护这个国家社会制度和经济体系的正常运转。这将成为每一个国家必须实现的目标，否则国家安全无从谈起。因此互联网安全问题将成为社会兴衰和国家存亡的关键。

国家主权网络的对抗是一场持久战。防御、相持和反攻是持久战必经的三个阶段。虽然目前西方在这场对抗中处于优势，但中国经过改革开放四十年的快速发展，已经完成了梯次防御的过程，目前在网络技术水平和信息产业规模上都接近和达到了西方同等水平，部分领域还有所超越。总体上中国主权网络开始由防御转入相持的阶段，正处于战略上的重大转折时期。

二、互联网安全现状和未来趋势

长期以来互联网技术发展的首要宗旨是保持开放和相互兼容，而在网络安全技术方面的关注度较小。从早期的军用 ARPA 网转变为全球互联网的过程中，大多数技术用于实现各种网络互联互通，以及提高网络通信速度。这是目前互联网上各种安全漏洞频现、网络攻击泛滥的根本原因。

网络体系设计遵从自下而上的原则，网络系统底层协议经过这么多年的发展已经被部署得极其广泛，任何底层协议修订和升级的成本都极高、影响面都极大。所以当前主流网络安全技术的发展大多集中在网络高层协议上（L4 传输层以上）。随着 HTTPS、SSH、TLS 等技术的快速进步，L4 以上协议层的安全方案已经稳步推广并趋于成熟。

网络底层协议（L3 网络层、L2 链路层）的安全技术一直以来没有被当作安全体系的重点来研究和发展。西方依赖长期积累的技术优势和产业优势，实际上在底层上的攻击手段更具威胁。未来主权网络攻防的重点必将向底层网络技术倾斜，L3 以下的安全技术将成为网络安全对抗的焦点领域。目前正在大力推广的 IPv6 协议，正是在 L3 以下可以实现安全功能的核心，有广阔的技术空间可以挖掘。

三、基于 IPv6 协议的全节点认证安全网络

IPv4 是第一代网络体系，也是目前的主流体系。这一代网络体系在设计之初主要针对的是网络功能的实现，缺乏安全功能的考量。因此，目前基于 IPv4 的安全技术和解决方案主要通过在应用层面的软件来实现，可以一定程度上提供抵御网络软件（病毒、木马等）和非法用户入侵的防护能力，但对于网络设备层面的入侵缺乏有效的防护方式。

IPv6 是未来全球网络的技术体系，在其协议栈中内置支持 IP SEC 安全协议，提供了两种安全传输模式：传输模式和隧道模式。其中传输模式提供端到端的数据签名和数据加密功能；而隧道模式可以在安全网关间建立一条安全的虚拟通信隧道。

然而对于主权网络所要求的高安全级别而言，这些安全功能是远远不够的。安全传输相关的认证算法和加密算法、安全网关的实现方法、与 IPv6 地址管理相关的安全功能等等，都需要进一步细化和明确。也就是说目前的 IPv6 协议中仅仅提供了一些最基本的安全功能，尚未形成完整的网络防护体系。

如何细化实施 IPv6 网络的安全防护体系是一个大课题，IPv6 在安全强度、完整性方面还有广大的探索空间。在这一方面，国内网络安全研究与西方的技术差距并不明显，完全有赶上甚至超越的机会。

在以安全性为最高要求的网络中，首先要保证接入这个网络的设备和用户的合法性。如果网络节点中某些设备和用户的身份不明或者系伪造，则网络的整体安全性是很难保证的。IPv4 体系已经实现了用户身份的验证（人类身份），但难以实现对网络设备身份的验证（物联网级认证）。IPv6 的出现使得对设备身份的验证（物联网级安全）成为可能，

【】
基于链路地址的网络节点设备间的互认证

要实现这样一个网络节点设备可以相互认证的安全网络，需要以 IPv6 的 NDP 协议为基础，在 IPv6 的链路地址层面进行设备身份认证和数据加密功能。通过在网络设备中加入带有数字证书的安全功能芯片，使得网络节点设备具备密码学运算功能。网络节点之间从建立连接开始就全面使用数字签名和加密传输。这样一来，任何试图伪造设备身份和伪造网络数据的行为都可以通过认证算法检测出来并且自动排斥在网络之外，从而使得非法侵入网络变得极其困难。

【】
IPv6 全节点认证网络

在一个高安全等级的网络架构中，从核心节点到边缘节点，从边缘节点到终端设备，直至最

终的网络用户，每一个节点都应当包含设备身份的芯片级保护措施，节点之间的相互通信（数据转发）都带有数字认证过程和数据加密，再加上对每个节点的行为加实施监控和分析。这样的“全节点认证网络”才能够最大程度的保证系统抗入侵和抗攻击的能力。简而言之，未来的安全网络不仅要像 IPv4 网络那样实现用户身份的实名制，还要基于 IPv6 技术实现网络设备的实名制，才能达到满足核心网络对安全性的要求。

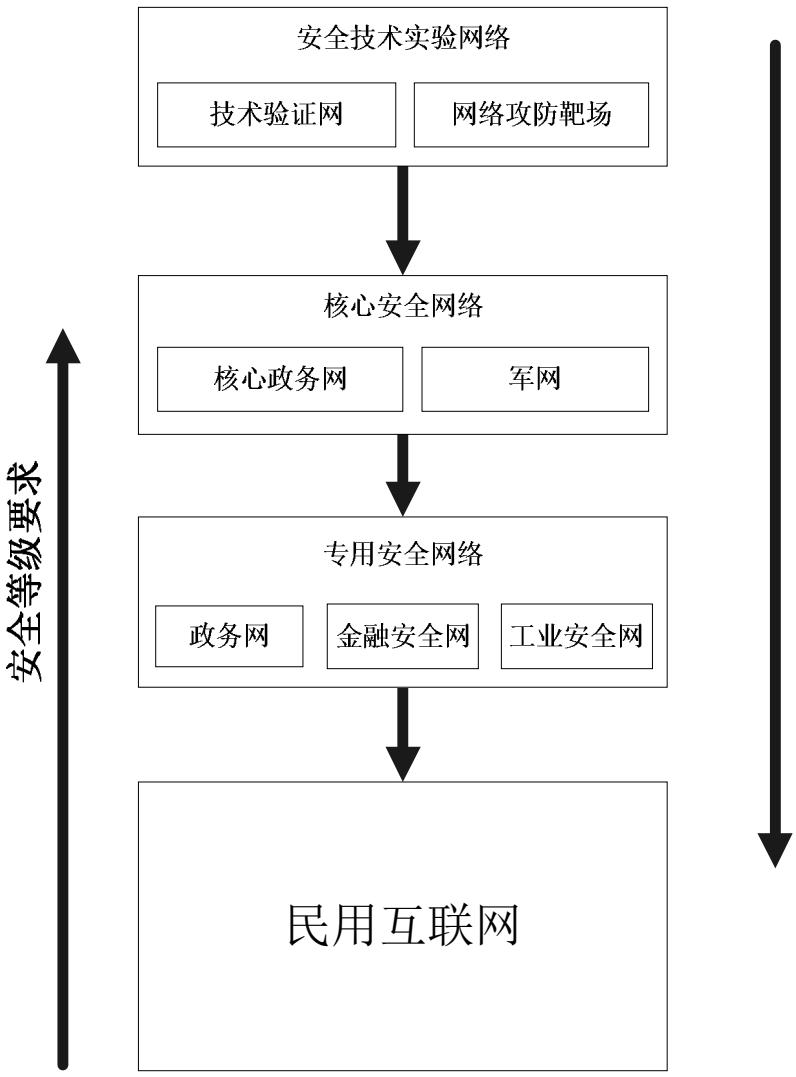
同时，基于 IPv6 的网络设备认证技术也同样适用于物联网安全领域，因此全节点认证网络在未来工业和商业物联网中也有广阔的应用场景。

四、IPv6 网络安全技术的研发和推广

目前中国基于 IPv4 的互联网的规模极其庞大，涉及国民生产生活各方面，已然成为国家经济的命脉之一。对于庞大的民用网络而言，网络速度和使用成本仍然是最受关注的问题，安全性与速度、使用成本又存在一定矛盾，所以普通民用领域尚不足以对 IPv6 的安全功能提出迫切的需求。虽然 IPv6 的推广是大势所趋，但必定是一个长期、渐进的过程。

另一方面，近年来各种针对工业网络、金融网络进行攻击的网络威胁越来越大，未来主权网络对网络安全的需求已经十分明显。在涉及国家核心机密和国民经济关键环节的网络通信中，已经迫切需要新一代安全技术提供更高等级的安全防护。

鉴于不同功能、不同规模、不同重要程度的网络对安全的需求存在明显的差异，网络安全技术研发需要针对不同的应用领域区分对待，网络安全方案的实施也需要要分领域、分层次、分阶段的进行。



网络安全技术研发推广关系

为配套网络安全研发，首先应当建立一套安全技术实验网络，专门用于网络安全技术的验证和测试，同时作为网络安全对抗的演习场。

经过充分验证测试的技术首先投入到核心安全网络的应用中去。在规模较小的网络范围内实施最高级别的网络安全，一方面可以控制部署成本，另一方面也有助于控制核心技术的扩散范围，提高保密性。

在核心安全网络的安全性得到充分保障后，可以研究安全技术扩散到其他专用网络中去的可行性。安全技术扩散的时候，需要考虑其他网络的规模差异、安全等级差异、运营成本差异等，对安全技术本身和实施方法需要做一定的调整。

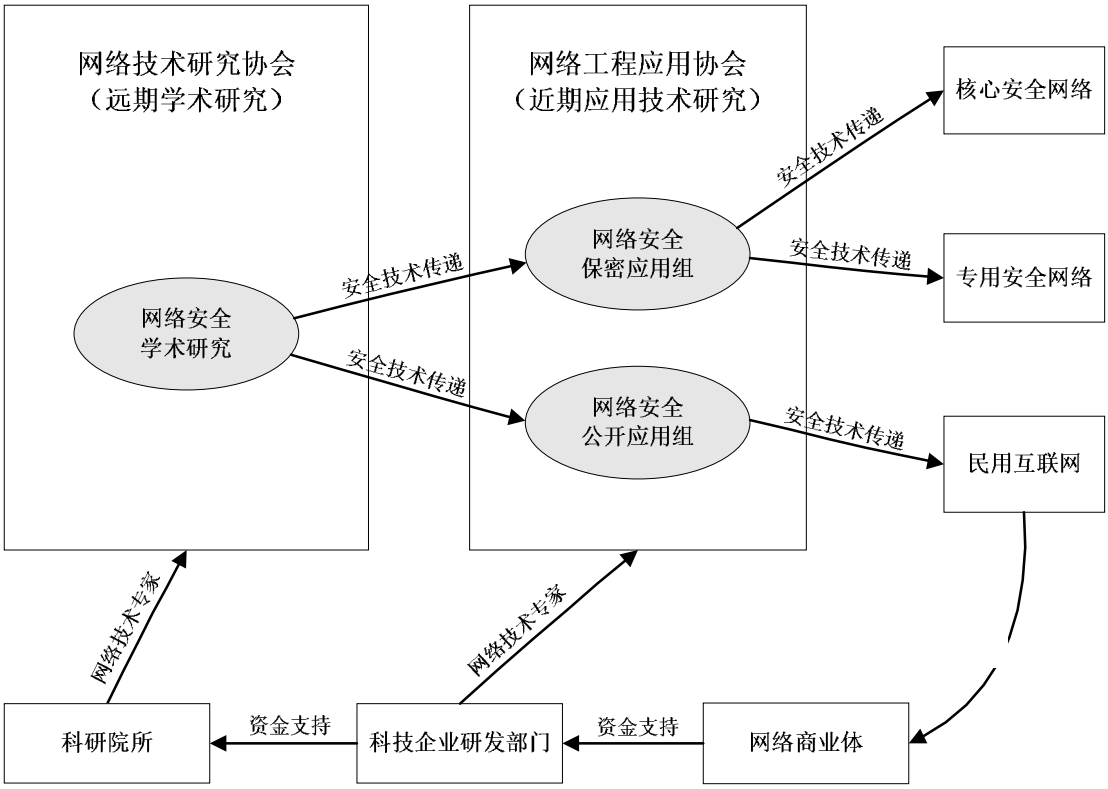
各种专用网络中被普遍使用的安全技术也可以根据需要逐步扩散到民用互联网中。当应用到民用网络中时，这一级别的安全技术将脱离国家保密技术的范畴，成为公开、通用的网络安全技术。公开、通用的网络安全技术不仅仅是专用安全网络技术的继承，同时也作为公开领

域接受大规模验证和公开学术评价的方法，有助于进一步促进核心安全技术的提高。

为了实现不同层级的安全研发目标，需要有不同的安全技术研究组织和团队，并且根据不同的安全需求做针对性的技术研发。各个研究组织和团队之间相互交流和协作又需要一个统一的管理方式，从而形成一个有效的网络安全研发体系。

五、未来网络安全研发体系建设

网络安全是一个需要多方参与、集中优势资源大力投入的研究领域。 为了保证深入和长期持续的研究工作，应当建立以科研机构为先导、科技企业为跟进、商业市场为支撑的网络安全产业梯队。



网络安全产业梯队

科研领域参照国际网络技术组织 IETF（互联网工程任务组） 和 IRTF（互联网研究专门工作组），在国内分别设立远期研究和近期应用的网络技术协会组织。组织成员可以由各个高校、科研机构和大型企业的网络技术专家选取。

其中网络安全部分又分为公开应用组和保密应用组，公开应用组负责民用应用及对外技术协作，保密应用组负责国家级核心安全的保密技术研究。无论是公开应用组还是保密应用组，都是为了集中科研力量，避免资源分散、各自为政的研究方式，加强各个学术机构的协作性，

提高科研效率。

在网络工程和产品层面，依托国内大型信息技术企业，如华为、中兴等，通过与科研组织的紧密协作，吸收消化科研成果，将其转化为具有技术优势和实用价值的网络软硬件产品，满足专用网络和民用网络的各种需求。科技企业与学术机构合作的过程中，应当充分运用实验网络、专用网络所提供的测试环境，对新技术进行充分测试和验证，确保在实际应用中达到预期的技术高度和实用价值，为投放到民用领域做好准备。

技术研究和产品研发需要巨额的资金支持。除了专项国家科研经费之外，专用网络技术向民用网络推广的过程也可以产生丰厚的经济收益和巨大的社会价值。科技企业通过技术转化，将新技术投入商业运营中去，再将其产生的商业收益反哺到科研工作当中去，进一步支撑科技企业和科研机构的研发任务，形成良性循环。

六、总结

未来全球的互联网会逐步形成各个以国家制度为边界的主权网络，各国主权网络之间存在持续的进攻与防御的态势。

在这样的环境下，网络安全将成为主权网络健壮性的核心问题，其中每个网络节点的安全性又成为整个网络安全性的基础，即所有网络节点的物联网级安全问题。

IPv6 作为下一代网络基础架构技术，在未来网络安全层面有很大的发展潜力，应建立集中资源建立专门针对 IPv6 网络安全的产业梯队，满足各种应用层面、各种安全等级的研发需求。

网络安全产业梯队以科研机构为先导、科技企业为跟进、商业市场为支撑，最终实现长期、持久、高效的网络安全研发体系，为中国主权网络安全提供基础保障。