成都信息工程大學
Chengdu University of Information Technology

网络空间安全导论

白杨
Alicepub@163.com

参考书目

教材

- 蔡晶晶等人编著.《网络空间安全导论》机械工业出版社

参考资料

- 杨义先等编著.《安全简史》电子工业出版社
- 郝玉洁等编著.《信息安全概论》电子科技大学出版社2007版
- 赵树生等编著.《信息安全原理与实践》清华大学出版社
- 曹天杰等编著.《计算机系统安全》高等教育出版社
- 华蓓等译.《计算机安全》人民邮电出版社

考察方法

考察

- 60%平时情况 + 40%期末考试成绩
- 平时成绩：平时作业（3次）、出勤情况（扣分）
- 期末成绩：考试
- 课程QQ群 助教：饶雨唐 1140171342@qq.com（作业）

课堂管理

- 不迟到，不早退，不吃东西
- 上课主要形式：讲课+讨论

本课程主要内容

一．网络空间安全概论（2课时）

二．密码学发展及其应用（2课时）

三．网络安全与物理安全（虚拟化、云计算）（2课时）

四．操作系统安全（病毒原理与防范）（2课时）

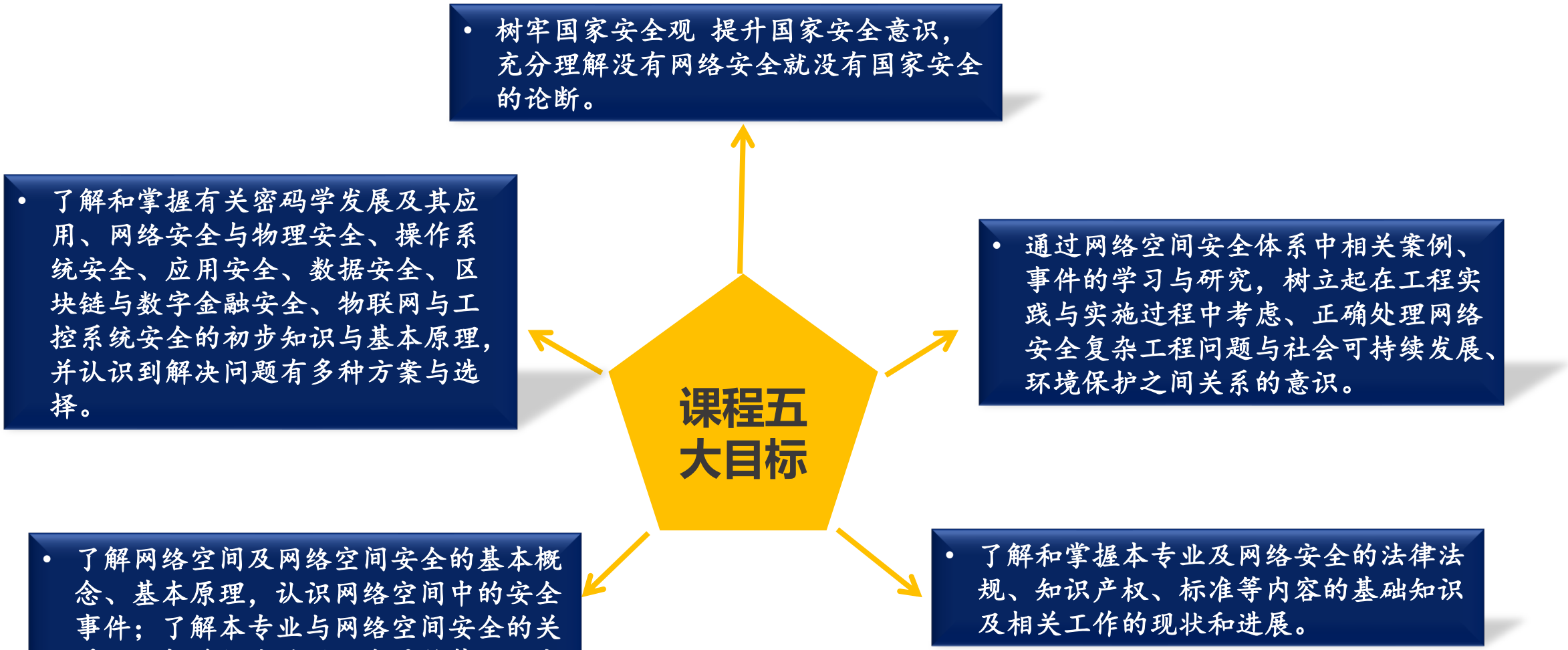
五．应用安全（主要web类）（2课时）

六．数据安全（大数据）（2课时）

七．区块链与数字金融安全（2课时）

八．社交网络与隐私安全（2课时）

课程目标


课程五大目标
• 树牢国家安全观 提升国家安全意识，充分理解没有网络安全就没有国家安全的论断。
• 了解和掌握有关密码学发展及其应用、网络安全与物理安全、操作系统安全、应用安全、数据安全、区块链与数字金融安全、物联网与工控系统安全的初步知识与基本原理，并认识到解决问题有多种方案与选择。
• 通过网络空间安全体系中相关案例、事件的学习与研究，树立起在工程实践与实施过程中考虑、正确处理网络安全复杂工程问题与社会可持续发展、环境保护之间关系的意识。
• 了解网络空间及网络空间安全的基本概念、基本原理，认识网络空间中的安全事件；了解本专业与网络空间安全的关系，及相关领域的国际发展趋势、研究热点。
• 了解和掌握本专业及网络安全的法律法规、知识产权、标准等内容的基础知识及相关工作的现状和进展。

内容概要

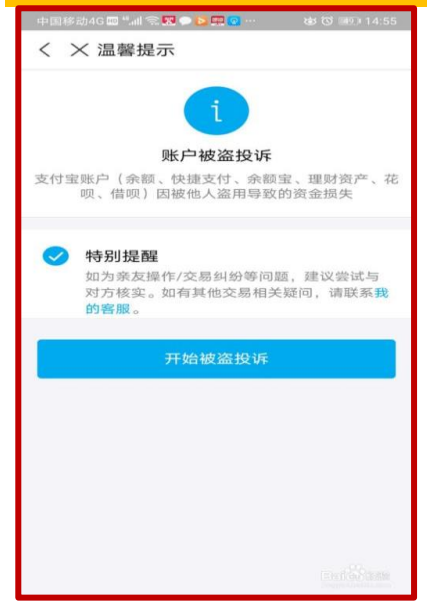
1. 网络安全事件
2. 网络空间安全的概念
3. 网络空间安全技术架构
4. 网络空间安全法律法规
5. 我国网络空间安全的机遇与挑战

生活中的网络空间安全

一提到网络安全，很多人就会想到“黑客”，觉得网络安全很神秘，甚至离现实生活很遥远。但实际上，网络安全与我们的生活是息息相关的，网络安全问题无处不在，比如现实生活中就经常听说类似如下列举的安全事件：

QQ账号密码被盗

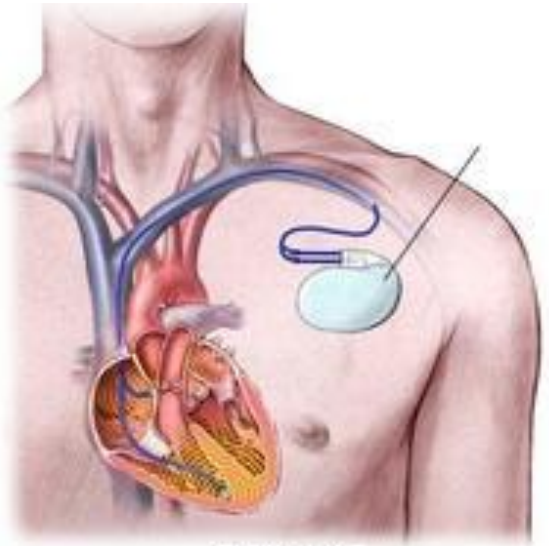
支付宝账号被盗



银行卡被盗刷

生活中的网络空间安全

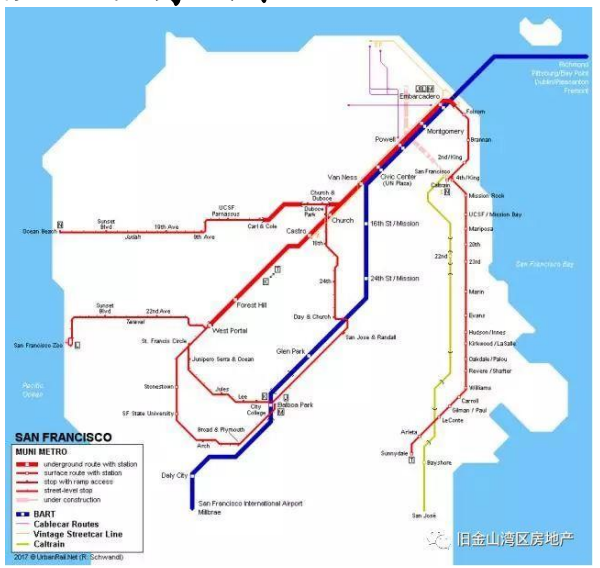
- 黑客大会
  - ATM机：2010年美国黑客大会上，黑客现场演示如何破解ATM机并让其不断吐钞票
  - 心脏起搏器：2013年黑客大会上，黑客现场演示如何侵入心脏起搏器，让遥控杀人成为现实



心脏起搏器系统

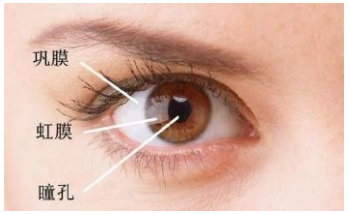
生活中的网络空间安全

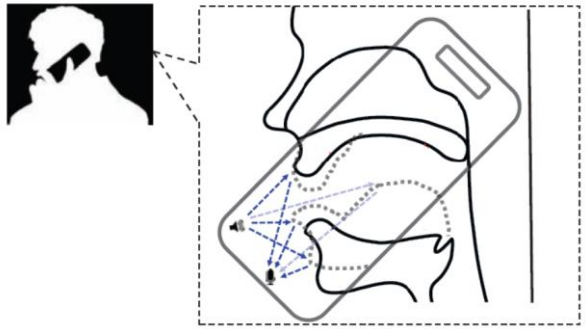
- 旧金山地铁系统遭受黑客攻击
  - 旧金山的Municipal地的电脑票价系统遭到黑客攻击，黑客索要100比特币作为赎金
  - 黑客篡改了旧金山地铁的票价

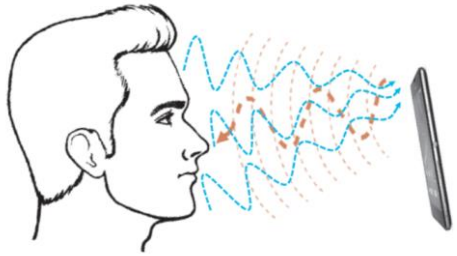


生活中的信息安全

- 基于生物特征的身份认证
  - 根据用户独特的体征来证明身份
  - 依靠指纹，视网膜，虹膜、脸型
  - 依靠签名、语音等







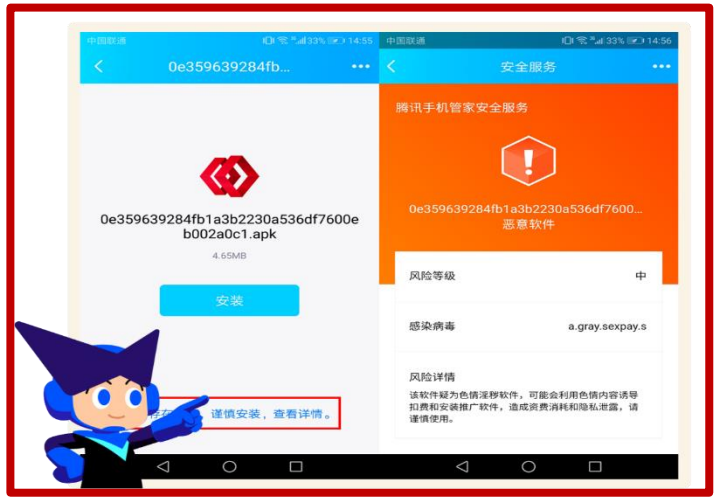
工作中的网络安全问题

在互联网时代，办公网络也成为各类网络安全问题的重灾区，工作中常见的网络安全问题主要有：

网络设备面临的威胁

操作系统面临的威胁

应用程序面临的威胁



军事中的信息安全——四渡赤水

➢军委二局的电台破译立大功

长征的行军途中，中央红军共有四部接收敌人电报的电台，每两部电台为一班，分作两班，此停彼开，轮流值班。

1934年10月，渡过湘江四道封锁线后，红军已损失过半，红军战略转移方向问题。李德主张联合红二军团北进湘西，曾希圣及时将刚截获的电报汇报给中央：“敌军已经集结重兵在湘西张网以待”。前敌司令部决定放弃北上，挺进贵州。

1935年1月，毛泽东同志率红军主力第一次渡过赤水河，抵达云南扎西镇。蒋介石命龙云为“剿匪军”第二路军总司令。**曾希圣破译电报**探清敌人兵力布防：

①龙云电令川军7个旅固守宜宾长江南岸一带以防止红军北渡

②另以川军5个旅分别依托金沙江、横江防堵我军西渡

③又调滇军3个旅直扑扎西而来，企图从南部夹击

④东部的遵义，龙云只安排了黔军5个团驻扎

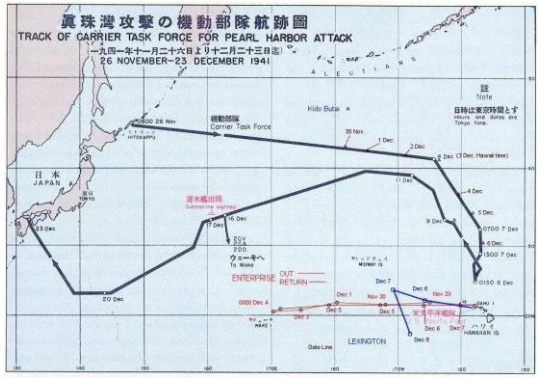
军事中的信息安全——二战风云

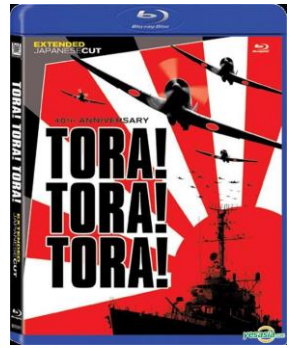
➢第二次世界大战，美军情报获破译得的战果

- 中途岛战役
- 山本五十六座机被击落

➢第二次世界大战，英军情报获破译得的战果

- 恩尼格玛密码机被破译，阿兰·图灵《美丽心灵》
- 1941年德国巨型战列舰俾斯麦号被击沉
- 1942年北非装甲油料枯竭输掉阿拉曼战役
- 1944年图灵改良机出现至少拯救2000万人





军事中的信息安全——现代战争

➢ 俄格战争中的“网络战”

2008年，俄罗斯与格鲁吉亚爆发冲突，俄罗斯军队在越过格鲁吉亚边境的同时，对格鲁吉亚展开了全面的“蜂群”式网络阻瘫攻击，致使格方电视媒体、金融和交通等重要系统瘫痪，机场、物流和通信等信息网络崩溃，急需的战争物资无法及时运达指定位置，战争潜力被严重削弱，直接影响了格鲁吉亚的社会秩序以及军队的作战指挥和调度。有意思的是，在网络攻击期间，俄罗斯网民可以从网站上下载黑客软件，安装之后点击“开始攻击”按钮即可进行网络攻击。媒体评论俄罗斯打了一场名副其实的“网络人民战争”。

政治中的网络空间安全

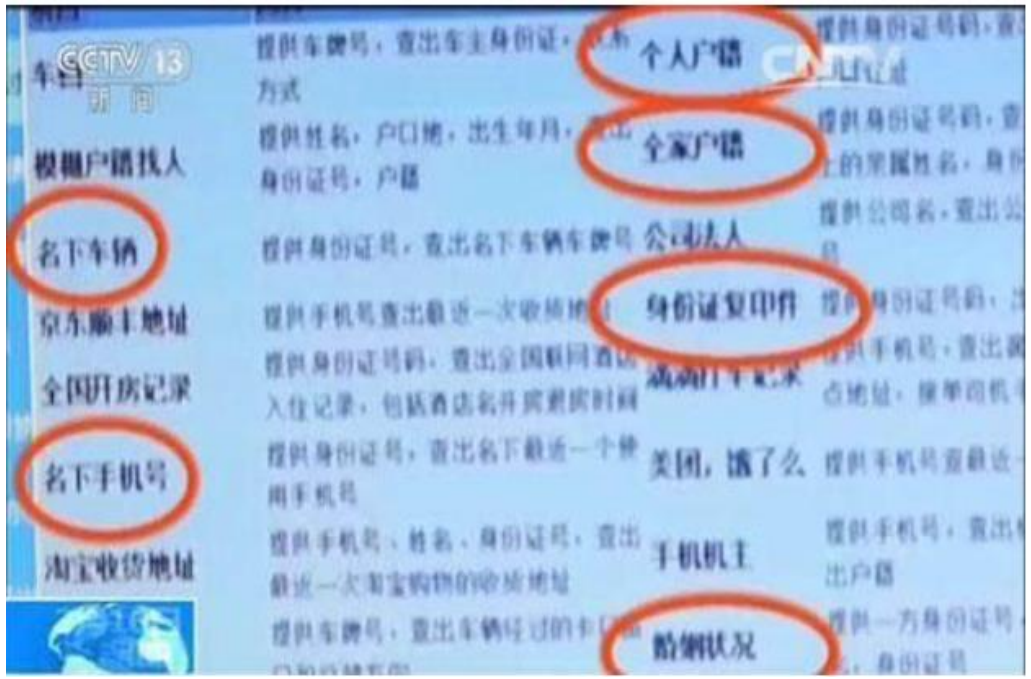
- 希拉里邮件门
  - 希拉里从2009到2013年之间，使用私人电子邮箱和位于家中的私人服务器收发大量涉密的邮件，面临调查时匆匆删除
  - 近2万封邮件被黑客恢复，并被维基解密披露
  - 严重影响了希拉里的选情

商业中的网络空间安全

- 洲际酒店信用卡数据泄露
  - 2017年2月，洲际酒店（IHG）旗下12家酒店支付系统被恶意软件入侵，顾客信用卡支付信息被窃取
  - 一旦顾客在酒店进行信用卡支付，恶意程序可从信用卡磁条中读取信用卡号码，有效期，内部验证码，持卡人姓名等信息（比微信支付，支付宝复杂)

商业中的网络空间安全

- 网上贩卖个人信息
  - 我们可能经常会收到不知名的推销电话
  - 记者发现个人信息的贩卖情况在网上十分活跃
  - 提供一个人手机号码，就能查到最私密的个人信息，包括户籍，婚姻，资产，通话记录，开房记录等



商业中的网络空间安全

- Facebook泄露五千万用户数据
  - 媒体揭露数据分析公司Cambridge Analytica获得了Facebook数千万用户的数据，并进行违规滥用
  - 创始人马克·扎克伯格发表声明，承认错误并开启调查

商业中的网络空间安全

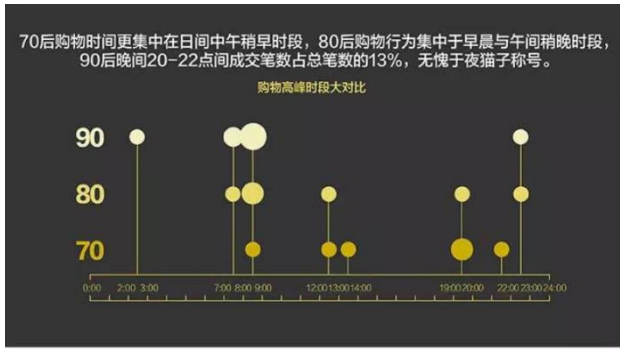
- 大数据带来的安全威胁
  - 全中国最熟悉消费者习惯的机构是淘宝，而不是工商局
  - 而这些信息，能够反过来产生巨大价值！
  - 例子1：根据用户浏览习惯推送广告
  - 例子2：银行利用这些信息判断信用度
  - 例子3：保险公司利用信息决定保额

商业中的网络空间安全

- 孟加拉国中央银行失窃
  - 孟加拉国中央银行在美国纽约联邦储备银行开设的账户2月初遭黑客攻击，失窃8100万美元
  - 赃款几经分批中转，最终流入菲律宾两家赌场和一名赌团中介商的账户

与新技术结合的攻击

- 大数据带来的安全威胁
  - 全中国最熟悉消费者习惯的机构是淘宝，而不是工商局
  - 而这些信息，能够反过来产生巨大价值！
  - 例子1：根据用户浏览习惯推送广告
  - 例子2：银行利用这些信息判断信用度
  - 例子3：保险公司利用信息决定保额



未来的信息安全隐忧

- 物联网遭受黑客攻击的忧虑
  - 物联网的目标是让一切联网：从汽车到冰箱、台灯，空调、甚至倒马桶 （5G）
  - 到2020年，全球联网设备的数量将从现在的30亿台增加至260亿台左右
  - 如果黑客入侵家庭智能系统，将会产什么多大的破坏？
  - 今年9月，一款可以感染路由器、恒温器、烘干机等许多物联网设备的恶意软件，组成了1.2万至1.5万台的大型僵尸网络，并在亚洲和美国实施了各种形式的DDoS攻击

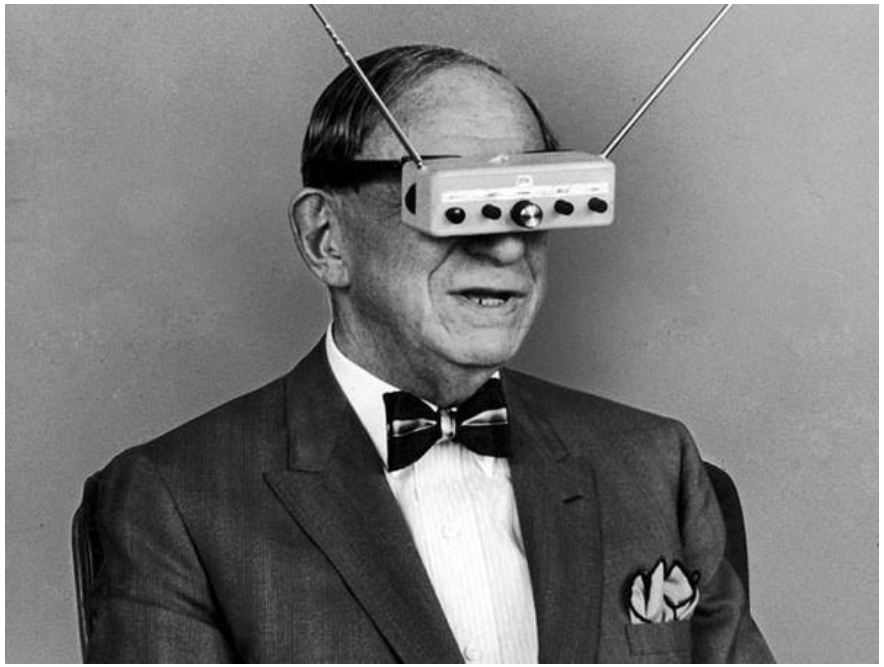
大家是否遇到过类似的网络安全问题，请发言分享

内容概要

1. 网络安全事件
2. 网络空间安全的概念
3. 网络空间安全技术架构
4. 网络空间安全法律法规
5. 我国网络空间安全的机遇与挑战

网络空间安全的概念

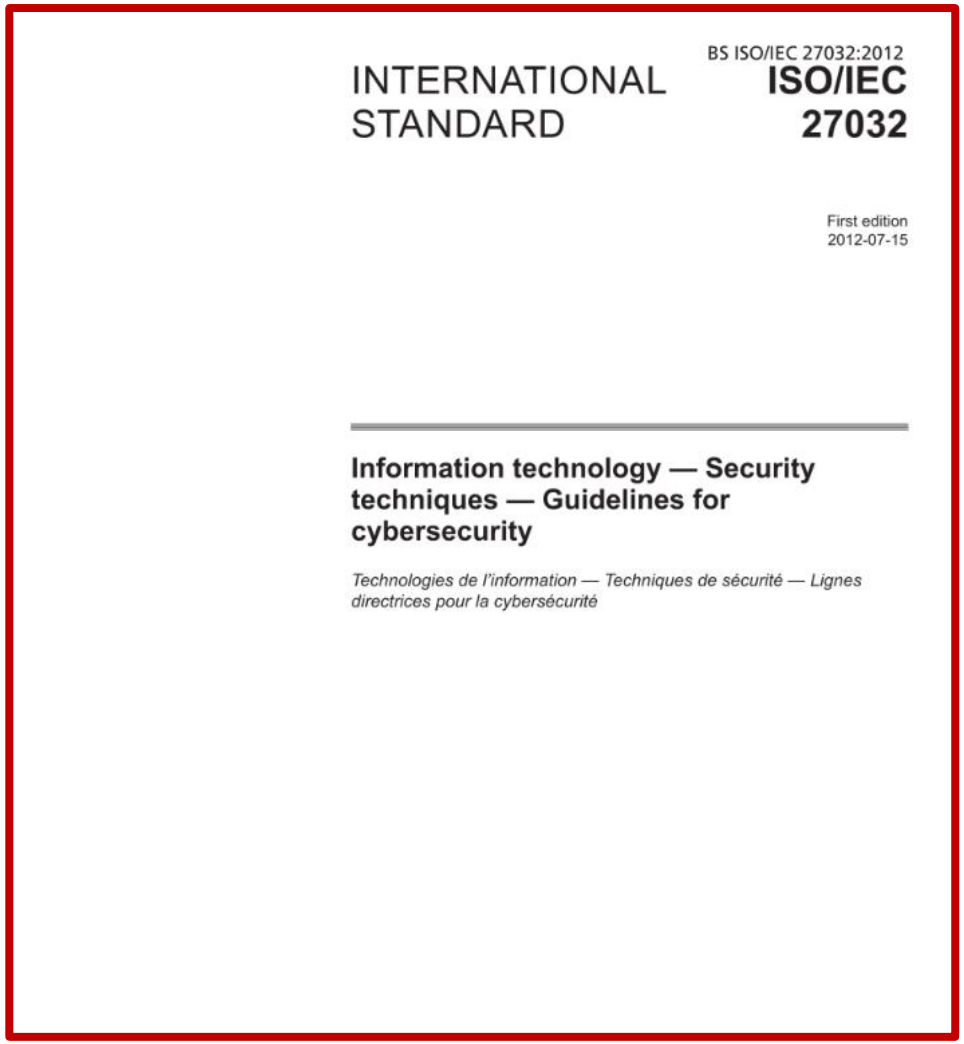
网络空间，是为了刻画人类生存的信息环境或信息空间。早在1982年，美国科幻作家威廉•吉布森William Gibson在其短篇科幻小说《燃烧的铬》中创造了Cyberspace一词，指由计算机创建的虚拟信息空间，Cyber在这里强调电脑爱好者在游戏机前体验到交感幻觉，体现了**Cyberspace不仅是信息的聚合体，也包含了信息对人类思想认知的影响。**



网络空间安全的概念

定义1：ISO/IEC 27032:2012——《Information technology–Security techniques–Guidelines for cybersecurity》：**"the Cyberspace"** is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form。

Cybersecurity is "preservation of confidentiality, integrity and availability of information in the Cyberspace".


BS ISO/IEC 27032:2012
INTERNATIONAL STANDARD
ISO/IEC 27032
First edition
2012-07-15
Information technology — Security techniques — Guidelines for cybersecurity
Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

网络空间安全的概念

定义2：ITU国际电联——The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment**.**

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: **availability; integrity**, which may include authenticity and non-repudiation; and **confidentiality**.

网络空间安全的概念

定义3：荷兰安全与司法部——freedom from danger or damage due to the disruption, breakdown, or misuse of ICT（information and communications technology）. **The danger or damage** resulting from **disruption, breakdown or misuse** may consist of **limitations to the availability or reliability** of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.

网络空间安全的概念

在国内，方滨兴院士则提出“网络空间是所有由可对外交换信息的电磁设备作为载体，通过与人互动而形成的虚拟空间，包括互联网、通信网、广电网、物联网、社交网络、计算系统、通信系统、控制系统等”。

虽然定义有所区别，但是研究人员普遍认可网络空间是一种包含互联网、通信网、物联网、工控网等信息基础设施，并由人－机－物相互作用而形成的动态虚拟空间。

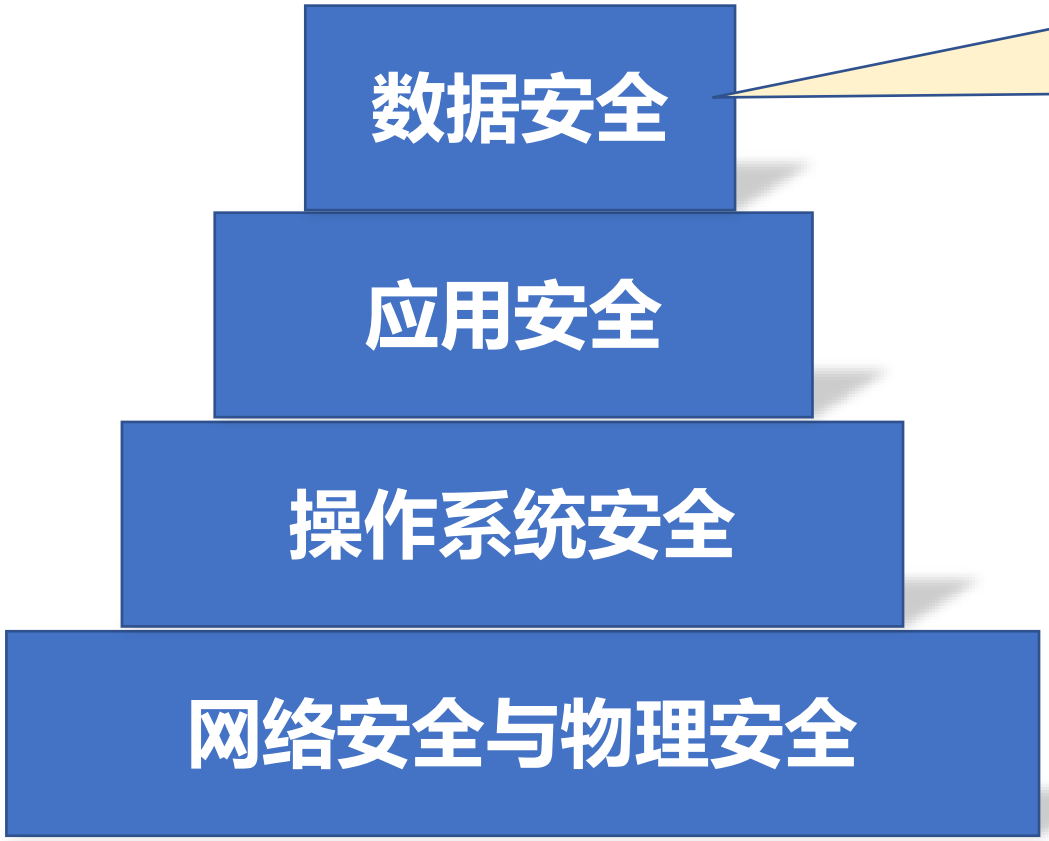
沈昌祥院士指出网络空间已经成为继**陆、海、空、天之后的第5大主权领域空间**，也是国际战略在军事领域的演进。

内容概要

1. 网络安全事件
2. 网络空间安全的概念
3. 网络空间安全技术架构
4. 网络空间安全法律法规
5. 我国网络空间安全的机遇与挑战

网络空间安全技术架构

网络空间安全架构分层



主要介绍数据安全的范畴、数据的保密性、数据存储技术以及数据备份和恢复技术

网络空间安全技术架构

网络空间安全架构分层

主要介绍恶意代码、数据库安全、中间件安全和Web安全等内容

网络空间安全技术架构

网络空间安全架构分层

主要介绍操作系统安全、病毒原理与防范

网络空间安全技术架构

网络空间安全架构分层

主要介绍物理安全概念、物理环境安全、物理设备安全；网络与协议安全、网络安全与管理、虚拟化与云计算安全。

网络空间安全技术架构

网络空间安全架构分层

关键技术与防护场景

- 密码学发展及其应用
- 区块链与数字金融安全
- 社交网络与隐私安全
- 物联网与工控系统安全
- 人工智能安全

网络空间安全的体系结构

应用安全理论与技术知识模块

信息隐藏	物联网安全	WEB安全	计算机数字取证	舆情分析及预警	数字版权保护技术
隐私保护技术	云计算安全	大数据安全	垃圾信息识别与过滤	数据存储与恢复	电子政务/电子商务安全

系统安全理论与技术知识模块

数据库安全	可信计算	代码安全与漏洞挖掘
操作系统安全	芯片安全	恶意代码分析与防御
访问控制技术	物理安全	可靠性技术

网络安全理论与技术知识模块

IPv4/v6安全	无线通信安全	网络漏洞检测与防护
VPN	通信网络安全	入侵检测与防御
网络安全协议	网络攻击与防护	防火墙技术

网络空间安全基础理论知识模块

网络空间安全导论	网络空间安全法律法规	网络空间安全管理基础		
操作系统	数据库	程序设计语言	计算机网络	计算机组成
数论	信息论	计算复杂性		

密码学基础知识模块

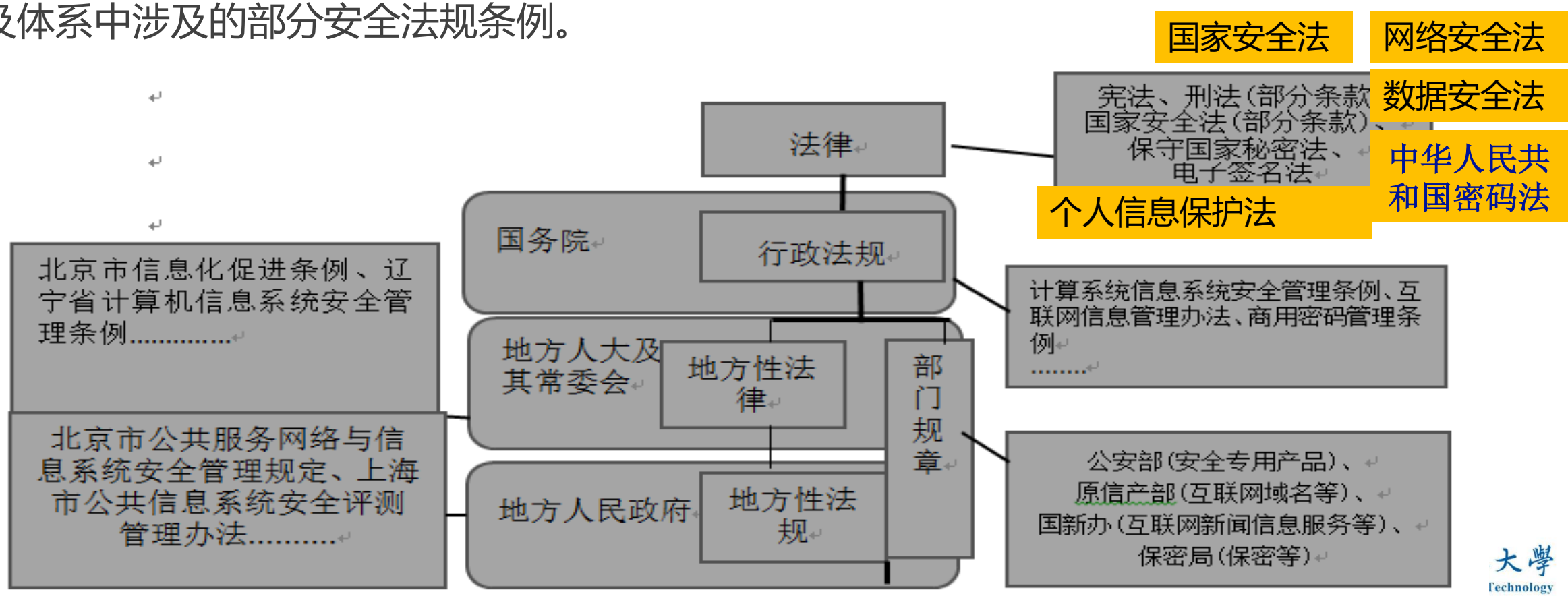
密码协议	
密码分析技术	量子密码
对称密码	公钥密码

内容概要

1. 网络安全事件
2. 网络空间安全的概念
3. 网络空间安全技术架构
4. 网络空间安全法律法规
5. 我国网络空间安全的机遇与挑战

网络空间安全法规与政策

我国实行多级立法的法律体系，包括**法律、行政法规、地方性法规、自制条例和单行条例、部门规章和地方规章，共同构成了宪法统领下的统一法律体系，网络空间安全所涉及的法规和政策，贯穿到了整个立法体系中的多个法规文件中**，图12-1形像的描述了我国的立法体系，以及体系中涉及的部分安全法规条例。



信息保护相关法律

国家秘密

国家秘密的基本范围主要包括产生于政治、国防军事、外交大事、经济、科技和政法等领域的秘密事项。

国家秘密的密级，按照国家秘密事项与国家安全和利益的关联程序，以及泄漏后可能造成的损害程度为标准，**划分为绝密、机密、秘密三级。**

国家秘密的保密期限，除另有规定外，**绝密级不超过三十年，机密级不超过二十年，秘密级不超过十年。**对不能确定保密期限的国家秘密，应当确定解密条件。

保护国家秘密相关法律

《中华人民共和国保守国家秘密法 》、《中华人民共和国刑法》。另外，《中华人民共和国国家安全法》、《中华人民共和国军事设施保护法》、《中华人民共和国统计法》、《中华人民共和国专利法》等法律也都有相应的条款明确规定了对泄漏国家秘密的犯罪行为的刑事处罚、对危害国家秘密安全的违法行为的法律责任。

信息保护相关法律

商业秘密

商业秘密，是指不为公众所知悉、能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。

保护商业秘密相关法律

我国现在还没有针对商业秘密进行保护的专门立法，对商业秘密的保护是通过《中华人民共和国反不正当竞争法》、《中华人民共和国合同法》、《中华人民共和国劳动法》和《刑法》等法律的有关规定来实施的

侵犯商业秘密的行为有三种情形：第一，以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密。第二，披露、使用或者允许他人使用上述手段获取权利人的商业秘密；第三，违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。

信息保护相关法律

个人信息

个人信息是指有关一个可识别的自然人的任何信息。个人隐私是指公民个人生活中不愿为他人公开或知悉的秘密。

保护个人信息相关法律

在没有针对个人信息进行保护的专门立法前，《中华人民共和国宪法》、《中华人民共和国居民身份证法》、《中华人民共和国护照法》、《中华人民共和国民法通则》《中华人民共和国侵权责任法》、《刑事诉讼法》、《民事诉讼法》等都有对个人信息进行保护的条款。

2021年8月20日，十三届全国人大常委会第三十次会议20日表决通过《中华人民共和国个人信息保护法》。对个人信息处理者在处理个人信息的过程中应履行的保护个人权益的责任提出了明确的要求。

《中华人民共和国个人信息保护法》2021年11月1日起施行。

打击网络违法犯罪行业相关法律

网络违法犯罪

网络违法犯罪的概念，在中国法学界一直存在争议。狭义的网络犯罪，指以计算机网络为违法犯罪对象而实施的危害网络空间的行为。广义的网络犯罪，是以计算机网络为违法犯罪工具或者为违法违法犯罪对象而实施的危害网络空间的行为，应当包括违反国家规定，直接危害网络安全及网络正常秩序的各种违法犯罪行为。

打击网络违法犯罪行业相关法律

目前，我国尚没有针对网络违法犯罪行为的专门立法，对网络违法犯罪打击是通过《中华人民共和国治安管理处罚法》、《刑法》等法律来实施的。

网络违法犯罪行为包括一下几大类：（1）破坏互联网运行安全行为；（2）破坏国家安全和社会稳定的行为；（3）破坏社会主义市场经济秩序和社会管理秩序的行为；（4）侵犯个人、法人和其他组织的人身、财产等合法权利的行为；（5）利用互联网实施以上四类所列的行为以外的违法犯罪行为。

网络空间安全管理相关法律

网络空间安全管理

网络违法犯罪的概念，在中国法学界一直存在争议。狭义的网络犯罪，指以计算机网络为违法犯罪对象而实施的危害网络空间的行为。广义的网络犯罪，是以计算机网络为违法犯罪工具或者为违法违法犯罪对象而实施的危害网络空间的行为，应当包括违反国家规定，直接危害网络安全及网络正常秩序的各种违法犯罪行为。

网络空间安全管理相关法律

在我国尚没有针对网络违法犯罪行为的专门立法前，对网络违法犯罪打击是通过《中华人民共和国治安管理处罚法》、《刑法》等法律来实施的。

《中华人民共和国网络安全法》2017年6月1日正式实施，网络安全法是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

网络违法犯罪行为包括一下几大类：（1）破坏互联网运行安全行为；（2）破坏国家安全和社会稳定的行为；（3）破坏社会主义市场经济秩序和社会管理秩序的行为；（4）侵犯个人、法人和其他组织的人身、财产等合法权利的行为；（5）利用互联网实施以上四类所列的行为以外的违法犯罪行为。

重要法律法规-国家安全法

2015年7月1日，第十二届全国人民代表大会常务委员会第十五次会议通过新的《国家安全法》。国家主席习近平签署第29号主席令予以公布。法律对政治安全、国土安全、军事安全、文化安全、科技安全、信息安全等11个领域的国家安全任务进行了明确，《国家安全法》共7章84条，自2015年7月1日起施行。

《国家安全法》第二十五条规定

国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

国家安全法的六大亮点

一是确立了以总体国家安全管理为指导思想

二是突出强调以人民安全为宗旨

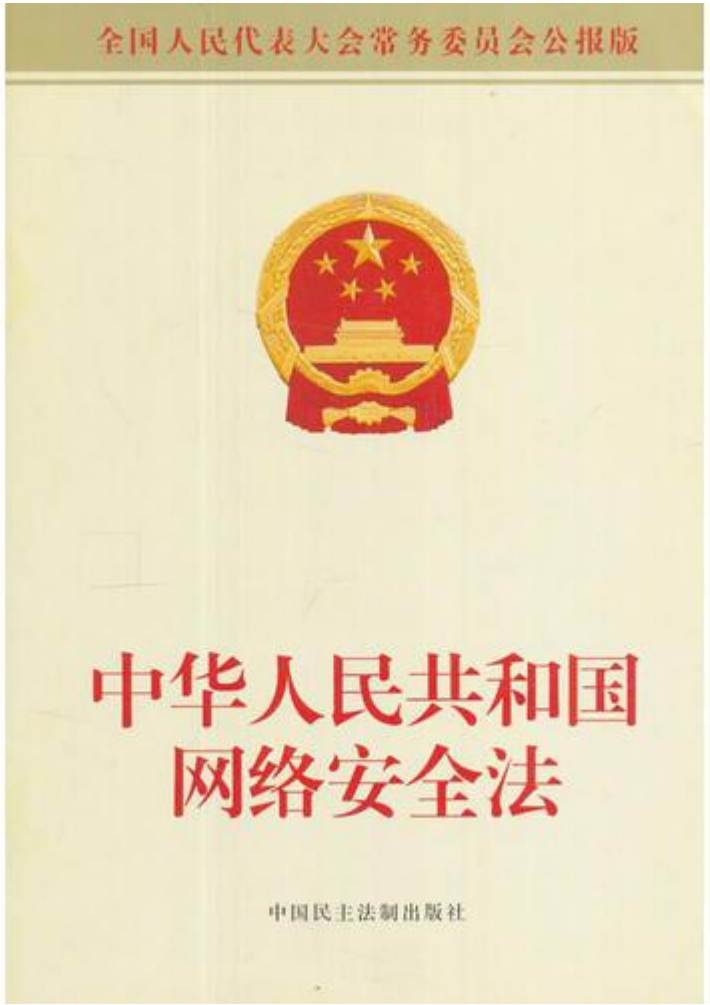
三是首次界定国家安全

四是确立了国家安全领导体制

五是首次提出网络空间主权这一概念

六是首次规定全民国家安全教育日

重要法律法规-网络安全法



2015年6月

十二届全国人大常委会第十五次会议对网络安全法草案进行首次审核

2016年6月

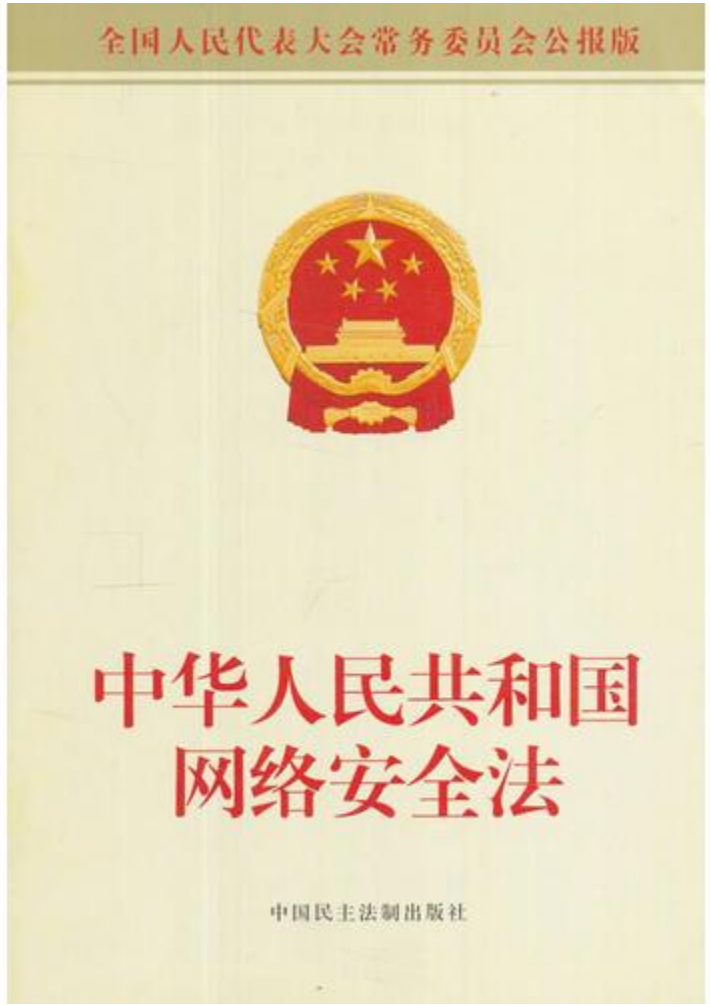
第十二届全国人大常委会第二十一次会议对网络安全法草案进行第二次审议

2016年11月7日

此网络安全法草案提交十二届全国人大常委会第二十四次会议进行第三次审议

2017年6月1日正式实施

重要法律法规-网络安全法



网络安全法共有7章79条，内容有6方面突出亮点

1.明确网络空间主权原则

2.明确了网络产品和服务提供者的安全义务

3.明确了网络运营者的安全义务

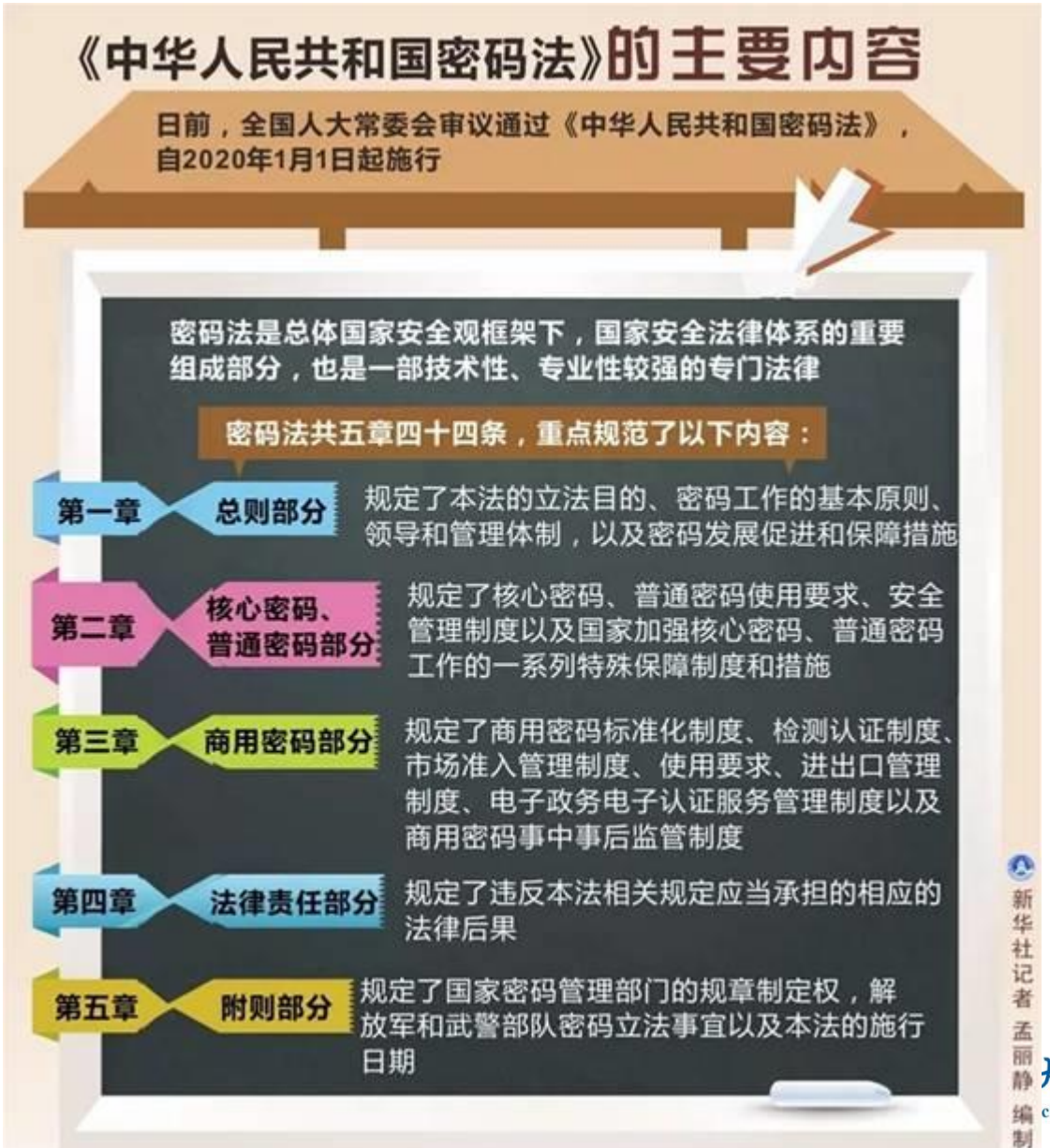
4.进一步完善了个人信息保护规则

5.建立了关键信息基础设施安全保护制度

6.确立了关键信息基础设施重要数据跨境传输的规则

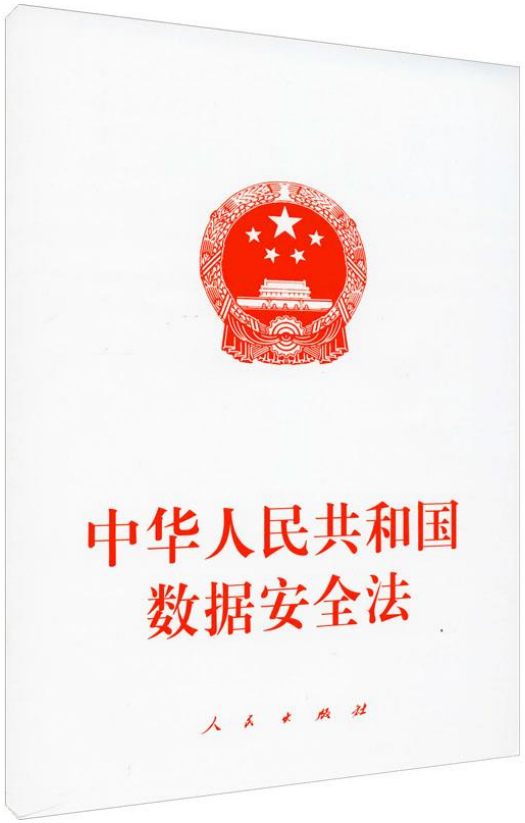
重要法律法规-密码法

2019年10月26日，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，自2020年1月1日起正式施行。《中华人民共和国密码法》是我国密码领域的第一部法律，旨在**规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法治化水平**，是我国密码领域的**综合性、基础性法律。**



重要法律法规-数据安全法

2021年6月，十三届全国人大常委会第二十九次会议通过了《中华人民共和国数据安全法》，并于2021年9月1日起施行.《数据安全法》是数据安全领域的基础性法律，其坚持总体国家安全观，统筹发展与安全，以基本法的形式明确了我国数据安全治理体系的顶层设计和“四梁八柱”，以安全保发展。



《数据安全法》共计7章，55条。以对数据、数据活动、数据安全的界定为出发点，厘清不同面向的数据安全风险，构建数据安全保护管理全面、系统的制度框架，以战略、制度、措施等来构建国家预防、控制和消除数据安全威胁和风险的能力，确立国家行为的正当性，提升国家整体数据安全保障能力。

重要法律法规-数据安全法

提出数据安全管理制度

数据分类分级保护、数据安全风险监测预警、数据安全应急处置、数据安全审查、数据出口管制等。

规定数据处理者责任义务

全流程数据安全、数据安全风险与事件处置、重要数据风险评估、重要数据处境安全、收集数据合法正当等。

明确数据安全监管架构

中央国家安全领导机构建立国家数据安全工作协调机制；国家网信部门负责统筹协调网络数据安全和相关监管工作；工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责；公安机关、国家安全机关。

强调政务数据安全保护，推动电子政务建设进程

国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开发利用。

鼓励数据依法合理开发利用、保障数据依法有序自由流动

数字经济发展、公共服务智能化、适老化、政务数据公开、政务数据开放等。

统筹数据安全与发展

国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数据经济发展；

坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

重要法律法规-个人信息保护法

2021年8月20日，十三届全国人大常委会第三十次会议20日表决通过《中华人民共和国个人信息保护法》。个人信息保护法自2021年11月1日起施行。《中华人民共和国个人信息保护法》包括共8个章节，对个人信息处理者在处理个人信息的过程中应履行的保护个人权益的责任提出了明确的要求。

- **明确了处理个人信息的合法性基础**
- **对个人信息处理规则提出规范性要求：**
  目的合理条件下的最小必要采集、 保存
  采取对个人权益影响最小的方式
- **区分个人信息和敏感个人信息：**
  要求对敏感个人信息进行专门的保护
- **充分赋予个人权利：**
  知情权、 决定权、 查阅、 复制权、 更正权、 删除权、 要求解释的权利
- **强化个人信息处理者义务**
  建立制度、 明确责任人、 加强审计、 加强评估、 强化大平台的义务
- **完善个人信息跨境规则**

法规和部门规章

1. 行政法规

《计算机信息系统安全保护条例》此条例从行政法规的层面，对计算机信息系统及其安全保护进行定义。

《商用密码管理条例》商用密码是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品，未经许可任何单位或者个人不得销售商用密码产品。

2. 部门规章

1. 国务院各部委，根据相关法律和国务院的行政法规、决定、命令，在其部门的权限范围内，制定了一系列有关信息安全相关事项的规章，以更好地执行法律和行政法规所规定的事项。
2. 为了加强计算机信息系统安全专业产品的管理，保证专业产品的功能，维护信息系统的安全，公安部制定并颁布了《计算机信息系统安全专用产品检测和销售许可证管理方法》此管理办法明确了两个必须：安全专用产品的生产者在其产品进入市场销售之前，必须申领《计算机信息系统安全专用产品销售许可证》；必须对其产品进行安全检测和认定。

等级保护相关政策

《中华人民共和国计算机系统安全保护条例》就对“等级保护”提出规定：计算机信息系统实行安全等级保护。

《计算机信息系统安全等级划分准则》，定义了等级保护的五个级别，**第一级：用户自主保护级；第二级：系统审计保护级；第三级：安全标记保护级；第四级：结构化保护级；第五级：访问验证保护级。**

信息安全等级保护法规政策体系如下图：

定级	备案	安全建设整改			等级测评		检查	
《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字【2007】861号）	《信息安全等级保护备案实施细则》（公信安【2007】1360号）	《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安【2009】1429号）	《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技【2008】2071号）	《关于进一步推进中央企业信息安全等级保护工作的通知》（公通字【2010】70号）	《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安【2010】303号）	关于印发《信息系统安全等级测评报告模板（试行）》的通知（公信安【2009】1487号）	《公安机关信息安全等级保护检查工作规范（试行）》（公信安【2008】736号）	《关于开展信息安全等级保护专项监督检查工作的通知》（公信安【2008】736号）
关于印发《信息安全保护办法》的通知（公通字【2010】43号）								
《关于信息安全等级保护的实施意见》（公通字【2004】66号）								
《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号，1994）			《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发【2003】27号）					

加强信息安全保障相关政策

2012年，《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发[2012]23号，国务院发布）该意见明确了我国的在大力推进信息化发展的同时，加强信息安全保障的指导思想、主要目标和近期主要任务。

加强信息安全保障的**指导思想是坚持积极利用、科学发展、依法管理、确保安全，加强统筹协调和顶层设计，健全信息安全保障体系，切实增强信息安全保障能力，维护国家信息安全，促进经济平稳较快发展和社会和谐稳定；主要目标是国家信息安全保障体系基本形成，重要信息系统和基础信息网络安全防护能力明显增强，信息化装备的安全可控水平明显提高，信息安全等级保护等基础性工作明显加强；**

近期主要任务包括：（1）健全安全防护和管理，保障重点领域信息安全。（2）加快能力建设，提升网络与信息安全保障水平。（3）完善政策措施。

信息安全标准基础-标准类型和代码

1983年美国国防部提出一套《可信计算机安全评价标准》（Trusted Computer System Evaluation Criteria, TESEC），即著名的“桔皮书”。这一标准最初用于美国政府和军方的计算机系统，近年来其影响已扩展到了公共管理领域，成为事实上大家公认的标准。目前在国内安全评估中，GB17859-1999《计算机信息系统安全保护等级划分标准》就是参照TCSEC标准制定的。

我国的国家标准分为强制性国家标准、推荐性国家标准和国家标准化指导性技术文件三类。

国家标准化指导性技术文件在实施三年内必须进行复审，复审结果的可能是有效期在延长三年，或者为国家标准，或撤销。

信息安全标准基础-标准编制过程

按照国家标准GB/T 16733-1997《国家标准制定程序的阶段划分及代码》，我国国家标准制定程序如下所示。

国家标准制定程序

阶段代码	阶段名称	阶段主要任务
00	预阶段	标准制定的前期研究，提出标准立项建议
10	立项阶段	标准立项
20	起草阶段	起草标准征求意见和编制说明
30	征求意见阶段	征求意见完成送审稿和意见汇总处理表
40	审查阶段	会审或函审 完成报批搞和审查会议纪要
50	批准阶段	主管部门审查并批准发布标准
60	出版阶段	提供纸质或电子版标准
90	复审阶段	对实施达五年的标准进行复审
95	废止阶段	对无存在价值的标准予以废止

此标准制定阶段的划分与国际标准制定阶段的划分有明显的对应关系，此阶段划分方法实施的标准化工作对促进国际贸易、技术和经济交流以及加强我国标准制定工作的管理与协调都将起到积极的作用。

信息安全标准体系

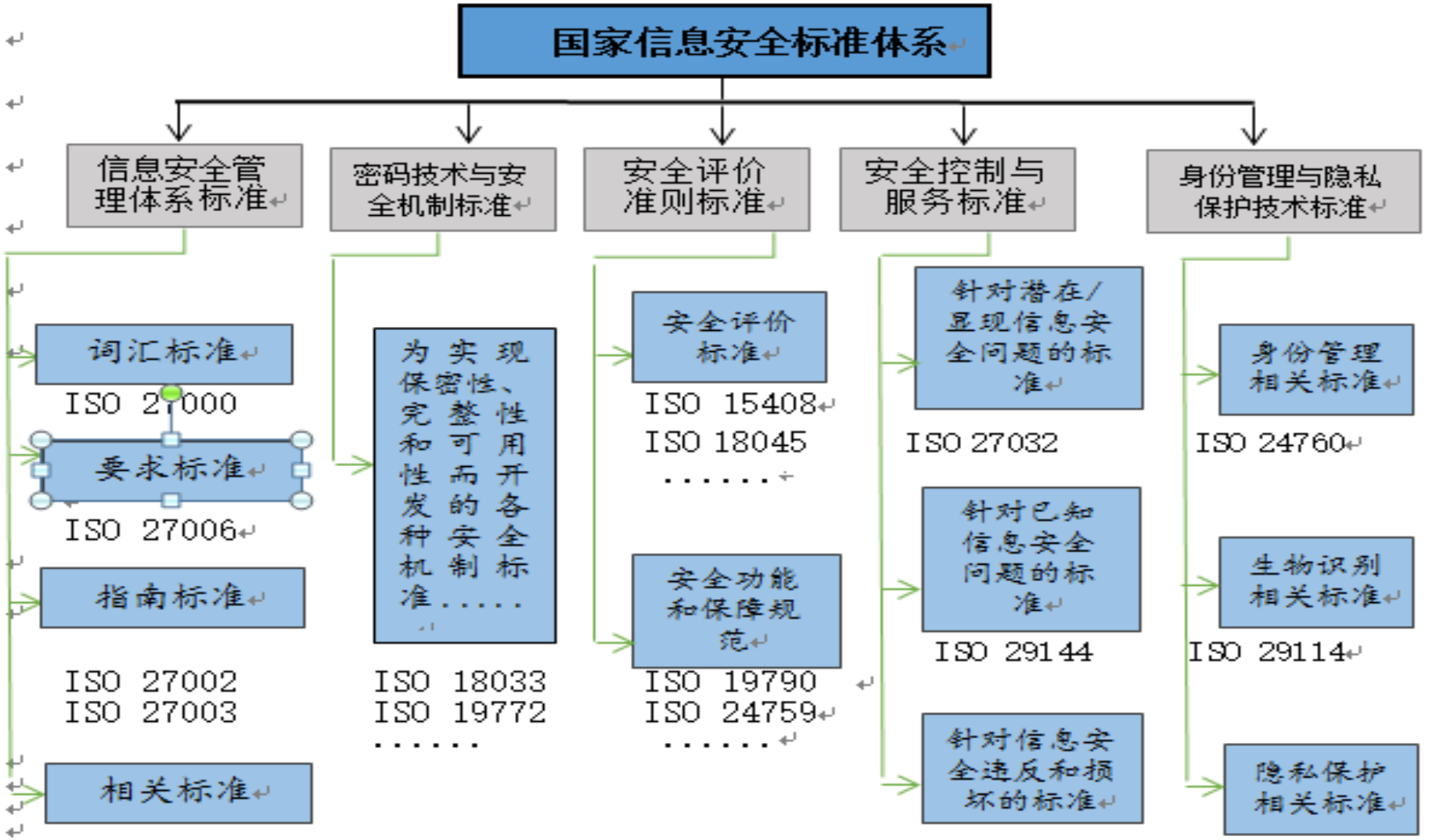


图 12-2

信息安全等级保护标准体系

为推动和规范我国信息安全等级保护的工作，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会以及其他单位组织制定了信息安全等级保护工作需要的一系列标准，形成了信息安全等级保护标准体系，为开展等级保护工作提供了标准保障。

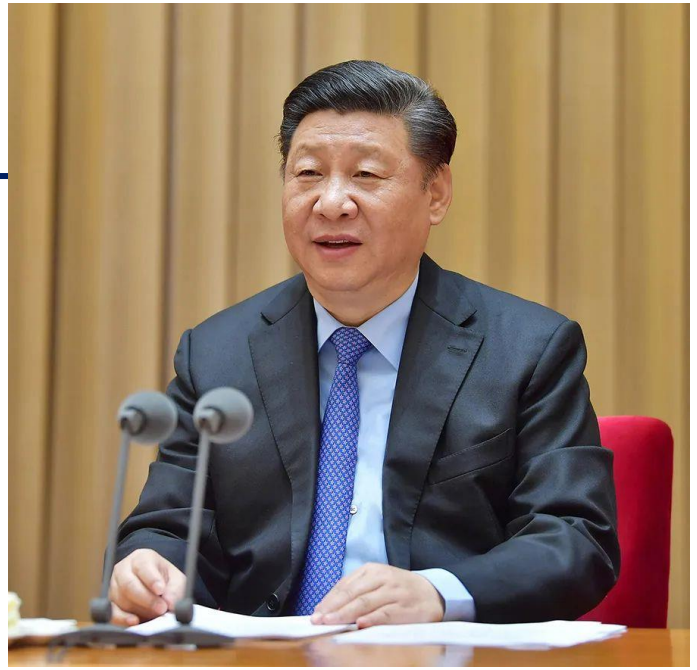
>>>等级保护1.0时期的主要标准如下：
信息安全等级保护管理办法（43号文件）（上位文件）
计算机信息系统安全保护等级划分准则 GB17859-1999（上位标准）
信息系统安全等级保护实施指南 GB/T25058-2008
信息系统安全保护等级定级指南 GB/T22240-2008
信息系统安全等级保护基本要求 GB/T22239-2008
信息系统等级保护安全设计要求 GB/T25070-2010
信息系统安全等级保护测评要求 GB/T28448-2012
信息系统安全等级保护测评过程指南 GB/T28449-2012

>>>等级保护2.0标准体系主要标准如下：
网络安全等级保护条例（总要求/上位文件）
计算机信息系统安全保护等级划分准则（GB 17859-1999）（上位标准）
网络安全等级保护实施指南（GB/T25058-2020）
网络安全等级保护定级指南（GB/T22240-2020）
网络安全等级保护基本要求（GB/T22239-2019）
网络安全等级保护设计技术要求（GB/T25070-2019）
网络安全等级保护测评要求（GB/T28448-2019）
网络安全等级保护测评过程指南（GB/T28449-2018）

内容概要

1. 网络安全事件
2. 网络空间安全的概念
3. 网络空间安全技术架构
4. 网络空间安全法律法规
5. 我国网络空间安全的机遇与挑战

我国网络空间安全的机遇与挑战



——2014年2月27日，习近平在中央网络安全和信息化领导小组第一次会议上的讲话

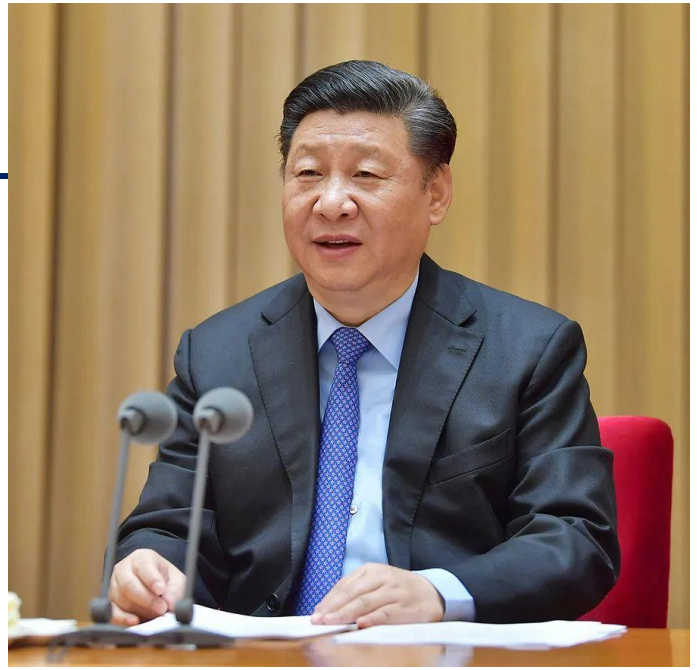
没有网络安全就没有国家安全，就没有经济社会稳定运行广大人民群众利益也难以得到保障。

——2018年4月，习近平在全国网络安全和信息化工作会议上的讲话

数字经济、互联网金融、人工智能、大数据、云计算等新技术新应用快速发展，催生一系列新业态新模式，但相关法律制度还存在时间差、空白区。**网络犯罪已成为危害我国国家政治安全、网络安全、社会安全、经济安全等的重要风险之一。**

国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。要坚持促进发展和依法管理相统一，既大力培育人工智能、物联网、下一代通信网络等新技术新应用，又积极利用法律法规和标准规范引导新技术应用。要坚持安全可控和开放创新并重，立足于开放环境维护网络安全，加强国际交流合作，提升广大人民群众在网络空间的获得感、幸福感、安全感。

我国网络空间安全的机遇与挑战



——2019年9月，习近平对国家网络安全宣传周作出重要指示

坚持网络主权理念，推动全球互联网治理朝着更加公正合理的方向迈进。

中国正在积极推进网络建设，让互联网发展成果惠及13亿中国人民。中国愿意同世界各国携手努力，本着相互尊重、相互信任的原则，深化国际合作，**尊重网络主权，维护网络安全，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的国际互联网治理体系。**

——2020年11月16日，习近平在中央全面依法治国工作会议上的讲话

坚持网络安全为人民、网络安全靠人民，增强网络安全防御能力和威慑能力

要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。

—— 2022年7月12日，国家主席习近平向世界互联网大会国际组织成立致贺信。

中国愿同世界各国一道，把握信息革命历史机遇，培育创新发展新动能，开创数字合作新局面，打造网络安全新格局，构建网络空间命运共同体，携手创造人类更加美好的未来。

……

我国网络空间安全的机遇与挑战

网络渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权，以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。

网络攻击威胁经济安全。网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。

网络有害信息侵蚀文化安全。网络上各种思想文化相互激荡、交锋，优秀传统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。网上道德失范、诚信缺失现象频发，网络文明程度亟待提高。

网络恐怖和违法犯罪破坏社会安全。恐怖主义、分裂主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动，直接威胁人民生命财产安全、社会秩序。计算机病毒、木马等在网络空间传播蔓延，网络欺诈、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在，一些组织肆意窃取用户信息、交易数据、位置信息以及企业商业秘密，严重损害国家、企业和个人利益，影响社会和谐稳定。

网络空间的国际竞争方兴未艾。国际上争夺和控制网络空间战略资源、抢占规则制定权和战略制高点、谋求战略主动权的竞争日趋激烈。个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。

网络空间机遇和挑战并存，机遇大于挑战。必须坚持积极利用、科学发展、依法管理、确保安全，坚决维护网络安全，最大限度利用网络空间发展潜力，更好惠及13亿多中国人民，造福全人类，坚定维护世界和平。

我国网络空间安全的机遇与挑战

信息传播的新渠道。伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。

生产生活的新空间。当今世界，网络深度融入人们的学习、生活、工作等方方面面，网络教育、创业、医疗、购物、金融等日益普及，越来越多的人通过网络交流思想、成就事业、实现梦想。

经济发展的新引擎。互联网日益成为创新驱动发展的先导力量，信息技术在国民经济各行业广泛应用，推动传统产业改造升级，催生了新技术、新业态、新产业、新模式，促进了经济结构调整和经济发展方式转变，为经济社会发展注入了新的动力。

文化繁荣的新载体。网络促进了文化交流和知识普及，释放了文化发展活力，推动了文化创新创造，丰富了人们精神文化生活，已经成为传播文化的新途径、提供公共文化服务的新手段。网络文化已成为文化建设的重要组成部分。

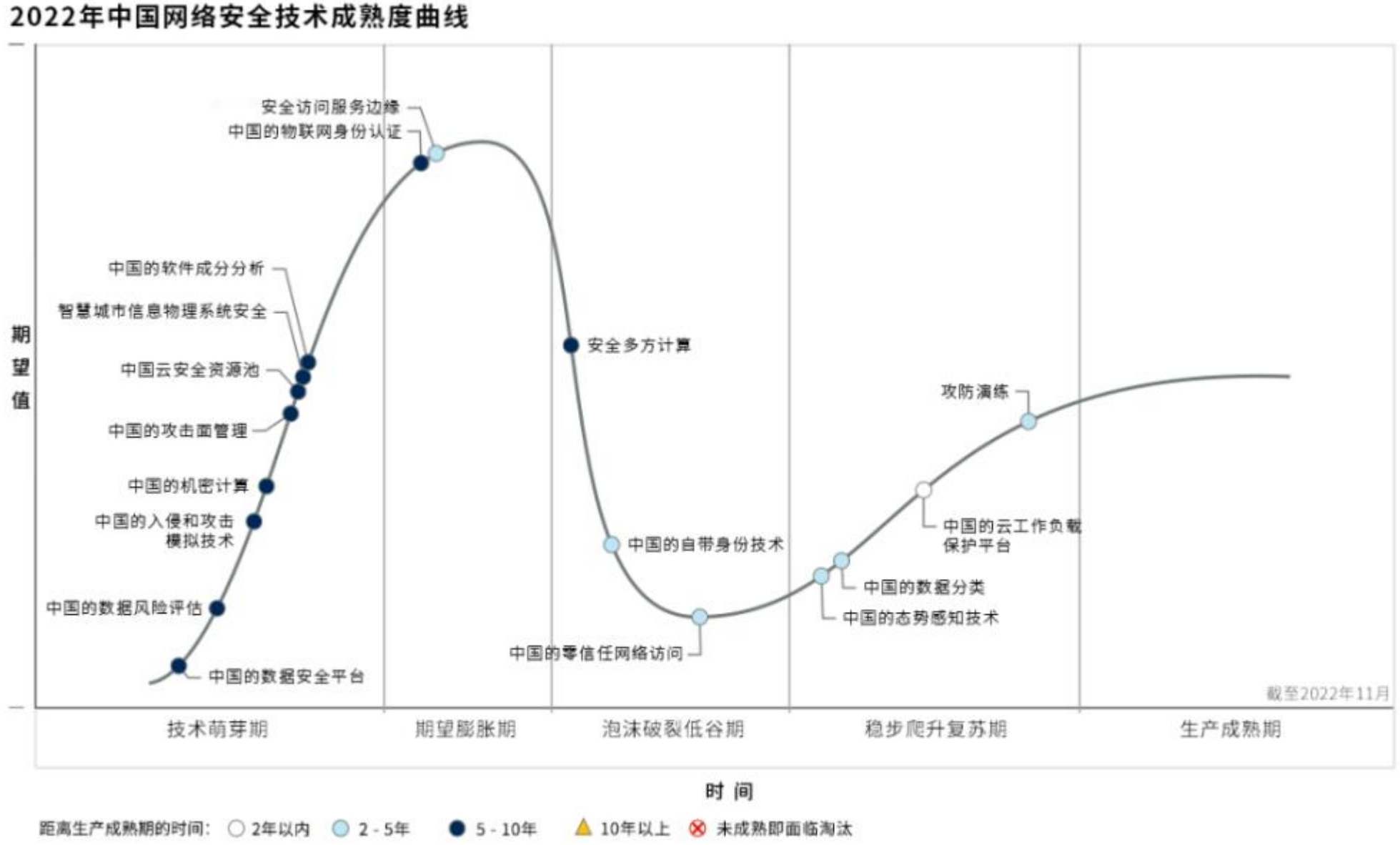
社会治理的新平台。网络在推进国家治理体系和治理能力现代化方面的作用日益凸显，电子政务应用走向深入，政府信息公开共享，推动了政府决策科学化、民主化、法治化，畅通了公民参与社会治理的渠道，成为保障公民知情权、参与权、表达权、监督权的重要途径。

交流合作的新纽带。信息化与全球化交织发展，促进了信息、资金、技术、人才等要素的全球流动，增进了不同文明交流融合。网络让世界变成了地球村，国际社会越来越成为你中有我、我中有你的命运共同体。

国家主权的新疆域。网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，国家主权拓展延伸到网络空间，网络空间主权成为国家主权的重要组成部分。尊重网络空间主权，维护网络安全，谋求共治，实现共赢，正在成为国际

网络空间安全相关领域的趋势及研究热点

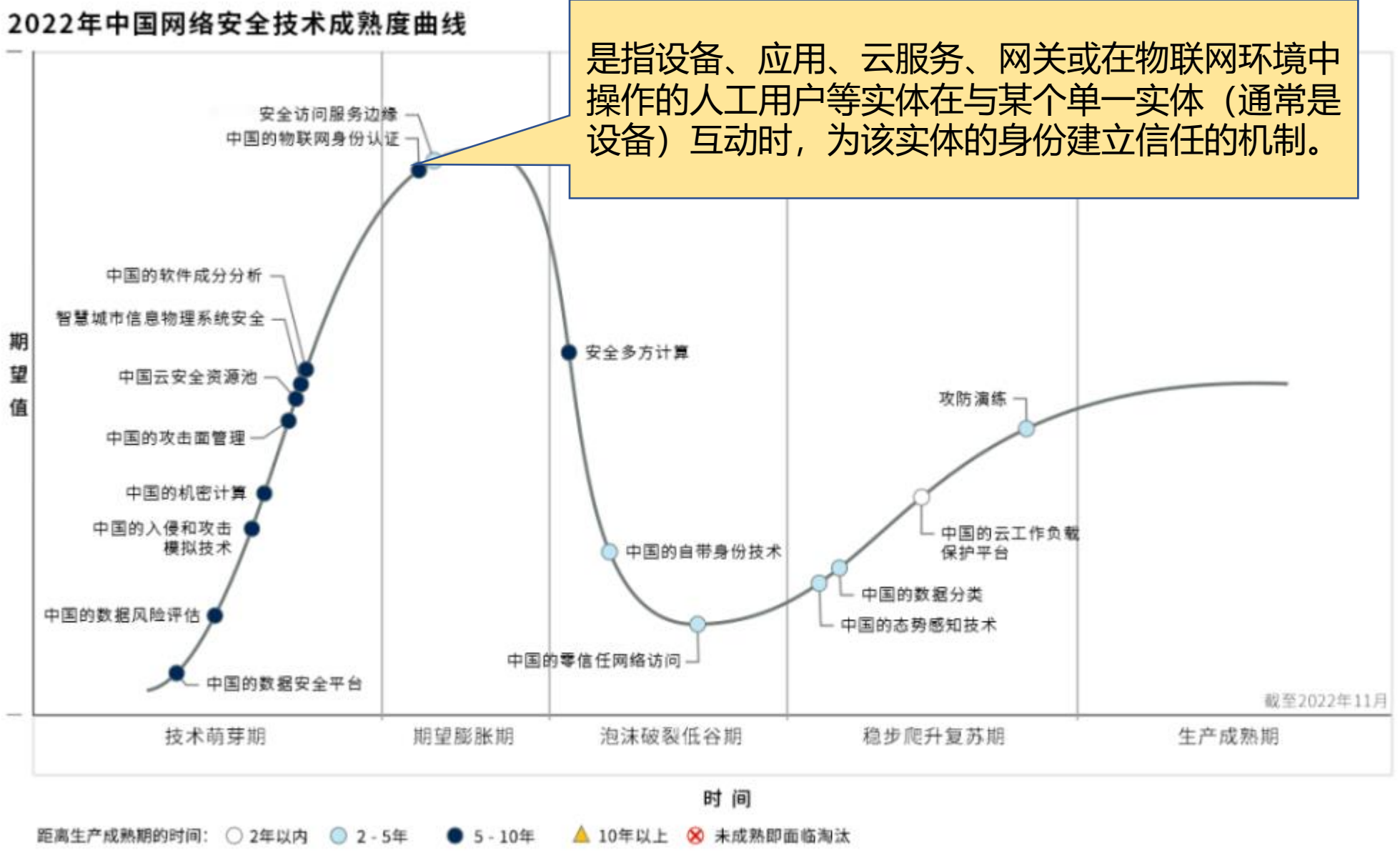
2022年，全球地缘政治冲突加剧，俄乌冲突陷入胶着，全球网络空间安全态势更加复杂紧张。数据泄露、高危漏洞、勒索软件、太空安全等问题也呈现出新的变化，严重危害国家关键基础设施安全和社会稳定，给全球安全态势带来了极大地不确定性。



网络空间安全相关领域的趋势及研究热点

网络空间安全学院
School of Cybersecurity

2022年，全球地缘政治冲突加剧，俄乌冲突陷入胶着，全球网络空间安全态势更加复杂紧张。数据泄露、高危漏洞、勒索软件、太空安全等问题也呈现出新的变化，严重危害国家关键基础设施安全和社会稳定，给全球安全态势带来了极大地不确定性。



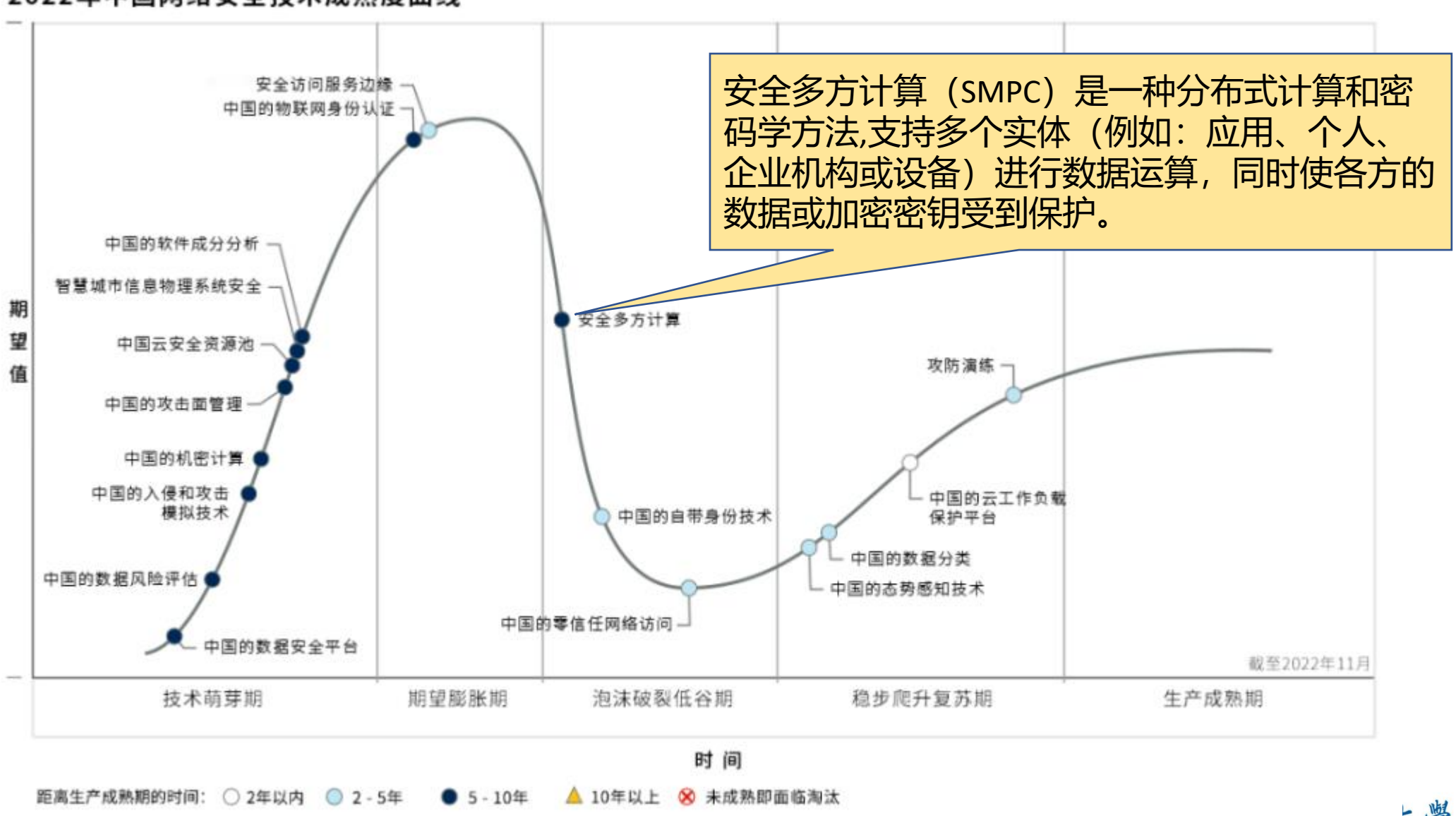
是指设备、应用、云服务、网关或在物联网环境中操作的人工用户等实体在与某个单一实体（通常是设备）互动时，为该实体的身份建立信任的机制。

Chengdu University of Information Technology
Gartner

网络空间安全相关领域的趋势及研究热点

网络空间安全学院
School of Cybersecurity

2022年，全球地缘政治冲突加剧，俄乌冲突陷入胶着，全球网络空间安全态势更加复杂紧张。数据泄露、高危漏洞、勒索软件、太空安全等问题也呈现出新的变化，严重危害国家关键基础设施安全和社会稳定，给全球安全态势带来了极大地不确定性。



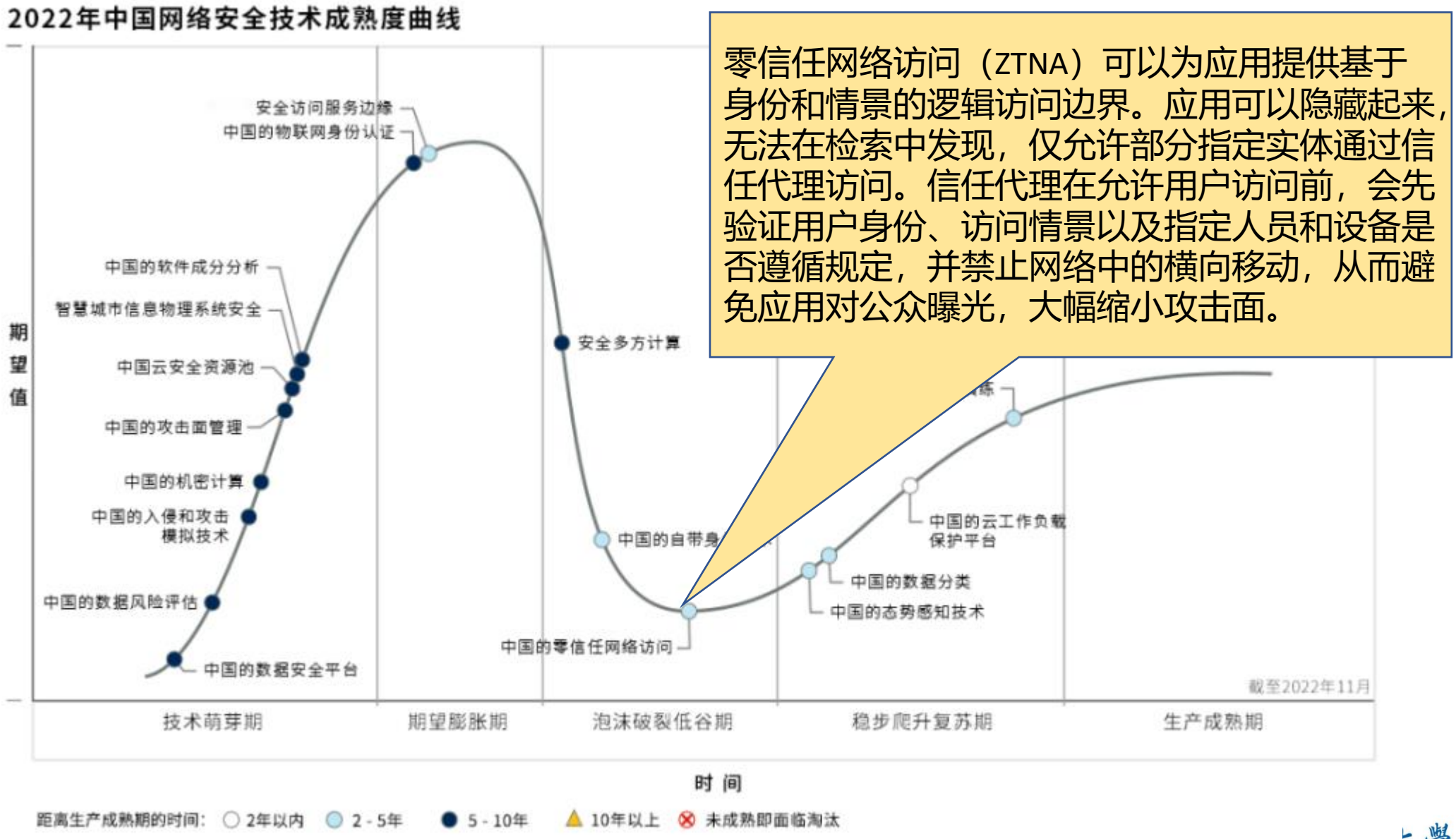
安全多方计算（SMPC）是一种分布式计算和密码学方法,支持多个实体（例如：应用、个人、企业机构或设备）进行数据运算，同时使各方的数据或加密密钥受到保护。

Chengdu University of Information Technology
Gartner

网络空间安全相关领域的趋势及研究热点

2022年，全球地缘政治冲突加剧，俄乌冲突陷入胶着，全球网络空间安全态势更加复杂紧张。数据泄露、高危漏洞、勒索软件、太空安全等问题也呈现出新的变化，严重危害国家关键基础设施安全和社会稳定，给全球安全态势带来了极大地不确定性。

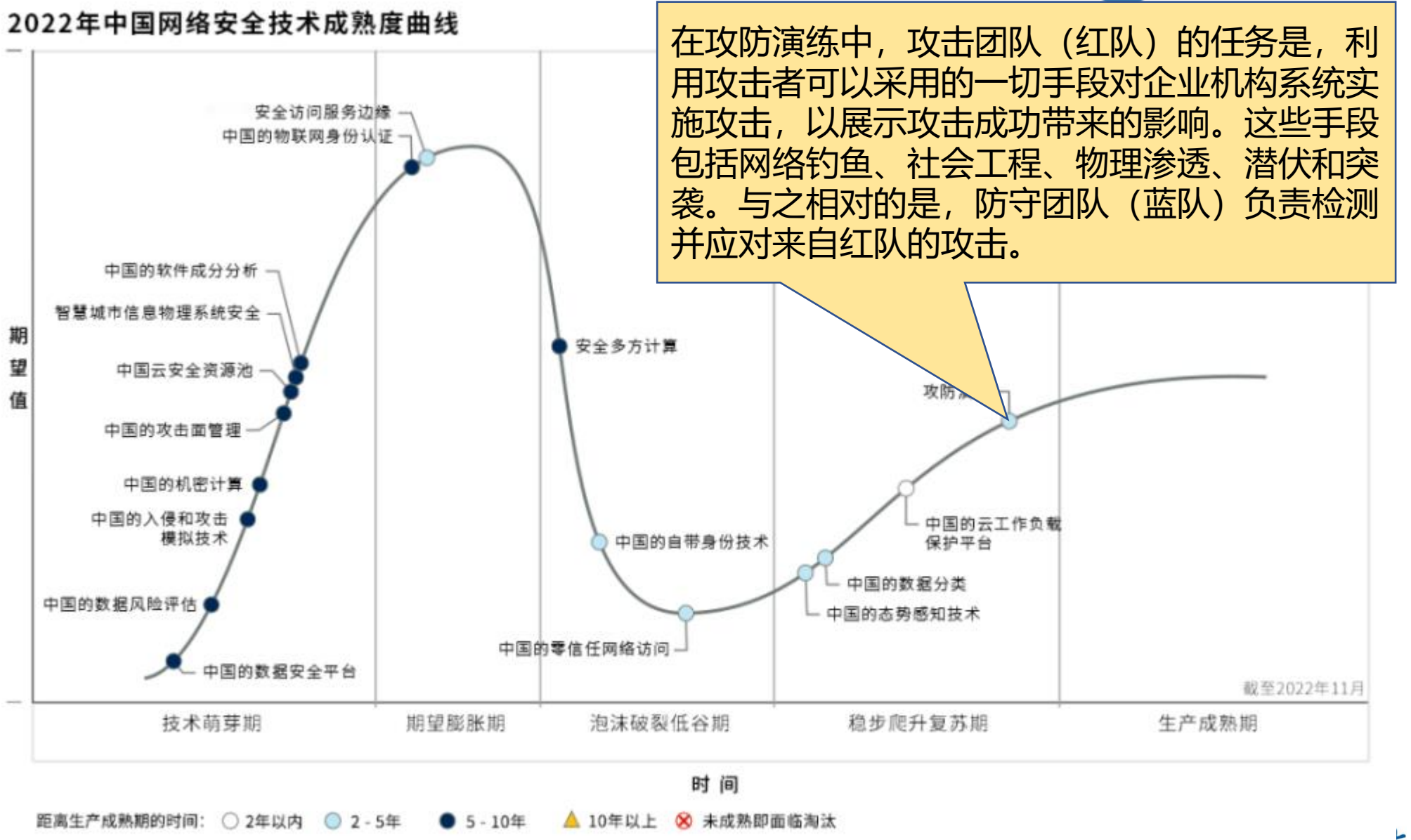
零信任网络访问（ZTNA）可以为应用提供基于身份和情景的逻辑访问边界。应用可以隐藏起来，无法在检索中发现，仅允许部分指定实体通过信任代理访问。信任代理在允许用户访问前，会先验证用户身份、访问情景以及指定人员和设备是否遵循规定，并禁止网络中的横向移动，从而避免应用对公众曝光，大幅缩小攻击面。



网络空间安全相关领域的趋势及研究热点

网络空间安全学院
School of Cybersecurity

2022年，全球地缘政治冲突加剧，俄乌冲突陷入胶着，全球网络空间安全态势更加复杂紧张。数据泄露、高危漏洞、勒索软件、太空安全等问题也呈现出新的变化，严重危害国家关键基础设施安全和社会稳定，给全球安全态势带来了极大地不确定性。



在攻防演练中，攻击团队（红队）的任务是，利用攻击者可以采用的一切手段对企业机构系统实施攻击，以展示攻击成功带来的影响。这些手段包括网络钓鱼、社会工程、物理渗透、潜伏和突袭。与之相对的是，防守团队（蓝队）负责检测并应对来自红队的攻击。

Chengdu University of Information Technology