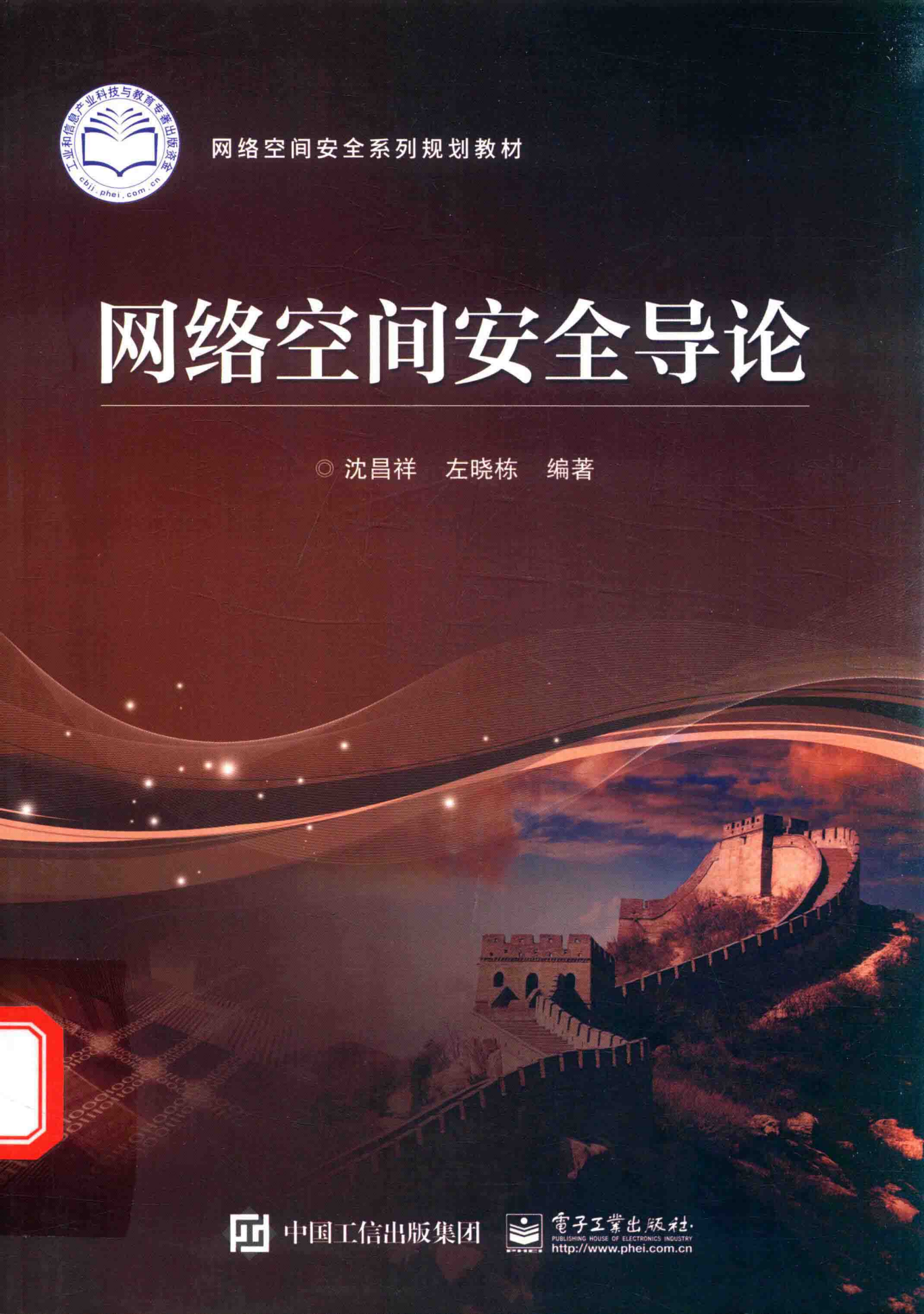

网络空间安全系列规划教材

网络空间安全导论

◎ 沈昌祥　左晓栋　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列规划教材
工业和信息产业科技与教育专著出版资金资助出版

网络空间安全导论

沈昌祥　左晓栋　编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书较为全面、系统地介绍了网络安全知识体系的主要方面，同时注重反映我国的治网主张和我国在网络安全领域的原创性技术。全书共10章，第1章从信息革命的背景切入，介绍了我国的网络强国战略；第2章侧重于介绍网络安全基础概念；第3章、第4章、第5章分别介绍了密码技术与应用、信息系统安全和可信计算技术，包括SM2、SM3、SM4密码算法和可信计算3.0等我国网络安全领域的重大原创性成果；第6章介绍了网络安全等级保护；第7章、第8章、第9章分别介绍了网络安全工程和管理、网络安全事件处置和灾难恢复，以及云计算、物联网、工控系统等面临的新安全威胁的应对；最后一章（第10章）介绍了网络安全法规和标准的相关概念及有关工作进展。

本书兼顾网络安全专业基础学习和其他专业学生选修网络安全课程的需要，建议作为大学本科第二学年的专业基础课教材，也可作为大学本科第二或第三学年的选修教材，初学者可以通过本书在较短的时间内掌握网络安全技术和管理的基本内容。

图书在版编目（CIP）数据

网络空间安全导论/沈昌祥，左晓栋编著．—北京：电子工业出版社，2018.4
ISBN 978-7-121-33243-2

Ⅰ．①网…　Ⅱ．①沈…　②左…　Ⅲ．①网络安全-高等学校-教材　Ⅳ．①TN915.08

中国版本图书馆CIP数据核字（2017）第307987号

策划编辑：章海涛　戴晨辰
责任编辑：戴晨辰
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编100036
开　　本：787×1 092　1/16　印张：18.5　字数：474千字
版　　次：2018年4月第1版
印　　次：2018年4月第1次印刷
定　　价：55.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888，88258888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

前　言

习近平总书记指出，得人者兴，失人者崩，网络空间的竞争，归根结底是人才竞争。建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。2016 年 4 月 19 日，习近平总书记主持召开网络安全和信息化工作座谈会，作出了“要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院”的重要指示。

2016 年 6 月，经中央网络安全和信息化领导小组同意，中央网信办、教育部等 6 部委联合印发了《关于加强网络安全学科建设和人才培养的意见》（中网办发文〔2016〕4 号）。文件对网络安全教材提出具体要求：网络安全教材要体现党和国家意志，体现网络强国战略思想，体现中国特色治网主张，适应我国网络空间发展需要。

为贯彻落实中央关于加强网络安全人才培养特别是教材体系建设的精神，我们决定对 2009 年出版的《信息安全导论》（ISBN 978-7-121-09921-2）进行修订，并更名为《网络空间安全导论》。此次修订主要集中在以下方面。

一是充分贯彻习近平总书记“网络强国”战略思想，充分反映中国对网络空间治理的主张、政策和工作部署。技术是中立的，但网络空间博弈不仅仅是技术博弈，还是理念博弈，话语权博弈。我国培养的人才，首先应该了解我国政府的理念，知晓和支持我们的“网络主权”主张，而不是被灌输西方的价值观。否则，我们就会输在起点上。

二是根据新形势、新情况的发展，对一些陈旧材料进行了更新。技术发展日新月异，网络威胁层出不穷，攻防对垒风云变幻，即使是入门级的基础教材，也要保持一定的更新频率。在网络领域，一本知识固化的书，难以激发创造力。我们希望，每一位读者在跨进网络安全的知识殿堂时，都能够有世界眼光、发展理念。唯有如此，才可培养学生的创新思维，这才是进步的动力。

三是增加了对国内自主网络安全重要技术成果的介绍，这也是本书的特色。国家强调自主创新，这些自主创新的成果理应在教材中得到反映，不能让学生被西方的技术体系牵着鼻子走。例如，本书介绍了可信计算 3.0，这是我国网络安全领域的重大原创性成果。本书还介绍了我国的 SM2、SM3、SM4 密码算法，但学习这些算法需要一定的数学基础，非专业学生可能会感觉有困难，教师可以根据具体情况选择授课重点。

四是调整了对读者范围的定位、适当降低了难度、缩减了课时。根据很多学校的反馈，第 1 版的内容偏多，不利于课时安排。此外，部分内容较深，且与后续一些专业课内容有所重叠。为此，我们不再将本书定位为仅是网络安全本科学生的专业基础课教材，而是兼顾网络安全专业基础学习和其他专业学生选修网络安全课程的需要。当然，写专业的书不难，写通俗的书难；把事情讲复杂不难，讲简单却难；写一个知识点不难，写清楚各知识点之间的逻辑关系，使读者形成整体框架却难。但我们努力做到通俗、简单、全面，目的是希望通过

这本书尽可能地发挥为读者指路的作用，培养读者对网络安全学习的兴趣。

建议本书作为大学本科第二学年的专业基础课教材，也可作为大学本科第二或第三学年的选修教材。全书共包括 10 章。第 1 章从信息革命的背景切入，介绍了我国的网络强国战略；第 2 章侧重于介绍网络安全基础概念，包括网络安全基本属性、网络安全概念的演变、网络安全风险管理、网络安全体系结构等；第 3 章集中介绍密码技术与应用，包括密码的基本概念、常用的密码算法，以及密码的有关应用；第 4 章从安全操作系统、通信网络安全等角度介绍了影响信息系统安全的重要方面；第 5 章介绍了可信计算技术，重点是我国的可信计算技术规范，以及可信计算平台体系结构；第 6 章介绍了网络安全等级保护，重点提出了分等级的信息系统安全设计要求，这些设计要求为读者揭示了安全的信息系统的主要技术特征，体现了高等级信息系统安全体系结构研究的新进展；第 7 章介绍了网络安全工程和管理的基础理论和有关要求，并对网络安全风险评估做了说明；第 8 章介绍了网络安全事件分类与分级标准、应急处理关键过程、信息系统灾难恢复等知识；第 9 章介绍了云计算、物联网、工控系统安全等面临的威胁和应对措施；最后一章（第 10 章）分别介绍了网络安全法规和标准的相关概念及有关工作进展。本书免费提供配套教学资源，读者可登录华信教育资源网（www. hxedu. com. cn）注册后下载。

历史上，人们对于“信息安全”、“网络安全”、“网络空间安全”等概念有不同的解读。中央网络安全和信息化领导小组（已改为中央网络安全和信息化委员会）成立后，相关概念统一到了“网络安全”或“网络空间安全”上。本书也对此做了相应调整，但在个别地方还保留了“信息安全”，如某些组织的固定名字、已发布标准中的相关名称等。

本书是很多人辛勤劳动的成果，参加本版修订的还有刘毅、孙瑜、赵勇、崔占华、张弛等同志。另外还要感谢张建标、胡俊、张兴、周艺华、杨宇光、蔡永泉等同志对本书做出的贡献。电子工业出版社刘宪兰编辑、章海涛编辑、戴晨辰编辑为本书的编辑出版耗费了大量心血。在此一并深表谢意！

本书第 1 版在使用中收到了很多专家、高校教师、学生反馈的意见和建议，这些意见和建议对本书再版修订帮助甚大，也在此对他们表示谢意！同时，希望有更多读者对本书提出意见和建议，这将有利于我们在今后继续更新、完善本书。

中国工程院院士　沈昌祥

2018 年 4 月

目　录

第1章 绪 论

本章要点

- 信息技术革命带来国家发展机遇
- 网络空间安全威胁
- 网络强国战略
- 网络空间国际博弈

1.1 没有网络安全就没有国家安全

人类社会经历了农业革命、工业革命，正在经历信息革命。农业革命增强了人类生存能力，使人类从采食捕猎走向栽种畜养，从野蛮时代走向文明社会；工业革命拓展了人类体力，以机器取代了人力，以大规模工厂化生产取代了个体工场手工生产；而信息革命则增强了人类脑力，带来生产力又一次质的飞跃，对国际政治、经济、文化、社会、生态、军事等领域发展产生了深刻影响。

当前，以信息技术为代表的新一轮科技革命方兴未艾，互联网日益成为创新驱动发展的先导力量。信息技术与生物技术、新能源技术、新材料技术等交叉融合，正在引发以绿色、智能、泛在为特征的群体性技术突破。信息、资本、技术、人才在全球范围内加速流动，互联网推动产业变革，促进工业经济向信息经济转型，国际分工新体系正在形成。信息化代表新的生产力、新的发展方向，推动人类认识世界、改造世界的能力空前提升，正在深刻改变着人们的生产生活方式，带来生产力质的飞跃，引发生产关系重大变革，成为重塑国际经济、政治、文化、社会、生态、军事发展新格局的主导力量。全球信息化进入全面渗透、跨界融合、加速创新、引领发展的新阶段。

1.1.1 网络空间成为人类生活新空间

网络空间（Cyberspace）的概念是伴随着互联网的成长而逐步产生、发展和演变的。这一概念的起源也有多种说法。

一种说法是，科幻小说家 William Gibson 于 1982 年发表短篇小说 *Burning Chrome*，此书中首次使用了 Cyberspace 一词。1984 年，他发表科幻小说 *Neuromancer*（国内译为《神经漫游者》），Cyberspace 一词得到进一步推广。在 William Gibson 的笔下，Cyberspace 是一个由“矩阵”（Matrix）构成的交感幻觉空间，人们可以通过在神经中植入电极把自己的意识接入这个空间并进行互动。William Gibson 进一步想象，Cyberspace 内不仅仅只有人类，还会有人工智能存在。

20 世纪 90 年代正值互联网产业蓬勃发展初期。那时，人们的众多新兴理念都可以借助 Cyberspace 的概念得到恰到好处的表达。1990 年 6 月 8 日，John Perry Barlow 在创建电子前哨基金会（EFF）的宣言《罪与罚》中描述道：“通过数以百万计的通信线路，人们相互连线在一起，形成了一张跨越了广阔空间并充满着电子、微波、磁场和光脉冲的网络——也就是科幻小说家 William Gibson 笔下的 Cyberspace”。从此以后，Cyberspace 才被人们赋予了更多的计算机网络或互联网的含义，并逐渐广为人知。对此，有观点认为，“相比万维网、信息高速公路，Cyberspace 更准确地描述了互联网真正的样子——一个全新的地域”。

在这段时期，Cyberspace 是崇尚自由、充满理想的第一代互联网人与工程师们喜欢用的概念，其更多地反映了技术专家对人类社会虚拟乌托邦的理想。但随着互联网的进一步普及，计算机病毒开始出现和扩散，原有意义上以奉行网络自由主义精神、显示高超技能的黑客们越来越多地与网络犯罪联系在一起，Cyberspace 的“技术自由”色彩开始变淡。与此同

时，很多国家开始注意到 Cyberspace 这个人造空间对社会发展和国家利益的影响。1998 年，美国政府在《崛起的数字经济》文件中声称：如果说以前美国是一个在汽车轮子上的国家，那么今天，美国已经是一个网络上的国家。不仅美国，各国政府在逐渐意识到网络空间具有的价值和重要性后，都开始急于把 Cyberspace 纳入其管控范围。

于是，官方的 Cyberspace 定义开始出现。美国在 2003 年《保护网络空间的国家战略》中界定了 Cyberspace 的含义："一个由信息基础设施组成的相互依赖的网络"，进而提出，"保障网络空间的正常运转对我们的经济、安全、生活都至关重要。" 2009 年 5 月，美国《网络空间政策评估》引述了 2008 年 1 月的第 54 号国家安全总统令，将 Cyberspace 定义为"信息技术基础设施相互依存的网络，包括互联网、电信网、计算机系统以及重要工业中的处理器和控制器。常见的用法还指信息及人与人交互构成的虚拟环境。"

中国对 Cyberspace 的认识已经走过了 20 多年的时间。1991 年 9 月号的《科学美国人》的封面上同时出现了 Network 和 Cyberspace 两个词。我国著名科学家钱学森先生看到这期杂志后，敏锐地注意到了其背后可能蕴含的重要意义。他立即要求对 Cyberspace 进行准确翻译，并向中科院负责同志写信，希望安排人专门跟踪研究 Cyberspace 及相关问题，密切关注该领域的进展。从此，Cyberspace 被中国的专家学者纳入研究视野。这之后，国内一直习惯于将其译作"网络空间"。对这样的译法，很多专业人士不以为然，认为没有体现本意，与 Network 无法区别。也有很多专家提出了"网际空间"、"赛博空间"、"电磁空间"等译法，但都没有被广泛接受，目前仍然使用"网络空间"这一约定俗成的名称。但其确实已经不是相互连接的网络那么简单。

网络空间不是虚拟空间，而是人类现实活动空间的人为、自然延伸，是人类崭新的存在方式和形态。我国政府的官方文件指出，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、服务和数据构成了网络空间，其已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域。

当前，网络空间正全面改变着人们的生产生活方式，深刻影响人类社会历史发展进程。网络技术突破了时空限制，拓展了传播范围，创新了传播手段，引发了传播格局的根本性变革，网络成为人们获取信息、学习交流的新渠道；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；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，促进经济结构调整和发展方式转变，为经济社会发展注入新的动力；网络促进了文化交流和知识普及，释放了文化发展活力，推动了文化的创新创造，丰富了人们的精神文化生活，网络文化已成为文化建设的重要组成部分；电子政务应用走向深入，政府信息公开共享，进一步推动了政府决策科学化、民主化，畅通了公民参与社会治理的渠道，网络成为保障公民知情权、参与权、表达权、监督权的重要途径；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，增进了不同文明的交流融合，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。

1.1.2 网络空间安全威胁

没有网络安全就没有国家安全。网络空间安全威胁与政治安全、经济安全、文化安全、

社会安全、军事安全等领域相互交融、相互影响，已成为当前面临的最复杂、最现实、最严峻的非传统安全问题之一。2014 年 4 月，中央国家安全委员会第一次会议提出了总体国家安全观的概念。习近平总书记指出，贯彻落实总体国家安全观，必须既重视外部安全，又重视内部安全，对内求发展、求变革、求稳定、建设平安中国，对外求和平、求合作、求共赢、建设和谐世界；既重视国土安全，又重视国民安全，坚持以民为本、以人为本，坚持国家安全一切为了人民、一切依靠人民，真正夯实国家安全的群众基础；既重视传统安全，又重视非传统安全，构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系。在总体国家安全观中，网络安全是重要组成部分。

1. 网络安全事关政治安全

政治安全是总体国家安全观的根本。互联网已经成为意识形态斗争的主战场，网上渗透与反渗透、破坏与反破坏、颠覆与反颠覆的斗争尖锐复杂。相比传统媒体，网络具有跨时空、跨国界，信息快速传播、多向互动等特性，对现实社会问题和矛盾具有极大的催化放大作用，极易使一些局部问题全局化、简单问题复杂化、国内问题国际化，给国家治理带来挑战。

2011 年初，突尼斯、埃及等国相继爆发被称为“阿拉伯之春”的街头政治运动。以互联网为代表的新兴媒体成为民众组织串联、宣传鼓噪的重要平台。突、埃反对势力利用推特、脸书等网站，频繁发布集会通知、游行示威等信息，大量传播极具刺激性、煽动性的游行画面，不断激发民众强烈的参与意识和反抗意识，使抗议浪潮迅速爆发。新兴媒体发挥的强大组织和煽动作用，直接影响和改变了突、埃民众的思维和行动，产生了连锁反应和“滚雪球”效应，引发抗议力量迅速聚积，最终导致两国剧变，甚至政权更迭。

2. 网络安全事关经济安全

金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。在当前的攻防形势中，“物理隔离”防线可被跨境入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，关键信息基础设施存在重大风险隐患。一旦遭受攻击，就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。

近年来，针对关键信息基础设施的网络攻击时有发生，对国家安全和经济社会稳定运行带来重大影响。2010 年 7 月，针对西门子工业控制系统的“震网”病毒感染了伊朗核设施，导致伊朗浓缩铀工厂内五分之一的离心机报废，大大延迟了伊朗核进程。2015 年 6 月，波兰航空公司地面操作系统遭受黑客攻击，致使系统瘫痪长达 5 小时，至少 10 个班次的航班被取消，1400 多名乘客滞留，造成航空秩序严重混乱。2016 年 1 月，乌克兰电网遭到黑客网络攻击，导致包括乌克兰首府在内的多个地区停电数小时，引发公众恐慌。

3. 网络安全事关文化安全

随着新兴媒体的快速发展，网络已成为文化的重要载体和传播渠道，网上各种思想文化相互激荡、交锋，优秀传统文化和主流价值面临冲击。与传统的文化传播渠道相比，网络具有极大的开放性和虚拟性。网民可以通过微博、微信、QQ 等网络社交工具随时发布和传播信息。

少数网民、“网络大V”充当网络不良信息的写手和推手，一些虚假信息和谣言通过网络空间迅速传播，一些淫秽色情内容通过网络空间污染社会环境，一些网民的议论和情绪通过网络空间发酵放大，一些局部矛盾和社会问题通过网络空间凸显升级。这些捕风捉影、添油加醋的谣言肆意质疑主流文化传统、污蔑英雄形象、破坏政府公信力，危害极大。网上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。

4. 网络安全事关社会安全

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，发布网络恐怖袭击，直接威胁人民生命财产安全、社会秩序。2014年6月24日，中央网信办发布《恐怖主义的网络推手——“东伊运”恐怖音视频》电视专题片，揭示了暴恐音视频危害及与暴力恐怖违法犯罪活动之间的联系。据统计，在中国发生的暴力恐怖案件中，涉案人员几乎无一例外观看、收听过宣扬、煽动暴力恐怖的音视频。

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。

5. 网络安全事关国防安全

网络空间已成为国际战略博弈的新领域，围绕网络空间发展权、主导权、控制权的竞争愈演愈烈。少数国家极力谋求网络空间军事霸权，组建网络作战部队、研发网络攻击武器、出台网络作战条例，不断强化网络攻击与威慑能力。

网络空间已成为引领战争转型的主导性空间，是未来战争对抗的首发战场。看不懂网络空间，就意味着看不懂未来战争；输掉网络空间，就意味着输掉未来战争。美国2009年正式成立网络空间司令部，2015年4月发布《国防部网络战略》，首次明确美国在何种情况下可以使用网络武器实施攻击，全面规划网络作战部队的编制结构，提出三年内建成133支网络部队。2015年底，美国白宫发布《网络威慑战略》，提出将采取一切手段，包括实施进攻和防御网络作战、运用海陆空和太空军事力量等应对对美发起的网络攻击。

1.2 网络强国战略

2014年2月27日，习近平总书记主持召开中央网络安全和信息化领导小组第一次会议并发表重要讲话。中央成立网络安全和信息化领导小组，习近平总书记亲自担任组长，再次体现了中国最高层全面深化改革、加强顶层设计的意志，显示出保障网络安全、维护国家利益、推动信息化发展的决心。

中央网络安全和信息化领导小组指出，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际、国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

2018年3月，中央网络安全和信息化领导小组改为中央网络安全和信息化委员会。2018年4月，中央召开全国网络安全和信息化工作会议，习近平总书记在讲话中强调，我