



教职工政治学习参考资料

(2020 年第 10 期)

苏州大学党委宣传部编

2020 年 10 月 12 日

教职工政治学习参考资料

(2020 年第 10 期)

苏州大学党委宣传部编

2020 年 10 月 12 日

● 学习内容

网络安全教育（一）专题学习

● 参考资料

- 一、《中华人民共和国网络安全法》 1
- 二、《网络信息内容生态治理规定》 21
- 三、《苏州大学网络安全管理条例》 32
- 四、常见网络安全风险与应对..... 41

《中华人民共和国网络安全法》

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构 and 高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当

按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检

测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工

作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规

定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目

的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不

得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对

来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

(二) 组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

(三) 向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规

定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以

下罚款。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依

法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪

活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传

输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果

果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规

定。

第七十九条 本法自 2017 年 6 月 1 日起施行。

(来源：中华人民共和国民政部信息中心，2017 年 05 月 15 日)

《网络信息内容生态治理规定》

第一章 总 则

第一条 为了营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 中华人民共和国境内的网络信息内容生态治理活动，适用本规定。

本规定所称网络信息内容生态治理，是指政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。

第三条 国家网信部门负责统筹协调全国网络信息内容生态治理和相关监督管理工作，各有关主管部门依据各自职责做好网络信息内容生态治理工作。

地方网信部门负责统筹协调本行政区域内网络信息内容生态治理和相关监督管理工作，地方各有关主管部门依据各自职责做好本行政区域内网络信息内容生态治理工作。

第二章 网络信息内容生产者

第四条 网络信息内容生产者应当遵守法律法规，遵循公序良俗，不得损害国家利益、公共利益和他人合法权益。

第五条 鼓励网络信息内容生产者制作、复制、发布含有下列内容的信息：

(一) 宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化的；

(二) 宣传党的理论路线方针政策和中央重大决策部署的；

(三) 展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的；

(四) 弘扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌的；

(五) 有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的；

(六) 有助于提高中华文化国际影响力，向世界展现真实立体全面的中国的；

(七) 其他讲品味讲格调讲责任、讴歌真善美、促进团结稳定等的内容。

第六条 网络信息内容生产者不得制作、复制、发布含有下列内容的违法信息：

(一) 反对宪法所确定的基本原则的；

(二) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统

一的；

(三) 损害国家荣誉和利益的；

(四) 歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；

(五) 宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；

(六) 煽动民族仇恨、民族歧视，破坏民族团结的；

(七) 破坏国家宗教政策，宣扬邪教和封建迷信的；

(八) 散布谣言，扰乱经济秩序和社会秩序的；

(九) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(十) 侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；

(十一) 法律、行政法规禁止的其他内容。

第七条 网络信息内容生产者应当采取措施，防范和抵制制作、复制、发布含有下列内容的不良信息：

(一) 使用夸张标题，内容与标题严重不符的；

(二) 炒作绯闻、丑闻、劣迹等的；

(三) 不当评述自然灾害、重大事故等灾难的；

(四) 带有性暗示、性挑逗等易使人产生性联想的；

(五) 展现血腥、惊悚、残忍等致人身心不适的；

(六) 煽动人群歧视、地域歧视等的；

(七) 宣扬低俗、庸俗、媚俗内容的；

(八) 可能引发未成年人模仿不安全行为和违反社会公德行为、诱

导未成年人不良嗜好等的；

(九) 其他对网络生态造成不良影响的内容。

第三章 网络信息内容服务平台

第八条 网络信息内容服务平台应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化。

第九条 网络信息内容服务平台应当建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度。

网络信息内容服务平台应当设立网络信息内容生态治理负责人，配备与业务范围和服务规模相适应的专业人员，加强培训考核，提升从业人员素质。

第十条 网络信息内容服务平台不得传播本规定第六条规定的信息，应当防范和抵制传播本规定第七条规定的信息。

网络信息内容服务平台应当加强信息内容的管理，发现本规定第六条、第七条规定的信息的，应当依法立即采取处置措施，保存有关记录，并向有关主管部门报告。

第十一条 鼓励网络信息内容服务平台坚持主流价值导向，优化信息推荐机制，加强版面页面生态管理，在下列重点环节(包括服务类型、位置版块等)积极呈现本规定第五条规定的信息：

(一) 互联网新闻信息服务首页首屏、弹窗和重要新闻信息内容页面等；

(二) 互联网用户公众账号信息服务精选、热搜等；

(三) 博客、微博客信息服务热门推荐、榜单类、弹窗及基于地理位置的信息服务版块等；

(四) 互联网信息搜索服务热搜词、热搜图及默认搜索等；

(五) 互联网论坛社区服务首页首屏、榜单类、弹窗等；

(六) 互联网音视频服务首页首屏、发现、精选、榜单类、弹窗等；

(七) 互联网网址导航服务、浏览器服务、输入法服务首页首屏、榜单类、皮肤、联想词、弹窗等；

(八) 数字阅读、网络游戏、网络动漫服务首页首屏、精选、榜单类、弹窗等；

(九) 生活服务、知识服务平台首页首屏、热门推荐、弹窗等；

(十) 电子商务平台首页首屏、推荐区等；

(十一) 移动应用商店、移动智能终端预置应用程序和内置信息内容服务首屏、推荐区等；

(十二) 专门以未成年人为服务对象的网络信息内容专栏、专区和产品等；

(十三) 其他处于产品或者服务醒目位置、易引起网络信息内容服务使用者关注的重点环节。

网络信息内容服务平台不得在以上重点环节呈现本规定第七条规定的信息。

第十二条 网络信息内容服务平台采用个性化算法推荐技术推送信息的，应当设置符合本规定第十条、第十一条规定要求的推荐模型，建立健全人工干预和用户自主选择机制。

第十三条 鼓励网络信息内容服务平台开发适合未成年人使用的模式，提供适合未成年人使用的网络产品和服务，便利未成年人获取有益身心健康的信息。

第十四条 网络信息内容服务平台应当加强对本平台设置的广告位和在本平台展示的广告内容的审核巡查，对发布违法广告的，应当依法予以处理。

第十五条 网络信息内容服务平台应当制定并公开管理规则和平台公约，完善用户协议，明确用户相关权利义务，并依法依约履行相应管理职责。

网络信息内容服务平台应当建立用户账号信用管理制度，根据用户账号的信用情况提供相应服务。

第十六条 网络信息内容服务平台应当在显著位置设置便捷的投诉举报入口，公布投诉举报方式，及时受理处置公众投诉举报并反馈处理结果。

第十七条 网络信息内容服务平台应当编制网络信息内容生态治理工作年度报告，年度报告应当包括网络信息内容生态治理工作情况、网络信息内容生态治理负责人履职情况、社会评价情况等内容。

第四章 网络信息内容服务使用者

第十八条 网络信息内容服务使用者应当文明健康使用网络，按照法律法规的要求和用户协议约定，切实履行相应义务，在以发帖、回复、留言、弹幕等形式参与网络活动时，文明互动，理性表达，不得发布本规定第六条规定的信息，防范和抵制本规定第七条规定的信息。

第十九条 网络群组、论坛社区版块建立者和管理者应当履行群组、版块管理责任，依据法律法规、用户协议和平台公约等，规范群组、版块内信息发布等行为。

第二十条 鼓励网络信息内容服务使用者积极参与网络信息内容生态治理，通过投诉、举报等方式对网上违法和不良信息进行监督，共同维护良好网络生态。

第二十一条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用网络和相关信息技术实施侮辱、诽谤、威胁、散布谣言以及侵犯他人隐私等违法行为，损害他人合法权益。

第二十二条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过发布、删除信息以及其他干预信息呈现的手段侵害他人合法权益或者谋取非法利益。

第二十三条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。

第二十四条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过人工方式或者技术手段实施流量造假、流量劫持以及虚假注册账号、非法交易账号、操纵用户账号等行为，破坏网络生态秩序。

第二十五条 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用党旗、党徽、国旗、国徽、国歌等代表党和国家形象的标识及内容，或者借国家重大活动、重大纪念日和国家机关及其工作人员名义等，违法违规开展网络商业营销活动。

第五章 网络行业组织

第二十六条 鼓励行业组织发挥服务指导和桥梁纽带作用，引导会员单位增强社会责任感，唱响主旋律，弘扬正能量，反对违法信息，防范和抵制不良信息。

第二十七条 鼓励行业组织建立完善行业自律机制，制定网络信息内容生态治理行业规范和自律公约，建立内容审核标准细则，指导会员单位建立健全服务规范、依法提供网络信息内容服务、接受社会监督。

第二十八条 鼓励行业组织开展网络信息内容生态治理教育培训和宣传引导工作，提升会员单位、从业人员治理能力，增强全社会共同参与网络信息内容生态治理意识。

第二十九条 鼓励行业组织推动行业信用评价体系建设，依据

章程建立行业评议等评价奖惩机制，加大对会员单位的激励和惩戒力度，强化会员单位的守信意识。

第六章 监督管理

第三十条 各级网信部门会同有关主管部门，建立健全信息共享、会商通报、联合执法、案件督办、信息公开等工作机制，协同开展网络信息内容生态治理工作。

第三十一条 各级网信部门对网络信息内容服务平台履行信息内容管理主体责任情况开展监督检查，对存在问题的平台开展专项督查。

网络信息内容服务平台对网信部门和有关主管部门依法实施的监督检查，应当予以配合。

第三十二条 各级网信部门建立网络信息内容服务平台违法违规行为台账管理制度，并依法依规进行相应处理。

第三十三条 各级网信部门建立政府、企业、社会、网民等主体共同参与的监督评价机制，定期对本行政区域内网络信息内容服务平台生态治理情况进行评估。

第七章 法律责任

第三十四条 网络信息内容生产者违反本规定第六条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向

有关主管部门报告。

第三十五条 网络信息内容服务平台违反本规定第十条、第三十一条第二款规定的，由网信等有关主管部门依据职责，按照《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律、行政法规的规定予以处理。

第三十六条 网络信息内容服务平台违反本规定第十一条第二款规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，按照有关法律、行政法规的规定予以处理。

第三十七条 网络信息内容服务平台违反本规定第九条、第十二条、第十五条、第十六条、第十七条规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，按照有关法律、行政法规的规定予以处理。

第三十八条 违反本规定第十四条、第十八条、第十九条、第二十一条、第二十二条、第二十三条、第二十四条、第二十五条规定的，由网信等有关主管部门依据职责，按照有关法律、行政法规的规定予以处理。

第三十九条 网信部门根据法律、行政法规和国家有关规定，会同有关主管部门建立健全网络信息内容服务严重失信联合惩戒机制，对严重违反本规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施限制从事网络信息服务、网上

行为限制、行业禁入等惩戒措施。

第四十条 违反本规定，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由有关主管部门依照有关法律、行政法规的规定予以处罚。

第八章 附 则

第四十一条 本规定所称网络信息内容生产者，是指制作、复制、发布网络信息内容的组织或者个人。

本规定所称网络信息内容服务平台，是指提供网络信息内容传播服务的网络信息服务提供者。

本规定所称网络信息内容服务使用者，是指使用网络信息内容服务的组织或者个人。

第四十二条 本规定自 2020 年 3 月 1 日起施行。

（来源：中国网信网，2019 年 12 月 20 日）

《苏州大学网络安全管理条例》

第一章 总 则

第一条 为贯彻落实《中华人民共和国网络安全法》，建立健全学校网络安全管理体系，落实校园网络安全工作责任制，提升校园网络安全整体水平，进一步保障校园网络正常运行，制定本条例。

第二条 本条例所称网络安全是指苏州大学校园网内的网络系统和信息系统的安全，包括设备设施安全、系统运行安全和内容数据安全等多个方面。

第三条 学校网络安全管理的目标是，完善网络安全技术体系和运行体系，不断提高网络安全保护能力，确保校园网络安全、稳定运行，保障学校信息化建设持续发展。

第四条 学校任何单位和个人都必须遵守《中华人民共和国网络安全法》。使用校园网络系统或信息系统的用户，应接受并配合上级主管部门、公安司法机关或学校的网络安全检查。

第五条 学校网络安全管理以“谁主管谁负责，谁运营谁负责，谁使用谁负责”为原则，落实网络安全分级责任制；以国家标准《信息系统安全等级保护基本要求》为指导，综合防范、突出重点，保障学校网络安全。

第二章 管理机构与职责

第六条 学校网络安全与信息化工作领导小组负责学校网络安

全工作，确定学校网络安全工作的政策方针，制定相关规章制度。提出学校网络安全工作的任务和要求，审定学校网络安全工作计划，组织查处学校网络安全事件。

第七条 学校网络安全与信息化工作领导小组办公室，贯彻执行上级网络安全部门的政策和要求，贯彻落实网络安全与信息化工作领导小组的任务要求，负责学校网络安全具体管理工作。主要职责如下：

1. 根据网络安全实际情况，拟订学校网络安全工作计划；
2. 统筹协调和监督管理各单位网络安全工作。审核各单位网络安全管理制度，并检查网络安全管理制度落实情况；
3. 组织监测全校网络运行情况，评估网络安全现状，形成全校网络安全报告。负责委托网络安全服务机构对学校信息系统进行安全风险检测评估，并落实相关改进措施；
4. 组织审核拟在校园网内实施的网络安全方案和方法，组织论证拟在校园网内部署的网络安全设备和系统；
5. 核定校园网内信息系统安全等级及其安全管理制度；
6. 发布涉及网络安全的通知、公告；
7. 组织开展经常性的全校网络安全宣传教育。组织开展面向各单位网络安全管理人员的技术培训；
8. 协助公安司法机关查处各种有关网络安全的违纪、违法行为。

第八条 信息化建设与管理中心（以下简称信息化中心），负责学校主干网络和关键信息系统的安全，同时负责所属各信息系统的

安全。主要职责如下：

1. 拟订学校主干网络和关键信息系统的安全管理制度。切实落实安全管理制度，保障学校主干网络和关键信息系统的安全；
2. 建立健全所属各信息系统的管理制度，并切实加以落实；
3. 加强技术人员队伍建设，不断提高防范、应对校园网络安全事件的能力；
4. 为校内其他单位提供网络安全相关技术支持和协助。

第九条 各部门、直属单位、学院（部）和其他单位负责本单位的网络安全工作。主要职责如下：

1. 负责本单位所属信息系统和自建网络系统的安全，包括设备设施安全、系统运行安全和内容数据安全；
2. 建立健全本单位网络安全管理制度，并切实加以落实；
3. 监控本单位所属信息系统和自建网络系统的运行状态，及时发现和消除安全隐患。如果发现危及全校网络安全的情形或者有害信息后，必须及时向网络安全与信息化工作领导小组办公室报告；
4. 组织开展对本单位师生员工的网络安全教育。

第十条 各单位党政主要负责人是本单位的网络安全第一责任人，对本单位的网络安全负领导责任。

第十一条 各单位必须指定网络安全管理员，承担本单位网络安全的具体工作。各单位应当及时向网络安全与信息化工作领导小组办公室报备网络安全管理员相关信息。

第十二条 各单位网络安全管理员一般应具有相关专业背景

景，在正式上岗前，应当参加网络安全培训，掌握网络安全相关技术，了解学校网络安全体系，理解网络安全制度，熟悉本单位网络安全措施。

第三章 网络系统安全

第十三条 学校网络系统分为学校主干网络和单位自建网络两级。

第十四条 学校主干网络由学校统筹建设和管理。信息化中心负责学校主干网络的线路铺设与维护、设备部署与运维、流量监测与管控，保障学校主干网络的安全畅通。各校区间网络链路应当实现冗余互联，做到核心设备冗余热备。校园网络应当部署相关网络安全设备，实现对网络攻击行为的实时监测和告警，实现对恶意代码的实时检测和防护。

第十五条 校园网络系统对外采用统一出口，实现一体化管理。信息化中心负责管控校园网络对外的统一出口，负责统一管理所有出口链路的公网 IP 地址。校园网络应该实现多出口链路，所有出口链路需接入防火墙、入侵防御系统等安全设备防护。

第十六条 校园网络系统对内实行按需接入，采取实名管理。信息化中心负责校园网络的接入管理，接入校园网络的每一个系统和每一件设备都应具有明确的属主。根据工作需要，各单位自建网络可以申请接入学校主干网络。

第十七条 各单位根据工作需要建设内部网络系统。各单位内

部网络系统如果需要接入学校主干网络，应向信息化中心提供内部网络系统的拓扑结构、系统组成和功能应用等要素，并通过信息化中心的综合评估。

第十八条 在建筑物设计与施工过程中，建设单位就弱电工程部分应征求信息化中心意见，相关设计方案须经过信息化中心审核。在建筑物施工完成后，弱电工程部分须由信息化中心参与工程验收。

第十九条 在维修或拆除涉及校园网络的建筑物时，在维护或开挖涉及校园网络的道路时，须事先通知信息化中心，以保护校园网络设备设施的安全。

第二十条 加强各楼宇内弱电间的管理，涉及校园网络的弱电间原则上由信息化中心单独使用。学校自建或与校外合作单位建设的弱电管网由信息化中心统一管理，任何单位使用弱电管网需提供设计和施工方案，并经信息化中心审核通过后，方可施工。

第二十一条 除信息化中心外，严禁其他单位或个人以任何方式登录校园网络主干的各类设备，实施修改、设置、删除等操作。严禁任何施工单位或个人以任何理由损毁校园网络设备设施。

第二十二条 师生员工使用校园网络，采取“实名注册、认证上网”制度。实名上网认证制度由信息化中心负责实施。

第四章 信息系统安全

第二十三条 学校各信息系统实行安全等级保护。由网络安全与信息化工作领导小组办公室参照国家标准《信息系统安全等级保护

基本要求》，审核确定校园网内各信息系统的安全等级。信息系统不仅包括关键信息系统和各个面向全校的重要业务系统，也包括各级各类应用业务系统，还包括各级各类网站系统。

第二十四条 关键信息系统由学校统筹建设和管理。信息化中心负责由统一身份认证平台、云计算平台、共享数据中心等构成的关键信息系统的建设和运营工作。

第二十五条 各单位负责所属信息系统的运营，应当按信息系统安全等级保护的要求，制定安全管理制度和操作规程，采取相应的安全保护技术措施，保障信息系统免受干扰、破坏或者未经授权的访问，防止信息系统数据泄露或者被窃取、篡改。相关安全管理制度等须经过网络安全与信息化工作领导小组办公室审核。

第二十六条 信息系统安全管理制度应当明确安全负责人和各项安全保护责任，应当明确各项安全保护技术措施。

第二十七条 信息系统安全保护技术措施至少包括下列项：

1. 完善系统安全配置，定期进行漏洞扫描、系统加固或升级；
2. 开启日志审计服务，有效检测、记录系统运行状态；
3. 分类管理数据，对重要数据进行备份、加密处理；
4. 实施用户分类管理，用户账号应能标识系统访问的不同角色，应尽量避免使用系统默认账号，账号只能具有符合用户角色的最小权限；
5. 系统管理员密码应满足强度要求。

第二十八条 信息系统的注册用户应该实名认证，由信息系统

的运营者负责实名认证的实施。

第二十九条 在建设阶段须充分考虑信息系统的安全防护。关键信息系统和各单位所属重要信息系统，应当具有支持业务稳定、持续运行的性能，并且安全技术措施必须同步规划、同步建设、同步使用。

第三十条 根据工作需要新建或升级在校园网内运行的信息系统，各单位应事先向网络安全与信息化工作领导小组办公室提出申请；同时应就信息系统设计方案向信息化中心征求意见。在上线运行前，信息系统须通过由信息化中心组织的安全检测。

第五章 应急处置

第三十一条 网络安全与信息化工作领导小组办公室按照规定通报网络安全监测预警信息。各单位应当根据国家、地方网络安全部门发布的预警信息及时做好相应防范工作，必须按照网络安全与信息化工作领导小组办公室通报的预警信息，做好相应处置工作。

第三十二条 网络安全与信息化工作领导小组办公室协调信息化中心和各单位，制定网络安全事件应急预案。网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第三十三条 各单位网络安全管理人员必须熟悉本单位网络安全事件应急处置措施。各单位应当定期开展网络安全事件应急预案演练。

第三十四条 校园网内发生网络安全事件，应当立即启动网络安全事件应急预案，各单位和相关人员须按照应急预案规定进行处置。

第六章 奖惩

第三十五条 网络安全与信息化工作领导小组办公室定期开展全校网络安全工作的检查，每年向学校网络安全与信息化工作领导小组汇报各单位网络安全工作总结信息。对网络安全工作成绩显著的单位和个人，学校给予表彰和奖励；对违反网络安全管理制度、网络安全工作存在不足和隐患且逾期不改的单位，学校给予通报批评。

第三十六条 对拒不执行网络安全管理相关制度、漠视网络安全工作以至造成重大事故和案件的单位，学校将追究该单位主要负责人和直接责任者的责任。对触犯法律的，将移送公安司法机关处理。

第三十七条 对损坏校园网络系统或信息系统设备设施的个人，学校将视其情节轻重追究责任，如触犯法律应移交公安司法机关处理。

第七章 附则

第三十八条 对于涉及国家秘密的网络系统或信息系统，按照国家保密工作部门的相关规定和标准进行保护，接受学校保密委员会办公室监督指导。

第三十九条 本条例自发布之日起施行，由网络安全与信息化

工作领导小组办公室负责解释。

(来源：苏州大学信息化建设与管理中心，2019年03月18日)

常见网络安全风险与应对

2020 年已过大半，因为疫情的爆发，各行各业都经历着前所未有的考验，网络安全行业也正面临着前所未有的压力。下面就让我们来盘点一下在过去的大半年里发生了哪些网络安全大事件。

一、土耳其黑客组织“图兰军”攻击篡改大量中国网站

2020 年 1 月，土耳其黑客组织图兰军（Turan Ordusu）在一个月内攻击篡改一百多个中国网站。大量政府、企业、医疗、教育、社会团体网站被该组织入侵。该黑客团体主要利用 SQL 注入、弱口令等获取后台管理权限，在管理后台插入了存储型的跨站代码，用户访问网站时将跳转至黑客制作的挑衅页面。

二、疫情期间，境外多个国家和地区对中国发动网络攻击

从 2020 年 1 月下旬开始，有一个黑客团伙用防疫和中医药相关的文件作诱饵，通过他们伪造的 QQ 邮箱界面盗取用户邮箱账号和密码。文件中没有夹带木马病毒，杀毒软件也不会发现。一旦点击，用户账户信息就会完全暴露在黑客面前。黑客们攻击的目标都是政府部门职员，安全风险大大增加。这伙黑客的手法与我国台湾地区某个具有政治背景的黑客团伙“绿斑”高度一致。

2020 年 2 月，印度 APT 组织“白象”（Patchwork、摩诃草）使用了一个伪装成我国卫生主管部门的域名，并借助新型肺炎为话题，伪造疫情相关文件，对我国医疗工作领域发动 APT 攻击。该组织于 2020 年 1 月注册仿冒域名“nhc****.com”，访问部分链接会直接下

载名为“武汉旅行信息收集申请表.xlsx”、“卫生部指令.docx”的恶意文档，打开后将下载具备信息窃取、远程控制功能的木马后门。

2020年5月，有国外机构披露，疑似与越南有联系的黑客组织 APT32（海莲花 OceanLotus）在过去的数月中，持续对我国重要卫生医疗机构发起网络攻击，以获取和新型冠状病毒相关的重要信息情报。该黑客组织用名为“冠状病毒实时更新：中国正在追踪来自湖北的旅行者.docx”、“湖南省家禽 H5N1 亚型高致病性禽流感疫情情况.docx”样本信息文件作诱饵，使用户执行木马程序，最终达到控制系统、窃取情报的目的。本轮攻击还使用了白利用手法绕过了部分杀毒软件的查杀。

三、微博 5.38 亿账号信息在暗网出售

2020年3月，5.38亿条微博用户信息在暗网出售，其中1.72亿条有账户基本信息，包括：用户名、关注数、地理位置、最后一次微博发布时间等微博公开信息，售价1388美元。有新京报记者在 Telegram 上向灰产人士购买了价值约12元人民币的积分，获得了201条微博用户信息，其中不少信息包括用户身份证号、手机号、密码、生日等私密信息。对于灰产人士提供的微博定向查询手机号服务，记者测试查询了3个已绑定手机的微博账号，结果有2个微博账号被查询到了正确的关联手机号码，其中1个还给出了微博绑定的QQ等更详细的信息。

四、新型比特币勒索病毒 WannaRen 爆发

2020年4月初一款名为 WannaRen 的勒索病毒爆发，在国内引起

网民热议。该勒索病毒由“匿影”家族进行传播。“匿隐”家族主要通过 BT 下载器、激活工具等传播病毒，曾在被攻陷机器上利用永恒之蓝漏洞用工具包攻击内网其它机器。它与 2017 年大爆发的 WannaCry 病毒类似。当用户电脑系统被入侵后，会弹出勒索对话框，提示勒索目的并向用户索要比特币。用户电脑上的所有重要文件都会被加密，加密文件的后缀名被统一修改为“.WNCRY”。用户电脑一旦被勒索病毒侵入，只能通过重装操作系统的方式来解除勒索行为，但是用户重要数据文件无法被直接恢复。

五、中国台湾发生重大个人数据泄露事件

台当局内务主管部门日前疑似遭黑客入侵，导致台湾超过 2000 万笔的个人信息被放在暗网贩售。有境外信息安全网站发现，在透过特殊方式才可以连接上的暗网中，有一个叫做“台湾房屋登记数据库”的档案，大小约 3.5GB，其中有超过两千万条台湾民众个人资料，内容包含姓名、地址、身分证字号等等。目前中国台湾人口为 2380 万人，这意味着几乎全体台湾人民的个人数据都遭到了泄露。

六、无锡市公安局破获全国首起“暗网”平台案件

“暗网”具有网站的使用者、访问者不可被追踪的特点，具有极强的匿名性和保密性。侦查难度比较大，“暗网”网站上交易的往往是一些非法的内容和商品，比如公民信息、电脑病毒等。无锡警方联合腾讯网御、微步在线等国内知名网络安全公司结成战略合作联盟，充分整合警企技术优势，一举锁定网站开办人真实身份情况。无锡警方专案组转战河北石家庄、北京等地，成功抓获了开办该“暗网”网

站的嫌疑人王某。涉“暗网”平台犯罪目前仍然是全球各国警方面临的难题，此前仅有美国破获的“丝绸之路”、德国破获的“华尔街市场”等少数直接打击暗网平台的成功案例。

通过这些事件，我们可以看到风靡全球的勒索病毒、各种手段的入侵、防不胜防的个人信息泄露等网络安全事件让我国网络安全面临层出不穷的新问题。维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。只有把网络安全意识上升并贯彻到全社会的层面中，网络安全的防线才能牢驻不倒。以下为常见的网络安全风险与防范方法。

一、计算机病毒

主要传播方式：

网页挂马传播：用户不小心访问了恶意的或被攻破的网站，浏览器自动下载病毒。

捆绑传播：病毒被其它恶意软件作为载荷下载。

邮件传播：病毒作为垃圾邮件的附件。

漏洞传播：病毒通过漏洞进入计算机系统。

社交网络传播：病毒以图片或者其它恶意文件为载体通过社交软件传播。

防范方法：

防毒杀毒：尽量到官方网站下载软件，安装正规杀毒软件，运行下载软件之前先进行病毒扫描。

及时更新：关注操作系统安全公告，及时安装安全补丁，尽早堵

住漏洞。

封堵端口：关闭无用的端口，如文件和打印共享功能。文件和打印共享有时是非常有用的功能，但是这个特性也会将你的计算机暴露给寻找安全漏洞的黑客。一旦进入你的计算机，黑客就能够窃取你的个人信息。

开启防火墙：开启 Windows 防火墙，减少被攻击的“通道”。

做好备份：使用光盘、移动硬盘等介质，对文档、邮件、数据库、源代码、图片、压缩文件等各种类型的数据资产定期进行备份并脱机保存。

警惕陌生文件：不要打开来自陌生人的电子邮件附件或打开及时通讯软件传来的文件。疫情期间要对邮件或其他渠道传播的与疫情相关的文件保持警惕，不要随意下载或打开文件名中带有“武汉疫情”、“新型冠状病毒”等热点词汇的 exe、csr 等可执行文件，这些文件可能包含木马程序。

二、个人信息泄露

泄露途径：

钓鱼网站泄露信息：黑客伪造与官网相似的域名和网页，用户在访问这些网页时被盗取个人账户信息。

社交软件泄露信息：用户使用社交软件聊天、晒照片时，无意间透露工作内容、工作地址、孩子的姓名学校，车票机票信息等，这些都有可能被不法份子利用。

各类小程序泄露信息：不法份子会用一些星座测试、性格测试、

领取奖品等小程序来收集有效的个人信息。

热点 wifi 泄露信息：在酒店、商场、车站等公共场所一般都设有免费 WIFI，这些无线网络的安全防护功能比较薄弱，不法份子很轻易地就能盗取用户的个人信息。

证件复印件泄露信息：用户在注册账户或办理业务时，常常都需要提供身份证复印件或者照片。若使用不当则很容易被不法份子获取。

弱密码泄露信息：个人账户密码薄弱时，不法份子可以轻松破解并获取个人信息甚至财产。

防范方式：

使用官网：在官方网址登录各账号。使用正规的、运营规范的网站是最基本的，不要使用小网站。网购交易时，不要另外加私人 QQ、微信等。

警惕小程序：凡是要求输入个人信息领取红包、星座测试、性格测试等都不要参加。

使用安全的网络环境：网上支付或处理重要文件时应确保在安全的网络环境中，如公司、家里这样的专属网络。如果在外进行操作，则应该使用流量数据上网，不要使用公共场所的 WIFI。

主动保护身份信息：不轻易将身份证复印件和照片给他人，必要时在身份证照片上打上水印，注明限制使用途径：“仅作为 XXXX 使用，他用无效”这类字眼，以防他人盗用。

避免弱口令：涉及个人信息的网站上，注册时使用的用户名和密

码最好都做到不一样，避免一个网站账户被盗，其他网站账户都遭殃。

密码的设置最好和自己的姓名和生日没有太大的关联性。

及时关注：关注信息泄露事件，及时调整设置口令、更换信用卡等。

三、密码安全

密码破解手段：

暴力破解：尝试所有可能的口令，越简单越短越易猜！例如，6位的数字口令有100万种可能，但借助口令破解软件可以读秒破解。

字典攻击：以标准词典或根据用户个人信息构造可能口令列表，可进行快速搜索攻击。

网络嗅探：口令不光本地用，还会经常上网。如果传输没加密，黑客怎能轻易截获。

拖库和撞库：一个网站的用户名口令数据库泄露（被拖库），攻击者拿着用户名口令到其它网站撞运气。

防范方式：

避免弱口令：用登录名、单词、曾经用过的口令、键盘上相邻的键，如qwerty、个人信息相关，如电话、生日等作口令都不安全。

设置强口令：设置口令时，至少使用8个字符，包含至少大写和小写字母（例如A-Z, a-z），包含至少一个数字（例如0-9），如果系统支持尽可能加入特殊字符（例如`!@#\$%^&*()_+=`），不同网站设置不同的用户名、口令。如果是很重要的密码，可以使用KeePass等软件来帮助管理口令。

(来源：苏州大学信息化建设与管理中心，2020年08月17日)