关乎你、我、他的生存和安危

漏洞

齐向东 著

VULNERABILITY

About You and Me
About Survival and Safety

同济大学出版社
TONGJI UNIVERSITY PRESS

漏洞

齐向东　著

同济大学出版社

图书在版编目（CIP）数据

漏洞 / 齐向东著. －上海：同济大学出版社，2018.8

ISBN 978-7-5608-8075-4

Ⅰ. ①漏… Ⅱ. ①齐… Ⅲ. ①计算机网络－网络安全－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2018）第180847号

漏洞

齐向东 著

出版策划人 李舒

出品人 华春荣

责任编辑 卢元姗 熊磊丽

责任校对 徐逢乔

封面设计 钱如潺

出版发行 同济大学出版社 www.tongjipress.com.cn

（地址：上海市四平路1239号 邮编：200092 电话：021—

65985622）

经　　销　全国各地新华书店

排版制作　南京展望文化发展有限公司

印　　刷　浙江广育爱多印务有限公司

开　　本　787mm×1092mm　1/16

印　　张　20.75

字　　数　415000

版　　次　2018年8月第1版　2018年8月第1次印刷

书　　号　ISBN 978-7-5608-8075-4

目　录

前言

前不久，在新员工入职360企业安全集团的训练营开营仪式上，我分享了一个感受：人生就是不断“二选一”的过程，每个看似无关紧要的“二选一”都会改变你以后的人生轨迹。

回首我自己的经历，在学生时代，我选择了每天比别人多学五小时，成为优秀的毕业生，摆脱了农民的宿命。参加工作后，我选择了没有怨言的付出，成为当时新华社里最年轻的局级干部之一。互联网大潮初起之际，我辞职下海，没有选择在大公司当高管，而是选择了与周鸿祎共同创办360。

这十几年，中国互联网产业飞速发展，我一直在思考和探索一个问题，是什么推动了互联网产业的发展？

不满足现状矛盾的渴望，推动互联网应用的发展。十九大报告指出，我们现在社会的主要矛盾是人民日益增长的美好生活需要和不平衡不充分的发展之间的矛盾。互联网应用的发展正是解决不平衡不充分发展的问题，搜索、移动支付、电子商务……一系列互联网应用的出现，解决了信息不对称的问题，提高了效率，美好了人们的生活。

不满足技术缺陷的渴望，推动互联网技术的飞跃。互联网的很多技术，都是基于对缺陷的改进，是不断快速迭代的发展过程。就拿360来说，每一代技术的创新，都是在与网络攻击浪潮的攻防对抗中产生的。病毒的大规模增长，黑名单的瞬息万变，推动我们创新了“白名

单”的第二代网络安全技术；APT攻击逐渐成为网络攻击主流，“白利用”攻击手段的多样化，推动我们创新了“查行为”的第三代网络安全技术。

不满足制度欠缺的渴望，推动互联网规则的完善。回想一下，欧盟《通用数据保护条例》的实施、我国网络安全法的出台、电子商务法的拟出台……一系列法律和规章，都是针对在经济社会发展中遇到的制度缺陷所采取的补救措施，规则的完善将推动互联网产业更健康地发展。

发展的路上有光明，也有阴影的存在。很多人背离了初心，利用手中掌握的技术、制度的漏洞，变得不择手段，网络“黑产”的规模正在指数级地快速增长，影响社会和人民稳定生活的高级别网络攻击正在不断发生。同时，在我们貌似强大的背后，也存在着自主信息技术的隐忧，与美国的贸易摩擦，戳穿了虚假的繁华。

没有安全的环境、载体、制度和保障，我们只是在透支互联网的价值，终将成为水中月、镜中花。

2015年，我创办了360企业安全集团。这是我人生中再一次重要的“二选一”。第四次工业革命的浪潮将把人类社会带进智能时代，现在我们所使用和遵循的传统IT的方法，都将成为过去时。在以往的信息化建设时代，发展是主，安全是辅。但在人工智能时代，人工智能、大数据、物联网是基础，安全成为发展的前提。人们的衣食住行都在被快速网络化，更重要的是，水电、煤气、地铁等关键信息基础设施全部联网以后，攻击者不费一枪一炮，通过网络攻击就可以战胜一个国家，这将是未来战争的形态。可以说，没有网络安全，就没有一切。

“有道无术，术尚可求，有术无道，止于术。”如果说，网络安全是互联网发展的“道”，漏洞则是互联网安全的“术”。

要谈网络安全，必须说清漏洞。若只谈漏洞，则不知言之所谓。本书从漏洞入手，谈网络安全，谈360企业安全集团的价值观。

齐向东

2018年7月6日

Chapter 1
第一章
善与恶漏洞是造成危害，还是推动进步

在漏洞的海洋里，我们看到的永远只是浪花。

我一直在思考一个问题，什么是推动互联网发展和完善的动力。按照马克思主义的哲学观点，社会基本矛盾是社会进步的根本动力；社会进步是社会本身的自我否定即“扬弃”的过程。

在互联网领域，矛盾体现在哪里呢？体现在技术、设备、制度、行为的缺陷方面，也就是人们常说的“漏洞”。

漏洞有危害吗？答案无疑是肯定的，危害通常就发生在身边，还毫无察觉。

漏洞只有坏处吗？不，它还在推动互联网的革命和进步。

从技术发展的角度来看，人从会使用工具开始，到逐渐掌握各种客观规律，再到今天网络社会的高度发达，人的本质都是在尝试凭借自身的能力和外力工具来补上各种短板，克服漏洞，追求完善。所以，高尔基才说：“人生的意义就在于人的自我完善。”

因此，无论我们是否追求自我完善，无论我们的能力、金钱和社会地位如何，漏洞都会裹挟着我们，左右着我们的生活，时刻与我们相伴。

“一念善，皆是善。一念恶，皆为恶。”凭借掌握的漏洞，有人为恶，有人行善。人如是，社会也如是。

第一节　漏洞，源自人性的缺陷

曾经有领导问我：“漏洞是天生的吗？”我不假思索地回答：“是天生的。因为漏洞是客观存在，而且无法消灭干净的。”领导追问：“既然是天生的，为什么设计者自己找不出来，需要你们去找？而且，被利用的可以叫漏洞，没被利用，能叫漏洞吗？”这个问题引起了我的认真思考。

天生缺陷，难免漏洞

辞典里对“漏洞”一词的解释有两个：一是小孔、缝隙；二是法律、法令、条约或协议中制订得不周密的地方，破绽。

我对漏洞的理解是：漏洞本质上是被利用的缺陷。就像一条船的船底和船舱门板上都有一个小孔，这两个小孔都是缺陷。其中，船底的小孔会导致进水，最终船毁人亡，所以它就是漏洞。

法律条文里可能有若干缺陷，能被利用的是漏洞，犯罪分子可能凭借漏洞逍遥法外；金融运行体制里也可能有不少缺陷，能被利用的才是漏洞，抓住这个漏洞可能赚得盆满钵满；甚至我们人也是一样，生来有多疑、贪婪等很多缺陷，一旦被利用，就会带来失败和痛苦。

1946年2月，世界上第一台电子数字式计算机埃尼阿克在美国宾夕法尼亚大学正式投入运行，此后万维网逐渐建立，世界开始以一种更紧密的方式联系在一起。与技术相伴随的，是技术中存在的一个个缺陷。

“漏洞”一词，在有了互联网技术后，更多时候是一个被用于计算机领域的专有名词。由于缺陷是天生的，漏洞是不可避免的，因此网络被攻击是必然事件。

▶漏洞——利用人性的博弈

拿破仑曾经说：“我是我自己最大的敌人，也是自己不幸命运的起因。”人，与生俱来就有贪婪、自私、猜疑、虚荣、恐惧、固执等弱点，当这些缺陷被利用时，就演变成致命的漏洞。因此，我认为，漏洞存在三个支点：漏洞因人而生，因人心而用，因人性而决定使用之道。

三国时期，魏国派大将军司马懿挂帅进攻蜀国街亭，诸葛亮派马谡驻守失败后，司马懿率兵乘胜直逼西城，诸葛亮无兵迎敌。但他沉着镇定，大开城门，自己在城楼上弹琴唱曲。本就生性多疑的司马懿怀疑设有埋伏，引兵退去。这是《三国演义》第九十五回的故事，是民间著名的空城计故事。诸葛亮正是准确把握了司马懿多疑而谨慎这一心理缺陷，利用主帅的这个心理“漏洞”，使其错误判断了局势。

空城计并非诸葛亮首创，《三国演义》也不是第一本描述这一计策的书。作为心理战的一种重要方式，它源于我国古代的军事杰作《三十六计》。书中第三十一计“空城计”，就是充分利用人的猜疑这一弱点。原文中有一句“虚者虚之，疑中生疑”，说的就是让敌人在疑惑中更加产生疑惑，造成错觉，从而在敌众我寡的情况下惊退敌军的战术。

“心理战”，本质上研究的就是如何充分利用人心理上的缺陷，把其打造成致命漏洞的方法，军事活动中尤为多见。

诸葛亮和司马懿的这一战虽然是虚构的故事，但历史上确有许多真实战例。从我掌握的史料来看，我国历史上第一个使用空城计的例子可

以追溯到春秋时期。

春秋时期，楚国的令尹公子元，在哥哥楚文王死后，非常想占有漂亮的嫂子文夫人。他用各种方法讨好，文夫人都无动于衷。于是他想建功立业，显示自己的能耐，以讨文夫人欢心。

公元前666年，公子元亲率浩浩荡荡的兵车六百乘攻打郑国。楚国大军一路连下几城，直逼郑国国都。郑国国力较弱，都城内更是兵力空虚，无法抵挡楚军的进犯。郑国危在旦夕，群臣慌乱，有的主张纳款请和，有的主张拼一死战，有的主张固守待援。这几种主张都难解国之危。上卿叔詹说：“请和与决战都非上策。固守待援，倒是可取的方案。郑国和齐国订有盟约，而今有难，齐国会出兵相助。只是空谈固守，恐怕也难守住。公子元伐郑，实际上是想邀功图名讨好文夫人。他一定急于求成，又特别害怕失败。我有一计，可退楚军。”

郑国按叔詹的计策，在城内做了安排。命令士兵全部埋伏起来，不让敌人看见一兵一卒。大开城门，放下吊桥，摆出完全不设防的样子。又令店铺照常开门，百姓往来如常，不准露一丝慌乱之色。楚军先锋到达郑国都城城下，见此情景，心里起了怀疑，莫非城中有埋伏，诱我中计？先锋不敢妄动，等待公子元。公子元赶到城下，也觉得好生奇怪。他率众将到城外高地眺望，见城中确实空虚，但又隐隐约约看到了郑国的旋旗甲士。公子元认为其中有诈，不可贸然进攻，决定先进城探听虚实，于是按兵不动。

这时，齐国接到郑国的求援信，已联合鲁、宋两国发兵救郑。公子元闻报，知道三国兵到，楚军定不能胜。好在也打了几个胜仗，还是赶快撤退为妙。他害怕撤退时郑国军队会出城追击，于是下令全军连夜撤走，人衔枚，马裹蹄，不出一点声响。

所有营寨都不拆走，族旗照旧飘扬。

第二天清晨，叔詹登城一望，说道：“楚军已经撤走。”众人见敌营族旗招展，不信已经撤军。叔詹说：“如果营中有人，怎会有那样多的飞鸟盘旋上下呢？他也用空城计在欺骗我，已急忙撤兵了。”

这就是中国历史上第一个使用空城计的战例。双方都使用了空城计，都是以为或者想当然地以为自己利用了对方的弱点。在中国的战争史中，空城计、利用心理漏洞的案例屡见不鲜，毛泽东在解放战争中巧妙用计吓退了国民党十万大军的案例堪称经典、精彩。

1948年10月下旬，当中国人民解放军在前线取得节节胜利的时候，中共中央得到北平地下党的紧急情报：驻守北平的蒋傅军，趁华北野战军主力远在绥远地区作战、冀中一线兵力空虚之际，决定以骑兵第九十四军、新编第二军共计10万余人的兵力，组织一支快速机动部队，经保定偷袭石家庄和西柏坡。

当时，解放军华北军区留守西柏坡的兵力只有1个约千人的团。华北军区共有3个兵团，一兵团在山西对付阎锡山部队，三兵团在绥远，只有二兵团在平绥路东段附近。从北平到石家庄有600多里，其中北平到保定300里的铁路线基本被国民党军队控制。保定到石家庄也只有300多里的路程，敌军快速机动部队只需两天，最多三天即可到达石家庄。华北二兵团从平绥路东段，即使日夜兼程，赶到保定以南地区也要四天，石家庄告急。

面对这一严峻形势，中共中央领导人立即紧急研究对策，进行了周密部署。

一方面，中共在军事上调动了部队和民兵以抗阻奔袭南进之敌；另一方面，运用新华社等媒体发动宣传攻势，揭露敌人的偷

袭阴谋。在这场特殊的宣传战中，毛泽东亲自组织和撰写了几篇重要新闻。

第一篇是胡乔木起草、毛泽东修改的新闻稿《蒋傅军妄图突袭石家庄》（新华社10月25日播出），把蒋傅军企图突袭石家庄的消息及时公布于众。

第二条消息是毛泽东写的《华北各首长号召保石沿线人民准备迎击蒋傅军进扰》（新华社10月26日播出），把这次偷袭的兵力组成、指挥官名单、装备等，揭露得一清二楚。甚至是明明白白地告诉敌人，解放区军民早已做好充分准备，严阵以待，必将歼灭敢于来犯之敌。

第三篇是毛泽东写的口播稿《蒋傅军已进至保定以南之方顺桥》（新华社10月29日播出）。文章报道郑挺锋率其两个师在28日推进到保定以南的方顺桥地区，显示解放军对敌人的具体行动了如指掌，一切均在我掌握中。

第四篇是毛泽东写的述评稿《评蒋傅军梦想偷袭石家庄》（新华社10月31日播出）。这篇评述把国民党面临的垂死挣扎的局势、偷袭石家庄的真实意图和经过等，剖析得一清二楚。

新华社播发的这些新闻，起到了巨大的震慑作用。在华北军区第七纵队和地方武装的顽强阻击下，进扰之敌进展缓慢，10月30日进到定县以北的唐河后再不敢冒进。与此同时，华北野战军第三纵队也已陆续赶到。这次偷袭的敌军指挥、第九十四军军长郑挺锋报告傅作义，称：“昨收听广播，得知对方对本军此次袭击石门（注：石家庄旧称石门）行动似有所警。广播谓本军附新二军两师拟袭石门，彼方既有所感，必然预有准备，袭击恐难收效。”傅作义得知阴谋暴露，大为吃惊，他见中共方面不仅详知自己的计划，做了准备，还有了歼灭部署。“疑中生疑”使他惧怕遭到埋伏，为了确保平津地区的防御，只好撤回军队，偷袭阴

谋彻底破产。

这场中共与国民党的对战中，首先是中共利用对方的漏洞获取了重要的军事情报，又利用傅作义的心理漏洞，毛泽东巧妙运用舆论武器，发动宣传攻势，导演了一幕中国现代史上的“空城计”，成为历史上的一段佳话。

▶互联网世界的“飞蛾效应”

在计算机领域，漏洞特指系统的安全方面存在缺陷，一般被定义为信息系统的设计、编码和运行当中引起的、可能被外部利用用于影响信息系统机密性、完整性、可用性的缺陷，英文单词是“vulnerability”。

但在日常生活中，人们经常用口头语“bug”来形容计算机程序中有漏洞，这与一只小飞蛾的故事有关。

20世纪40年代，美国海军中尉、电脑专家格蕾丝·霍波（Grace Hopper）的主要任务是编写软件，她曾为世界上第一部通用计算机Mark Ⅰ，以及后续机器Mark Ⅱ、Mark Ⅲ编写了大量软件。一次，她为Mark Ⅱ的17000个继电器设置好程序后，技术人员进行整机运行，此时Mark Ⅱ突然停止了工作。她在Mark Ⅱ计算机的继电器触点里找到了一只被夹扁的小飞蛾，正是这只小虫子“卡”住了机器的运行。霍波将这只飞蛾夹到工作笔记里，并诙谐地用“bug”来表示导致程序出错的原因。

但霍波没有想到的是，她这个举动给单词“bug”赋予了一个新的含义，在未来互联网时代中，它成为指代程序缺陷的通用词。继电器里飞进飞蛾，这本是偶然事件，但程序一定存在缺陷，一定会被有意或无意地利用，我想，这可以称作互联网世界的“飞蛾效应”。

▶漏洞是怎样炼成的

统计表明，程序员每写1000行代码，就会有1个缺陷，一个大型的IT应用系统，代码行数动辄几十万行，甚至更多。可以说，从世界上第一个操作系统或应用软件诞生的那天开始，缺陷就存在于IT系统的各个环节，而且始终会存在。

首先，漏洞来自操作缺陷。

程序员编程序时的疏忽、运维人员设置安全配置时的不当操作、用户设置的简单口令和泄露……这些人为的、无意的失误就是操作缺陷。

比如，微软每个月的第一个星期二叫补丁日，用户每个月都会收到提示，提醒你给系统漏洞打上补丁。在我的印象里，微软每个月平均打的补丁有几个到几十个不等，这意味着微软每个月至少会有几个到几十个漏洞。

这些年，我们不断给微软、苹果、谷歌、Adobe、VMware等用户覆盖全球的软件公司提交漏洞。2017年，我们提交了519个漏洞，连续两年位居漏洞致谢数全球第一。

其次，漏洞来自认知缺陷。

漏洞会随着时间推移而产生，在其产生之前，我们对这个问题是没有认知的。比如2000年的“千年虫”危机。这个危机的根源始于20世纪60年代，当时计算机存储器的成本很高，如果用四位数字表示年份，就要多占用存储器空间，增加成本。为了节省空间，计算机系统的编程人员采用两位十进制数来表示，比如1980年就是80，到1999年，80年出生就

是99—80=19岁，20世纪90年代末，大家突然意识到，用两位数字表示年份将无法正确辨识公元2000年及其以后的年份，因为到了2000年，就会变成00—80=—80岁了。这无疑将引发各种各样的系统功能紊乱甚至崩溃，这就是所谓的“千年危机”，这一危机正是由于认知的局限性造成的。

还有一个典型的例子是2018年1月曝光的安全漏洞“熔断”（Meltdown）和“幽灵”（Spectre）。为了提高CPU处理性能，芯片企业用乱序执行（Out-of-Order Execution）和预测执行（Speculative Prediction）。通俗的理解就是，CPU并不完全严格按照指令的顺序来执行，而是会自己预测可能要执行的内容，以及为了更好地利用CPU资源将指令顺序打乱，以便能同时执行一些指令。

但设计者没有考虑到，或者没有认为这个问题是重要的，即：由于CPU缓存内容没有同步恢复到原始状态，导致缓存中存储的重要信息可以被漏洞利用者获取，可能会造成受保护的密码和敏感信息泄露。

这也是认知缺陷造成的。虽然当前还没有任何黑客们从漏洞中获取利益，但由于“熔断”和“幽灵”两大漏洞是芯片底层设计上的缺陷导致的，在短时间内无法从根本上消除漏洞，需要产业链一起携手解决。目前，英特尔、ARM、AMD、苹果、谷歌等企业以及产业链相关企业都在积极修复和更新软件，应对漏洞存在的安全威胁。

最后，漏洞来自知识缺陷。

很突出的一个例子就是工控安全。原本的工业控制系统，大多以系统功能作为第一要素，多数系统在设计之初是封闭的“单机系统”，连联网需求都没有考虑过，就更不要提在设计、研发和集成阶段考虑网络

安全问题了。物联网时代到来以后，这些工控系统都开始在互联网上“裸奔”，黑客可以轻而易举地利用系统漏洞进行攻击，造成严重后果：

2007年，加拿大一个水利SCADA控制系统被入侵，取水调度的控制计算机被破坏；

2008年，波兰某城市地铁系统被入侵，导致四节车厢脱轨；

2010年，伊朗核设施遭受“震网病毒”攻击，严重威胁核反应堆安全运营；

2011年，美国伊利诺伊州城市供水系统遭入侵，致使供水泵遭到破坏；

2012年，发现攻击多个中东国家的恶意程序Flame火焰病毒，能收集各行业的敏感信息；

2013年，以色列Haifa公路控制系统遭受黑客入侵，造成数千美元的损失和严重的后续问题；

2014年，黑客入侵土耳其某石油管道网络系统，导致石油管道大幅增压，发生爆炸；

2015年，乌克兰电厂被黑客入侵导致数十万户家庭断电，并在2016年被再次攻击导致断电；

2016年，全球首次大规模物联网攻击，导致美国东海岸大面积断网，严重影响当地人民生活秩序和社会稳定；

2017年，“永恒之蓝”勒索病毒肆虐全球，多个基础设施瘫痪……

国家工业信息安全产业发展联盟统计的数据显示，2016年至2017年，全球工业信息安全漏洞增长率超过50％，当下，我国工业控制系统95％以上存在漏洞，其中，65％属于中高危漏洞，33％属于高危漏洞。

漏洞不等同于缺陷

并不是所有的缺陷都是漏洞，只有可以被外部利用的缺陷才称为漏洞。这句话可以换一个角度来理解，当利用缺陷的方法出现时，漏洞导致的现实威胁就出现了。就像“心脏滴血”漏洞，引发这个漏洞的缺陷在爆发前两年的版本中就已经静悄悄地存在，当黑客利用这个缺陷获取服务器里用户的敏感信息，影响了数据的机密性，就构成了漏洞。

2014年4月，全球爆发了一次严重的网络安全事件。黑客利用“心脏滴血”（Heartbleed）漏洞获得用户的银行密码、私信等敏感数据。全球在线支付、电商网站、门户网站、电子邮件等重要网站纷纷中招。

“心脏滴血”好比互联网的心脏出了问题，从这个漏洞的名字就可以看出事件的严重性。黑客可以利用这个漏洞，向全球的网站发起攻击。也许有人会产生疑问，一个漏洞真的能引起这么大的危害吗？

原因在于这个漏洞存在于一个通用的安全套件——OpenSSL中。OpenSSL囊括了主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议，在全世界各大网银、在线支付、电商网站、门户网站、电子邮件等重要网站中被广泛使用。比如在浏览器地址栏常见的https前缀的网址以及小锁图标，通常就是指该网站经过SSL证书加密。

OpenSSL好比一把保护用户信息安全的锁，当它出现漏洞，就变成了一把废锁，不用钥匙都能打开。黑客利用这个漏洞每发起一次攻击，服务器就能泄露一点数据（理论上一次最多泄露64K）。黑客只要有足够的耐心和时间，就可以获得足够多的敏

感数据。

当时，国内超过3万台主机受到波及。网易、微信、QQ邮箱、陌陌、雅虎、比特币中国、支付宝、知乎、淘宝网、京东、YY语音……从消费到通讯、社交，国内知名网站几乎无一幸免。

为了抢修网站中的漏洞，国内网站和安全厂商技术人员彻夜不眠。有的连夜测试有多少网站受到影响；有的统计漏洞信息，并向客户解释问题的严重性；有的开始紧急预警，及时修复升级系统版本……当然，全球的黑客也不睡觉了，因为他们要抢在安全人员补上这个漏洞之前，在全球的网站上偷取信息。幸好，OpenSSL官方很快发布了漏洞的修复方案。当天下午，淘宝、京东等网站就修复完毕。

其实，这个漏洞在两年前的版本中就已经静悄悄地存在，只是一直没有被曝光。直到2014年4月，谷歌一支研究团队和芬兰安全公司科诺康（Codenomicon）的研究人员曝光了这个漏洞，才引起人们的重视。

没人知道有多少数据已经被泄露，更没有人知道在漏洞存在的两年期间，有多少黑客利用这个漏洞发起过网络攻击。

“心脏滴血”漏洞是网络安全领域的一次标志性事件，它充分表明，虽然漏洞的本质是一种缺陷，但不完全等同于缺陷，当这个缺陷能被利用，进而产生安全性危害时，缺陷才成为漏洞。

所以我说，缺陷是天生的，漏洞是不可避免的，网络攻击是必然的。

第二节　一切漏洞皆被利用

缺陷是怎么被利用的

下面我将列举政治、经济等领域中互联网漏洞的一些真实案例，重现缺陷被利用的过程，也就是重现一个漏洞是怎么影响国家机密信息安全、政治选举和商业交易的。

▶泄露国家重要机密的漏洞

——新加坡遭最大规模网络安全攻击，李显龙信息外泄

2018年7月20日，新加坡卫生部表示，新加坡某保健集团遭黑客攻击，150万人的个人信息被非法获取，其中包括新加坡总理李显龙本人和政府多名部长的配药记录、门诊信息也被黑客获取。这起事件被当地媒体称为“新加坡遭遇的最大规模网络安全攻击”。李显龙表示，此次网络攻击的目标是他本人，黑客为盗取他的门诊配药记录进行了多次尝试，希望找到一些国家机密或令他本人难堪的信息。

据新加坡《联合早报》报道，黑客以恶意软件入侵了新加坡某保健服务集团的系统，从2018年6月27日至7月4日盗取了150万名病患的个人资料，其中16万人的开药记录也被盗窃。失窃的个人资料包括姓名、身份证号码、地址和出生日期等。

新加坡总理李显龙当天表示，此次网络攻击的目标是他本人，黑客为盗取他的门诊配药记录进行了多次尝试，希望找到一些国家机密或令他本人难堪的信息。

新加坡网络安全局负责人表示，黑客的攻击行动是蓄意和精密筹划的。他们先从新加坡某保健服务集团的电脑侵入，植入恶意软件后，有目标地攻击其数据库中的具体个人资料，不断试图盗取和复制总理李显龙的个人医疗记录并顺利得逞。

新加坡卫生部表示，他们将进行一次彻底的公共卫生保健系统检查，以提高防范网络攻击、侦查和响应的能力。对于在新加坡非法获取信息或泄露隐私的行为，政府将采取严肃态度对待，并针对此事成立调查委员会进行彻查。

——美国国家安全局（NSA）数字武器库遭黑客攻击

2017年3月，维基解密发布了近9000份美国中央情报局（CIA）的机密文件，显示其网络情报中心拥有超过5000名员工，利用硬件和软件系统的漏洞，总共设计了超过1000个黑客工具。利用这些工具可秘密侵入手机、电脑、智能电视等众多智能设备，比如三星智能电视被攻击后能变为可录音的窃听器。

维基解密表示，公布的这些文件只是第一部分，不到中情局文件的1%，这是中情局迄今为止最大规模的机密文件泄露事件。维基解密还披露，这些“黑客武器”面临着失控风险，最近中情局称“对其黑客武器库中的大部分工具失去控制”，这些工具“似乎正在美国前政府的黑客与承包商中传播”，存在“极大的扩散风险”。

不只是CIA，NSA也未幸免。

2016年8月13日，黑客组织“影子经纪人”声称攻破了为NSA开发网络武器的“方程式组织”的系统，获取了其用于网络攻击的网络武器库。从2001年开始，“方程式组织”就在帮助美国国家安全局开发网络武器，利用软件漏洞作为网络武器，协助美国

政府在全球各地进行网络攻击。

为了证明自己确实黑掉了NSA旗下的全球顶级的黑客部队，“影子经纪人”在网上释放出了一些“方程式组织”的武器库文件供安全界各路专家围观鉴定。他们将盗取的大量黑客工具和漏洞利用代码，以5.65亿美元的价格在网上打包出售。他们在宣布此消息的同时公布了第一批工具，并在2017年1月13日、2017年4月9日、2017年4月14日分别再次公布了另外3批相关工具。

360威胁情报中心对这些网络武器进行了分析，第一批公布的工具主要是针对边界设备，也就是我们经常说的防火墙的漏洞利用工具。比如我国大量使用思科的路由器和防火墙，NSA曾经利用基于思科防火墙的漏洞工具，控制过运营商、高价值企事业单位的网络基础设施，通过重定向网络流量窃取秘密信息、提取重要情报，甚至可以通过篡改数据，实施毁灭性的破坏。

第二批公布的工具主要是NSA黑客组织使用的一些样本。第三批公布的工具主要是针对Unix类系统的远程漏洞利用工具及后门模块。

第四批公布的工具主要是针对Windows系统，包含了一套远程漏洞攻击的通用技术框架，通过这套框架黑客可以对一台Windows主机进行远程攻击。2017年5月肆虐全球的“永恒之蓝”（WannaCry）安全事件，利用的就是该武器库中的一个漏洞利用工具，传播蠕虫病毒。“永恒之蓝”勒索蠕虫攻击了150多个国家和地区的政府、机构和各类组织，在短时间内造成了巨大损失。

从目前被曝光的美国网络武器库信息中我们可以看到，基于漏洞的网络武器制造已经是庞大的系统工程，这些武器都讲究先进性、通

用性、易用性和隐蔽性。借助漏洞挖掘和利用能力，攻击者能打通网络隧道，每个攻击目标都可以成为一个网络节点，持久地控制被攻击目标。从事网络攻击的人员不需要非常强的技术功底，这些工具做得很易用，使用方式简单，并且有一整套的脚本来指导他们进行攻击。美国国家安全局和中情局的这些网络武器库的泄露，震惊了全世界。

这两个案例充分证明，漏洞带来的威胁无处不在。无论你是国家元首，还是NSA，在挖掘漏洞的黑客面前，都显得不堪一击。在万物互联的世界，大到国家和社会、小到机构和个人都面临着如何保护自身信息安全的问题。

▶影响美国总统竞选的漏洞

——利用脸书的漏洞盗取数据，挖掘数据，特朗普获得选举胜利

2018年3月16日，外媒曝光了著名社交平台脸书泄露用户隐私一事。美国一家名为“剑桥分析”的网络公司利用脸书开放平台的漏洞，获取到了5000万份的个人隐私数据。之后结合智能算法，这些用户就能被定向推送那些有利于支持己方候选人的消息和新闻，引导这部分人支持票数的走向。外媒称这间接地影响了2016年的美国总统大选。

事情的起因是“剑桥分析”网络公司在脸书平台上发表了一款“测试情绪”的小程序，用户只需完成测试便可获得5美元的奖励金。但没有天上掉馅饼的好事，一旦用户使用了这款小程序，系统就会获取测试用户的脸书个人信息，这些信息包括用户所在城市、工作内容、居住地址等。

2018年4月4日，脸书公司承认共有8700万用户隐私被泄露给

了剑桥分析公司，大大超出了此前媒体报道的5000万人。脸书首席执行官马克·扎克伯格（Mark Zuckberg）在美国国会上作证时证实，这些数据被政治咨询公司“剑桥分析”不当利用，用于向用户投放定向广告，并在2016年美国选举时支持特朗普团队。听证会结束后，一些重量级投资者呼吁脸书任命一位独立董事长来取代扎克伯格。

然而，这并不是最大的麻烦。据国外媒体报道，美国联邦贸易委员会（FTC）理论上最高可向脸书开出7.1万亿美元的罚款。2011年，FTC就对脸书用户数据保护问题进行过调查，脸书在同FTC达成的用户隐私和解协议中对外承诺，限制对外分享用户的信息，并阻止外部不正当的获取信息，每个违反规定的个案可处以最高4万美元的罚款。

一个脸书客户信息泄露事件最终演变成重大的政治事件、经济事件、金融事件、大数据事件，事件的严重程度远远超过公众预期。之所以引起各界如此程度的讨论，不仅在于8700万用户信息被泄露，更在于这关乎脸书等拥有海量数据的超级平台上该如何使用这些数据，以及如何堵住大数据被滥用的漏洞。特别是，大数据成为政治选举的工具，这是令人吃惊的。

——希拉里遭遇“邮件门”，竞选失败

大选中利用互联网漏洞的案例还不止一个。同样是在2016年美国总统大选中，呼声一度很高的希拉里最终落败。对于失败的原因，外界普遍认为媒体热炒的“邮件门”事件最终对希拉里的落选造成了致命影响。某种程度上说，希拉里“邮件门”事件直接改变了美国的政治格局。

希拉里“邮件门”的过程可以说是一波三折：第一次风波发生在2015年3月。希拉里被曝担任国务卿期间，在自己家里架设了服务器，用私人邮箱处理公务邮件，包括机密邮件，这严重违反了美国《联邦档案法》。迫于压力，希拉里承认用私人邮箱处理了大约6万封邮件，其中3万封因涉及私人生活已被其团队删除，剩余约3万封公务邮件已于2014年底全部上交国务院，算是暂时平息了第一次风波。

第二次风波发生在2016年7月22日，维基解密公开了美国民主党国家委员会内部绝密的近2万封邮件。泄露的账户来自民主党委员会中的7个重要人物，包括公关主任、国家财务总监、人事财务总监、数据和决策财务总监等。

维基解密公开的邮件揭露了希拉里涉及的多项“黑幕”。比如，勾结民主党高层、内定党内候选人，并参与“洗钱”和操控媒体；其公关部副主任在邮件中明确提议，冒充特朗普公司发布招聘“热辣女人”的帖子，给特朗普“泼脏水”；民主党委员会高管还列出了22个特朗普可以被攻击的主要黑点，利用一切营造特朗普“危险”形象等。

2016年10月8日，维基解密再次公开了希拉里竞选团队主席约翰·波德斯塔（John　Podest）私人邮箱里的数千封邮件。据外媒报道，约翰·波德斯塔在半年前曾收到一封警告邮件，这封宣称来自谷歌官方的邮件称，波德斯塔需要立即更改密码，因为有人试图侵入他的账号。但所谓的警告邮件其实是黑客发送的一封钓鱼邮件，导致邮箱被成功入侵，大量邮件泄露。

这些泄露的邮件显示，希拉里及其团队为赢得大选曾暗中派人去特朗普演讲现场闹事，她自己的克林顿基金会还接受过卡塔尔和沙特捐助，数目达到上千万美金，占其竞选资金的20%。这一系列丑闻使希拉里的竞选活动受到重击，希拉里的支持率不断

下跌。

第三次风波发生在大选前夕。2016年10月28日，距离大选还有10天左右，FBI局长詹姆斯·科米（James Comey）致信美国国会高层，宣布重启对希拉里担任国务卿期间使用私人服务器处理机密邮件的调查。原因是FBI在另一起与希拉里无关的调查中，发现了一些与希拉里“邮件门”调查相关的大量机密政务邮件，并且绝大多数都不在希拉里上交给国务院的邮件中。因此，FBI决定重启对邮件门事件的调查，这件事成为压垮希拉里的最后一根稻草。

“希拉里邮件门”事件是希拉里政治生涯里最大的一个转折点。一方面，希拉里通过私人邮箱处理公务的行为违反了规定；另一方面，维基解密公布的邮件曝光了她的多个丑闻，使得希拉里的人品和诚信度遭受质疑，选民对希拉里的支持率也因此大幅度下降。

以上两个案例展现出，在政治竞选和政治营销过程中，对系统和人性漏洞的利用会影响政治选举，甚至会直接左右政治选举结果。当影响力能被更加直接、却更加隐秘地以大数据的形式营销给每一位选民，并影响他们的态度时，被隐瞒、欺骗和利用的选民怎么可能不愤怒。但这显然不会阻挡西方政治家们继续利用网络漏洞的步伐。

▶造成巨大经济损失的漏洞

▶——墨西哥银行支付系统遭黑客袭击，损失数千万美元

2018年5月，墨西哥中央银行表示，黑客通过国内银行间支付系统从五家公司窃取了大约3亿比索（1535万美元），并利用数百次转账分散到不同账号，在全国数十家银行取现。

攻击发生在4月下旬，黑客利用各个银行和支付系统之间的联系发送虚假指令，将钱转到受控账号。墨西哥中央银行花了数周时间调查事情经过，但尚未找出黑客利用的手法。

据外媒报道，三家银行4月27日在软件筛查过程中发现漏洞，其他银行继而马上进入安全检测模式，发现巨款“窟窿”。墨西哥官方电子支付系统SPEI没有受到破坏，可能是由其他机构或第三方提供的连接支付系统的软件出现了漏洞。

墨西哥中央银行的银行间支付系统SPEI和SWIFT（国际通用的银行间结算系统）系统类似，每天可以转出数百亿美元资金。过去数年里，黑客通过入侵SWIFT系统已经窃取了数亿美元资金，包括孟加拉国中央银行、马来西亚中央银行、中国台湾远东国际商业银行、俄罗斯中央银行等均遭受过攻击。

▶——加拿大两家银行遭黑客攻击，9万名客户信息被盗

2018年5月，加拿大蒙特利尔银行（Bank of Montreal）和加拿大帝国商业银行（Canadian Impertial Bank of Commerce）的网上银行金融系统被黑客入侵。黑客采集了总计9万名账户持有人的个人信息，并威胁索要价值100万美元的赎金，否则将公布被窃取的客户信息。

这两起攻击事件很相似，两家银行事先均未发觉自身已遭入侵，直到犯罪分子发送勒索邮件要求支付赎金，才知晓情况并采取补救措施。邮件里还附加了数条被盗客户信息，包括姓名、身份证号、生日、余额等，这令两家银行的客户担心不已。

据媒体报道，黑客要求银行支付价值100万美元的XRP币（XRP币是区块链初创公司瑞波开发的一种加密货币）赎金。黑客在邮件中表示：“我们使用了一种算法创建账号，这些账号可

以冒充银行真正的账户持有人，由于银行没有双重认证安全功能，我们可以获取到两家银行客户相关信息。”

蒙特利尔银行是加拿大第四大银行，帝国商业银行是第五大银行。两家银行均表示，正在与警方合作，调查此次泄漏事件。

银行、支付巨头，这些与每个人密切相关的平台和场所，积累了每个人每天的支付和购买痕迹，更关键的是，支付信息这类隐私一旦泄露，就相当于将每一个人的财产安全置于公开的、危险的环境下。财产权在现代社会中与每一个人息息相关，经济信息一旦大量流失，如果不及时弥补和解决，随之而来的将是一触即发的社会危机。

上述这几个案例，是近些年来中外互联网领域被黑客攻击的众多事件中的冰山一角。随着信息社会不断深化演进，网络安全已经和国家安全、经济稳定、人民的衣食住行融为一体，难分彼此。无论是对国家层面、部门层面、企业层面，还是个人层面而言，漏洞引发的实际利益损失正在成倍增长。

内部威胁是最大的危害

古希腊典故“特洛伊木马”中，希腊联军围攻了一座名叫特洛伊的坚固之城，久攻不下后假装撤退，留下一具巨大的木马，特洛伊守军把木马作为战利品运进城中，木马腹中躲藏的希腊士兵深夜打开城门，特洛伊一夜间城陷国崩。从此，人们记住了这只有名的木马——特洛伊木马，更深深懂得了一个道理：最坚固的堡垒往往是从内部攻破的。

人类在历史走廊行进中，无数次重复地演绎着类似的故事。尽管数字时代的技术创新层出不穷，人仍然是每个组织网络安全中最强大和最

薄弱的环节，因为人是最重要和最脆弱的操作资源。一个组织可以花大量的资金购买技术解决方案来保护其网络边界，但仍然无法阻止来自内部的攻击。越来越多的攻击者利用社会工程学来瞄准最易受攻击的资产：人，然后从内而外攻击系统并达到自己的目的。

漏洞最大的来源，是人。我从FBI和犯罪现场调查（CSI）等机构联合做的一项安全调查报告上看到，超过85％的网络安全威胁来自内部，危害程度远远超过黑客攻击和病毒造成的损失。这些威胁绝大部分是内部各种非法和违规的操作行为所造成的。

在当今信息时代，组织机构面临的最大安全威胁，依然是源自内部人对于网络资源设备的攻击和对于机密数据文档的窃取，我们称其为内部威胁。内部威胁危害巨大，现有安全机制作用微乎其微，内部威胁现已成为攻破网络安全防线的最大敌人。

▶最坚固的堡垒总是从内部攻破的

2013年震惊全球的“棱镜门”事件是内部威胁的一个典型案例。爱德华·斯诺登（Edward Snowden）是美国从事涉密安全工作的一名承包商雇员，他利用职务便利获得了对关键性系统的访问权，从美国国家安全局拷贝了数十万份机密文件，并将这些资料提供给媒体发表，这些文件揭露了美国有史以来最大规模的一个秘密监控项目。斯诺登因此被媒体评价为“人类史上影响力最大的泄密者”，他凭一人之力，撬动了全球各国政府以及公众对信息网络安全的关注。

“内部威胁”是内部管控风险的表现。过去，我们把泄露公司机密信息的人称为“内鬼”或者“细作”，在信息系统领域则统称为“内部人”。简单来说，内部威胁就是由内部人威胁企业或组织安全的行为。

2012年，美国计算机安全应急响应组（CERT）基于其内部威胁的案例数据，提出了一个内部威胁的完整定义，明确了内部威胁中的主体与客体，在实际中具有很好的适用性，可以作为参考：

“内部威胁攻击者一般是企业或组织的员工（在职或离职）、承包商以及商业伙伴等，其应当具有组织的系统、网络以及数据的访问权；内部威胁就是内部人利用合法获得的访问权对组织信息系统中信息的机密性、完整性以及可用性造成负面影响的行为。”

根据上述定义，内部威胁包含了与企业或组织具有某种社会关系的所有个体，在职员工、离职员工、承包商、供应商、商业伙伴等都有可能构成内部威胁。

美国CSI/FBI在2008年公布的《计算机犯罪和安全调查》中对信息安全事件当中的事件来源做了统计，发现内部安全事件所造成的损失明显要高于外部事件。有时，一个内部威胁就会危及数十年的工作，可能会造成数百万或数十亿美元的损失，并可能影响国家稳定和社会的安全。

▶内部威胁的五件事

内部威胁和业务风险问题随处可见。在企事业单位内部，从来都不是风平浪静。不同角色的员工和用户出于不同的动机，以合法的身份，做出了不当的行为，对企事业单位带来了极大的危害。从内部威胁的类型来说，可分为数据泄露、供应链威胁、外包商威胁、间谍活动、蓄意破坏等。

数据泄露

2018年6月，特斯拉（Tesla）起诉了一名前员工，称其盗取了该公司的商业机密并向第三方泄露了大量公司内部数据。特斯拉前技术人员马丁·特里普（Martin Tripp）承认，他曾开发恶意软件进入特斯拉内部生产操作系统，偷取大量数据并交给第三方。这些被泄露的数据包括“数十份有关特斯拉的生产制造系统的机密照片和视频”。

美国内华达州联邦法庭公布的诉讼文件显示，特里普开发的恶意软件安装在了三台不同员工的电脑上，所以当他离开特斯拉后，他还能继续从该公司传输数据到第三方。诉讼文件写道：“在特里普加入特斯拉几个月后，特里普的领导认为他的工作绩效不佳，并时常与同事发生冲突。由于这些原因，在2018年5月17日前后，特里普被安排到了新岗位。特里普对此表示不满。”

诉讼文件还显示，特里普曾向媒体发表不实言论，比如，他称有缺陷的电池元组被用在了部分特斯拉Model 3车型中，但这个说法是不属实的。不仅如此，他还夸大了特斯拉在生产制造过程中生产的有缺陷物料的数量。

特斯拉首席执行官埃隆·马斯克（Elon Musk）在一封发给员工的邮件中提到了此事。马斯克表示，特里普的行为曾对公司的运营造成“持续性的、蓄意的破坏”，虽然还不清楚他的全部罪行，但目前确认的行为已经造成了“极坏的影响”。

世界通信技术行业巨头威瑞森公司（Verizon）最新发布的《2018年数据泄露调查报告》显示，超过四分之一的数据泄露是由内部人员造成的，内部威胁逐渐成为数据泄露的主要原因之一。

供应链威胁

2018年7月，美国网络安全公司UpGuard的研究员发现，加拿大汽车供应商Level One的数据库后门大开，可以轻松访问到其合作伙伴的机密文件。Level One在全球拥有100多家合作伙伴，从通用、菲亚特克莱斯勒、福特、丰田，大众到特斯拉，合作伙伴的机密数据如工厂原理、制造细节、保密协议甚至员工信息等统统被曝光，包含近47000个文件。

UpGuard研究员经过反复的检查和确认，通过Level One的文件传输协议rsync可以无障碍访问上述所有隐私数据。rsync是一种广泛使用的应用程序，经常用于大型数据传输和备份，但如果不采取适当的步骤限制rsync服务，数据可能就有泄露的风险。

Level One的数据泄漏错在没有限制使用者的IP地址，让非指定客户端也能连接，并且也没有设置用户访问权限，而且在漏洞发现时，rsync服务器上设置的权限表明，服务器竟然是可公开写入的。这意味着一些人可能已经更改了里面的文档，比如可能直接替换存款指令中的银行账号或嵌入恶意软件。

这是一次严重的安全事故，并且给100多家的合作伙伴带来的安全风险后患无穷，甚至没人知道这个安全风险何时开始，也无法知道是否还有别人发现，更不知道数据是否已经外泄。

近年来，我们观察到了大量基于软硬件供应链的攻击案例，比如，针对Xshell后门污染的攻击机理是攻击者入侵软件厂商的网络修改构建环境，植入特洛伊木马；针对苹果公司的集成开发工具Xcode的攻击，则是通过编译环境间接攻击了产出的软件产品。这些攻击案例最终影响了数十万甚至上亿的软件产品用户，造成了盗取用户隐私、数字资产、植入木马等危害。

外包商威胁

继斯诺登泄密风波之后，美国国家安全局再次遭遇了由外包商威胁导致的信息泄露事件。2016年8月，美国国家安全局承包商哈罗德·马丁（Harold Martin Ⅲ）因窃取NSA数据被捕。调查人员在马丁家中和车内搜出大量美国政府高度机密文件的复印文本和数字文档，其中数字文档至少有数个TB，还包括6份“敏感情报”。

> 据美国媒体报道，马丁是美国国家安全局承包商博思艾伦咨询公司（Booz Allen Hamilton）的雇员，博思艾伦协助打造和运作国安局大部分敏感的网络行动，“棱镜门”泄密者斯诺登也曾是该公司的员工。
>
> 刑事起诉书写道，马丁一开始否认他有违法行为，但面对事实证据后，他承认自己将工作中接触的重要文件和数字文档带走，并表示他“所做的一切都没有经过授权，是错误和不应该发生的”。除这些机密文件外，调查人员还发现马丁窃取了总价值超过1000美元的政府财物。

我国也发生了不少由外包商导致的数据泄露事件。比如，我们前几年曝光的“黄金眼”事件就是一件非常具有代表性的案例。简单来说，国内的一个软件外包商在给金融机构提供软件时，利用预埋的后门操控金融交易平台来获利。等到发现时，这个软件已经装在二十多家金融机构的主交易平台上，潜伏了几年的时间，产生了非常大的危害。我在后面的章节中将详细讲述这个事件。

由于外包业务的不断发展，外包服务商逐渐成为企业另一种形式的“内部人”，也成为新的安全威胁。尤其是在IT领域，负责开发和维护企业应用系统的外包合作人员通常都掌握合法账户，可以顺利通过认证，进入到组织内部的核心网络区域。一旦外包人员成为“内鬼”，数据泄露等安全问题就很容易发生。

间谍活动

2018年6月，郑州市国家安全局对涉嫌泄漏我国尖端武器机密给境外间谍情报机关的张某实施抓捕。张某在出国期间被境外间谍组织策反叛变，长期潜伏在我国军工重要科研领域，把我国尖端武器的核心机密毫无保留地透露给了间谍情报机关。

调查发现，张某除了掌握我国重要武器装备的研究外，还从事着某重点领域的研究，这种技术事关我国尖端武器的研发和装备，也是目前全世界最尖端、最前沿的科研项目之一，更是世界各军事大国争夺的制高点，同时更关乎着我国的重大安全。

早在2011年，张某第一次踏上国外的那一刻就受到了西方谍报机构地严密监视。境外的间谍通过接近张某，主动赠送一些小恩小惠，让张某感动不已。在送给张某的电子产品安装间谍软件，利用付费咨询的幌子，从张某那里套取他所掌握的核心机密，再通过金钱攻势，让张某一步步地屈服于他们，成为长期潜伏于我国重要军工科研机构的间谍。

在现实生活中，还有很多类似的策反案例。别有用心的境外间谍情报机关瞄准的，不仅仅是我国国防军工单位的核心技术人员，任何外围人员乃至每一个公民都有可能在不知情的情况下被利用。

蓄意破坏

2018年3月，北京某互联网科技公司运维工程师仲某，以涉嫌非法获取计算机信息系统数据罪被检察机关依法逮捕。他使用管理员权限插入代码，修改公司服务器内应用程序，盗取了该公司100枚比特币，价值数百万元。

据媒体报道，仲某在进行日常维护时，发现服务器内数据异常，随后发现有人试图通过黑客手段入侵公司服务器，并尝试盗取比特币。排除异常干扰后，他禁不住利益的诱惑，利用管理员权限登录服务器并插入一段代码，将公司的100枚比特币转移到自己在国外网站注册的比特币钱包中。

为了消除痕迹、躲避追踪，仲某还尝试使用该网站的私密钱包功能，将10枚比特币投入私密钱包内，但该功能后被证实为钓鱼网站，存入的10枚比特币已无法找回。案发后，仲某将剩余的90枚比特币退回了公司。

员工禁不住利益的诱惑，利用漏洞蓄意破坏重要数据，是内部威胁的重要来源。试想一下，如果写代码的人本身出了问题，只要他的技术水平足够高，完全可以在代码中写入只有他自己知道的漏洞。随后，他可以卖掉这些漏洞，或者隐秘地利用它们。

▶牢牢筑就管好“身边人”的防线

在大多数单位，有可能接触数据、使用数据的内部人员大致可分为三类：无意导致破坏的内部人员、伪装成内部人员的外部人员和蓄意破坏的内部人员。

无意导致破坏的内部人员可能为了方便，或者因为安全意识淡薄和安全知识不足，对公司数据的权属意识差，从而导致了内部威胁的发生。比如，他们可能设置弱密码，为工作便利共享口令给同事；或者把核心资料存在云盘，用U盘拷贝时没有将资料及时销毁等，导致数据的无意识泄露或流失；或者可能被钓鱼邮件、恶意软件利用，带来外部安全风险。

伪装成内部人员的外部人员可能是盗用了员工虚拟身份，冒用他们的账号进行操作。他们会访问以前从未处理的敏感数据，发送垃圾邮件和传播恶意软件，窃取、篡改、破坏数据，甚至可能冒充老板向财务、法务等部门索要机密数据。

蓄意破坏的内部人员可能是出于对组织管理不满意，或者因为绩效低被解雇，产生不满情绪，从而有意识、有计划地破坏、盗取内部数据，比如，在离职前导出大量数据，把数据提供给公司的竞争对手，或者利用自己的权限获取数据后倒卖获利。有的员工甚至会主动利用内部管理漏洞或技术漏洞，有计划、有步骤地完成踩点、试探、入侵、窃取等一系列过程。

企业管理层应当充分认识内部威胁的危害，高度重视，采取切实有效的措施应对内部威胁挑战，比如，科学分析员工期望、建立有效的激励机制、引导员工情绪、消除员工的破坏动机等。

除此之外，我们还可以采取技术手段应对内部破坏威胁，及时发现内部人员的异常行为，并及时检测和阻断来自内部的攻击。关于这一部分，将在第七章详细展开。

第三节　左右互搏的自我革新

在前文中我已说到，漏洞并非是计算机的产物，是自古以来皆有的，人类利用漏洞的案例比比皆是。

在信息化浪潮席卷全球的时代，人类在漏洞的利用和反制中不断博弈，除陈推新，在挫折中创新，在迭代中前行，不断推动互联网在矛盾运动中发展和完善。

利用与反制，永无止境

从莎草纸到互联网，从第一台计算机的庞然大物状，到如今的各种便携、超薄、超轻计算机和手机等移动终端，人类的技术在不断发展和进步，但这并非意味着漏洞会由此减少。相反，网络世界的漏洞会越来越多、越来越复杂、越来越隐蔽、越来越严重。

现在，计算机再也不可能飞进飞蛾，但IT系统的设计、实现与配置运行都是由人来完成的，是人就有可能犯错误，操作系统或应用软件程序编写中的逻辑错误一定会导致安全缺陷，系统的错误安全配置也会引入安全缺陷。

可以说，漏洞的利用与反制永无止境。这是一场针尖对麦芒的对抗，这种对抗，不是现在才有，也不是未来才有，而是将一直存在。

更具体一些，未来的漏洞将会有哪些趋势？我们应该如何以一种未来和发展的眼光看待它？

▶趋势一：数量越来越多

随着工业互联网、云计算、“互联网+”等技术的发展，数据交换越来越频繁，这就导致网络的边界越来越模糊。而这也意味着，漏洞的数量越来越多。

360网络安全响应中心发布的《2017年度安全报告——漏洞势态》显示，从2013年至2017年，这五年间发现的漏洞数量呈缓慢上升的趋势。其中，2017年披露的漏洞数量较往年有明显上升的趋势，漏洞披露数量环比上升120%。

报告数据显示，2017年一共披露了15120个漏洞，其中高危漏洞4406个。这些漏洞覆盖1444家厂商或组织的近4千种产品，累计影响的版本超过13万个。这说明网络安全形势非常严峻。

国外安全公司的数据同样验证了这一结果。2018年2月，美国安全公司Risk Based Security发布的报告显示，2017年安全漏洞披露数量达创纪录的20832个。该公司的《漏洞数据库速查》（Vuln DB Quick View）报告称，2016年披露的漏洞数量环比上升31.0%而美国国家漏洞数据库（NVD）收录的漏洞数量也同样增加了。

在2017年美国安全公司披露的漏洞中，有7900个并未收录进MITRE的通用漏洞列表（CVE）和美国国家漏洞数据库（NVD），其中44.5%的漏洞在新版通用漏洞评分系统（CVSSv2）中得分处于7.0～10.0之间，这一分值表示，它们都属于高危漏洞。

从勒索病毒新增变种数来看，也反映了漏洞越来越多这一趋势。360企业安全研究院的数据显示，2017年1—11月，共截获电脑端新增勒索病毒变种183种，新增控制域名238个。全国至少有472.5多万台用户

电脑遭到了勒索病毒的攻击，平均每天约有1.4万台国内电脑遭到勒索病毒攻击。

从整体态势来看，未来勒索软件的攻击质量和数量将不断攀升，勒索软件的自我传播能力将越来越强，定向攻击能力将更加突出，受害者支付赎金的数量也会越来越多。

▶趋势二：危害越来越大

当前，新一轮科技革命和产业变革正蓄势待发。随着物联网、工业互联网的发展，越来越多的物体被互联网联系在一起，这在给世界带来方便、进步的同时也意味着，未来一旦因漏洞导致网络安全事件，那么它的危害值也将翻倍。

物联网的诞生，极大颠覆了人们的生活。如果物联网产品存在安全问题，将会带来不可估量的危害。电影《窃听风云》中，男主角为了进入警察局的档案室偷取资料，利用漏洞黑入警察局的监控系统，将监控视频替换为无人状态，以隐藏潜入者的行踪，防止被警察发现。这样的场景在现实生活会越来越多地发生。

早在2011年，InGuardians的高级安全分析师杰尔姆·拉德克利夫（Jerome Radcliffe）就成功对自己的胰岛素注射器实施了黑客攻击。他说，黑客能以使设备失灵的方式，给糖尿病患者造成重大伤害，或在最远达150英尺（45.72米）的地方将胰岛素注射量推高至危险的水平。

2013年，美国著名黑客巴纳比·杰克（Barnaby Jack）本打算在“黑帽大会”上展示一项惊人的“黑客绝技”——在9米之外入侵植入式心脏起搏器等无线医疗装置，然后向其发出一系列830V高压电击，从而令“遥控杀人”成为现实。杰克指出，心脏起搏器等设备都是有无线接收装置

的，可以调节它们的工作模式。然而，就在他打算曝光这个漏洞时，却突然神秘死亡。

这两个例子充分表明，如果物联网的漏洞被利用，将会直接威胁到人们的生命安全。而工业互联网一旦被黑客攻击，可能会导致产业、地区甚至国家的瘫痪。比如电厂、水利工程、核电站，都是工业互联网的一部分，如果一个水电大坝的闸门控制系统遭到了黑客攻击，或者核电站的“核按钮”被控制，这就会给整个社会带来巨大灾难。

事实上，360的安全专家确实在某大型水电站的控制系统里发现了入侵的痕迹。更严重的是，核电站正成为网络攻击的新目标。据外媒报道，国际原子能机构表示，从2013年开始，黑客就开始了对核电站进行网络攻击，此类设施的安全威胁正在逐渐增强。

2017年，黑客对核电站进行网络攻击已经广为人知。6月份，乌克兰切尔诺贝利核电站的防控系统遭到Not Petya勒索病毒攻击。攻击导致基于Windows系统的传感器失灵，切尔诺贝利核电站不得不通过手动方式来监控核辐射水平。在核电站工作人员的极力控制下，暂时没有核辐射泄露，但工业区内的监测系统改由人工操作，核电站的网站也被暂时关闭。

英国最大保险组织劳合社（Lloyd’s）的一份报告显示，网络攻击对全球经济的危害远超人们想象，损失程度超过飓风。在“永恒之蓝”和Not Petya勒索病毒肆虐全球的过程中，公共机构、企业和个人损失严重，仅欧洲和亚洲的公司因网络攻击造成的损失累计就可能高达数十亿美元。

▶趋势三：价格越来越高

漏洞如何定价呢？漏洞的价格取决于利用难易程度和能影响到的人群规模。利用方式越简单，使用的人群规模越大，漏洞的攻击范围就越大，价格也越高。

随着移动互联网的发展，手机应用程序覆盖到的人群越来越庞大，比如Signal、Telegram、WhatsApp以及微信等通信应用程序已被世界各地的数十亿人使用。在这样的趋势下，漏洞的收购价格不断上升。

2015年11月，法国漏洞收购平台Zerodium宣布，它同意为苹果iOS某漏洞利用代码支付100万美金，该漏洞可以完全入侵该移动操作系统。过去，这样的漏洞的平均价格在数千至数万美元水平，并且只有极少数交易的价格超过10万美金。

与此同时，寻找和发现漏洞的难度逐渐加大，也导致了漏洞价格的攀升。比如，在2012年，谷歌提升了对Chrome浏览器漏洞的赏金额度，表明发现新安全漏洞的难度正在加大。收购了原惠普公司漏洞研究团队的趋势科技公司（Trend Micro）全球威胁公关经理克里斯托弗·巴德（Christopher Budd）称：“由于安全性的提升，我们在过去几年中看到的产品已经很难找到漏洞。这影响了供求关系，也提升了研究人员的需求。”

最终，随着软件变得更加强大，开发者对安全的了解进一步深入，黑客如果想要得到稳定的控制权限，必须同时使用多个漏洞和多项技术。这将需要更高的技能和时间成本，也将提升寻找漏洞能力的价值。

从漏洞的上述三个发展趋势中我们能看到，互联网领域的漏洞严重程度正在不断加深，这值得每一位网络安全工作者警醒，也需要每一位互联网用户提高警惕。

博弈催生创新，矛盾推动进步

股神巴菲特曾自述自己之所以成功，是因为克服了内心的贪婪和恐惧；索罗斯称自己的投资能常胜不败，只是在寻找各个经济体的漏洞，是寻找漏洞并利用漏洞的过程，他还认为，正是由于他提前刺破这些漏洞，让经济体能更快完善、进步……

互联网领域也是一样，人们正是在利用漏洞与如何堵住漏洞的博弈中不断创新，矛盾推动着互联网不断进步。

▶大数据与区块链的对垒

区块链技术的诞生可以说是一个典型例证。数据对企业来说至关重要，随着互联网巨头产品线汇集，这些公司聚集了大量数据。

数据集中导致数据泄露的风险更大。前文我提到的脸书8700万用户数据遭泄露就是一个例证。2018年5月25日，欧盟发布的GDPR（《通用数据保护条例》）正式实施，其目的就是规范并约束企业对用户个人数据的收集和使用，加强对欧盟境内居民的个人数据和隐私保护。

数据集中还从客观上产生了数据寡头的现象，带来数据垄断。数据垄断比技术垄断更难突破，容易产生数字鸿沟问题，形成“信息孤岛”，不利于行业良好发展。

在这样的矛盾和博弈中，具备“去中心化、信任强化、分布式共识、不可篡改”的区块链技术应运而生。数据从采集、交易、流通，到计算分析的全过程可以完整存储在区块链上，不但能够规范数据使用、

提高数据质量、获得强信任背书，还保证了数据挖掘效果及分析结果的正确性。

所以区块链技术的出现，使得企业不再需要把用户信息存储在易被定位的“孤岛”中，这样能防止企业违规使用用户数据，给用户信息安全提供了技术上的保护。同时，也有利于突破“信息孤岛”，建立数据横向流通机制，逐步推动形成基于全球化的数据交易场景。

▶逼上“梁山”的流氓软件

360的创新过程也是与技术漏洞、市场机制漏洞等漏洞不断博弈的过程。

互联网刚出现时，为了抢占互联网入口，很多互联网公司发布了浏览器战略。只要在浏览器导航条里输入中文，就能直接到达相关网站。由于地址栏只有一个，各家公司为争夺用户电脑，先是互相卸载对方，然后为了不被对方卸载而不断开发出更强的捆绑插件，逐渐发展到连用户都难以卸载。

最后争夺的结果就是流氓软件泛滥成灾。流氓软件有几大主要特征：不请自来（强制安装）、赖着不走（难以卸载）、卸了复活（卸载不完全，用残渣复活）。当时，我看到最严重的情况是，有的电脑中了十几款流氓软件，每个都要开机启动。有位记者给我看他的电脑，开机要半个小时，开机后鼠标还不能正常工作。

由于流氓软件不算病毒木马，属于民事行为，并不犯法，当时所有的安全软件都不管。但我们认为，解决用户的痛点、为用户创造价值是

大事，产品也才有前途。由此，360安全卫士在和流氓软件的博弈中正式诞生了。

2008年我们进军杀毒领域，当时的杀毒技术主要是人工分析病毒的特征码，通过扫描文件进行匹配、查杀。但这种“非黑即白”的杀毒方法只能管已知的病毒，并且查杀是滞后的。当病毒增长速度暴增以后，这种依靠已知“黑名单”的方法宣告失效，我们开始寻找新一代网络安全技术的突破口，首创了“查白”的网络安全技术，推动了网络安全产业的技术变革。关于这一博弈，我将在后面的章节中详细展开。

现在，互联网逐渐深入人们生活，网络安全领域的博弈更加错综复杂。利用漏洞发起的网络攻击已经产业化，形成了庞大的“网络黑色产业”，给人们的日常生活和社会的正常运行带来了巨大的威胁。

互联网技术不再是一个单纯的技术问题，在裹挟了政治利益、经济目标和人性满足等因素后，网络的漏洞会被放大，甚至无限放大，其危害无法估量。这是我们必须时时刻刻警惕，甚至是比以往任何一个时刻都需要警惕漏洞的现实原因。

人有弱点并不可怕，真正可怕的是明知自己有很多弱点，却不去认识和积极改正。如果不深刻地认识到自身的弱点，学会自我控制，提高自我纠错的能力，人是无法走向成功的。

同样，面对网络漏洞，我们也需要以同样的逻辑来面对它。既然我们已经发现了漏洞的规律，总结和梳理出了漏洞的趋势。下一步，就需要更加深入地挖掘当前网络领域是如何利用漏洞的，各个环节和要素如何在其中发挥作用，以及在这场左右互搏的对抗中，我们如何战胜庞大的“网络黑产”，推动互联网的健康、快速发展。

Chapter 2
第二章
黑与白是“黑产”魔高一尺，还是“白产”道高一丈

当前，互联网应用加速向人工智能、大数据、物联网和云计算演进，企业数字化转型不断提速。当越来越多的关键业务和应用需要依托互联网来完成时，这也意味着，攻击者透过漏洞可以攫取更多、更大的“价值”。

攻击者针对网络系统发起攻击的起点是漏洞，他们持续不断地挖掘和发现更多的漏洞，并针对性地开发攻击工具武器和攻击方法战法，偷隐私、盗数据、破坏系统、网络诈骗。从最早的“bug”到后来的黑客职业化、漏洞攻击专业化、市场开拓产业化，漏洞带来了巨大的地下经济产业。公开资料显示，中国“网络黑产”从业人员已超过150万人，市场规模高达千亿级别。

随着互联网渗透到经济社会发展的方方面面，网络安全已经直接关乎人民群众的权益和利益，网络犯罪成为新的犯罪形式。因此，我们需要对漏洞的产业链条形成理性、完整、客观、深刻的认识，以彼之道还施彼身，才能有对策性地、科学地完成有效的漏洞产业链条治理。

在这样的大背景下，基于漏洞的发现、响应与防御，也形成了产

业，我将其称之为“白色产业”。例如，通过漏洞响应平台把安全人才、技术和资源向社会共享，通过网络安全众测协同企业和政府主管部门共同保护网络安全等，这就是典型的“白产”。

第一节　网络黑色产业

“有利益的地方，就有犯罪。”自互联网诞生以来，利用漏洞获取非法利益的网络犯罪就应运而生，并催生出巨大的地下经济，即网络黑色产业。

网络黑色产业，是指以计算机网络为工具，以盈利为目的，有组织、分工明确的团伙式犯罪行为。

光明背后的阴影

2018年4月，湖北警方抓获了一个贩卖公民信息团伙，八名犯罪嫌疑人利用咨询公司的幌子在网上贩卖公民信息牟利。可怕的是，他们贩卖信息的数量高达500余万条、容量达60GB，非法获利20余万元。

从淘宝信息、金融信息、医疗信息、社保信息、车辆信息，到一应俱全的个人信息，甚至身份证、家庭住址、电话号码等，都是地下经济窃取倒卖的目标。

据媒体报道，北京某高校的一位博士生马某交代，他在2015年博士毕业后，曾到北京某国有大型科技公司短暂工作。期间，他有机会接触到该公司的数据库。他利用“黑客”技术手段，将网站的海量数据导出保存。这些数据包括大量个人手机号码、手机物理地址和用户公开访问记录以及个人隐私信息。

很快，马某从该公司辞职，与大学同窗张某合伙成立了一家投资咨

询有限公司，将之前获得的海量个人信息导入张某的云服务器上，张某按月支付“服务费”。这些信息以每条1～5分钱的价格打包倒卖，并根据数据新旧、购买数量的不同浮动价格。例如，仅2017年8月28日这一天，该公司就出售个人信息51000条，获利3500元。

数字货币成为“黑产”地下交易的支付手段之后，黑客们不再害怕因为“一手钱、一手货”而暴露身份，交易变得公开并且更加活跃，漏洞因市场扩大而产生了越来越大的价值，黑色产业产值飞速增长，并衍生出多个细分领域。

这里把网络犯罪分为两类：一类是传统网络犯罪。这类犯罪行为，是传统犯罪的网络化。这些犯罪形式一直存在，即使不利用网络技术犯罪分子也能得手，但利用网络技术以后，作案成本更低，隐蔽性更强，获取的利润更巨大。

另一类可称为新型网络犯罪。这类犯罪行为是基于网络技术创造的新型犯罪行为。这些犯罪形式只有通过网络技术才能实现，随着网络空间与物理空间的深度融合，这类犯罪会造成超乎常人想象的、更为严峻的后果。我们必须时时警醒，予以更高重视。

传统犯罪网络化

▶数据交易

2017年电商安全生态联盟首度发布的《电子商务生态安全白皮书》显示，地下黑色产业已经掌握了数十亿对账号密码关系，“黑产”通过撞库、刷库造成的账号被盗占到整体被盗账号的80%，而盗号所衍生

的“黑产”年获利超百亿元。

过去，不法分子需要通过“黑市”或者买通内部人员等方式，才能获得人们的隐私数据，获取成本很高。互联网出现后，黑客只需要利用漏洞攻击目标网站，就能获得大量数据，大大降低了数据交易的成本，网络技术让数据交易变得更容易、更频繁。

近年来，关于网络数据交易的报道屡见报端。2018年4月，据媒体报道，在网络上有卖家专门销售外卖平台的客户订餐信息。这些信息以5000条起售，10000条只要800元，平均每条信息不到一毛钱，价格便宜得惊人，信息更是详细具体到用户的姓名、联系方式和地址。

数据交易已经成为不法分子通过网络获取利益的一种主要手段。这些数据被贩卖给相应机构后，往往被用于含有骚扰性质的“精准推广”，或者干脆用于诈骗。

▶电信诈骗

电信诈骗没有技术门槛，吸引了大量的低端诈骗分子。他们处于网络“黑产”的最下游，也是最大的“黑产”变现渠道。不法分子从处于产业链中游的盗窃团队那里购买最“鲜活”的静态和动态个人隐私信息，把骗术生活场景化和个性化，实施精准诈骗和高额诈骗。

2016年8月，山东临沂一位名叫“徐玉玉”的高中生考上了南京邮电大学，由于家庭困难，向教育部门申请了助学金。一天下午，徐玉玉突然接到一通电话，通知她马上就可以领到这笔助学金，这让她欣喜不已。可她怎么也不会想到，这个自称教育局工作人员其实是骗子。当天下午，徐玉玉将9900元学费取出后存

入了骗子发来的银行账号。徐玉玉发现9900元的学费被骗后，万分难过，当晚和家人去派出所报了案。但在回家的路上，这个18岁女孩突然晕厥，不省人事，最终没能走进憧憬中的大学，永远离开了这个世界。“徐玉玉”案引发了舆论的强烈关注，并推动了立法，在这起悲剧发生后的两个月，民法总则二审稿首次加入了保护个人信息的内容，这在此前的民事权利中从未涉及。

数据显示，2017年上半年，来自中国大陆以外的诈骗电话量翻倍增长，诈骗电话来自71个国家和地区，诈骗短信量已经占到整体的近5%，通讯网络诈骗的国际化趋势愈发明显。而且，从各个主要国家的统计数据看，各种利用互联网技术实施偷盗、诈骗、敲诈的案件数正在以每年超过30%的增速增长。

▶赌博诈骗

自古以来，有赌桌就有“老千”。当赌博搭上网络技术“新手段”，这个“千术”就更让人难以识破。那些幻想着一夜暴富的人最终大多都倾家荡产，一些人因欠了一身赌债，不停地参与赌博来争取“翻身”的机会，结果却是越输越多。

2017年5月，广西贵港警方破获的一起案件揭开了赌博诈骗的部分猫腻。这个犯罪团伙利用一个游戏软件进行聚众赌博，诈骗金额高达1200多万元。参赌人员下载游戏软件后，用现金购买相应的游戏分值进行赌博。但这个游戏软件就是诈骗工具，犯罪团伙设定了输的概率一定高于赢的概率，而且后台还可以根据需要上调或者下调赔率。这就意味着，该犯罪团伙一定会盈利。

另外，赌博团伙也可以从后台直接封杀一些经常赢钱的参赌账号，这样即使你赌赢了钱，也一样拿不到现金。可以说，只要

有人玩他们的游戏，他们就绝对是稳赚不赔。

与赌博相关的网络犯罪还有很多，并且“骗术”越来越隐蔽。比如一些赌客使用微信拼手气红包，通过猜庄家的随机红包尾数或大小来赌博，但是庄家使用了外挂软件，提前就用该软件设置好了红包尾数，这样就能稳赚不赔。再比如，庄家用手机远程控制赌博机，当有“大鱼”上钩时，立即用手机调整机器，让赌客输得一分不剩。

赌博“水太深”，不少人把赌博作为他们通向发财之路的捷径，沉迷其中，其结果是往往是家庭破裂、倾家荡产，甚至走上犯罪的道路。

▶非法集资

互联网是风口经济，市场上有一种说法，“在风口上，猪都能飞起来。”骗子把“非法集资”这头猪挪到了风口上，愣给吹得飞上了天。他们打着“互联网金融创新”“经济新业态”等幌子，把非法集资规模扩大了数百倍，大大突破了诈骗的地域界限。

2015年，“e租宝”案轰动全国。钰诚集团将收购的一家网络平台命名为“e租宝”，打着“网络金融”的旗号上线运营。据媒体报道，“e租宝”共推出过6款产品，预期年化收益率在9%至14.6%之间，远高于一般银行理财产品的收益率。但是这些项目几乎都是假的，“e租宝”抓住了部分老百姓对金融知识了解不多的弱点，用虚假的承诺编织了一个“陷阱”。

短短一年半时间内，“e租宝”非法吸收资金500多亿元，受害投资人遍布全国31个省市区。据警方介绍，“e租宝”从一开始就是一场“空手套白狼”的骗局，其所谓的融资租赁项目根本名不副实。2016年1月，“e租宝”平台的21名涉案人员被北京检

察机关批准逮捕。

据媒体报道，2017年全国新发涉嫌非法集资案件5052起，涉案金额高达1795.5亿元。非法集资新发案件几乎遍布所有行业，呈现“遍地开花”的特点，投融资类中介机构、互联网金融平台、房地产、农业等重点行业案件持续高发。大量民间投融资机构、互联网平台等非持牌机构违法违规从事集资、融资活动，发案数占总量的30％以上。

从案件情况看，非法集资组织化、网络化趋势日益明显，涉案地区快速从东部向中西部扩散，从一二线城市向三四线城市蔓延。案件集中于东部沿海地区和中西部人口大省，但中小城市、城乡结合地区、农村地区的案件也在逐渐增多，潜在风险不容忽视。

▶网络传销

随着我国对传统传销模式打击力度加大，一些传统的传销组织纷纷利用网络平台“改枪换炮”，开展更具欺骗性的传销活动。他们引入电子商务、投资理财、新经济模式等概念，借助互联网传播，短时间内就能聚拢数量庞大的参与者。但无论采用哪种包装手段，网络传销的获利方式与传统传销没有本质的区别，同样是交纳会费，然后再拉人进入作为自己的下线，如此炮制。

2018年7月，在全国引起广泛关注的“跨亚欧公司”特大网络传销案在海口市开庭审理，涉案金额共38亿余元。该公司对外宣称拥有国资、央企背景，利用互联网平台推销虚拟货币“亚欧币”，以“高返点、高收益”为诱饵吸引会员，仅一年时间便忽悠了几万名会员。

据媒体报道，“亚欧币”实际为虚拟产品，没有任何实体产

业。犯罪嫌疑人夏某与刘某等人编造各种身份，通过在国内多省市的高端酒店召开推介会、举办论坛以及网络宣传等方式，大肆虚假宣传“亚欧币”的合法性和盈利前景。

“跨亚欧公司”的经营模式是典型的传销模式，即“三级代理、三级分销”层级，其中省级代理提成30%，往下逐级递减3%，最低到10%。省级代理资格需交纳1000万元市场保证金或完成业绩9000万元以上，最终收集的资金都转入了夏某等人的私人账户。

由于网络的便利性、虚拟性，近年来涉及网络传销的人数迅速增长。目前，常见的传销模式包括：一是“消费全返”模式。比如2018年5月被警方成功摧毁的“云联惠”，以“消费全返”等为幌子骗取财物。二是“金融理财”模式。比如2017年12月被警方调查的“钱宝网”，以项目年化收益率高达50%以上吸引投资者，大量非法吸收资金。三是“慈善公益”模式。比如警方2017年7月破获的“善心汇”，以“扶贫济困、均富共生”的名义，通过“拉人头、布施、受助”的方式非法获利。

▶洗钱

洗钱纵容了不劳而获，让犯罪违法获得的资金逍遥法外，破坏社会公平和市场公平，一直是世界各国重点打击的犯罪之一。洗钱主要有四种形式：其一，明知是赃款，为帮其隐瞒来源和性质而提供资金账户；其二，协助把财产转为现金或证券等；其三，协助资金转移；其四，协助把资金汇往境外。

进入互联网时代，新型的加密货币让洗钱变得更加方便和隐蔽。与法定货币相比，加密货币没有集中的发行方，完全由网络节点的计算生成，兑换和使用非常自由，交易过程可以越过所有的金融系统监控，非

常难以追踪溯源，所以受到洗钱者们的青睐。

2017年7月，美国警方在希腊逮捕了一位名为亚历山大·文尼克（Alexander Vinnik）的俄罗斯人，该男子涉嫌利用比特币为犯罪组织洗钱超过40亿美元，而他是比特币交易平台BTC-e的背后主要人物。

据媒体报道，文尼克和其团队成员自成立BTC-e以来，为犯罪分子客户群创造了机会，因为该平台不要求用户进行身份验证，这使得犯罪分子利用这个平台进行匿名交易并掩盖资金来源，该平台也缺乏任何反洗钱相关流程。

除了比特币以外，第三方支付平台也成为洗钱的一种方式。2018年3月，深圳警方破获一起诈骗案，相关涉案团伙在10余天内骗取700多万元，而这一犯罪链条的最后一个环节，就是利用第三方支付平台快速转款取现。

据深圳市反电信网络诈骗中心介绍，利用第三方支付平台转移赃款和洗钱的手段一般有三种：通过第三方支付平台发行的商户POS机虚构交易套现；将诈骗得手的资金转移到第三方支付平台账户，在线购买游戏点卡、比特币等物品后转卖套现；将赃款在银行账户和第三方支付平台之间多次转账切换，逃避公安追查。

可以说，只要洗钱者冒用他人身份资料或者伪造身份资料，一人注册多个账户，就能将非法所得“洗白”。

网络犯罪花样化

▶暗网

暗网有多“黑暗”？我可以告诉大家，那里是网络空间的罪恶天堂。

暗网技术起源于1996年美国海军的一个构想，在这个系统中用户连接互联网时处于匿名状态，不会在服务器上留下真实身份。因为保护访问路由器的密码像洋葱一样层层叠加，也被称为“洋葱网络”（Tor，The Onion Router）。

Tor2.0版后改为开源软件，暗网脱开军方，成为互联网上最大的网中网，它有自己的域名体系，还有自己的网站百科目录。暗网普遍用于违法交易和网络攻击，比特币是暗网货币。

暗网就好像互联网上的一个黑洞，普通的网络访问、用户和服务器之间的访问记录（日志）是可以回溯的。理论上讲，张三独立访问了A网站，就会在A网站上留下张三的IP地址，警察动用行政力量，就能找到张三的真实身份。如果使用代理服务器，它能更改隐藏访问者IP，但一旦代理服务器被攻陷，也能拿到访问者身份。

暗网的原理是引入P2P分布式机制，每一个装了Tor软件的用户电脑变成中继连接，每一次访问路径都随机经过多个中继连接，变化在任何一个中继服务器上，找不到完整的痕迹。

“丝绸之路”毒品交易网站是藏身于暗网的电商平台。一名澳大利亚记者经过数年跟踪，在一篇报道中说，在暗网电商平台上，赏金猎人价格在2万美元，而花6美元可以买一个含HIV病毒的针筒，自己动手。如果你的目标对手罪不至死，可找特种部队吓唬他一下，花5美元特种部队会安排几个警察教训他一下，花20美元特种部队就会亲自出马。

2018年2月，美国司法部宣布对Infraud网络犯罪团伙的36名嫌疑人提出指控，罪名包括盗窃个人身份信息、对银行实施欺

诈、电信诈骗和洗钱，等等。美国司法部称，这是迄今为止受理的最大规模网络欺诈案件。

Infraud表面上是一个匿名在线论坛，实际上买卖从全球各地窃取而来的个人社保账号、生日和密码等个人信息。截至2017年初，这个论坛共有超过1万名注册会员，会员售卖的“商品”无奇不有，从79.5万个汇丰银行的登录账户，到网络支付平台贝宝（Paypal）的账户，再到数不清的信用卡卡号。就这样，Infraud成长为迄今为止最大的“暗网”之一，已导致商家、银行损失了5.3亿美元。

如今，各国政府和执法机关都在抓紧清扫暗网上的非法行为。但暗网并不是罪恶之源，只要需求存在，仍会不停地发展。

▶木马攻击

“木马攻击”这个词来源于一个古希腊神话故事，攻击特洛伊城的士兵使用木马来伪装实现攻城，这一特点与木马病毒相似度极高，也自然而然地成为电脑木马程序的名字。

木马是一个专门的恶意软件类型，主要是指通过伪装等手段，掩盖自己的真正意图。从原理上来说，由于木马的通用性，在任何类型的网络犯罪当中几乎都会见到木马的身影，包括窃取信息、破坏计算机、横向渗透整个网络，甚至进行国与国之间的APT攻击等。因此木马也被称为“网络犯罪的枪和子弹”。

木马攻击已经形成了非常完整的黑色产业链，分工包括木马制作、木马代理、包马人、洗钱人等一系列角色。

其中，木马制作和木马代理经常是公司化运作，实现木马编写、避

免被杀毒软件查杀的“一条龙服务”。之后，包马人负责在网页上植入木马，从中招用户的电脑中盗取各类有价值的信息，再把这些数据出售给洗钱人，由洗钱人进行变现操作，与其分成获利。

在PC网银发达的年代，攻击者通常会向浏览器注入木马，篡改网银客户端，使受害人将钱转入指定账户，或者利用受害人的账户购买游戏点卡等方式进行获利。现在，随着虚拟货币的火爆，向网站植入“挖矿木马”逐渐成为一种主流的获利方式。

2017年11月，360安全中心监测到一款新型木马在国内大规模爆发，上百家网站感染该木马。用户在浏览这些网站时，电脑会自动执行挖矿代码，中招的电脑会出现卡慢、变热、CPU占用率飙高等情况，严重影响设备的正常使用。

受影响的网站除了一些伪色情网站、境外赌博站点外，还有大批涉及教育、民生、政务等领域的网站，其中“巨人学校论坛”“云盘视频分享站”等浏览量庞大的网站全站遭受攻击，打开网站内任意页面都可能自动运行挖矿程序。

由于“挖矿木马”隐蔽性极强，未来这类木马数量还将继续增加。不法分子可能会将“挖矿”目标转移到网页游戏和客户端游戏中，通过游戏的资源高消耗率掩盖“挖矿机”的运作。

▶网站挂马与篡改

“网站挂马与篡改”是网络犯罪行为中常用的一种攻击方法。攻击者会利用各种手段，包括病毒感染、零日漏洞（0day）利用、SQL注入漏洞、网络劫持、恶意广告投放等，向网站页面中加入恶意代码，修改页面内容，当网站访问者访问被加入恶意代码的页面时，计算机就会自

动访问被转向的地址或者下载木马病毒。这种方法就像把木马病毒挂在了网页里，一触即发，因此被形象地称为“挂马”。

“挂马”整个攻击过程可大致分为三个环节：恶意代码开发维护、获取修改网站页面权限并植入恶意代码、持续控制“肉鸡”并挖掘价值。围绕这个三个环节，网络犯罪进行了专业分工，并形成了真正意义上的“黑色产业链”。

2006年，以MPack为代表的商业化攻击代码库开始出现，任何人只需要花500～1000美元就可以获得一套完整的商业化攻击代码。攻击者利用攻击代码库可以非常轻易地获得网站访问者计算机的控制权，并通过窃取账号密码、出售DDoS（Distributed Denial of Service，分布式拒绝服务）攻击等各种方式进行变现，“黑产”由此迅速发展成熟。

近几年，“挂马”攻击行为不断演进，甚至通过合法在线广告系统给客户端软件、移动APP、网站植入恶意代码。2015年，FireEye监测到有攻击团伙利用顶级在线广告商OneClickAds的系统投放了包含CVE—2015—5119漏洞利用程序在内的“挂马”广告。

2018年4月，有国内的攻击团伙通过页面广告，向大量客户端软件资讯和新闻窗中插入带有CVE—2016—0189漏洞利用代码的挂马页面，漏洞利用代码执行后，在设备上植入后门，进而在用户设备上植入后门，后续进行勒索、挖矿、软件推广等多种恶意操作。

更严重的是，“挂马”越来越多地出现在了“高级持续威胁”这类有组织、有针对性的攻击行为中。在2014年5月、9月，以及2015年1月，“海莲花”组织针对多个政府机构、科研院所和涉外企业的网站进行篡改和挂马。在该组织被曝光并沉寂一段

时间以后，2017年11月又监测到“海莲花”组织对某大型能源企业发起了“挂马”的攻击行为。

可以预见的是，只要互联网的主要展现形式还是网站，“挂马”这种攻击方式一定会长久存在，并会随着互联网环境和攻防对抗的发展，不断发生新的变化。

▶网站“拖库”与“撞库”

数据泄露一直是网络安全的焦点，服务商和黑客之间在用户数据这个舞台上，一直在进行着旷日持久的攻防战。在这场攻防战中，“拖库”与“撞库”成为我们必须重视的问题。那什么是“拖库”和“撞库”呢？

“拖库”顾名思义就是黑客从有价值的网站把用户资料数据库拖走。而“撞库”则是指黑客通过收集互联网已泄露的用户和密码信息，生成对应的密码字典表，尝试批量登录其他网站后，碰撞出一系列可以登录的账户。用户在不同网站登录时使用相同的用户名和密码，相当于给黑客配了一把“万能钥匙”，一旦丢失后果无法想象。

“撞库攻击”需要一定的攻击成本，其中最重要的是撞库的源数据。这些源数据主要通过三种方式获取：一是黑市购买；二是同行交换；三是自行入侵网站并“拖库”。这三种源数据的获取方式都是由黑客入侵网站后进行“拖库”而流出来的。

随着网站数据库泄露事件频繁发生，加上地下黑色产业日渐成熟，不法分子获取网站用户数据后，可以通过诈骗、推广等方式迅速变现，“撞库攻击”逐渐成为主流的盗号方式。

2014年年底，12306网站由于“撞库攻击”导致大量用户数据泄露。根据铁路公安机关通报，不法分子通过收集互联网某游

戏网站以及其他多个网站泄露的用户名加密码信息，尝试登录其他网站进行“撞库”，非法获取用户身份认证信息共计60余万组，并谋取非法利益。2014年12月25日晚，涉嫌窃取并泄露他人电子信息的蒋某某、施某某被抓获。

黑客盗取到大量账号后，通常会对这些账号进行分类，最后再根据不同的类型分别变现。例如，游戏类的账号可以转移虚拟货币、出售游戏账号、盗取装备；金融类的账号可以用来进行金融犯罪和诈骗；其他类型的账号还可以直接出售给专门的广告投放公司，用于发送广告、垃圾短信、电商营销等。

随着网络诈骗问题日益增多，“拖库”与“撞库攻击”所衍生的问题也越来越受到重视。要防止“拖库”，主要是要做好网站自身的安全，杜绝网页漏洞、管理员弱口令，同时还可以和专业安全厂商合作，通过渗透测试的方式，全面检查网站所存在的漏洞和脆弱点。而防止“撞库攻击”，重点则是在网站登录时做好相对严格的验证流程和防御措施，如限制同一个IP的请求频率、添加无法通过机器去识别的滑块验证码等。

▶APT攻击

APT是“Advanced Persistent Threat”的缩写，又称“高级持续性威胁”，通常以政治或商业为动机，针对特定目标实施长久持续且隐匿的网络攻击活动。APT攻击的实施者通常具有国家、政府或情报机构背景，或是由它们资助的攻击组织，而非普通网络黑客或网络犯罪团伙。

“APT”一词普遍认为是美国空军分析师格雷格·拉特雷（Greg

Rattray）上校在2006年首次提出。2010年6月，著名的“震网”蠕虫被发现，其目标是破坏伊朗核设施。“震网”事件完全具备APT攻击的特点，是一起由国家和政府背景支持的APT攻击。

近年来，APT攻击活动的动机多和地缘政治冲突、军事行动相关，主要攻击意图是长久性的情报刺探、收集和监控，其攻击目标除了政府、军队、外交相关部门外，也包括科研、海事、能源、高新技术等领域。

2018年4月，360在全球范围内率先监控到了一例使用0day漏洞的APT攻击，捕获到了全球首例利用浏览器零日漏洞的新型Office文档攻击，并将该漏洞命名为“双杀”漏洞。该漏洞影响最新版本的IE浏览器和使用了IE内核的应用程序。用户在浏览网页或打开Office文档时都可能中招，最终被黑客植入后门木马完全控制电脑。

360当即向微软提交了该漏洞的相关细节，微软在4月20日早上确认了这个漏洞，随后在5月8日发布了官方安全补丁，对该漏洞进行了修复，并将其命名为CVE—2018—8174。

通过对该APT攻击进行分析和追踪溯源，360确认其与APT—C—06组织存在关联。APT—C—06组织是一个长期活跃的境外APT组织，其主要目标为中国和其他国家，攻击活动的主要目的是窃取敏感数据信息进行网络间谍攻击。在针对中国地区的攻击中，该组织主要针对政府、科研领域进行攻击，且非常专注于某特定领域，相关攻击行动最早可以追溯到2007年，至今仍非常活跃。

当前比较知名且活跃的APT攻击组织还有“海莲花”“摩诃草”等，本书第五章中将对其展开详细介绍。

如今，随着APT攻击组织与安全人员的日益对抗升级，APT组织利用多层次的加密混淆、多阶段载荷投放等方式，加大了分析取证难度，攻击来源的研判更加困难，APT威胁的攻防博弈将长期延续。

▶DDoS攻击

DDoS是Distributed Denial of Service的缩写，意为“分布式拒绝服务”。通俗地说，DDoS攻击就是使被攻击的系统“拒绝提供服务”，一般是利用这个系统的功能缺陷，或者直接消耗其系统资源，使系统无法正常提供服务。

DDoS攻击由来已久。可以说，自互联网通讯协议（TCP/IP）诞生之日起，DDoS这种攻击方式就伴随而生。

互联网上最经典的DDoS攻击方式之一是SYN Flood攻击（SYN为Synchronization的首3字母缩写，意为“同步”），它利用的是TCP/IP设计的天然缺陷。简单来说，TCP在交换数据之前有一个“三次握手”建立连接的过程，这是一种协商机制，只有握手成功才能建立成功连接。然而，目标主机缺乏有效的校验机制，不论是谁发起“握手请求”（即SYN请求），目标主机都要作出响应。这就给攻击者提供了可乘之机，当攻击者蓄意发起大量的SYN请求时，目标主机就不得不对这些请求做出响应，导致出现内存不足和CPU满负载的情况，从而无法正常地提供服务。

和SYN Flood攻击的原理类似，DNS（域名系统）服务器也成为DDoS攻击的重灾区。DNS被称为互联网的基石，不论是谁发起DNS请求，DNS服务器都需要响应。如果遇到蓄意的DDoS攻击，DNS服务器因为要大量响应、查询大量的表项，最后导致无法正常提供服务。

2016年发生的“美国东海岸断网”事件就是一个典型案例。当地时间10月21日，美国域名解析服务提供商戴纳基（Dyn）的域名服务器遭受三波DDoS攻击，导致推特（Twitter）、美国有线电视新闻网（CNN）、华尔街日报、星巴克等超过1200家网站无法访问，美国主要公共服务、社交平台、民众网络服务瘫痪。仅Dyn一家公司的直接损失就超过了1.1亿美元，事件的整体损失不可估量。

2017年12月，FBI宣布“美国东海岸断网”案件告破，并公开致谢360在破获这起案件中所做的协助工作。360作为东半球唯一参与事件处置的公司，依托其安全大数据资源，率先发现并持续追踪溯源了这个由摄像头等智能设备组成的名为“Mirai”的僵尸网络，为案件告破提供了重要线索。

▶勒索与敲诈

勒索软件和敲诈病毒是近几年盛行的新型网络犯罪。它的原理是，通过对用户的数字资产（如Office文档、图片、视频、源代码、数据库等文件）进行加密，造成使用者无法访问这些文件，或篡改系统密码锁定系统，迫使用户交付赎金。

已知的勒索软件最早可追溯到1989年，哈佛大学毕业生约瑟夫·帕普（Joseph Popp）编写了一个名为AIDS Trojan（也称为“PC Cyborg”）的病毒。它会隐藏硬盘上的文件，并对文件名进行加密，然后声称用户的软件许可已经过期，要求用户向“PC Cyborg”公司寄去189美元以获得修复工具。可以说，AIDS Trojan开启了勒索与敲诈攻击的先河。

2013年底，黑客首次采用比特币作为赎金支付形式，通过勒索软件Crypto Locker获取了价值2700万美元的赎金。由于比特币具有很强的隐

秘性，很难抓捕到恶意软件的作者，因此这几年出现的勒索病毒几乎都使用加密数字货币作为交付赎金。

现在，勒索软件开始呈现爆发之势，技术手段不断更新，攻击目标也逐渐从个人转向企业。黑客通过漏洞利用、弱密码攻击等手段入侵政企客户的高价值服务器，加密其核心业务数据，企业客户迫于业务运营的压力，不得不尽快支付赎金，而且数额也更大。

早在2016年9月召开的首届国际反病毒大会上，我就强烈呼吁要警惕勒索病毒泛滥成灾，这个预警不幸成为了事实。

仅2018年前三个月，就发生了多起勒索软件攻击事件：3月22日，美国亚特兰大市遭遇了一场大规模勒索软件攻击，政府机构的一些关键系统不幸中招，迫使官员只能使用传统的纸笔记录方案；2月20日，美国海恩斯维尔市市政府遭遇了一起勒索软件攻击，导致多项城市在线生活服务被迫中断，需要支付水费的居民必须亲自去营业厅进行现场缴费。

还有2017年5月，全球爆发的著名的“永恒之蓝”勒索蠕虫，席卷了150多个国家和地区。仅一个月后，Not Petya勒索病毒变种在乌克兰等地肆虐，让人们对于勒索软件的关注达到了空前的高度。

对于当前的勒索软件形势，事前的防范远比事后的补救来得重要，用户需要养成良好的安全意识，设置高强度系统密码，及时安装系统补丁，将核心业务数据备份，同时安装安全防御软件并保持实时更新，将勒索软件的攻击风险降到最低。

▶私服外挂

私服一度是网络安全领域的热门词语，指的是未经版权拥有者授权，非法获得服务器端安装程序之后设立的网络服务器，本质上属于网络盗版，与在互联网上共享未经授权的版权作品的本质差别不大。随着时间的流逝，越来越多的私服开始转入地下，我们可以从私服的兴起之路来回顾一下这种新型的网络犯罪手段。

在网络游戏中，拥有特殊需求的玩家大有人在，为满足这部分人的需求，私服“应运而生”。其主要目的是通过以包月或者点卡等方式，向游戏玩家收费，满足玩家的特殊需求。由于利润可观，私服实际造成的危害比其他网络盗版行为更为严重。

2001年网络游戏兴起，来自韩国的MMORPG（Massive Multiplayer Online Rote-Playing Game，大型多人在线角色扮演游戏）游戏《传奇》火遍中国，但由于其苛刻的等级升级制度，玩家往往要耗费大量精力及财力，才能获得较好的装备及较高的等级。这种情况下，一些私服运营者开始扮演GM（Game Master，游戏管理员）角色，比如提升游戏初始等级、减少升级所需经验等，同时向愿意付费的玩家出售装备。

私服的兴起催生了多条产业链。首先是DDoS产业链，为了抑制对手扩张，私服的运营者会提供费用招揽黑客，以DDoS的方式致使其他私服不可用；其次是雇佣黑客针对网络游戏开发公司进行渗透，例如，某老板贿赂巨人网络游戏公司的开发者，从其手中购买网络游戏源码以供架设私服；最后是因私服大量兴起而伴随而生的“外挂”产业链。

严格来说，“外挂”在私服兴起之前就已经存在了。“外挂”的早期雏形是针对单机游戏的游戏修改器。随着网络游戏兴起，流行的外挂技术包括封包修改法、Hook网络游戏客户端关键函数等。同时，“外挂”产业链也逐渐变大，包括外挂开发者、销售、客服等各个角色，外

挂产业中还借用了一些与游戏运营相同的理念，如外挂的会员制度、包月制度等。

如今，几乎流行的网络游戏中都存在外挂，包括最近火遍全球的“吃鸡”游戏《绝地求生》。随着某平台主播使用外挂事件的爆出，FPS（First-person shooting game，第一人称射击类游戏）的外挂泛滥问题也逐渐浮出水面。这些外挂的主要功能包括射击无后坐力、透视、穿墙爆头、千里狙击等。在国内某外挂销售网站上，我了解到类似功能的外挂售价高达100元／天，更有甚者号称其外挂功能强大并开出了8000元／月的高价。由此可见，整个外挂产业链的利润十分可观。

随着电竞行业的完善，网络游戏除了休闲的功能外，也逐渐体现出某些竞技性，某些游戏在发行时就提供了创建服务器等功能。因此，私服产业逐渐衰败，但外挂仍旧是困扰电竞产业最大的威胁，一些国家甚至为反外挂推出了专门定制的法律。预计在未来的游戏产业中，关于游戏安全及外挂的技术对抗，仍旧会此消彼长。

▶域名劫持攻击

域名劫持攻击离我们有多远？我可以告诉大家，其实我们每天上网都会遇到。

域名系统（DNS，Domain Name System）是互联网最为关键的基础设施，它是一个分布式数据库，能与IP地址相互映射，从而使用户不用死记硬背那些复杂的、能被机器直接读取的IP地址，就能方便地访问互联网。域名一旦被劫持，将会引导用户进入攻击者伪造的网站或导致网站无法访问，造成无法估量的后果。

域名劫持攻击一般有多种形式。一种是利用各种恶意软件修改浏览

器、锁定主页或不停弹出新窗口，强制用户访问某些网站，或者在用户访问A站时将其替换成B站。目前因为有安全软件和安全浏览器的存在，这种威胁基本已经消除。

更高级的攻击是通过冒充原域名拥有者，修改网络解决方案公司的注册域名记录，将域名转让到另一团体，让原域名指向另一个服务器，使正常的域名访问被指向攻击者所想引导的内容。

2018年4月，流行的以太网钱包MyEtherWallet遭遇DNS劫持攻击，黑客将用户定向到恶意版本的网站并盗用了他们的私钥。据媒体报道，攻击持续了几个小时，黑客从中获得了大约价值15万美元的加密货币。

不仅是网站，黑客还利用DNS劫持攻击智能手机。2018年4月，卡巴斯基实验室研究人员报告了一种最新的安卓恶意软件。该恶意软件通过DNS劫持技术进行传播，主要针对亚洲地区的智能手机进行攻击。其目的是窃取包括凭证在内的用户信息，从而让攻击者可以完全控制被感染的安卓设备。研究人员在超过150个用户网络中检测到了这种恶意软件，主要受害者位于韩国、孟加拉国和日本，而且受害者可能更多。

DNS安全是网络安全的第一道大门，如果DNS的安全没有得到有效的防护，也未制定应急措施，即使网站主机安全防护措施级别再高，攻击者也可以轻而易举地通过攻击DNS服务器使网站无法提供服务。

▶攻击工业控制系统

2010年的伊朗“震网”病毒事件，给全球工业控制系统敲响了警钟。这次事件让人们认识到，互联网在拓展工业控制系统发展空间的同时，

也带来了工业控制系统的网络安全问题。

工业控制系统通常指由计算机设备和工业生产控制部件组成的系统。20世纪70年代至90年代，许多系统与业务网络完全隔离，因此，针对工业系统的网络攻击被认为是“可管理的”。随着信息技术（IT）和运营技术（OT）逐渐融合，原本在隔离网络中几乎完全被忽视的工业控制系统网络成为黑客、病毒、木马攻击的主要目标之一。

工业控制系统中大量使用的各种Windows及开源的Linux操作系统，通常数年甚至是十余年未打补丁和升级，存在大量漏洞，任何针对这些漏洞的攻击都将造成难以估量的损失。除了操作系统的漏洞外，大量工控系统的设备、协议及应用程序在设计之初没有考虑安全问题，更没有采用认证和加密机制等网络安全对抗措施，因此近年来针对工控系统的网络安全事件频发。

2017年12月，黑客利用恶意软件Triton攻击了施耐德电气公司（Schneider Electric）Triconex安全仪表系统（Triconex Safety Instrumented System，SIS），意图关停系统并尝试修改系统到危险失效状态。攻击者已经不满足于攻击常规工控系统（如分布式控制系统（DCS）、可编辑逻辑控制器（PLC）等），造成停车或停产，而是开始攻击工业领域最核心的安全保护系统，尝试造成爆炸、有害物质泄露等更严重的危害，该威胁被RSAC2018评为最危险的五大攻击之一。

2018年1月至5月，根据国家信息安全漏洞共享平台（CNVD）统计，工业控制系统漏洞总数已达到190个，主要分布在能源、制造、商业设施、水务、市政等重点领域，且高危漏洞比重增多，攻击破坏力不断增强，对关键信息基础设施的安全防护存在重大威胁。

随着工业控制系统受攻击的风险日益严重，工业互联网安全受到政府高度重视，相关法律法规也相继推出。2017年12月29日，工信部正式印发《工业控制系统信息安全行动计划（2018—2020年）》，提出到2020年基本建立全系统工控安全管理工作体系，工业控制系统的安全已经成为国家安全的重要组成部分。

▶攻击关键信息基础设施

在万物互联的今天，利用技术上的漏洞，攻击水电、通信、交通、金融、医疗、卫生、军事等关键信息基础设施，并使其陷入瘫痪，这种威胁变得十分现实。

关键信息基础设施所涉及的范围比较广泛，并兼具着多种不同身份与职能，这也使得其暴露面增多。一旦关键信息基础设施运行、管理的网络设施和信息系统遭到破坏，丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益。

关键信息基础设施被攻击的危害在2017年的“永恒之蓝”勒索蠕虫事件中体现得尤为明显。“永恒之蓝”在国内波及医疗、能源（加油站）、公安（出入境、户籍管理）、制造业（产线停摆）、教育等众多行业，直接对社会公共利益造成了较大的影响。而在国外，很多病人甚至因此错过了手术时间。

2018年第一季度，发生了多起关键信息基础设施网络安全事件：4月5日，黑客利用思科设备的漏洞攻击了伊朗，造成数十台大型路由器瘫痪。4月6日，“JHT”黑客组织又攻击了俄罗斯和伊朗的大规模网络基础设施。攻击不仅导致网络中断，还将路由器的一个文件篡改为警告消息：“不要干扰我们的选举……—

JHT”，并留下了一面用字符组成的美国国旗；4月9日，德国纳图（Natus）医疗设备被曝出多个漏洞，这些漏洞可导致远程代码攻击和拒绝服务攻击，影响脑电图设备。

2018年3月，美国联邦调查局和国土安全局表示，俄罗斯网络黑客正在攻击美国关键基础设施，包含了能源网、核设施、航空系统以及水处理厂等。这是美国方面首次公开确认遭到基础设施网络攻击。

随着关键信息基础设施攻击事件日益频繁，我国加大了对关键信息基础设施的保护程度。

2017年7月，国家互联网信息办公室发布了《关键信息基础设施安全保护条例（征求意见稿）》，划定了关键信息基础设施的保护范围，规定了安全保护的基本制度，关键信息基础设施防护进入全面提速期。

当梳理完网络“黑产”的类型后，我们会发现，在这条黑色产业链中，有的人负责提供技术，有人负责搭建平台运营，有的负责扩大组织规模。如果按照“上游、中游、下游”进行分类：上游是提供技术的黑客，中游为黑色产业犯罪团伙，下游则是支持黑色产业犯罪团伙的各种周边组织。

目前，对网络犯罪的打击主要是从下游犯罪出发，对上游和中游的打击还存在力度不足等诸多困难。现在，国际社会已经加强了在网络犯罪打击方面的合作。例如联合国毒品与犯罪问题办公室一直在就网络犯罪做出战略响应，为全球70多个国家提供技术支持和能力建设，与全球政治领导、司法官员、执法部门及专家学者合作，共同推动打击网络犯罪、在线儿童色情、毒品贩卖、人口贩卖、武器交易以及恐怖主义等领域的国际合作。

2017年9月，在360主办的中国互联网安全大会（ISC）上，联合国毒品与犯罪问题办公室网络犯罪全球项目主管尼尔·沃尔什（Neil Walsh）做了一场精彩的主题演讲。他说，作为联合国框架下刑事事务的负责部门，他们已经把帮助各成员国打击网络犯罪纳入工作日程之内，并在全球范围内开展技术支持和能力建设，提供反网络犯罪政策法律支持，推动有关网络犯罪的国际新合作、新动议。

我国也先后跟美国、俄罗斯、英国等全球多个国家在合作打击网络犯罪领域达成了共识，积极推进网络安全国际执法合作，通过广泛的国际合作，积极营造全方位、宽领域、多层次、讲实效的打击网络犯罪国际执法合作格局。

“黑产”的四大趋势

至此，我们可以说对网络黑色产业完成了“庖丁解牛”的工作。未来，网络“黑产”的攻击重点、发展趋势又是哪些呢？从近几年发生的网络安全事件中，我总结了网络“黑产”的四大趋势。

趋势一：关键信息基础设施逐渐成为攻击重点

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。一旦被攻击，就可能导致交通中断、金融紊乱、电力瘫痪等问题，带来灾难性的后果。我在很多公开场合曾经呼吁过，一系列真实发生的案例告诉我们，关键信息基础设施已经成为网络空间安全战争的主战场。

2018年4月10日，华盛顿自由灯塔网（Free Beacon）刊载了一篇文

章《美国入侵外国网络基础设施威慑中国和俄罗斯》，其中提到“美国军事网络战士准备在未来的冲突中，通过网络入侵来关闭中国和俄罗斯的关键信息基础设施”。

美国网络司令部指挥官的提名人保罗·纳卡森（Paul Nakasome）指出，对关键信息基础设施网络的网络攻击是“国家盔甲的关键弱点”，对美国的安全构成了重大威胁。

据公开资料统计，全球信息基础设施发生重大网络安全事件的类型主要有敏感信息泄露、系统破坏、金融资产盗窃等。从共性上看，不同领域关键信息基础设施一般都会遭遇敏感信息泄露问题，而不同领域也呈现出一定的自身特点，例如，金融领域的窃取金融资产的事件明显偏多，通信、能源领域的系统破坏事件较多，而教育行业领域网站遭篡改的事件明显多于其他领域。

根据360威胁情报中心对监测数据分析，关键信息基础设施中金融、交通、能源等领域最容易遭受网络攻击，其中金融（33.1%）、医疗卫生（12.7%）、交通（9.9%）、工业（6.3%）等领域信息基础设施发生的重大网络安全事件最多。

关键信息基础设施面临着巨大安全风险，可引发级联危害。此类攻击可以让网络攻击者不费一枪一炮，就达到破坏社会正常秩序、引发混乱甚至政权更迭等目的。

趋势二：虚拟货币将成为网络犯罪交易的主流支付方式

由于虚拟货币可以完全隐藏交易记录，所以这类货币交易从理论上确实可以逃避监管和追责。因此，类似比特币之类的虚拟货币，未来可能成为网络犯罪交易的主流支付方式。

我们曾协助警察追查过一起能源行业网络犯罪事件，涉案金额超过千万元。黑客入侵了某能源行业网络系统，盗取了千万额度的充值卡并在网络上通过代理商进行销赃。整个过程从技术角度做得非常隐蔽，在技术侧，根本找不到这名黑客的真实身份。

传统的网络类犯罪事件侦破多数依靠经济途径，但在此案中，黑客巧妙地通过比特币代购中间人进行洗钱。流程是：黑客向代理商销售充值卡后，将货款直接打入比特币代购中间人的账户，黑客再联系中间人直接购买对应金额的比特币，中间人并不知道钱的来路，只当是买比特币的货款，买成比特币打入黑客的比特币钱包地址。

在这起案件侦破的过程中，警察找到了比特币代购中间人，经过确认，中间人对钱的来源并不知情。整个交易期间，黑客不需要露面，全程互联网指挥交易。最终该案件不了了之，黑客带着约3000枚比特币销声匿迹。

趋势三：“零日漏洞”被视为珍贵的资源甚至武器

“零日漏洞”是指被发现后，还处于未被公众和对应软件厂商所知，还未有相应补丁的漏洞。此类漏洞由于其扩散范围非常小而且又没有对应的防护措施，使得对漏洞的利用具有极高的隐秘性和成功率，是黑客真正的“撒手锏”。

虽然目前软件设计、编程范式在安全性方面不断更新，漏洞测试人员的水平不断提升，软件商研发漏洞补丁的速度日趋加快，但“零日漏洞”还是无法完全避免。

正因如此，“零日漏洞”已被视为一种珍贵的作战资源，甚至武器，由此产生了“零日漏洞”的交易市场。

“零日漏洞”的发现者主要是独立的黑客以及专门从事漏洞挖掘的安全公司。“零日漏洞”从被发现到被软件厂商修复，可能需要长达数年的时间。“震网”病毒中使用的Lnk漏洞在多年前就被Zlob木马使用过，但直到“震网”事件曝光微软才了解到情况。

在发现“零日漏洞”后，发现者有可能将其出售给各类买方，以换取利益。根据买方的不同，随漏洞信息一起出售的内容可能还包括但不限于：完整的漏洞利用程序、漏洞利用程序所需要的攻击载荷、特洛伊木马、监听工具包等。

过去几年中，市场上对于“零日漏洞”的需求大幅增长，以漏洞挖掘为主业的小公司越来越多。大型安全承包商纷纷招募职业黑客团队，以完成为政府开发漏洞利用程序的任务。这个市场变得更加商业化，价格也随成交量水涨船高。随着买家和卖家数量暴增，“零日漏洞”交易的地下黑市逐渐变成了网络武器集市。

趋势四：处于混沌状态的网络“灰产”日益庞大

除了传统的黑色产业，还有庞大的网络灰色产业市场，其市场份额是“黑产”的无数倍。这类灰色产业市场包括水军、小贷等多种打擦边球的产业形态，没有人真正治理。

传统安全市场纯投入、少产出，各公司在安全方面的投入都比较有限，但大部分公司在推广、包装方面会投入较多资源资金，这方面的灰色产业规模巨大。比如，部分创业公司、自媒体、P2P等公司，为了数据或报表雇佣该类团伙进行数据作假，从而达到完成指标、欺骗资方等目的。

据我了解，在数据交易部分，尤其是征信数据，曾有公司想整合小

贷、P2P公司的内部征信数据进而形成征信联盟，但并没有做成。经过分析发现，各家小贷和P2P公司都在想着扯竞争对手的后腿，因此经常出现假数据的情况。

上文提到的“零日漏洞”交易中也出现了日益庞大的灰色市场。“零日漏洞”灰色市场的主要买家是各国的情报机构、安全承包商和专职的私营漏洞交易商，他们的客户往往来自政府。买卖双方参与漏洞交易的初衷都是为了利用“零日漏洞”来保障公众安全和国家安全，但谁也不敢保证买方在拿到了漏洞后，是否会对其进行滥用。这使得一些原本会流向软件厂商、会被修复的漏洞，流入了那些只想利用这些漏洞的个人和组织机构手里。

值得关注的是，这类灰色产业达到了一种相对的共赢模式，目前没有形成明显的攻守关系。我判断，网络“灰产”的市场份额还将进一步扩大。

第二节　网络白色产业

有罪犯的地方就有警察，有黑就有白，有攻就有防。前一章中我讲到，缺陷是天生的，漏洞是不可避免的，人类将永远与漏洞作战。如果我们想把每一个技术环节的漏洞全部挖掘并且修复，这肯定是不可能完成的任务。只有专业安全人才能对特定漏洞进行以人为本的审查和分析，才能为系统安全提供决定性的帮助和提升。

围绕漏洞展开的安全攻防对抗是网络安全行业永恒的主题。在人们对抗网络“黑产”的过程中，以防漏洞为核心的网络白色产业应运而生，网络安全行业在持续不断地开发相应的产品、系统、平台、模式与攻击者对抗，网络“白产”呈现出如火如荼的态势。

从广义上来看，整个网络安全产业都属于“白产”，包含网络安全厂商所提供的各种安全产品和服务。比如，防火墙在内部网和外部网之间、专用网与公共网之间的界面上构造了一道保护屏障；网闸从物理上隔离、阻断具有潜在攻击可能的一切连接，增强网络的抗攻击能力等。

从狭义上来说，网络白色产业是围绕漏洞的评估、发现与响应工作而形成的产业。其中，漏洞挖掘技术是“白产”的核心技术，漏洞防护是“白产”快反的高级手段。随着漏洞响应平台、安全众测、实战攻防演练等不断发展壮大，“白产”已经渗透到了社会各个层面。

漏洞挖掘是“白产”发展的核心技术

在网络世界中，我们一直说“未知攻，焉知防”，与攻击者对抗的核心就是漏洞挖掘能力。这里的漏洞既包括IT产品自身存在的技术漏洞，也包括系统防护体系可能存在的管理漏洞。

从这方面来说，如果单个公司一对一比较，360与美国任何一家网络安全公司相比，能力都是不相上下的。2017年2月，在美国的信息安全大会（RSA　Conference）上，360派出的30多位专家与美国同行进行了全面交流，我们专家的能力令美国同行相当吃惊。

2017年底，美国联邦调查局官方宣布“美国断网事件”告破，并向360等协助破获该案件的公司和组织公开致谢。2016年，美国东海岸大面积断网，严重影响当地人民生活秩序和社会稳定，360本着共建网络空间命运共同体的原则，一起参与了这次事件的追踪、分析、溯源和响应处置工作。联合行动小组的参与者包括全球多家顶级网络供应商和顶级安全公司，而360是东半球唯一参与处置该事件的公司。

2018年6月，施耐德电气官方致谢360协助修复了旗下产品U.motion builder中的两个严重漏洞。360安全监测与响应中心研究员发现漏洞后，第一时间上报给施耐德电气，并协助其修复安全隐患。

漏洞防护是“白产”快反的高级手段

安全公司的核心业务是补漏洞、防攻击，围绕漏洞防护而形成的网络安全产品是“白产”快速反击的高级手段。

比如漏洞扫描与评估是一类重要的网络安全产品，通过对网络系统的扫描，安全人员能了解安全配置缺陷，及时发现安全漏洞，客观评估

网络风险等级，在黑客攻击前采取安全防范措施，这是一种主动的安全防范技术。

传统的漏洞扫描与评估产品是网络安全产业中的一个非常成熟的细分市场，已经有二十多年的发展历史。经过长年的发展，这些产品对标准的操作系统Windows、Linux和标准的数据库等应用的支持都已经非常完善，扫描的准确性和性能也很难分伯仲，而且它们都在不断优化和强化资产识别、漏洞优先级分析和评估、漏洞报告等功能。

漏洞扫描产品主要有基于网络和基于主机两种形态。基于网络的扫描器就是通过网络来扫描远程计算机中的漏洞；而基于主机的扫描器则是在目标系统上安装了一个代理或者是服务，以便能够访问所有的文件与进程，这也使得基于主机的扫描器能够扫描到更多的漏洞。安全配置评估产品则是基于安全缺陷知识库，检测和发现网络系统配置中存在的安全缺陷。

我们谈到的漏洞扫描与评估产品往往是这两类工具的集成，这种产品的区分可以帮助我们更好地理解这个市场。虽然漏洞扫描产品和技术已经非常成熟，但是安全配置评估却可能随着具体应用环境和场景的不同而体现出更多的产品差异化。

漏洞平台是“白产”打黑的基础设施

漏洞防护的最终目的是为了及时发现漏洞，并及时进行响应。为了提高漏洞发现能力，专门关注、收集漏洞的漏洞响应平台由此诞生。目前，国内民间的漏洞响应平台主要以补天、先知、漏洞盒子等为代表。

补天漏洞响应平台成立于2013年3月，是专注于漏洞响应的第三方公益平台，通过充分引导和培养民间的“白帽”力量，建立实时、高效的漏洞报告与响应机制。补天平台作为负责任的民间漏洞响应平台，主动担当起了民间安全爱好者正向成长、政企用户安全能力有效提升、“互联网+”经济新形态健康发展的历史责任和社会使命。

截至2017年12月，补天平台汇聚4万余名“白帽子”，累计发现超过25万个各种类型的安全漏洞。面对复杂多变的网络安全态势和层出不穷的攻击手段，补天平台通过创新的安全众包模式服务广大用户，让“白帽子”以黑客思维，站在攻击的立场上去帮助用户发现问题、解决问题，促进用户树立动态、综合的防护理念，维护用户的网络安全。

阿里云旗下的云盾先知（安全情报）平台（简称“先知平台”）主要通过现金激励的方式，公开收集通用软件，特别是阿里云上的通用软件的零日漏洞，从而帮助软件商提前发现并修复潜在的漏洞威胁，降低网站遭受漏洞攻击的风险，提升阿里云的安全防范能力。

漏洞盒子（隶属于创业公司上海斗象信息科技有限公司）是一个企业级互联网安全测试平台，也是国内互联网安全咨讯网站Free Buf（Free Buf.com）的兄弟产品。漏洞盒子通过契约精神、有效沟通以及“白帽子”资源的合理配置，为企业提供互联网安全众测服务。

为了提高漏洞发现能力，目前各大漏洞响应平台都推出了漏洞奖励计划。简单来说，漏洞奖励计划是软件厂商向发现软件安全漏洞的安全人员付费。安全人员将发现的漏洞出售给软件厂商，以获取利益。软件厂商在通过漏洞奖励计划购买了安全人员报告的漏洞后，将很快推出针对此漏洞的软件更新补丁。

攻防大赛是“白产”聚智的重要平台

网络空间的攻防对抗，归根结底是人才之间的竞争。网络攻防大赛正是在全民中聚集网络安全人才的最好途径之一，攻防大赛既可以提升人才的技术水平，也能提升各方的协作能力。

网络攻防大赛最早起源于“BBS黑客竞赛”，由电脑黑客秘密大派对（DEFCON）创始人杰夫·莫斯（Jeff Moss）于1993年发起。此后，在各界的广泛参与下，各类网络攻防大赛开始蓬勃发展。

比如，全球著名的攻防大赛Pwn2Own创立于1997年，由美国五角大楼网络安全服务商零日计划（Zero Day Initiative，ZDI）主办。微软、谷歌、苹果、零日计划等全球知名软件厂商和安全解决方案提供商提供赞助，它们提供最新和最安全的主流桌面操作系统、浏览器以及桌面应用作为攻击对象，同时为获胜参赛队提供奖金。

在Pwn2Own 2017世界黑客大赛上，360安全战队在Pwn2Own官方积分榜占据榜首，成功加冕“世界破解大师”（Master of Pwn）总冠军，这代表着中国在网络攻防最高水平的对决中登上世界之巅。

在我国，攻防比赛的热度近几年也明显升温。据不完全统计，2017年全年国内各类不同规模的攻防演练超过了100场，各类网络安全攻防比赛的总数近200场，参与比赛人次近60000人。

2018年，360企业安全集团参与协办了公安院校内实力强、规格高的网络安全技能选拔比赛——“蓝帽杯”。这是中国首个针对公安院校的大学生网络安全技能大赛，聚集了中国公安院校内顶级的网络安全人才参与，也体现了公安院校网络安全技能的最高实力。

安全众测和实战攻防演习是“白产”推广的重要途径

相比于传统的漏洞防护模式，安全众测突破了人员、时间、空间等诸多限制，可以在短时间内借用社会力量开展全天候的安全测试工作。不同人员的经验背景和测试分析角度的差异，使得他们能够从不同层面发掘安全漏洞，更全面地提升安全水平。

实战攻防演习以实际系统为战场，以日常运维的实际队伍为防守方，最大程度模拟真实攻击，攻击模式不限制单个系统、不限制内网渗透、不限制通过周边系统迂回，以拿到目标系统控制权为目标，来发现安全防御体系中包括流程、协同人员能力、系统设备等方面可能存在的薄弱环节和漏洞，指导修复，提升防御能力。

美国五角大楼是安全众测和实战攻防演练的忠实拥趸。从“黑掉国防部”“黑掉陆军”到“黑掉空军”，演练的层次、深度和效果越来越深入，引发了全球网络安全行业“跟随效应”。

2016年4月，美国国防部举行了名为“黑掉五角大楼”的黑客大比武，悬赏邀请民间高手寻找五角大楼网站漏洞，结果找到超过上百处隐患。这次众测吸引了超过1400人参加，在五角大楼5个对外开放的网站中寻找安全隐患。五角大楼为这次竞赛花了15万美元，其中半数是奖金。一名参赛者发现多处漏洞，获得最高奖1.5万美元，其余获奖者最少拿到100美元。

2016年11月，美国国防部又展开了“黑掉陆军”项目。与“黑掉五角大楼”不同，“黑掉陆军”不仅邀请黑客评估静态网站，关注重点还放在

征兵网站和申请者及现役军官的个人信息数据库上。

我国对安全众测和实战攻防演习的重视程度也不断加大。在承办某城市2018年实战攻防演习活动中，360用一周的时间，进入了9家单位的内网系统，获得了域控服务器、工程管理系统、节目编排系统、监控系统、校园一卡通系统等重要系统的服务器权限。

“白产”的三大趋势

上一节，我总结了网络黑色产业的四大趋势，对它做出了科学预判。按照相似的逻辑，我总结了网络白色产业的三大趋势。

趋势一：漏洞扫描与评估产品的应用场景将不断扩展

随着云计算、虚拟化数据中心、移动应用、IoT/OT设备等IT技术的持续演进和应用的深入，传统的漏洞扫描与评估技术面临着新的技术挑战，产品的功能和支持的应用场景也在不断扩展，主要包括：

支持基于主机代理软件（agent-based）的扫描器，以适应云计算和虚拟化数据中心的应用场景；为提高资产的发现与识别能力，提高漏洞扫描的效率，漏洞评估产品需要与虚拟化管理平台、企业移动管理（EMM）平台以及云服务提供商的应用程序编程接口（API）等的集成能力；拓展扫描能力，支持虚拟化环境中的容器技术；增强开源组件的漏洞扫描检测能力；支持IoT/OT应用场景，能够支持可编程逻辑控制器（PLC）、因特网连接共享（ICS）、数据采集与监视控制系统（SCADA）等工业控制设备的漏洞扫描与评估；支持SaaS模式交付；支持移动设备和应用的漏洞扫描与评估等。

虽然传统的漏洞扫描与评估产品在持续不断地扩展能力，但某些应用场景由于其技术特殊性，需要进行更加深入的漏洞检测与评估，需要特定的资源，甚至需要采用完全不同的漏洞检测技术和评估方法，同时，这些场景的应用程度又要足够广泛，这样就有机会发展成为独立的漏洞扫描与评估产品品类。

趋势二：威胁情报和机器学习将发挥巨大作用

漏洞扫描与评估只是漏洞管理工作的第一步，根据评估的结果进行漏洞的修复或缓解，才能够排除安全风险。

理想状况下，漏洞扫描与评估工作完成后，大家就应该立刻进行修复或缓解工作。但现实往往不是这样，我们遇到的第一个挑战就是，我们的资源和时间都是有限的，在实际工作中不可能立刻修复和缓解发现的每一个漏洞。因此，对发现的大量漏洞进行风险评估和修复优先级排序极为重要。

传统的优先级排序算法主要考虑资产重要性和漏洞严重性这两个因素：风险=资产重要性×漏洞严重性。漏洞严重性可以采用通用漏洞评分系统（CVSS）定义的0～10分值，或者简单采用“高／中／低”这样的表述，计算出风险分值，根据风险分值，排定漏洞的优先级。市场上有的漏洞评估产品还引入了更多的因素，采用了更加复杂的算法进行细粒度的排优。但即使采用更加复杂的算法，用户面临的大量需要处理的问题可能还是很难解决。

如果我们回到问题的本源，风险是与威胁相对应的概念，在排优算法中加入威胁相关的数据，可以极大缩减待处理漏洞的数量，优化漏洞排优算法。2011年在美国芝加哥创立的漏洞管理和风险智能安全公司肯

纳安全（Kenna Security）就采用了这种方式，在漏洞排优中引入了威胁情报和机器学习算法。

肯纳的技术将外部互联网的泄露数据、零日漏洞威胁情报与内部漏洞扫描数据进行结合，可以实时监控组织内部的网络安全风险程度，并在风险程度超过预设的阈值之后通过告警系统通知组织相关人员采取相应行动。

可利用的威胁情报及上下文数据包括：观测到的与漏洞相关的安全事件数量、公开已获得的漏洞利用代码、已知的恶意代码家族或攻击工具套件使用的漏洞、监测到相关的组织受到类似的攻击等。可以说，这些情报和数据在未来将越来越重要。

趋势三：传统的漏洞管理平台将逐渐转变为“漏洞响应平台”

在新的安全态势下，漏洞信息和漏洞利用代码借助安全社区和社交软件，传播的速度大大加快，很快就会形成安全热点事件，传统的按部就班、周期性执行的漏洞管理流程已经很难应对快速的漏洞攻防态势，这就需要我们改变观念，把传统的“漏洞管理平台”转变为“漏洞响应平台”。这个平台的关键要素有三点。

第一点是数据驱动。这里的数据主要包括两大类：漏洞情报库和本地漏洞库。通过两类数据的关联分析，形成安全事件和漏洞处理工单，驱动整个漏洞响应流程的运转。

漏洞情报库将整合国内外主要漏洞库、各种漏洞发现平台等的漏洞数据，建立统一化的漏洞库，之后通过平台支撑，监控各种安全社区、整合威胁情报数据（与漏洞相关）、收集验证漏洞证明（POC），等等，使用这些数据对统一化的漏洞库进行丰富化处理，形成以漏洞为核

心的漏洞情报库。

本地漏洞库以本地漏洞数据为中心，使用资产数据、企业环境数据等进行丰富化处理，给每个漏洞打上内容丰富的标签，同时支持各种漏洞扫描与评估结果的数据归一化处理。

第二点是及时响应。能够与资产管理系统、系统级芯片（SOC）平台、漏洞扫描与修复、漏洞修复与缓解等产品集成，构建事件触发、工单处理的流程和系统模块，形成自动化响应。

第三点是人的参与。漏洞的安全运营需要专业安全分析人员、安全决策人员的参与，平台系统需要建立不同的角色和任务流程引擎。

第三节　打造凝聚“白产”力量的平台

2005年前后，木马病毒呈指数级爆发，流氓软件泛滥成灾，给网民上网造成了极大的不便。为了保证用户的上网体验和网络安全，360创新推出了“非白即黑”的技术，并宣布将个人安全软件免费。我们的这个决定改变了中国安全市场格局，几乎没有人再买收费杀毒软件了。

由于动了整个行业的奶酪，360的品牌受到了巨大伤害。如果上网搜索360，出来的结果都是360是流氓公司。很多网民，包括一些高学历的知识分子，都对我们不信任，认为360为了赚钱肯定做了坏事。有一段时间，我们招人都很困难。

更严重的是，网络白色产业也受到了巨大伤害。我们原本是想做“白产”的领头人，发动网民的力量一起对抗“黑产”。但是如果大家对我们不信任，那么对抗“黑产”的力量就变成了一盘散沙，各自为战，甚至会有越来越多的网民失去了对抗“黑产”的意愿和能力。

在这样的背景下，迫切需要打造一个凝聚“白产”力量的平台，通过搭建一个安全产业的交流沟通平台，把中国的安全从业人员、创业人员，以及国外的安全产业、学术代表聚集在一起，共同推动产业发展。因此，我们产生了举办中国互联网安全大会（ISC）的想法。

办法总比困难多，向安全从业者致敬

举办ISC的第一年，我们面临着重重困难。互联网公司认为我们是竞争者，安全同行认为我们是砸他们饭碗的人，几乎没有人支持我们。一些同行甚至在会议当天闹事，在展区人流量最大的地方发避孕套，造成人流堵塞，并雇人把侮辱性的文章贴在厕所，或者是贴在肚子上全展区走动，目的就是破坏会议。

面对这些阻碍，我们更加坚定了决心，要开一个真正对从业者有价值的会。我们制定了两个原则：第一，绝对不卖主会、分会演讲，不卖冠名，一定要以高水平的技术演讲为主；第二，ISC永远不盈利，卖票和展区招商是为了提升听会和参展质量，但全部都要再投入到会议中去。同时，为了保证围绕技术主题的分论坛的质量，我们决定每个分论坛都请一个在该领域最权威的机构来做主办单位。

2013年，第一届ISC召开的前一天下了一场大雨，我们非常担心会影响观众参会。但第二天一大早，就有观众从外地坐火车赶了过来，最后参会人数超过了3000人。当主会开场视频最后一句话“向所有互联网安全从业人员致敬”出现的时候，现场响起了掌声，很多人都哭了，他们明白这是第一个为安全从业人员开的会，也是第一个安全产业的会。2014年，有了第一届ISC的成功摸索，我们决定邀请更多的国内外知名安全专家，以世界级的眼光共同对网络安全进行深入有效的探讨。我们邀请到了美国首任国土安全部部长汤姆·里奇（Tom Ridge）、计算机病毒之父弗雷德·科恩（Fred Cohen）、派拓网络（Palo Alto Networks）联合创始人兼前首席科学家弓峰敏等嘉宾，会议盛况空前，成了当时安全产业界规模和影响力最大的会议。

2015年，ISC成了中美双方两轨对话的舞台。“斯诺登”事件爆发后，我们第一时间联系到了美国网络司令部首任司令基斯·亚历山大（Keith Alexander）将军，当时他刚刚退役，我们希望他与多位中国网

络安全智库一起共同探讨网络空间安全问题。同时，我们也邀请到了国家创新与发展战略研究会副会长、总参四部退役少将郝叶力。这一届“中美将军对话”成为最大亮点。

2016年，ISC的影响力已经不仅限于中国安全产业界，开始影响到了国际安全界。主会演讲嘉宾来自中、美、俄、韩等多个国家的产业界代表，包括中国工程院院士邬江兴、美国前陆军少将约翰·戴维斯（John Davis）、著名安全软件迈克菲（McAfee）创始人约翰·迈克菲（John McAfee）、俄罗斯安全互联网联盟总干事丹尼斯·达维多夫（Denis Davydor）、IBM安全事业部威胁防护与认知安全首席技术官巴尼·桑切斯（Barny Sanchez）、韩国KITRI 主席（BOB计划负责人）刘俊相（Yoo Joon-Sang）、微软可信赖计算部网络安全战略总监褚诚云等。这些院士、学者组成的顾问专家团达到了上百人，他们贡献自己的智慧、人脉和资源，让第四届ISC成为一个世界级的智库平台。

我们也举办了多个高水平论坛，尤其是由郝叶力将军担任主席的“观潮”网络空间论坛首次成功举办。来自中、美、俄及欧洲多国的安全产业代表就网络空间问题进行了热烈探讨，郝叶力提出的“三视角下网络主权的对立统一”理论得到了国际社会的广泛认同，让国际社会听懂并开始认同“中国声音”。

2017年，参加ISC的嘉宾更加多元丰富，既有原美国海军四星上将威廉·A.欧文斯（William A.Owens），联合国毒品与犯罪问题办公室（UNODC）网络犯罪全球项目主管尼尔·沃尔什（Neil J.Walsh）等专家，围绕国家和国家间的网络空间战略进行演讲，还有传奇黑客、电影《我是谁》（*Who Am I*）的原型人物本杰明·昆兹·梅杰里（Benjamin Kunz Mejri），世界著名的漏洞搜集平台ZDI负责人布莱恩·戈伦茨（Brian Gorenc）等世界知名黑客从技术角度进行演讲。国际著名生物

黑客帕特里克·鲍门（Patrick　Paumen）还在大会现场演示了如何运用体内植入物获取信息、解锁门禁手机，以及发送加密邮件等。他的黑客秀让人大开眼界，让公众对于黑客技术的扩展有了更多想象。

永不落幕的盛会，产业趋势的风向标

五年来，ISC累计接待人次达13.6万人，演讲议题超过700个，演讲嘉宾覆盖20个国家，涵盖部级领导、两院院士、国外将军等，参会安全机构共计300多个，与国内外15个研究机构有合作，与全球超过27所知名大学有过交流，全球著名的165家的安全公司来安全大会做过演讲和交流。

现在，ISC不再只是一个每年开两天的安全盛会，每个月都有相关活动，多个分论坛在日常也会开研讨会、外地沙龙。ISC已经变成了亚太规模最大、影响力最大的安全会议平台，成为一个永不落幕的ISC。

ISC不仅将整个中国的互联网白色产业聚集了起来，也在人才培养和产业上也取得了很大进展。为了提升安全从业人员人员的能力和见识，ISC已经连续5年在大会上举办安全攻防培训“安全训练营”，邀请国内外最知名的安全“白帽”来给国内从业人员培训，已经累计培训了超过2000多名从业人员，开创了安全高端培训的先河。

成功举办了两届的“观潮”网络空间论坛已经形成了固定运营机制。论坛以“凝聚共识，携手共治”为宗旨，致力于打造一个开放包容的国际化交流平台，汇聚各国顶级专家学者和企业精英，分析研讨网络空间政策和安全动态，实现和推动各域、各界的深层次互动，为网络空间研究与治理提供多维全息视角。

同样，举办了两届的“安全创客汇”推动了安全产业创业水平。两年的冠军分别是身份安全领域的芯盾科技、区块链领域的众享比特，都因为获得了比赛冠军分别获得了上亿元投资，增强了安全创业人员的信心，激发了安全基本方的投资热情。

更让我感到自豪的是，每年ISC大会的主题都对未来一年的网络安全研究和产业起到了风向标的作用。从“共筑网络安全世界”“互联世界、安全第一”到“数据驱动安全”“协同联动共建安全+命运共同体”，再到“万物皆变：人是安全的尺度”，我们每年提出的主题都成为安全行业的趋势和主要技术方向，成为未来一年网络安全领域的核心关键词。

2018年的秋天，来自世界各地的观众将如约相聚在北京，共谈互联网安全产业热点，沟通全球互联网安全技术趋势。

至此，我们可以说已经完成了对漏洞产业化的全面剖析。在漏洞的生产和产业中，黑客作为技术主体，其地位和作用不言而喻。接下来将重点分析黑客，讲述这个充满传奇色彩的职业和故事，如果没有他们，那么关于漏洞产业的说法无从谈起。毕竟，他们才是追漏洞的人。

Chapter 3
第三章
权杖之手黑客是以武犯禁，还是侠之大者

黑客是追求极致的漏洞捕捉者，对计算机科学、编程和设计具有高度理解。他们似乎总是带着隐秘的面纱，在网络的世界里无所不能。

360从成立就开始“追”这些挖漏洞的黑客。第一个加盟360的黑客是“mj0011”郑文彬。我还记得第一次看见他是在大冬天，郑文彬从广州飞到北京的时候，还穿着拖鞋。

在我和周鸿祎坚持不懈的“追逐”下，著名反黑客工具冰刃和狙剑的作者、墨者公司创始人及其主创团队，还有国际知名的少年攻防专家被我们揽入麾下。他们的加盟让我们的产品和能力不断提高，同时也让360成为黑客交流、沟通的最好平台。

若干年后，各大安全厂商和互联网公司，也开始了对这些挖漏洞高手的“追逐”。黑客成为安全领域最热门的“抢手货”，他们挖出来的漏洞，动辄价值百万、千万元以上。

随着网络空间成为第五空间，黑客开始从幕后走向台前，承担起更重要的历史使命。如今，360在过去数十年间培养的黑客分散在世界各

地，成为一股守卫网络空间安全的重要力量。

第一节　黑客演化史

什么是黑客？黑客到底是什么人？如果让我来回答，答案很简单——黑客是追漏洞的人。

“黑客”一词是英文“Hacker”的音译，通常是指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员。随着时代的发展，黑客与英文原文Hacker、Cracker等含义不能够达到完全对译，这是中英文语言词汇各自发展中形成的差异。随着时代的发展，逐渐被人们区分为“白帽”“灰帽”“黑帽”等。

黑客从诞生之日起，就随着计算机和网络的发展而不断发展。从单纯对技术痴迷到臭名昭著，从“白”变“黑”，这群特殊的人慢慢地“黑化”了。

20世纪60—70年代：黑客诞生

麻省理工学院（MIT）的学生把解决计算机难题的方法称为“Hack”，相应地，从事“Hack”的人就是“Hacker”，也就是“黑客”。在他们看来，要完成一次“Hack”，需要高度的革新、独树一帜的风格和出色的技术。“黑客”这个词刚出现的时候，完全是正面意义上的称呼。

黑客最早诞生于20世纪60年代。1961年，MIT得到了第一台计算机，吸引了许多学生的兴趣。MIT有一个学生团体，叫做“铁路模型技

术俱乐部”（Tech Model Railroad Club），一群计算机鬼才们天天聚在一起，热衷挑战，畅游在技术的海洋中。

当时，俱乐部成员们为修改功能而黑了他们的高科技列车组。然后，他们从玩具列车推进到了计算机领域，试图扩展计算机能够完成的任务，探索、改进和测试计算机程序的极限。

后来，这个俱乐部诞生的“黑客”，成为MIT人工智能实验室的核心成员。《黑客》（*Hackers*）一书的作者史蒂文·利维（Steve Levy），把他们称为“计算机革命的英雄”。

到了20世纪70年代，黑客持续繁荣，诞生了“电话飞客”——玩弄电话系统的黑客。其代表性人物是黑客约翰·德拉浦（John Draper），他被人们称为“嘎吱上尉”，曾是许多人崇拜的英雄，包括苹果联合创始人斯蒂夫·沃兹尼亚克（Stephen Wozniak）。

当时，美国电话电报公司（AT&T）垄断了长途电话业务，收费极高，价格很不合理。对很多黑客来说，闯入其电话系统成为当时最有趣也最富有挑战性的信息技术。约翰·德拉浦是其中感兴趣的黑客之一，于是他疯狂钻研，试图入侵系统实现免费拨打。结果，他发现通过“嘎吱嘎吱船长”（Cap’n Crunch）牌麦片盒里赠送的玩具口哨，可以实现成功入侵。原来这个口哨可以发出2600赫兹的声音，电话交换机收到这个频率的信号以为通话中断便停止计费，于是可以继续打免费电话。

在口哨的帮助下，德拉浦又发明了另一个有名的电话盗打器——蓝盒子（Blue Box）。蓝盒子是一个信号发生器，它能发出各种电话网上的模拟信号频率，而早期的电话网又都是模拟网。直到1972年，电话公司发现他的账单很奇怪，每次通话都只有短短一两秒，德拉浦因此被判

入狱2个月。

德拉浦可以说开创了“盗用电话线路”的先河，其他“电话飞客”也开始玩弄电话系统，免费享用长途通话。“电话飞客”文化不仅仅造就了德拉浦这样有影响力的黑客，也打磨出一批具备数字远见的人。

20世纪80—90年代：黑客的分水岭

虽然大量黑客仍然专注于改进操作系统，但一群更关注利用技术为个人带来利益的“新”黑客渐渐浮出了水面。他们将自己的技术用于盗版软件、创建病毒和侵入系统盗取敏感信息等犯罪活动。

20世纪80年代，完备的个人计算机进入了公众视野，同时也成为黑客历史的分水岭。计算机不再局限于大公司和名校所有，每个人都可以用计算机干自己的事。个人电脑的广泛普及，引爆了黑客的快速增长。

在这一时期，中国黑客也开始由星星之火渐成燎原之势。当时，中国互联网处于起步阶段，一些热爱新兴技术的青年受到国外黑客技术的影响，开始研究安全漏洞。

这些黑客大多出于个人爱好而走上这条道路，好奇心与求知欲是驱使他们前进的动力，没有任何利益追求。他们通过互联网看到了世界，他们崇尚分享、自由、免费的互联网精神，并热衷分享自己最新的研究成果，与西方发达国家同时期诞生的黑客精神是一脉相传的。

1981年，《纽约时报》（*New York Times*）曾详细描写了黑客这一群体：“黑客是技术上的专家，技艺精湛，通常很年轻，总是带着奇思妙想来试探计算机系统的防御系统，总是探寻着机器的极限和可能性，

尽管他们总是看起来像是在破坏系统，但他们是计算机行业中重要的资产，通常来说非常有价值。”

“黑客是能做好事也能做坏事的数字专家”这一概念开始进入人们的认知。一系列的书籍和电影推广了这种认知，例如1983年上映的美国科幻电影《战争游戏》（War Game）。

这是开黑客电影之先河的一部电影，讲述的故事发生在里根总统任期，当时正值美苏冷战高峰。影片主角中学生戴维是一位电脑天才，误打误撞地进入了北美空防司令部专门用于对苏战争的军用电脑，并用它玩起了“第三次世界大战”的模拟游戏，从而引发了一连串风波，险些引发真正的第三次世界大战。这部电影让人们初次感受到地下技术的能量，激发了人们对地下技术的好奇和向往，而这名电脑天才戴维的原型，正是著名的“世界头号黑客”凯文·米特尼克（Kevin Mitnick）。

凯文·米特尼克、凯文·鲍尔森（Kevin Poulsen）、罗伯特·莫里斯（Robert Morris）和弗拉基米尔·勒文（Vladimir Lewyn）是这一阶段著名的黑客。他们屡屡犯下网络罪行，包括盗取大公司专利软件、欺骗电台以赢取豪车、制作传播第一个计算机蠕虫病毒，以及主导第一起数字银行劫案。

为了回击这些网络犯罪行为，1986年，和黑客相关的首部立法《联邦计算机诈骗和滥用法案》出台。1990年，美国特勤局执行了一系列清晨突袭，查封了很多用来架设论坛以及为黑客们提供服务的服务器，并逮捕了大量黑客。

这一系列事件让美国的黑客一夜回到解放前，很多黑客团队都解散了，甚至有一小部分人遭受了牢狱之灾。大量的高调抓捕，让“黑客”这

个词开始变得臭名昭著。

21世纪前十年：“新”黑客崭露头角

21世纪，网络技术与现实世界进一步深度融合，人类社会进入数字时代。在这一时期，恶意黑客拥有了更多攻击目标，针对政企的新一类危险黑客开始崭露头角，黑客社区变得更加隐秘复杂，网络黑色产业开始浮出水面。

最早的黑色产业是游戏盗号，黑客通过木马偷装备、卖钱，有的甚至可以月入十几万美元。盗号生意持续火了很长一段时间，随着各大厂商反盗号手段的升级，黑色产业开始转向广告联盟作弊，然后是钓鱼诈骗、贩卖漏洞、制作恶意软件，以及以赢利为目的的攻击行为。

不仅如此，很多黑客组织开始互相攻击，最主要的方式就是DDoS攻击。微软、易贝（eBay）、雅虎和亚马逊等大型公司都曾沦为大范围DDoS攻击的受害者，而美国国防部和国际空间站则是被15岁的小男孩入侵了系统。这个小孩就是之后我要提到的世界著名黑客之一——凯文·米特尼克。

一些小型的黑客组织日益活跃，他们或者在优化软件，或者在发起勒索软件和Wi-Fi攻击。还有一些激进黑客组织，比如“匿名者”，他们发布机密文档，揭露政府秘密，以保护公众免受伤害、利用和蒙蔽的名义，成就所谓的“数字侠客”。

与这些黑客组织一同成长起来的还有网络安全产业。2010年左右，整个网络黑色产业每年都会给互联网造成数十亿美元的损失，黑色产业

日益成熟。为了应对激进黑客和网络罪犯，政府实体和大公司竞相改善安全，计算机巨头努力调整系统，并招募网络安全专家。

对于掌握安全技术的黑客们来说，他们就像是孤独地站在十字路口，面临着两难抉择：做“黑产”项目每年能赚到几百甚至上千万美元，而做网络安全每年辛苦地只能赚到几十万美元。

尽管“黑产”充满诱惑，但越来越多的黑客选择并坚持走上了“白帽”黑客的道路，陆续成长为安全领域的高级人才，成为维护世界网络、计算机安全的主要力量。

第二节　最牛的黑客传奇

有人的地方就是江湖，更何况是神秘的黑客。这些具有传奇色彩的世界最牛黑客，亦正亦邪，寻求刺激、挑战权威。在正义与邪恶的较量中，在攻与守的角逐中，黑客客观上推动了网络安全技术的进步，也使得黑客江湖更加血雨腥风，同时也赢得了普通大众对黑客的关注。

世界上一“黑”成名的黑客

互联网始于1969年美国国防部的阿帕网，也是在美国最先开始民用。前文提到的许多大名鼎鼎的黑客，都诞生在美国。他们对网络技术极度痴迷，追寻漏洞似乎是一种本能，他们都充满了传奇色彩。

▶世界“头号电脑黑客”凯文·米特尼克

凯文·米特尼克是第一个被美国联邦调查局通缉的黑客，有评论称他为世界上“头号电脑黑客”。他在15岁时仅凭一台电脑和一部调制解调器，就闯入了北美空中防务指挥部的计算机系统主机，之后他又黑进了五角大楼。现在，这位世界级的黑客成了一名网络安全咨询师。

1963年，凯文·米特尼克出生在美国加利福尼亚州洛杉矶市。3岁时父母离异，他跟着母亲生活。早年时期，米特尼克性格孤僻，在学校成绩比较差，但他其实极为聪明，喜欢钻研。

20世纪70年代末，上小学的米特尼克迷上了无线电技术，并

且很快成为这方面的高手。15岁时，米特尼克凭一台电脑和一部调制解调器闯入了北美空中防务指挥部的计算机系统主机，世界首部黑客电影《战争游戏》正是以此为原型。

1981年，米特尼克和同伙潜入洛杉矶市电话中心盗取了一批用户密码，毁掉了电脑内的一些档案，并用假名植入了一批可供他们使用的电话号码。由于当时米特尼克年纪尚小，被判监禁3个月，外加1年监督居住。之后，他没有收手，五角大楼、摩托罗拉、诺基亚等公司都成为他的入侵对象。他曾使用一台大学里的电脑闯入了美国五角大楼的电脑，被判管教6个月。

1988年他再次入狱。美国数字设备公司（Digital Equipment Corporation，DEC）指控他从公司网络上盗取了价值100万美元的软件，并造成了400万美元损失。由于重犯，他没有了保释机会，被判处一年徒刑，并且被禁止从事电脑网络的工作。

一年后，他又成功地侵入了几家世界知名高科技公司的电脑系统。根据这些公司的报案资料，FBI推算损失共达3亿美元。正当FBI准备再度逮捕他时，米特尼克赶在抓捕前逃之夭夭，从此开始了长达两年的“逃亡生活”。

最后，FBI在另一名黑客高手下村勉（Tsutomo Shimomura）的帮助下，追踪到了米特尼克的行踪，将他抓捕。米特尼克被指控犯有23项罪，后又增加25项附加罪。审判一直进行到1999年3月，米特尼克被判刑68个月，外加3年监督居住。2000年，美国法庭宣布他假释出狱，并要求他三年内不允许接触任何数字设备，包括程控电话、手机和电脑。

禁令到期后，很多公司邀请他去做安全方面演讲，米特尼克逐渐走上“白帽子”的路，华丽转身蜕变成世界顶级安全咨询专家。他开办了网络安全公司，全世界巡回演讲，还出版了《反欺

骗的艺术：世界传奇黑客的经历分享》（The Art of Deception: Controlling the Human Element of Secruity）、《反入侵的艺术：黑客入侵背后的真实故事》（The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers）和《线上幽灵：世界头号黑客米特尼克自传》（Ghost in Wires: My Adventures as the World’s Most Wanted Hacker）等著作。

▶“黑客罗宾汉”朱利安·阿桑奇（Julian Paul Assange）

朱利安·阿桑奇是“维基解密”的创始人，被称为“黑客罗宾汉”。他认为，透露公共治理机构的秘密文件和信息，对大众来说是一件有益的事。至今为止，维基解密已公开了超过1000万个解密档案，卷入了大约100场泄密官司。

1971年，阿桑奇出生在澳大利亚东北海岸的汤斯维尔市。父母离异后，阿桑奇跟着母亲过着吉普赛人式的流浪生活。中小学时期，阿桑奇一共上过37个学校，他的性格因此变得越来越孤僻。

16岁时，朱利安成为一名网络黑客，并和另外两名黑客组成了一个名为“跨国颠覆”的小组，他们曾闯入欧洲和北美的保密计算机系统。他逐渐建立了自己的声誉，被称为“能够闯进最安全网络的高级程序员”。

2006年，阿桑奇创建“维基解密”网站。同年12月，这家网站公布了首份文件：这是一份密件，由索马里反政府武装“伊斯兰法院联盟”领导人签署。不过，这份文件的真实性始终没有得到确认，而关于“维基解密”的新闻很快取代了对密件本身的关注。

维基解密的架构设计极为巧妙，能够最大限度地规避审查，服务器设在瑞典和比利时境内，两国都有全世界最严密的保护消息来源的法律。维基解密成立的第一年中，资料库内就拥有了120万份来自全球各地网络志愿者提供的资料，而且以每天1000份的速度递增。

2010年，维基解密曝光了美国关于阿富汗战争的9万多份机密文件，引起巨大轰动和争议。同年11月，阿桑奇因涉嫌强奸受到瑞典检方调查。随后，身处英国的阿桑奇向伦敦警方自首，被押送到威斯敏斯特地方法院出席引渡聆讯，保释申请被驳回。2012年5月，英国最高法院裁定，可以引渡阿桑奇至瑞典，但是阿桑奇在保释期间进入了厄瓜多尔驻英使馆寻求庇护。

在厄瓜多尔驻英大使馆进行“政治避难”期间，阿桑奇也没有闲着。2016年7月，在美国民主党大会前夕，维基解密公布了民主党内部2万封邮件，最后导致了民主党主席下台。

2018年1月11日，厄瓜多尔外交部表示，厄瓜多尔政府已于2017年12月12日授予阿桑奇厄瓜多尔公民身份。

阿桑奇和他创立的“维基解密”一直以来饱受争议。反对者指责阿桑奇打着自由的旗号，威胁相关国家的国家安全，并影响国际外交；支持者认为他捍卫了民主和新闻自由，他甚至被打上了“新英雄”的标记。

▶“流浪黑客”阿德里安·拉莫（Adrian Lamo）

阿德里安·拉莫被称为“流浪黑客”。他技术高超，居无定所，作案方式十分隐蔽，每次行动都在不同地区的公用电脑上进行。他喜欢使用咖啡店、快印店或图书馆的网络来进行黑客行为，又被称为“不回家的黑客”。

2001年9月，拉莫成功侵入雅虎网站，并篡改了这家网站的新闻内容。之后，他专门找大组织下手，例如微软、《纽约时报》、雅虎、花旗银行和美国银行等知名公司，在入侵后免费为这些公司修补网络安全漏洞。

2002年，他入侵《纽约时报》的电脑系统后，掌握了该报员工大量的个人隐私材料，并将自己的名字添加到专栏版（Op-Ed）投稿人名单中，这次入侵使拉莫成为顶尖的数码罪犯之一。

这一系列入侵使拉莫成为联邦调查局追捕的对象。2003年，他向加利福尼亚州一家联邦法院自首，被判处六个月家庭禁闭、两年缓刑，以及6万美元的罚款。

2010年，拉莫向联邦当局举报士兵布拉德利·曼宁（Bradley Manning）向维基解密网站泄露了美国当局数百份敏感文件。后来，曼宁因拉莫的举报被逮捕，而拉莫则遭到了全国维基解密支持者以及黑客们的声讨。

2018年3月，这位著名的“流浪黑客”突然去世，年仅37岁。据外媒报道，美国堪萨斯州塞奇威克县的验尸官证实了拉莫的死讯，但没有提供进一步的细节。

3月16日，拉莫的父亲马里奥·拉莫（Mario Lamo）在脸书《2600黑客季刊》（2600｜The Hacker Quarterly）中写道：“一个拥有智慧和富有同情心的灵魂已经离开了，他是我亲爱的儿子。”

▶“年少成名”的乔纳森·詹姆斯（Jonathan James）

乔纳森·詹姆斯在互联网上的名字是“c0mrade”，他曾在16岁时因为入侵美国国防部和美国航空航天局（NASA）计算机系统被捕，成为世界上第一个因为黑客行为而被捕的未成年人。后来，他成了网络

安全的守护者，曾帮助FBI找到了电脑病毒“梅丽莎”的制造者。

1999年6月，詹姆斯非法进入了美国国防部总共13个计算机系统，使用两个不同的互联网服务提供者的原始地址发起攻击。他下载了大量美国国家航空和宇宙航行局的专用软件，这些软件支持着国际空间站的物理环境，包括舱内实时温度和湿度的控制，最后导致国家航空和宇宙航行局的计算机系统死机21天，损失巨大。

同年8月到10月，他入侵了美国国防威胁防御机构（DTRA）使用的军队计算机网络。他在入侵的路由器上安装了一个隐蔽程序，拦截了3300多名DTRA员工的电子信息。

这两次入侵事件被发现后，年仅16岁的詹姆斯被判处为期6个月的有期徒刑。服刑结束后，詹姆斯立志开办一家电脑安全公司，开始对网络安全投入大量的注意力，并和FBI展开合作，找出电脑病毒的制造者。

“梅丽莎病毒”的发布者戴维·史密斯（David Smith）就是FBI在詹姆斯的帮助下追踪到的。1999年，美国爆发了“梅丽莎病毒”，詹姆斯成功跟踪到了这个病毒的发布者，并协助FBI成功将其抓捕。次年5月，詹姆斯又帮助FBI找出了席卷全球的“爱虫病毒”的来源。

2008年，詹姆斯被传患癌症去世，年仅25岁。也有媒体报道他用自己的手枪结束了生命，一直到现在，詹姆斯真正的死因仍不得而知。尽管英年早逝，但是他做的很多事情受到了人们的称赞，成为黑客发展历史上浓重墨彩的一笔。

▶“蠕虫病毒之父”罗伯特·莫里斯（Robert Tappan Morris）

罗伯特·莫里斯毕业于康奈尔大学，是美国国家计算机安全中心

前首席科学家莫里斯的儿子。他天资聪颖，在一次工作过程中戏剧性地散播出了网络蠕虫病毒，成为首位依据1986年《计算机欺诈和滥用法》被起诉的“黑客”。现在，他是麻省理工学院计算机科学和人工智能实验室的一名终身教授。

1988年，正在康奈尔大学攻读计算机科学硕士学位的莫里斯，突然心血来潮想探究互联网到底有多大，于是他编写出一个蠕虫病毒的软件程序，这个程序可以通过互联网进入电脑，在当时属于全新的电脑病毒。

原本莫里斯只是想搞清当时的互联网内到底有多少台计算机，但他低估了蠕虫病毒的传播速度和破坏力。1988年11月2日，莫里斯从麻省理工学院释放蠕虫病毒，这个病毒立刻化身网络中的超级间谍，不断截取用户口令等网络中的“机密文件”，利用这些口令欺骗网络中的“哨兵”，长驱直入互联网中的用户电脑。当晚，从美国东海岸到西海岸，互联网用户陷入一片恐慌。

“蠕虫”事件最终导致15.5万台计算机和1200多个连接设备无法使用，国家航空和航天局、军事基地和许多研究机构的网络陷于瘫痪，不计其数的数据和资料毁于一旦，经济损失巨大，对当时的互联网几乎构成了一次毁灭性攻击。随后，莫里斯向联邦调查局交代了自己的罪行。1990年，纽约地方法庭判处莫里斯三年缓刑，罚款一万美元。

现在，莫里斯是麻省理工学院的教授。因为在操作系统、分布式计算和计算机网络上做出的卓越贡献，莫里斯还在2014年当选了国际计算机学会（ACM）的研究员。

我身边的黑客

前文介绍了很多传奇黑客，实际上，他们在广为人知之前，和我们身边的普通人并无二致。现在，我们身边许多看似普通的人，也有可能是水平极高的黑客。尤其在我创办的公司里，由于专业从事网络安全，黑客的比例更高。

▶MJ——360的头号黑客

360有一个代号“mj0011”的黑客，他本名郑文彬，在业界有很多称谓：“国内内核第一人”“驱动神童”“网络奇才”、最早揪出“熊猫烧香”的人，等等，是网络安全领域充满传奇色彩的“明星”。他第一次被广为人知是发现了微软Windows“DirectShow视频开发包”漏洞，被微软官方公开致谢，因而成为业内标杆。2016年，他被中国互联网发展基金会评为“十大网络安全杰出人才”。现在，郑文彬是国家信息安全漏洞库特聘专家，也是360伏尔甘团队（Vulcan Team）负责人。

郑文彬2006年加入360的时候，只有19岁。他的代号是“mj0011”，“mj”是拼音“majia（马甲）”的两个首写字母，刚开始他想注册“mj001”，但是被注册了，于是又加了一个“1”注册了“mj0011”。他经常沉浸在各个技术论坛，很大一部分技术积累都是从网友的帖子中汲取的。他小时候就对计算机技术非常热爱，上高一时，就开始尝试做一些编程，当时电脑还没有普及，最艰苦的时候他只能在草稿纸上写好代码，然后再把代码输入设备里。正是在这个时候，他开始更深入地接触到一些更底层的内核和攻防等技术。

2015年，《人民日报》对他的一篇专访报道称他是“与网络病毒赛

跑”的人。当时，他刚带领360的黑客团队Vulcan Team，从世界黑客大赛Pwn2Own上载誉归来。他们仅仅用时17秒就攻破了Win8.1+64位IE11浏览器，成为自2007年Pwn2Own举办以来，首个攻破IE的亚洲团队。

郑文彬跟我讲，他之前对安全方面的技术只停留在爱好者阶段，进入360之后才有了深入的研究。郑文彬形象地将与黑客之间的攻防战形容为“打CS（反恐精英）游戏”，他认为寻找系统漏洞的过程如同在地图中找到藏着的枪，黑客发现它就会用来“杀人”；但“白客”发现它会藏起来或者销毁，如果“白客”速度更快，就可以保护用户不被攻击，所以要做到“魔高一尺，道高一丈”。

2017年3月11日，携带一揽子“神奇漏洞”的郑文彬和360安全战队队员抵达加拿大温哥华，参加Pwn2Own 2017世界黑客大赛。在赛前缺少测试环境、厂商赛前狂补漏洞和报名失误、规则变化、抽签不利的情况下，郑文彬最终带领360安全战队拿下了分数最高的连环攻击项目，这也是全场唯一一个连环攻击成功的项目。

▶古河——微软Top100安全贡献榜中排名最高的华人、EOS“史诗级”漏洞发现者

2017年，微软发布了TOP100安全贡献榜，表彰为微软系统和软件安全做出杰出贡献的全球100名安全专家，有30名安全专家是华人，其中10名来自360公司。古河名列全球第三，是排名最高的华人。

2018年5月，360发布了市值百亿元的区块链软件EOS的重大安全漏洞，古河正是这个漏洞的发现者。他通过利用这个漏洞完成了远程控制EOS服务端程序的演示，获得了EOS官方致谢和奖金。

古河是国内最高产的桌面软件漏洞研究者之一，也是360伏尔甘团

队的核心成员。他在微软、谷歌、苹果、Adobe等软件中发现了200个以上的高危漏洞并获得厂商致谢。他曾和360伏尔甘团队一起在Pwn2Own、Pwn Fest等世界大赛中攻破包括IE、Chrome、Edge、Flash、Windows10等多个目标。

如果古河坐在你身边，你一定认不出来他就是那个名声在外的黑客。这个瘦弱的安全研究员戴着一副眼镜，看上去斯斯文文，话也不多，似乎遇到什么事都波澜不惊。有媒体记者形容他是“史上最喜怒不形于色的安全研究员”。

不过，当他们拿下Pwn2Own 2017世界破解大师总冠军时，古河也没能按捺住内心的激动。有媒体是这样形容的：“他嘴角微微抽动，双手握拳甩动，摆出一个激烈的手势——说了声‘Yeah’。”

在第十五届全球安全盛会太平洋安全大会（PacSec2017）上，古河解读了一直被业界忽略的浏览器漏洞——内存压力漏洞的巨大威力，并首次公开了利用该类漏洞完成的Pwn2Own史上最难破解之谜。他们利用了这个内存压力漏洞，攻破了以安全性著称的最新款Edge浏览器，再加上另外两个漏洞的精巧配合，成功地在一分钟内完成了“Edge+Win10+VMware”三连击，也因此拿下了Pwn2Own史上的最高得分。

▶杨卿——“无线电钢铁侠”

杨卿是360无线电安全研究院掌门人、360独角兽安全团队（UnicornTeam）创始人，也是国内首个地铁无线网（Wireless）与公交卡（NFC）安全漏洞的发现及报告者，有媒体形容他是“无线电钢铁侠”。

2009年，刚刚加入360的杨卿破解了北京公交一卡通。他利用的是一个早就在国外论坛里爆出来的漏洞，当时国内并没有黑客做类似的研究。对此，杨卿花了几个月时间，最后完成了破解，从此一战成名。

2015年央视“315晚会”上，杨卿在现场展示了如何利用Wi-Fi窃取用户手机中的数据，移动设备只需与钓鱼Wi-Fi相连，手机中的大量隐私数据即会被钓鱼Wi-Fi所获取。在当年的美国DEFCON全球黑客大会上，他还展示了利用软件无线电设备发射虚假定位信号，欺骗手机、智能汽车、无人机的GPS导航攻防技术，可以让手机原地不动，却在地图上环游世界。

杨卿也是美国、欧洲、亚洲黑帽大会，DEFCON黑客大会和CanSecWest等国际安全会议的演讲者及DC010（DEFCON团队）技术顾问、网络安全试点示范项目评审专家。

杨卿选择无线电领域的原因很简单，就是因为小时候觉得科幻电影里的特工很酷，他的偶像是钢铁侠。也正因如此，杨卿被媒体形容为“无线电钢铁侠”。2018年，独角兽团队在知名学术期刊出版社斯普林格（Springer）出版了《深入无线电：攻防指南》（*Inside Radio：An Attack and Defense Guide*），这让杨卿更坚定了自己的选择。他告诉我，接下来他将脚踏实地为下一个阶段的目标努力。

▶黄琳——第一位出现在世界黑客大会上的中国女黑客

网络安全行业中，女性的比例非常低，而其中能够有所建树的更是凤毛麟角，黄琳就是其中一位。她身上有诸多让人羡慕的标签，她是“女学霸”“女博士”和“女黑客”。

2014年，黄琳正式加入360，成为独角兽团队高级研究员。在此之

前，她已经是圈内有名的软件无线电专家。目前，她是360公司无线电安全研究部的负责人、360公司3GPP标准组织SA3参会代表，还担任北京邮电大学硕士研究生企业导师。

2014年底，黄琳开始着手GPS信号伪造方面的研究。之前国内外相关的研究主要是基于一些昂贵的GPS模拟器和实验设备，而黄琳则关注于低成本的攻击手段。通过三个多月的努力，她和团队最终成功实现了一种低成本的GPS欺骗攻击，能够成功误导汽车接收错误定位信号，甚至欺骗无人机主动降落。

2015年8月，黄琳作为演讲嘉宾登上了第23届DEFCON大会讲台，成为第一位来自中国的女黑客。2016年，黄琳又在荷兰HITB（Hack in the Box）黑客大会上针对LTE伪基站的相关内容发表了演讲，该议题在发布之前就受到了苹果、华为、高通等公司的关注；黄琳和团队成员还继续推动该协议漏洞在3GPP标准中的修复，在2017年底成功实现了标准的修复。

在一次采访中，黄琳提到，她觉得自己的工作有点像是在“鸡蛋里挑骨头”，可能会在新技术前进的道路上，起到“拉后腿”的作用。不过，她相信，技术会在不断拉扯的过程中呈现一个螺旋式前进的路径，而安全应该得到每一个人的重视。

▶徐贵斌——知名反黑工具“狙剑”的作者

加入360之前，徐贵斌已经在圈内小有名气。当时，互联网上木马病毒泛滥，为了解决这个问题，徐贵斌写出了功能强大的安全反黑工具——“狙剑”。之后，他领导360查杀部门，把360的查杀能力提升了一个大台阶，并颠覆了网络安全产业技术创新。

“狙剑”一经推出，很快就在圈内打响了名气。这个反黑工具功能强大，可以提供系统监视、进程管理、磁盘文件管理、注册表检查、内核检查等多个功能，防止恶意软件修改文件及注册表，从而方便地手工查杀木马。

徐贵斌刚加入360时，被安排在查杀组，他的能力在团队中很快得到了凸显。比如2008年，我们推出的360系统急救箱就是徐贵斌带领团队开发出来的。360系统急救箱对各类流行的顽固木马查杀效果极佳，能够强力清除木马和可疑程序，并修复被感染的系统文件，抑制木马再生。

这只是徐贵斌能力的冰山一角。更重要的是，他领导查杀部门把360的查杀能力提升了一个大台阶。简单来说，当时业内主要是基于病毒库来扫描查杀木马病毒，也就是俗称的“黑名单”机制。但360创新推出了以“查白”为核心的网络安全技术，应用了搜索引擎、云技术、人工智能等互联网技术，攻克了黑名单瞬息万变不可捕捉的难题，积累了比较全面的白名单样本数据库。

现在，徐贵斌是360企业安全集团华南基地的负责人。在360新一代网络安全技术体系的突破和实践中，徐贵斌做出了不可磨灭的贡献。在之后的章节中，我将详细介绍网络安全产业的技术变革和我们的具体实践。

著名的黑客组织

当互联网刚发展的时候，黑客基本上都是各做各的事，并不知道在网络的另一端，会有与自己相似的高手。随着互联网的影响从社区延伸

至全世界，黑客从BBS社区中找到了志同道合的伙伴。逐渐地，这些黑客开始结成联盟，形成了黑客组织。

▶黑吃黑的高手——影子经纪人（Shadow Brokers）

2016年，一个叫做“影子经纪人”的神秘黑客组织宣布成功黑掉了“方程式组织”（Equation Group），使“方程式组织”的黑客工具大量泄露。其中，2017年5月爆发的“永恒之蓝”勒索病毒事件，就是黑客利用“影子经纪人”曝光的网络武器，对全球150多个国家发动了网络攻击。

“影子经纪人”攻入“方程式组织”后，免费向所有人泄露了其中部分黑客工具和数据。更绝的是，“影子经纪人”还宣称将通过互联网拍卖所获取的这些“最好的文件”，如果他们收到100万枚比特币，就会公布更多工具和数据。

黑客利用“影子经纪人”曝光的第四批网络武器，制造了“永恒之蓝”勒索病毒，袭击了全球150多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业等。

之后，“影子经纪人”宣称将会继续曝光更多窃取自NSA的工具。他们表示，他们拥有美国75％的“网络武器”，并将发布更多工具，这些工具可以利用浏览器、路由器以及手机的漏洞。

▶网络核武器的制造者——方程式组织（Equation Group）

“方程式组织”的行踪可以追溯至2001年，团体成员数超过60人。“方程式组织”被评价为“网络武器王冠的制造者”，是“最隐秘、最先进、最复杂”的黑客组织之一。从2001年开始，这个组织就在

帮助美国国家安全局开发网络武器。上文提到的“永恒之蓝”漏洞，只是他们开发出的网络武器的冰山一角。

“方程式组织”的名字是由发现他们的卡巴斯基实验室命名的。卡巴斯基在报告中说，之所以叫他们“方程式”，是因为在他们的行动中，比较偏爱加密算法、模糊策略等比较复杂的技术。由于恶意软件开发、行动技术突破和对目标封锁所花费的时间、金钱均由美国政府资助，项目资源几乎不受限，“方程式组织”得以成为全球“最牛”的黑客组织。

他们的攻击水平极高。多年来，他们向全世界释放的恶意代码各具特色，分别采用不同的传播手法，设定了不同的攻击目标，成功攻破了政府部门、电信、航空航天、核能源、军事、金融、伊斯兰宗教等组织机构的加密技术，给全世界的网络安全造成了极大破坏。

“方程式组织”拥有一个庞大而强悍的攻击武器库，传统的病毒往往是单兵作战，攻击手段单一，传播途径有限，而“方程式组织”动用了多种攻击工具协同作战，发动全方位立体进攻，可以说是世界上最强的网络攻击组织。

▶全球影响力最大的黑客团体——匿名者（Anonymous）

“匿名者”源于2003年成立的4chan论坛，这个论坛聚集了许多喜欢搞恶作剧的黑客和游戏玩家。由于所有用户都被标记为“匿名者”，他们便以“匿名者”作为自己的代号。“匿名者”在全球范围内有数百万名成员，他们在行动时以数百人的小组为单位，进入大公司和政府部门内部网站，中断它们的服务、删除备份信息、截取电子邮件以及盗取各种文件。

“匿名者”脸上戴着的盖伊·霍克斯（Guy　Fawkers）面具（电影《V

字仇杀队》中主角的象征物）是他们最鲜明的标志。他们的核心观点是“互联网自由”，并在政治上形成了一些共识。虽然入侵公司和政府部门网站的行为违反了法律，但他们辩称违法是出于“道德”目的，是为了监督大公司和政府，曝光他们的错误行为。

2008年，“匿名者”攻击了美国山达基教会（Scientology）的网站，正式进入公众视野。当时，有网民恶搞美国影星汤姆·克鲁斯（Tom Cruise）对山达基教会的支持言论。对此，山达基教会警告称：“将把发布或共享视频的用户诉诸法律”。“匿名者”认为，这违反了互联网自由，因此发起了网络攻击。这次事件使“匿名者”迅速走红。

之后，“匿名者”的行动变得越来越频繁。比如，2010年，他们攻击Visa网站、万事达网站和支付网站PayPal，以表示对维基解密的支持；2011年，在阿拉伯之春事件中，他们协助网民突破突尼斯等国家的网络管控；2015年，他们表示将对恐怖分子宣战，并声称已经控制或摧毁了1000多个“伊斯兰国”的相关网站、社交媒体账号以及电邮地址。

“匿名者”的成员分散在世界各地，这为抓捕带来了难度。2010年维基解密事件发生后，FBI和英国、荷兰等国家对攻击PayPal的黑客进行搜捕，但最终只逮捕了16人。与此同时，“匿名者”的其他成员则继续高调地行动，丝毫不受影响。

这些黑客组织，许多都干着危害国家安全、破坏社会秩序的事。为应对这些组织的肆虐蔓延，各国政府纷纷成立了专门机构，增加经费，培养网络安保人才，相继出台了法律法规，加大打击力度，并联合其他国家共同应对。

另一方面，民间网络安全产业不断发展壮大，聚集了一批网络安全攻防高手，由他们组成的团队成为保卫国家网络安全的重要力量。下面，我简要介绍360公司中几个有代表性的团队。

▶“Master of Pwn”——战无不胜的360伏尔甘团队

上文说到郑文彬，就不得不说他带领的360伏尔甘团队，伏尔甘团队是360互联网安全创新中心旗下的二进制漏洞安全团队。团队成员具备高水平的漏洞挖掘能力、系统安全理解能力和产品研发能力。多名成员入选微软全球Top100贡献榜，并多次获得微软Bluehat、Edge浏览器赏金项目奖励。

360伏尔甘团队的日常工作主要是通过挖掘软件的安全漏洞和漏洞威胁，帮助第三方厂商修复漏洞和提升产品安全性；通过在漏洞攻防领域的研究经验，创新设计更有效的安全解决方案。2014年360安全卫士推出的XP盾甲漏洞防御产品，其核心技术就是由360伏尔甘团队设计开发的。

360伏尔甘团队曾在Pwn2Own 2015比赛中攻破IE项目，在Pwn2Own 2016比赛中攻破Adobe Flash Player以及Google Chrome项目，在Pwnfest 2016比赛中攻破微软Edge浏览器以及Adobe Flash Player。

在Pwn2Own 2017赛事上，360伏尔甘团队上演了一出黑客历史上最高难度破解，只用一个网页就连环攻破Edge、Win10和VMware的最新版本。他们还攻破了Apple Safari、Mac OS和Adobe Flash Player，拿下赛事总冠军，成功加冕“世界破解大师”。

▶全球首个入选GSMA移动安全研究名人堂的团队——360独角兽团队

360独角兽团队对无线通信、智能硬件以及汽车安全领域的研究一直处在国内领先地位。2017年6月，世界著名的全球移动通信系统协会（GSMA）更新了安全名人堂名单，360独角兽团队凭借发现全球首个4G网络协议高危漏洞，成为自GSMA移动安全研究名人堂设立历史以来全球第一个获得该荣誉的团队，并获得GSMA颁发的“CVD＃0001”首位漏洞编号。

上文提到的杨卿是独角兽团队的创始人，还有第一位出现在世界黑客大会上的中国女博士黄琳也是独角兽团队的核心成员。团队成员研制了360安全充电接口、卡套、卡防、天巡等一系列软硬件安全产品，并撰写了国内首本无线通信安全书籍《无线电安全攻防大揭密》《硬件安全攻防大揭秘》《智能汽车安全攻防大揭密》等书，让无线电安全概念进入公众视野，团队研究成果多次被《福布斯》（*Forbes*）、福克斯新闻频道（Fox News）、《美国国家地理》（*National Geographic*）、《连线》（*Wired*）等海外媒体报道。

2017年6月，360独角兽团队发现全球首个4G网络协议高危漏洞，并对这个4G通信协议的严重漏洞进行了深入分析。他们发现，所有的4G终端都会被该漏洞影响，包括手机、智能设备、智能汽车等。这造成攻击者可劫持任意终端的4G网络，仿冒受害者手机身份拨打或接听电话从事电信诈骗，或监控受害者手机短信息，绕过各类网络平台的短信验证码身份认证机制，仿冒受害者登录相应网络平台，造成信息、财产等损失。

在对漏洞进行详尽分析后，独角兽团队将漏洞细节与修补方案相继通报给了手机网络运营商、终端及网络模块等相关厂商，并同步通报给GSMA做全球统一漏洞预警与修复协调处理。GSMA协会相关负责人对该漏洞表示认可，并发来致谢邮件。该漏洞议题同年在美国黑帽大会

Blackhat与黑客大会DEFCON同时入选，并获得安全界称之为“黑客奥斯卡”的黑帽Pwnie奖（Blackhat Pwnie Awards）最具创新研究奖提名。

▶获得国际各权威机构60多次公开致谢的团队——360代码卫士团队

360代码卫士团队一直致力于软件源代码与可执行码漏洞分析技术研究和产品开发，团队推出的“360代码卫士”系列产品是国内第一个成熟的商用代码安全分析产品，打破了代码安全领域长期被国外品牌垄断的局面。团队多次发现Windows/Linux操作系统、浏览器、Adobe Flash、Adobe Reader、Cisco等网络设备、施耐德等工控设备、各种区块链系统、各种开源基础组件的安全漏洞，获得国际各权威机构或厂商的60多次公开致谢。

360代码卫士团队中既有二进制漏洞挖掘高手、微软全球TOP100贡献“白帽子”、Pwn2Own2017冠军队员，又有程序分析专家、开源软件安全大拿。团队主要研究方向涵盖Windows/Linux/MacOS操作系统、应用软件、开源软件、网络设备、工控设备、物联网设备、区块链等多个方向。在Pwn2Own 2017世界黑客大赛上，由360代码卫士团队与360Vulcan、360Marvel团队组成的360安全战队拿下微软、苹果、Adobe、VMware等巨头厂商的六大高难项目，获得“破解大师”总冠军。

360代码卫士团队也是国家发改委大数据协同安全技术国家工程实验室下属代码安全实验室的承担单位，负责国家工程实验室在代码安全、漏洞分析方面的研究工作规划和组织实施。

团队目前运营着国内规模最大的开源软件源代码安全检测公益计划。该计划目前已经对2200多款开源软件进行了安全检测，积累了大量

的开源软件源代码安全缺陷基础数据。这些数据对于软件开发者了解并消减开源代码的安全风险，有很好的指导意义。

第三节　黑客的宿命与使命

黑客通常隐藏在电脑屏幕后面，看不见摸不着，就像“世外高人”一样，不“黑”则已，一“黑”惊人。随着网络空间成为第五空间，黑客也开始从幕后走向台前，并承担起更重要的历史使命。

从幕后到台前

这些组织各自代表了当时黑客团体的精神和力量。他们的崛起，也说明了黑客活动在这二十年多年间，方式从个人活动到集体行动、出发点从私人利益到政治目的的转变。

20世纪80年代，个人电脑还未普及，计算机网络也只是将一个办公室里的几十台电脑连接在一起，懂计算机的人更是少之又少。在当时，能够令整个计算机网络瘫痪的人就是了不起的人物。上文提到的全球最著名的五大黑客，他们的活跃年份都是在这一时期。在全民都不懂计算机的时代，出现一个以当时最顶尖的技术来进行犯罪活动的人，引起的轰动可想而知。

20世纪90年代初期，黑客的行动仍然只是“小打小闹”。具体地说，他们以个人为单位寻找和发现系统中的漏洞，然后发动攻击。即使到后来电子邮箱、新型Web BBS等开始发展时，他们依然是通过注册一些马甲账号、借助个人或处理程序，将自制的病毒和木马散布出去。当时互联网还没有将全世界的人联系起来，黑客基本上都是各做各的事，并不知道在网络的另一端，会有与自己相似的高手。

随着互联网的影响范围从社区延伸至全世界，不少黑客从各种BBS社区中找到了与自己志同道合的伙伴，彼此之间也有了越来越多的交流。逐渐地，这些黑客开始结成联盟，以集体为单位进行有目的性的攻击。

目前，全球范围内影响力最大的黑客团体是“匿名者”。前一节中提到，“匿名者宣言”和他们脸上戴着的盖伊·霍克斯面具是他们最鲜明的标志。

全民皆黑客

21世纪，个人电脑和网络逐渐普及，上网对于人们来说已经非常普遍。与此同时，制作病毒的门槛越来越低、获利越来越大，使得全民皆网民的时代，将向全民皆黑客的时代演进。

我们可以从六个角度，来理解“全民皆黑客”时代的特征。

第一，传播极速化。随着众多漏洞细节的曝光，攻击代码的“窗户纸”一点就透，黑客能力被插上翅膀，电脑木马病毒开始肆虐。比如，2001年一名赋闲在家的程序员开发出了“求职信”病毒，这个病毒没有太高的编程技术，但传播速度惊人。

再如，“灰鸽子”病毒自2001年诞生之后，曾连续三年被国内杀毒软件厂商列入10大病毒，并在2007年大规模爆发。当时，全国每10台感染病毒的计算机中，就有超过一台感染了此病毒。有记者调查发现，在百度中搜索“灰鸽子”病毒，弹出了200多万条相关词条，其中关于如何用“灰鸽子”抓“肉鸡”的教程随处可见。

还有“冲击波”“震荡波”等病毒，都是一些年龄较小的编程者学习顶级黑客的“成果”。他们毫无顾虑，没有任何目的地编写电脑病毒，但这类病毒传播速度快、变种多，往往让人猝不及防，容易造成极大的损失。

第二，使用简单化。模块组装型木马的流行使成为黑客的门槛越来越低。由于木马制作工具的泛滥，病毒的制作逐渐呈商业化运作模式。某些制作小组甚至可以根据使用者的要求，为其提供针对特定目标的专门版本。

比如，前文提到的“永恒之蓝”勒索病毒事件，黑客就是把网上流传的标准漏洞攻击代码、非对称加密技术、匿名网络技术等进行了重新组合，编制成了完整的攻击程序。攻击者不需要任何技术功底，只需要执行攻击命令，就能完成对目标的攻击，并且攻击成功率极高。

第三，分工专业化。一个不懂任何电脑技术的人都可以成为黑客。在网络黑色产业链中，有人专门从事木马以及病毒的开发，有人负责销售和利用这些木马病毒获取利益。

以“肉鸡买卖”为例，黑客制作出网络游戏盗号木马、远程控制木马等各类木马工具后，出售给木马播种环节的人，由他们负责实施“挂马”。用户一旦访问被“挂马”的页面，则立即中招，成为“肉鸡”。能够使用几天的“肉鸡”在国内可以卖到0.5元到1元一只；如果可以使用半个月以上，则可卖到几十元一只。这些黑客从中招用户电脑中盗取各类有价值的信息，然后再把信息进行“套现”，获取了大量利润。

第四，知识普及化。网络攻防大赛如雨后春笋般出现，让黑客进一步进入大众视野。从2017年开始，国内攻防演练和攻防比赛的热度明显

升温。据不完全统计，全年国内各类不同规模的攻防演练超过了100场，各类网络安全攻防比赛的总数近200场，参与比赛人次近6万人。

与前几年相比，攻防演练迭代升级趋势明显。一方面，演练的针对性、规模和实战性都有明显提升，以验证防御系统的效果，发现潜在的威胁和漏洞，尤其是针对特定目标的深度攻防。另一方面，演练组织者包括国家、行业、地区、银行、电力等关键信息基础设施机构和企业，甚至一些电商、互联网企业、家电企业也开始组织攻防演练。

第五，能力产业化。安全服务市场将催生“准黑客”产业大军。传统的网络安全市场中，政企用户更倾向于购买安全设备，把硬件盒子放在企业，能够让人更放心。但随着网络安全威胁形势的不断变化，以及越来越严苛的网络安全监管环境，政企用户对于安全的需求不断增强，从基本合规逐步转向真正的安全防护需求。

从2017年我们服务的几起政企服务案例来看，已经有政企客户在网络安全采购中从购买产品转到了购买服务。这些企业在与安全厂商签订的网络安全合同中，安全服务成了最主要的内容，而安全的软硬件产品则成了配合选项。

安全服务化是未来的趋势。随着大数据安全、威胁情报、机器学习、云安全被越来越多地应用于安全防护体系中，新的技术、新的知识对于企业现有的安全管理人员来说是一种挑战。换句话说，企业需要专业的安全人才来更及时、有效地应对网络安全威胁，这也将催生“准黑客”产业大军。

第六，教育正规化。网络安全人才培养有普及之势。2015年6月，“网络空间安全”正式被国务院学位办和教育部获批为国家一级学

科。《网络安全法》第二十条将培养网络安全人才确定为一项基本法律制度：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。

近两年，各相关高校响应国家培养网络安全人才的号召，陆续设立了“网络空间安全学院”。2015年至今，中国科学院大学、北京邮电大学、四川大学、电子科技大学、暨南大学等高校相继成立了“网络空间安全学院”或“网络空间研究院”。

从网络安全市场需求来看，我国仍面临着巨大的人才缺口。2018年5月，网络安全与信息化产业联盟发布的报告显示，我国最近三年培养的安全专业人才仅有3万人，不足70万需求的5％。预计到2020年，需求量将达到140万人。

为了尽快填补这个缺口，2018年3月，360在四川绵阳建设了网络安全人才培养绵阳基地，预计每年培养1200名具备实战能力的网络安全工程师。我们还和一些高校联合组建了360网络空间安全学院，培养攻防兼备的实战型人才。

从这六点来看，“全民皆黑客”的时代已经到来。这些黑客也许是通过技术获取非法利益的人，也可能是维护网络空间安全的“攻防高手”。很多黑客有着自己的事业和工作，在平时他们不会轻易表露自己“黑客”的身份，其中还在学校上学的学生也不少见，各行各业都暗藏着黑客精英，而且，他们很有可能就在你我的身边。

黑客精神与黑客使命

黑客，并不都是坏人，他们既能做好事也能做坏事。他们中有一些黑客具有英雄主义色彩，敢于克服困难，主动承担责任，向社会反动和黑暗势力进行坚强不屈的斗争，反映了当时的历史潮流和社会正义。黑客精神与黑客使命，也在一定程度上制约和规范着黑客的行为。

▶黑客精神

在我看来，黑客都有着强烈的好奇心，对能够充分调动大脑思考的问题感兴趣，并且总是带着质疑的眼光思考问题。当碰到棘手的问题时，他们从不会轻易放弃，而是想方设法刨根问底。总之，“黑客精神”本质上是一种工匠精神、钻研精神、职业精神和侠义精神，这种精神在任何行业都值得赞扬。

2011年，一群中国顶尖黑客们制订了《COG黑客自律公约》，其中写道：金钱不等于罪恶，但金钱绝对不是彰显和证明黑客能力的标准，以买卖社会普通公众隐私信息为目的的活动不是黑客行为。

“公约”还重新定义了“黑客精神”：黑客是用来形容那些热衷于解决问题、克服限制的人的。因此“黑客精神”并不单单指（限制于）电子、计算机或网络。“黑客精神”的特质不是处于某个环境中的人所特有的，而是可以发挥在其他任何领域，例如音乐或艺术等方面。“公约”中提到：好奇、怀疑、独立思考、开放、共享都是“黑客精神”的表现特质。

▶黑客使命——未来网络安全的守护者

在网络技术越来越发达的今天，黑客在网络安全中扮演的角色越来越不容忽视。安全不仅关乎个人的信息隐私防护，关乎企业的财产以及数据保护，更关乎国家安全。黑客可以从恶，也可以从善。守护未来的网络安全将是黑客的使命。

2017年5月发生的“永恒之蓝”勒索病毒事件就是一次例证。当时，病毒突袭了全球150多个国家，许多用户的电脑被病毒锁定，无法正常使用。十万火急之下，360技术团队闪电出击，发起火线营救，搭建起多重防护体系，力保用户平安无恙。

此次勒索病毒传播速度之快、破坏性之大、影响范围之广，为互联网历史上罕见。面对严峻的勒索软件攻击形势，360安全团队连夜加班加点，对病毒进行取证分析，开发免疫工具，提供应急补丁，升级防御系统，推出了“NSA武器免疫工具”“360安全卫士离线救灾版”“360勒索蠕虫病毒文件恢复工具”等一系列应急工具，构建多重防护体系，确保了5亿用户免受勒索病毒困扰。

在这场正义与邪恶的较量中，360安全卫士与“永恒之蓝”勒索病毒大战三天三夜，最终以勒索病毒失败告终，再一次证明了360作为“东半球最强白帽军团”的实力。

就像360头号黑客郑文彬给伏尔甘团队定下的标语“Live long and pwn（生生不息，破解不止）”，这些挖漏洞的黑客对网络攻防有着一股近乎固执的热情，他们的这份坚持对网络空间的安全有着不可取代的重要意义。

在智能化的未来，这些掌握高超技术的黑客，不仅是网络攻防的关键性人才，更是维护网络安全的重要力量。我们会看到越来越多的年轻人一步步登上世界舞台，他们也许玩世不恭，但却固执地坚守着道义。

Chapter 4
第四章
智能时代新技术是漏洞帮凶，还是克星

人类的历史，是一部人类运用技术的发展史。18世纪60年代，蒸汽机的广泛应用，标志着人类进入工业时代；19世纪70年代，内燃机的广泛应用，标志着人类进入电气时代；20世纪四五十年代，电子计算机和信息技术的广泛应用，标志着人类进入信息时代；21世纪，人工智能等技术的应用，标志着人类进入智能时代。

智能时代是万物互联的世界，更多的设备和系统连接在互联网上。更多的连接点意味着更多的漏洞和攻击点；追求方便和小巧意味着资源受限和安全性的牺牲。

2014年，我们成功破解特斯拉，利用电脑实现了远程开锁、鸣笛、闪灯、开启天窗等操作，让很多人深刻地体会到“智能生活”的威胁就在身边。不仅如此，在我们举办的HackPWN安全极客狂欢节上，几乎所有的智能硬件都被我们的“白帽”黑客一一攻破。

智能时代，是人类未来的美好生活，也是滋生漏洞的沃土。支撑智能时代的大数据、云计算、物联网、工业网络、人工智能等新技术，既是创新发展的膨化剂，也是网络安全问题的催化剂。

第一节　“智能生活”的便利与威胁

智能设备在我们生活中无处不在，但“智能生活”也意味着：你的计算机最了解你。我们在享受着技术带来的便利的同时，也面临着技术带来的威胁。

正如我在本书中一直强调的，缺陷是天生的，漏洞是不可避免的，网络攻击是必然的。在这些智能设备与人们日常相伴的同时，安全漏洞问题也逐渐显现了出来。下面是我亲历的几个故事，很能说明这一点。

当威胁就在身边

▶我的特斯拉报废了

我们研究发现，特斯拉传感器系统并不绝对可靠。它需要传感器、毫米波雷达、摄像头等多个部分配合，融会贯通后特斯拉才会做出报警、刹车等反应。但是在黑客简单的干扰下，传感器“致盲”，就会发生误报。所以，在真正行驶过程中，驾驶员稍不注意，就可能发生车毁人亡的灾难事故。

2014年7月的一个下午，我突然接到我们网络安全攻防实验室负责人林伟的电话。他在电话里焦急地告诉我，他开着我买了不久的特斯拉出了车祸，情况很严重，车可能彻底报废了。我赶紧问他，人有没有事？还好，人没事。“人没事就好，赶紧把车牌搂回来。”当时全北京只有几辆特斯拉，我可不希望成为车祸

新闻的主角。

车祸发生一周后，我们在SyScan360国际前瞻安全信息大会的现场，演示了我们发现并已经提交给特斯拉的应用程序系统漏洞，重现了这个漏洞的安全隐患，成功利用电脑实现了远程开锁、鸣笛、闪灯、开启天窗等操作。其实这只是攻防实验室的一部分研究成果，出于公众情绪的考虑，我们并没有演示其他成果：成功做到让汽车在行驶过程中偏航，以及在充电过程中烧掉电池。

当时，特斯拉是唯一最彻底的电子智能化汽车，类似于一台大型PC。我本能地意识到，如果特斯拉存在漏洞并被黑客利用，可能会车毁人亡。从这个角度而言，特斯拉非常有研究意义。当汽车模块化以后，每一个独立的单元都会拥有独立的IP地址、独立的端口，这就和PC很类似，黑客们可以通过各种方式（网络探测）扫描探测各个组件的IP地址和端口，以图谋破解。

▶一切智能硬件皆可破解

安全技术并不神秘，在HackPWN安全极客狂欢节的展示舞台上，这些“白帽”黑客用实际案例告诉我们，一切智能硬件皆可破解，安全意识时刻不可放松。

2015年8月，360伏尔甘团队和独角兽团队在北京发起了首届HackPWN安全极客狂欢节。我们邀请了国内外数十位知名“白帽”黑客、领先的智能设备公司和安全公司，展示和探讨最新的漏洞挖掘和破解技术，研究智能时代的智能汽车、智能家居、物联网和智慧城市的安全防护方案。

当时，我在开幕致辞中提到，面对突然到来的物联时代，整个世界都准备不足，厂商准备不足、用户准备不足、安全厂商也

准备不足。要解决万物互联的安全问题，需要全面的协作，厂家和用户之间的协作、厂家之间的协作、行业之间的协作，还要有广大极客的全面参与，他们是全世界智能硬件安全测试员。

在这次活动中，这些“白帽”黑客在现场演示了智能家电被攻破的过程。小米手环、汽车、电视、豆浆机……几乎所有的智能硬件无一幸免。

360网络安全攻防实验室负责人林伟在现场展示了通过蓝牙协议而非小米官方应用绑定、读取和操作小米手环。通过lightblue软件配对读取手环内加速度传感器输出的数据，别人就能获得用户身体特征、步数、睡眠时间等数据。除了获得个人数据外，还可以通过软件控制手环，让现场所有观众的小米手环实时震动。

我还记得，活动当天比亚迪宣布暂时关闭汽车的云端服务器。因为美国传奇黑客萨米·卡姆卡尔（Samy Kamkar）要在现场演示“无线偷汽车”技术。萨米自己开发了一款名为Rolljam的无线电设备，可以破坏汽车和车库门厂商使用的无线遥控解锁码，截取密码进而可以随意打开汽车和车库的门锁。

▶八成摄像头存在安全漏洞

我们对国内近百个品牌的智能摄像头进行测试后发现，有近八成产品存在用户信息泄露、数据传输未加密、APP未安全加固、代码逻辑存在缺陷、硬件存在调试接口、可横向控制等安全缺陷。

在2016年5月举办的2016亚洲消费电子展（CES Asia 2016）上，360攻防实验室的专家刘健皓现场演示了一款智能摄像头的破解，这个过程仅仅只有几分钟。

刘健皓首先在某品牌摄像头的手机客户端注册了一个账号，

他随便填了一个手机号就通过了，甚至不用进行验证。注册完成后他进行了几个简单的操作，就成功地连接到了这个摄像头，摄像头拍摄的场景一览无余，甚至包括一些家庭的客厅、卧室。

理论上来说，手机账号必须和摄像头“一对一”，才可以远程看到摄像头内容。但是这款摄像头并没有对手机身份进行验证，这个漏洞非常严重，黑客通过漏洞，用一个虚拟的绑定就可以查看数百个摄像头的实时画面。我们发现，有类似漏洞的摄像头至少有数十款，其中包括了一些著名的品牌。

大部分智能摄像头都存在绕过身份验证控制设备的问题，这会直接导致用户隐私泄露。此外，还有一些摄像头使用实时流传输（Real Time Streaming Protocol，RTSP）协议传输，但是协议内容是明文传输的，这样只要把地址复制到一个支持RTSP协议的播放器内，就可以获得当前智能摄像头的界面。还有一部分摄像头通过分析可以查看到用户和设备的对应关系，黑客通过修改设备标识，就可以横向越权控制其他用户的摄像头。

毫无疑问，技术以其便利给我们的生活带来了无限可能和想象，人工智能能够帮助人们实现诸多以前不敢相信的事情，但是，我们绝对不能陷入技术万能论的泥沼之中。如果我们不时时刻刻对人工智能保持警惕，不意识到人工智能漏洞被利用的可能。那么，你将会对危机的发生难以招架，一击即溃。

当科幻成为现实

我们经常看一些影视作品，但你是否会想过这些原本经过艺术加工的内容有一天会在现实中上演呢？

“棱镜计划”、纽交所暂停股票交易、人工智能与人类对弈、比特币协助黑帮洗钱、政府悄然构建庞大面部识别系统等这些科幻片《疑犯追踪》（*Person of Interest*）中的剧情，在现实生活中一一被应验。《实习医生格蕾》（*Grey's Anatomy*）中医院被黑客入侵勒索的情节，现在就在我们身边不断上演着……

▶预言“棱镜计划”

2011年开播的美剧《疑犯追踪》中，出现了和“棱镜计划”几乎一样的剧情，而且细节还原度高得离奇，就连时间也对得上号，被称为“神预言”。其实，这不仅仅是巧合。随着科技的发展，一切科幻都可能成为现实。

“今天的新闻，我是不是前几天已经在剧里看过了？”这可能是看过美剧《疑犯追踪》的人的最大感受。2011年9月，美剧《疑犯追踪》开播，该剧讲述了一位推定死亡的前CIA特工与一位神秘的亿万富翁联合起来，运用一套独特的办法制止犯罪的故事。

第一季第22集的片头揭示了本剧的核心设定——“你正在被监视着，政府有一个秘密系统，一台机器正在每时每刻监视着你。它为了预防恐怖袭击而诞生，但是它却看到了所有的罪恶。”剧中，政府为了防范恐怖袭击制定了一套计划，主角芬奇（Finch）用了7年的时间终于在2009年制作出机器“The Machine（TM）”，拥有所有电子设备最高权限的TM对人类展开了全面监控，并从中判断即将发生的恐怖袭击。随后Finch将“相关人”的号码发给政府处理，而“非相关人”的号码则交给主角团队处理。剧集中“非相关人”是一名国安局情报分析员，在工作过程中发现了这一计划，并因此而遭到政府追杀。

美国的“棱镜计划”（PRISM）就是剧情的翻版。2013年6月，前CIA职员爱德华·斯诺登将两份绝密资料交给英国《卫报》（The Guardian）和美国《华盛顿邮报》（The Washington Post），美国国家安全局代号“棱镜”的秘密项目被曝光。“棱镜计划”是一项由美国国家安全局自2007年起开始实施的绝密电子监听计划，正式名号为“US—984XN”。2012年，它作为“总统每日简报”的一部分，项目数据被引用1 477次，国安局至少有1/7的报告使用了该项目数据。

“棱镜计划”之所以能够对即时通信和既存资料进行深度监听，原因之一就是利用了系统漏洞。FBI和NSA通过漏洞挖掘了各大技术公司的数据，包括微软、雅虎、谷歌、脸书、Pal Talk、优兔（YouTube）、Skype、美国在线（AOL）、苹果等。消息爆出之后，美国舆论随之哗然，也震惊了世界。

▶纽交所暂停股票交易

2015年7月9日，美国纽约证券交易所（以下简称“纽交所”）由于技术故障，一度暂停了所有股票交易，经过四小时修复才恢复正常。巧合的是，美剧《疑犯追踪》中又一次“神预言”了此次故障，科幻再一次成为现实。

在2015年1月播出的美剧《疑犯追踪》第四季第11集中，对手利用AI技术制造出的“机器”Samartian，试图控制整个城市。这台机器通过攻击证券市场，试图制造新的金融危机来影响美国乃至世界。

类似的剧情半年后在现实中上演。据媒体报道，在纽交所出现技术故障的两周前，纽交所就曾通知交易公司和其他用户，交易所将关停部分老化系统。当天股市开盘前，纽交所又发出了一

条警示通知，交易所的一些网关被发现有问题，网关是连接纽交所执行交易命令的连接点。通知说，这些问题将会影响到一组股票交易，但并没有说是哪一组。

当天上午10点49分，纽交所发出通知说，所有技术问题都已解决，股票可以正常交易，但交易所就在这个时候出现了宕机。

值得注意的是，著名黑客组织“匿名者”在前一天晚上曾用账户“YourAnonNews”发布推文说：“不知道明天会不会成为华尔街的‘坏日子’……我们只能希望。”纽交所故障发生后，这个账户又发出多条相关推文，甚至呼吁民众前往纽交所抗议，还倡议“卖掉股票，救济穷人”。虽然，纽交所第一时间否认了“黑客攻击”的说法，但是这一系列“巧合”很难不让人怀疑这是被黑客利用系统漏洞攻击所致。

▶医院被黑客利用漏洞入侵

随着医院信息化建设力度的加大，医院的信息安全问题也成为关注的焦点。美剧《实习医生格蕾》中医院被黑客入侵勒索的情节，如今也开始在我们身边不断上演。

2018年2月，湖北省某县人民医院系统被黑客入侵植入“升级版勒索病毒”，要求医院支付比特币才能恢复。一天后，湖南省某医院也发生黑客攻击事件。黑客利用系统漏洞入侵医院系统，然后植入勒索病毒，要求院方在6小时内为每台中招机器支付1个比特币（约合人民币6.6万元）。医院系统大面积瘫痪，导致治疗进程无法正常运转。

早在2017年5月，就有新闻爆出“黑客倒卖医院数据落网，广州医药圈震荡”，黑客团伙将非法获取的医院药品数据，倒卖给诸多医药代表。对此，警方传唤了广州多名医药代表，部分医

院的药剂和采购部门也牵连其中。业内人士称，被调查的医药代表来源广泛，不乏知名药企，涉案医院包含国内诸多著名医院。

这些真实发生的事情告诉我们，人们在享受着技术带来的便利的同时，也面临着技术带来的威胁。系统越复杂，漏洞存在的可能性越大，越有可能被入侵；网络的连接点越多，被攻击的机会越大；设备越智能越便捷，所带来的后果越严重。

第二节　智能时代的工业物联网安全

谈到智能时代，不得不说物联网。物联网的英文名称是“Internet of Things（IoT）”。顾名思义，物联网就是物物相连的互联网。一方面，物联网是在互联网基础上的延伸和扩展的网络，另一方面，物联网强调的是用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。

物联网的前景广阔，已经成为新一轮科技革命与产业变革的核心驱动力之一。全球知名咨询公司麦肯锡预测，到2025年，物联网这项将实体和数字世界连接起来的技术，经济价值可达每年11.1万亿美元。美国计算机技术工业协会（CompTIA）的调查报告也显示，从计算机到家庭监视器再到汽车，联网设备的数量在2014年至2020年间的年复合增长率预计将达到23.1％，到2020年，物联网的设备连接数将达到501亿个。

2017年，中国移动的物联网连接数总量已超过2.65亿，物的连接净增规模超过了个人和家庭连接，在总净增连接中占比达到61.8％，成为驱动连接规模增长的第一动力。中国联通、中国电信的连接数也分别突破了5000万户和6000万户，并将很快突破1亿户。

从全球范围看，截至2017年11月，已有28张移动物联网商用。整个国际物联网建设呈现出增强机器类通信（eMTC）和窄带物联网（NB-IoT）共同发展的特点，美国电话电报公司（AT&T）、威瑞森（Verizon）等5家运营商商用了5张LTE-M网络；中国电信、中国联通、中国移动、沃达丰、韩国电信、德国电信等运营商共商用了23张

NB-IoT网络。

物联网不仅已经深入到人们生活的方方面面，工业也正在实现万物互联。工业物联网一方面使传统工业得到换代升级，劳动力得到解放，生产力得到提高；另一方面，工业互联网也使工业安全面临严峻的威胁。

工业是经济发展的重要引擎，是推动经济高速发展的重要力量。一旦工业互联网中的某个漏洞被黑客发现而入侵，后果不堪设想，可能引发蝴蝶效应，好比一只南美洲亚马逊河流域热带雨林中的蝴蝶，偶尔扇动几下翅膀，就可以在两周以后引起美国德克萨斯州的一场龙卷风。

什么是工业物联网

什么是工业物联网？我认为，工业物联网使物联网领域创造出了更多的连接端点，它包含“IT网络（互联网）+OT网络（工业控制系统网络）+IoT网络（物联网）”，因此也简称“IIoT”。这种复杂性增加了工业环境中的“攻击面”，如工业控制系统、监控和数据采集（SCADA）系统、制造业、智能电网、石油和天然气、公用事业和运输业等，也增加了被攻击的可能性。

美国通用电气（GE）提出了一个工业互联网计划：在其产品中增加更多的传感器来获取海量数据，用以提高效率。比如，一个机器学习专家小组通过测试筛选2万台喷气发动机的各种细小警报信号，作为发动机维修的前瞻性评估数据。这套正在研发的航空智能运营服务系统，采用专业计算算法，能够提前一个月预测哪些发动机急需维护修理，准确率达到了70％。据统计，每年航班延误给全球航空公司带来约400亿

美元的损失，其中10％的延误，源自飞机发动机等部件突发性维修。

这套智能运营服务系统的最大价值，就是可以实时监控从飞机设备收集的各项数据，在飞机出现故障隐患前做出诊断预测，大幅降低飞机的误点率，最终目标是“将计划外的停飞时间降为零”。GE公司发表的《工业互联网：打破智慧与机器的边界》白皮书认为，在全球，如果工业互联网仅仅将铁路、航空、医疗、电力、石油天然气这5个行业的工业生产效率提高1％，就可以在未来15年为世界贡献2760亿美元增长。

通过工业互联网、智能制造的导入，富士康已经有非常多的生产线和工厂实现了完全自动化，不需要人，甚至不需要开灯。2011年起，富士康就宣布将在5到10年之内，装配100万台机械手臂。随着人工智能和大数据兴起，2016年富士康推出“无人工厂”，在成都和贵阳，已经有6条生产线投入生产。“无人工厂”的好处是显而易见的，不仅节省人力，还体现在制造技术的精进、品质管控的提升、能源损耗的降低，以及信息和生产安全的提升。富士康工业互联网公司副总裁陈冠棋称，富士康不仅要在自己的工厂实现智能制造，还要带动千万家中小企业结构升级，利用精密电子制造的工艺技术作为基础，结合各行各业的行业知识开展工业互联网平台的上层应用开发。

很多人都知道，特斯拉的生产线自动化程度很高，比如目前Model 3的生产线自动化水平已经高达95％，包括传输、装载和焊接等。特斯拉还在整条生产线的各个扫描站部署了47个机器人，这些机器人会测量每台Model 3上的1900个测试点，以满足精确度为0.15毫米的设计指标，对每个固定的螺栓、扭矩测量等数据自动记录，并把所有这些数据都以每辆车的独一“车辆身份编码”（VIN）进行存储，因此服务中心可以追溯任何车间的制造问题。这背后的理念是，即便车辆已经交付到客户，特斯拉仍有能力改进这些车辆。

工业互联网给特斯拉带来的不仅仅是智能化生产，还能为每一位特斯拉的消费者提供个性化订制。消费者可以通过官网的设计室，自己选定车辆的动力、外观、舒适性配置等每个细节，继而排入生产线生产。特斯拉从下订到生产，是完全按照车主的意愿和喜好产生的，而不是仅仅在成品上加减配置或者刻个名字这样的“个性化定制”。甚至在车辆交付后的使用过程中，每一辆特斯拉仍然是个性化的，比如智能悬挂，可以记住每次升高底盘的地点，下次路过坑洼路段，或者进入车库、过减速带的时候，就会自动升起；多达十个的驾驶员记忆、动能回收、方向盘力度等诸多细节设置，是真正全方位的个性化订制。

工业互联网还让工业生产的网络化协同成为现实。例如，中国航天科工集团旗下的航天云网，通过搭建以INDICS为核心的工业互联网公共服务平台，把分散在全国各个角落的市场主体连接起来，横向整合固化于千万个企业中的同质化资源，实现“企业有组织、资源无边界”的生产资源配置，优化业务流程，打通云端应用工作室中的协同制造、智能制造全链条业务流程，为工业企业提供供需对接、信息共享以及包括创意、设计、制造、投资等全产业链的配套服务。

例如，贵阳的一家食品企业每天生产250万瓶调味品，每瓶都有唯一的二维码。通过航天云网的网络协同，山东的一家企业帮助这家食品企业，将对每瓶进行二维码防伪追溯的成本降低到了1分钱；成都的若克精密机械制造有限公司与航天云网耗时6个月打造的一条智能制造生产线，可以将其设备运行、生产管理等数据都传输到航天云网云平台，根据上传的数据，航天云网可以为其匹配合作商，寻找商机，将生产能力和市场对接最大化。

目前，航天云网的云端注册企业已经近170万家，发布协作与采购需求近12万条，金额近4000亿元；平台整体协作配套成交额共计1600亿

元；40多万台设备接入了云平台。

服务化延伸、智能化生产、个性化定制、网络化协同……物联网业务正在渗透到越来越多的领域，带动工业、汽车行业、城市建设等领域的智能化升级。

在生产领域，新型的商业模式催生出新的需求，为满足这些需求，需要将全球的工业系统与高级计算、分析、感应和通信技术进行融合，需要实现智能机器间的连接并最终实现人机连接，结合软件和大数据分析，重构全球工业，激发生产力。

由此，工业信息系统迎来了万物互联的时代。换句话说，工业物联网的时代已经到来。

当前，世界主要国家都对工业信息系统和互联网的融合非常重视。例如，2012年美国发布“先进制造业国家战略计划”，将网络与先进制造融合放在了未来工业发展的战略层面；2013年，德国政府在汉诺威工业博览会上提出了“工业4.0”战略，其核心是制造业的网络化和智能化；2015年，我国正式发布了“中国制造2025”战略，通过互联网+先进制造技术促进制造业转型升级，力争跻身制造强国行列。

企业界也表现出极大的兴趣，形成了美国工业互联网产业联盟（IIC）、工业互联网产业联盟（AII）、边缘计算机产业联盟（ECC）等行业和产业联盟，通用电气、西门子、罗克韦尔等装备制造业企业，华为、思科、中兴、AT&T等通信企业，微软、谷歌、亚马逊、阿里巴巴、腾讯等IT服务供应商等都纷纷加入这些联盟，并逐渐形成了新的产业生态。

例如，美国AT&T公司在其总部所在地达拉斯建立了智能城市生活

实验室，应用物联网技术远程控制路灯，使用环境传感器测量不同类型的污染物以及温度、空气湿度和大气压力等，并已与全球排名前24家的汽车厂商中的20家建立了合作关系，使用户可以获得更佳的驾驶体验和更高的安全性。

工业物联网遭攻击的典型案例

工业物联网在拓展了工业控制系统发展空间的同时，也带来了网络安全问题。近年来，随着安全事件的频繁发生，工业物联网安全越来越受到政府、工业用户、科研机构和工控系统厂商的重视。

由于信息技术和操作技术的一体化，传统病毒和工控病毒相互渗透，可利用的漏洞数量和类型同时增长，安全事件不断增多。与单一的互联网相比，工业物联网系统有不同的攻击向量和威胁，它所造成的社会混乱和损失也更严重。

从近些年来全球发生的一系列工业物联网安全事件来看，这些攻击都造成了重大的社会和经济损失，也给人们的生活带来了最直接的影响。

▶以工业系统为目标的网络武器

2017年，一款专门针对工业控制系统的网络武器CrashOverride/Industroyer被公开，这是迄今为止第一款可以直接与电网硬件进行交互的公开恶意软件。安全研究人员认为，该恶意程序与2016年12月发生在乌克兰首都基辅输电变电站的网络攻击事件有关。

2017年6月，位于斯洛伐克反病毒厂商ESET和美国的工业网络安全企业Dragos公司的安全研究人员公布了一种针对关键的工业控制系统的恶意软件，该恶意软件可以攻击电力系统导致停电。ESET将该恶意软件命名为“Industroyer”，Dragos公司将该恶意软件命名为“CrashOverride”。

这款恶意软件可以支持四种协议：IEC 60870—5—101、IEC 60870—5—104、IEC 61850以及OLE处理控制数据访问协议，这四种协议广泛应用于变电站、交通管理、供水系统等关键信息基础设施中。开发者可以利用这款恶意软件重新设置程序，攻击任何使用这些协议的工业控制系统，并可以实施多种攻击。

比如，这个恶意软件扩展DNP3协议支持就可以攻击北美电力系统，还可以对西门子SIPROTEC系列保护继电器进行溢出攻击，从而导致其停止响应，必须手动重启设备才能恢复，也可以导致变电站的继电保护和控制系统无法正常工作，攻击一个变电站可能导致几个变电站级联断电，从而导致大面积停电。

研究人员认为，这款恶意软件的开发人员对电力行业基础设施中工业控制系统工作方式有比较全面的了解，因为如果没有接触过这些设备和硬件，很难开发出这样的恶意软件。

▶新型物联网僵尸网络HTTP81

2016年发生的Mirai僵尸网络攻击，导致了美国东海岸大面积断网。2017年4月，我国也出现了控制大量物联网设备的僵尸网络HTTP81，该僵尸网络感染控制了超过5万台网络摄像头。

2017年5月，360网络安全研究院发布公告，披露了一个名为HTTP81的新型IoT僵尸网络。

早在4月15日，360全球网络扫描实时监控系统就发现HTTP81

僵尸网络活跃度异常增加，当日扫描事件数量比平时增长4～7倍，独立扫描IP来源增长幅度达到40～60倍。4月22日，HTTP81活跃度更是达到高峰，扫描来源的IP地址超过57000个。与普通僵尸网络100到1000个IP节点的规模相比，HTTP81已经成为一个巨型僵尸网络。

HTTP81僵尸网络的幕后操控者远程入侵了大量没有及时修复漏洞的网络摄像头设备，在这些摄像头中植入恶意代码，只要发出指令就可以随时向任何目标实施DDoS攻击。由于网络摄像头属于长期在线的设备，普遍拥有比较高的带宽，与由电脑组成的僵尸网络相比，具备更强的杀伤力。

此外，HTTP81僵尸网络借鉴了Mirai的端口嗅探手法和部分基础代码，但是对比僵尸网络的关键特性，HTTP81在传播、C2通信协议、攻击向量等方面与Mirai完全不同，属于新的僵尸网络家族。

360网络安全研究院的监测数据显示，HTTP81僵尸网络主要分布在国内，尤其是北京、河南、山东、江苏、广州等地区，每日活跃的设备数量一般在2700到9500个之间。这意味着HTTP81一旦展开DDoS攻击，国内互联网很可能成为重灾区，其他国家和地区也不能完全排除受感染或受攻击的可能性。在我们持续监控的基础下，相关部门协同处置，HTTP81僵尸网络没有造成太大危害。

▶工业电厂的安全系统被攻破

2017年12月，黑客利用恶意软件攻击了施耐德电气公司Triconex安全仪表系统，导致一座工业电厂的安全系统停止运营。这是第一起针对能源基础设施安全保护系统发起的攻击事件，攻击者已不满足于

攻击常规工控系统，造成停车或停产，而是开始攻击最核心的安全保护系统，试图造成更严重的危害。

施耐德电气公司的Triconex安全仪表系统（Safety Instrumental System，SIS）广泛应用于能源行业，包括石油天然气和核设施的功能安全保护，该系统失效有可能造成极为严重的后果。美国国土安全部的国家网络安全和通信集成中心（NCCIC）对此攻击事件进行了调查分析。

调查显示，恶意软件HatMan主要以施耐德电气的Triconex安全仪表系统控制器为目标，旨在关停系统并尝试修改系统到危险失效状态。HatMan通过专有的TriStation协议与SIS控制器进行通信，允许攻击者通过添加新的梯形图修改SIS安全逻辑。

Triton恶意软件对SIS控制器的攻击非常危险。一旦控制器被攻破，黑客就可以重新编程，触发安全状态，并对目标环境的操作产生巨大影响。此外，攻击者也可以重新编写SIS控制器程序，倘若控制失败，这将可能导致系统数据被覆盖及服务器运算崩溃，严重扰乱工业控制系统和基础设施系统，如能源生产和供水系统等的运行。

检测到此次攻击后，施耐德发布了一项安全警告，建议避免将Triconex控制器钥匙开关处于“Program”模式，并表示将积极与其客户、网络安全组织等密切合作，以降低此类攻击风险。

上述三个案例是近几年发生的典型工业物联网安全事件，我们从中可以看到，工业物联网安全系统的复杂程度远高于传统的IT网络系统——风险来源较多，发生安全事件的后果相当严重。

我国的工业物联网安全情况也并不乐观。2017年，国家工业信息安全发展研究中心监测处理的工控安全漏洞达到380个。这些漏洞中，接

近六成都属于高危漏洞，它们对重要工业控制系统造成了极大威胁。

下面我再讲两个360处置的案例。

▶某汽车厂商的工业控制系统被勒索病毒攻击而停产

2017年某日，某汽车制造商的工业控制系统开始出现异常。当日晚上19点，该机构生产流水线的一个核心部分：动力电池生产系统瘫痪。该生产系统日产值超百万元，停产直接损失严重，同时也意味着其汽车的电力电机模组部分出不了货，对该企业的生产产生了极其重大的影响。该机构紧急向360安全监测与响应中心进行了求助。

这是“永恒之蓝”勒索病毒的二次突袭，而该企业的整个生产系统已经幸运地躲过了5月份的第一轮攻击，却没有躲过第二次。监测显示，这种第二轮攻击才被感染的情况大量存在，并不是偶然的。

我们安服人员在现场实际勘测后发现，这家汽车制造商的工业控制系统已经被病毒感染，运行异常，但办公终端系统基本无恙，这是因办公终端系统上安装了比较完善的企业级终端安全软件。但在该企业的工业控制系统上，没有部署任何安全措施。感染原因主要是由于其系统与企业办公网络连通，间接存在公开暴露在互联网上的接口。后经综合检测分析显示，该企业生产系统中感染病毒的工业主机数量竟然占到了整个生产系统工业终端数量的20％。

该企业此前早已制定了工业控制系统的安全升级计划，但由于其生产线上的设备环境复杂，操作系统五花八门，硬件设备也新老不齐，所以整个工控系统的安全措施迟迟没有部署。我们测试发现，流水线上最老的电脑设备有10年以上历史，部署安全措施将面临巨大的兼容性考验。

由于厂商的生产系统中没有企业级终端安全软件，于是只能逐一对其电脑进行排查。我们花了一天时间，也仅仅只是把动力电池的生产系统救活。之后，我们差不多用了两个月时间，才把企业生产网中的带毒终端全部清理干净。

▶某知名汽车合资厂商工控软件带毒运行

2017年11月，某知名汽车合资厂商邀请360工控安全联合实验室对其生产系统进行安全检测。我们发现，生产系统中的监控主机上存在大量木马病毒，包括大量感染型病毒，某些木马病毒样本的历史甚至超过10年以上。同时，该系统的工业控制部分也存在大量已知安全漏洞。虽然上述问题暂未对该企业的生产活动产生实质性影响，但安全隐患已经非常明显。

我们进一步检测发现，导致该汽车厂商生产系统感染大量木马病毒、存在大量安全漏洞的主要原因有两个方面：一是生产系统部分设备过于老旧，疏于维护，二是缺乏有效的安全运维和管理。

一方面，该企业使用的自动化生产系统中，有大量设备已经超过原厂提供的质保期或自动化集成商的维保期，如：西门子S7—300PLC等。某些设备的使用时间超过10年以上，系统长期处于无人进行升级维护的状态，上位机监控系统中存在大量老旧病毒并且带毒工作多年。

另一方面，USB管理疏失和网络管控不严。首先，尽管该企业明令禁止员工在工控系统的USB接口上进行手机充电或插拔其他无关设备，但并没有采取任何技术手段对USB端口的使用进行限制；其次，尽管该企业的生产系统并不需要互联网协同工作，但其部分设备的端口却暴露在了互联网上，可以从互联网自由访问，这就使该生产系统随时处于来

自互联网攻击的巨大威胁之下。

鉴于相关设备早已超出保修年限，不仅得不到设备供应商的维护保养，而且也已经很难获得所需驱动程序样本。这时如果直接用原生操作系统驱动替换被感染文件，可能立即造成相关设备失灵，进而无法再生产。

结合这样的情况，我们给该汽车厂商定下了四条具体的处置方案：第一，排查内部网络，封禁生产系统暴露在互联网上的端口，网络内部做好访问控制；第二，请专业技术人员协助清除目前工业主机上可以清除的病毒；第三，使用终端安全管控软件等技术措施，封禁生产系统中所有主机设备的USB端口；第四，在不影响生产的情况，直接物理封禁所有USB端口。目前该厂商全国的三个工业园区都已经完成工业主机防护部署。

这些真实发生的典型工业物联网安全事件充分表明，物联网如同达摩克利斯之剑，它拥有强大的力量，但一旦被夺走，就如同末日降临。智能技术可以造福人类，也可威胁人类。

工业物联网面临的安全挑战

从整体来看，随着制造业的转型升级，万物互联已经成为工业信息系统中不可逆转的趋势。在工业信息系统逐步与互联网进行融合的过程中，安全问题也逐渐凸显出来。由于工业信息系统安全水平相对较低，漏洞较多，这些漏洞极容易被黑客利用。

安全漏洞，成了工业物联网面临的首要安全问题。根据美国工业控

制系统网络应急响应小组（ICS—CERT）的统计报告，2015年漏洞总数为486个，2016年美国关键信息基础设施存在492个安全漏洞。报告指出，相关漏洞涉及供水、能源和石油行业等关键信息基础设施，工业控制系统的信息安全问题亟待解决。

而根据我国国家信息安全漏洞共享平台（CNVD）统计，2017年新增信息安全漏洞4798个，其中工控系统新增漏洞数351个，与去年同期相比，新增数量几乎翻番，工业控制系统漏洞呈快速增长趋势。

未来，工业物联网领域的安全事件还会继续呈现高发状态。我认为，工业物联网面临的安全挑战可以分为外部和内部两方面。

▶工业物联网面临的外部挑战

暴露在外的攻击面越来越大

信息技术与操作技术（IT/OT）一体化后端点增加，给工业控制系统（ICS）、数据采集与监视控制系统（SCADA）等工业设施带来了更大的攻击面。与传统IT系统相比较，IT/OT一体化的安全问题往往把安全威胁从虚拟世界带到物理世界，可能会对人的生命安全和社会的安全稳定造成重大影响。

软件漏洞容易被黑客利用

黑客入侵和工控应用软件的自身漏洞通常发生在远程工控系统的应用上。另外，对于分布式的大型工控网，人们为了控制监视方便，常常会通过开放虚拟网络隧道（VPN tunnel）等方式接入甚至直接开放部分端口，这种情况下也不可避免地给黑客入侵打开了方便之门。

操作系统安全和工业软件漏洞难以修补

工业控制系统操作站普遍采用PC+Windows的技术架构，任何一个版本的Windows自发布以来都在不停地发布漏洞补丁。为保证过程控制系统的可靠性，现场工程师通常在系统开发后不会对Windows平台打任何补丁，更为重要的是，即使打过补丁的操作系统也很少再经过工控系统原厂或自动化集成商测试，存在可靠性风险。

与之相矛盾的是，系统不打补丁就会存在被攻击的漏洞，即使是普通常见病毒也会遭受感染，可能造成Windows平台乃至控制网络的瘫痪。由于工业软件开发工程师更关注工业流程控制以及工艺相关问题，其编程的安全水平普遍不如IT工程师，导致工业软件的漏洞数量远高于IT软件。

恶意代码不敢杀、不能杀

基于Windows平台的PC广泛应用，病毒也随之泛滥。全球范围内，每年都会发生数次大规模的病毒爆发。目前全球已发现数万种病毒，并且还在以每天数十余种的速度增长。这些恶意代码具有更强的传播能力和破坏性。此外，还有蠕虫病毒的死灰复燃。蠕虫病毒随着第三方打补丁工具和安全软件的普及，近些年来几乎绝迹。但随着“永恒之蓝”“永恒之石”等网军武器的泄露，蠕虫病毒又重新获得了生存空间。

基于工控软件与杀毒软件的兼容性，在操作站（HMI）上通常不安装杀毒软件，即使是有防病毒产品，基于病毒库查杀的机制，其在工控领域使用也有局限性。网络隔离性和保证系统稳定性的要求导致病毒库对新病毒的处理总是滞后的。因此，工控系统每年都会大规模地爆发病毒，特别是新病毒。此外，即插即用的U盘等存储设备滥用，也给这类病毒带来了泛滥传播的机会。

DDoS攻击随时可能中断生产

在本书第二章中，我对DDoS攻击进行了详细介绍。该攻击是一种危害极大的安全隐患，它可以人为操纵也可以由病毒自动执行，通过消耗系统的资源，如网络带宽、连接数、CPU处理能力、缓冲内存等，使正常的服务功能无法进行。

DDoS攻击非常难以防范，原因是它的攻击对象非常普遍，从服务器到各种网络设备，如路由器、防火墙等，都可以被拒绝服务攻击。控制网络一旦遭受严重的拒绝服务攻击就会导致严重后果，轻则控制系统的通信完全中断，重则可导致控制器死机等。目前的工业总线设备终端对DDoS攻击基本没有防范能力。另外，传统的安全技术对这样的攻击也缺乏有效的手段，往往只能任其造成严重后果。

高级持续性威胁时刻环伺

高级持续性威胁的特点是：目的性非常强，攻击目标明确，持续时间长，不达目的不罢休，攻击方法经过巧妙构造，攻击者往往会利用社会工程学的方法或利用技术手段对被动式防御进行躲避。

传统的安全技术手段大多是利用已知攻击的特征对行为数据进行简单的模式匹配，只关注单次行为的识别和判断，并没有对长期的攻击行为链进行有效分析。因此，对于高级持续性威胁，无论是在安全威胁的检测、发现还是响应、溯源等方面都存在严重不足。

▶工业物联网面临的内部挑战

除了外部的威胁，工业系统自身安全建设的不足，也给工业信息系统带来挑战。

工业设备资产的“底数不清”

工业设备“底数不清”严重阻碍了安全策略的实施。要在工业物联网安全的战斗中取胜，“知己”是重要前提。许多工业协议、设备、系统在设计之初并没有考虑到复杂网络环境中的安全性，而且系统生命周期长、升级维护少也是巨大的安全隐患。

很多工控设备缺乏安全设计

各类机床数控系统、PLC、运动控制器等所使用的控制协议、控制平台、控制软件等，在设计之初基本未考虑完整性、身份校验等安全需求，存在输入验证，许可、授权与访问控制不严格，不当身份验证，配置维护不足，凭证管理不严，加密算法过时等安全挑战。

例如，生产系统中广泛使用的PLC产品未设计身份校验机制。控制器对命令发送方不作身份鉴别，因此可以被攻击者进行欺骗，重放攻击。

设备联网机制缺乏安全保障

工业控制系统中越来越多的设备与网络相连。如各类数控系统、PLC、应用服务器通过有线网络或无线网络连接，形成工业网络；工业网络与办公网络连接形成企业内部网络；企业内部网络与外面的云平台、第三方供应链，以及客户的网络连接。

由此产生的主要安全挑战包括：网络数据传递过程中的常见网络威胁（如：拒绝服务、中间人攻击等），网络传输链路上的硬件和软件安全（如：软件漏洞、配置不合理等），无线网络技术使用带来的网络防护边界模糊等。

IT和OT系统安全管理相互独立，互操作困难

随着智能制造的网络化和数字化发展，工业与IT的高度融合，企业内部人员，如工程师、管理人员、现场操作员、企业高层管理人员等，其“有意识”或“无意识”的行为可能破坏工业系统、传播恶意软件、忽略工作异常等。

因为网络的广泛使用，这些挑战的影响将会急剧放大；而针对人的社会工程学、钓鱼攻击、邮件扫描攻击等大量攻击都利用了员工无意泄露的敏感信息。因此，在智能制造+互联网中，人员管理也面临巨大的安全挑战。

生产数据面临丢失、泄露、篡改等安全威胁

智能制造工厂内部生产管理数据、生产操作数据以及工厂外部数据等各类数据存在安全问题。不管数据是通过大数据平台存储，还是分布在用户、生产终端、设计服务器等多种设备上，海量数据都将面临数据丢失、泄露、篡改等安全威胁。

工业物联网安全的四大趋势

在“工业4.0”的趋势驱动下，工业物联网的网络安全将是国家关键信息基础设施安全的重要组成部分。对于这个重大难题，我们需要把握工业物联网安全的发展趋势，运用科学、系统、全面的安全理念构建工业信息系统的安全防护体系，更好地保障工业信息安全。

趋势一：勒索软件将继续影响工业网络

由于军用级武器库的泄露，黑客掌握了大量可用的安全漏洞和漏洞利用工具，比特币等数字货币的普及得到广泛认可，给勒索软件提供了可靠的匿名赎金支付方式，这些因素共同影响促使勒索软件地下产业链形成。在这个地下产业链中，黑客们分工协作，甚至出现了勒索软件即服务（RaaS）的模式，因此勒索软件在未来一段时期内还将持续出现。

工业网络是企业生产的基础设施，一旦系统感染勒索软件，企业的生产经营活动将受到直接影响，造成经济损失，支付赎金的可能性更大，因此，工业网络更易成为勒索软件攻击的目标。加之工业网络的特性和需求导致很难及时安装补丁，安全防护水平较弱，感染的可能性增加，因此我们判断，未来一段时间内工业网络中很有可能还会出现勒索软件感染的安全事件。

趋势二：专门针对工业系统的恶意软件将继续出现

从Industroyer恶意软件事件可以看出，已经有部分黑客掌握了工业控制系统协议和工作流程的相关知识，加之工业网络使用的设备和协议安全防护水平较低，更容易发现零日漏洞，出于投入产出比的考虑，将会有越来越多的黑客进入这一领域。

另外，工业网络往往承载着诸如供电、供水、石油石化等关系国计民生的国家基础设施的运行，对其攻击可能导致较大的政治、经济和社会影响，以国家为背景的APT组织也很有可能将在此领域投入大量的精力，因此将会有越来越多的专门针对工业控制系统的恶意软件涌现出来，这类软件甚至会被黑客进行有目的地精准投递。

趋势三：通过互联网扩散到控制网的恶意软件将越来越多

传统工业企业中，控制网络一般与办公网和互联网是物理隔离的，

因此，互联网中的安全威胁很难影响控制网络。工业物联网环境下，控制网将与办公网、互联网发生更多的数据交互，也会有越来越多的连接。虽然这些连接过程中都会考虑安全问题，但一旦建立连接，恶意软件和安全威胁就有可能通过这些连接渗透到控制网，扩大了控制网的攻击面。

在以往的安全事件中，恶意软件也是通过移动存储介质、违规连接等方式，通过办公网扩散到控制网中去的。工业物联网环境下的控制网与互联网有了更多的连接和交互，也将会有越来越多的恶意软件从互联网扩展到控制网络。

趋势四：通过物联网设备构建的僵尸网络短期内很难消除

物联网设备数量多，计算能力弱，安全防护水平较差，随着Mirai利用僵尸网络发动DDoS攻击事件影响的扩大，黑客将继续利用物联网设备构建僵尸网络进行攻击。

虽然各物联网设备制造商都已经采取了相应的安全措施，世界主要国家也发布了物联网设备准入的法规，新部署的物联网设备安全性会大大提高，但是数量众多的存在漏洞的存量资源还是足以构成大型的僵尸网络，随时可能发动新一轮的DDoS攻击。

另一方面，物联网设备难以自动升级，分布在不同的国家和地区，现有的存在漏洞的设备很难被替换，已经构建的僵尸网络也很难在短期内消失，这些僵尸网络可能还会发动类似的网络攻击。此外，通过控制大量物联网设备攻击其他互联网基础设施造成恶劣影响的思路可能会被后续的攻击者采用。

第三节　云计算的安全困扰

当我们说起人工智能，就自然会说到云计算。人工智能的背后是海量数据的积累和学习，如果没有云，这种积累和学习是无法想象的。

从2006年谷歌提出云计算开始，11年过去了，云计算已经渗透到了各个行业。有报告称，未来五年，向云上的转移将会直接或间接影响超过1万亿美元的IT开支。

云计算的核心技术是虚拟化技术，它彻底改造了IT的组织和运营方式，在这个过程中，云计算的稳定性、安全性等问题受到广泛关注，尤其是云安全，越来越被重视。

云的传统安全威胁

云计算安全可以分为传统安全威胁和新的安全威胁。传统安全威胁主要包括以下几种。

▶DDoS攻击

大家都知道DDoS攻击是一种拒绝服务攻击行为，这里所说的是针对云平台业务系统的攻击行为以及由云平台内部外发的攻击行为，这是整个云平台的安全隐患。

▶僵木蠕威胁

在云平台内，如果租户隔离、区域隔离措施不当，僵木蠕（僵尸网

络、木马、蠕虫）威胁将会更快、更迅速地传播，给云平台带来极大的安全隐患。

▶业务系统威胁

云上业务系统同样面临着结构化查询语言（SQL）注入、跨站脚本攻击（XSS）、跨站脚本伪造（CSRF）等传统的Web应用攻击威胁。

▶主机威胁

云平台上，各类操作系统、网络交换设备、数据库及中间件等都面临着安全漏洞风险，传统的漏洞利用方式和攻击手段对它们依然有效。

▶恶意代码病毒

恶意代码和病毒仍然会对云内的业务系统、操作系统、云管理平台、中间软件层（hypervisor）等造成安全威胁。

在云环境下，上述传统安全问题，可能会造成比其在传统环境下更严重的后果。

例如，2018年初爆出的CPU漏洞是由英特尔处理器设计缺陷引发的一系列漏洞的“漏洞”，影响范围极广，几乎波及了全球所有的手机、电脑、服务器以及云计算产品，但它对云厂商的潜在威胁是最高的，几乎全球所有主要云厂商，包括中国主流云厂商，都高度重视并投入巨大，以消除此漏洞的影响。在普通物理服务器上，仅涉及物理机打补丁修复。而在云环境下，解决该安全隐患的完整修复方案则需要包含两个部分，一是云平台虚拟化宿主机修复，二是客户侧的操作系统更新。只有两部分都修复，才能彻底消除影响。反之，一旦某台虚拟机被利用，同一物理机上其他用户的云主机中的数据都会存在风险。

云计算的新安全威胁

云安全的最大挑战，一是来自其本身，也就是云上的安全；二是云计算的动态化、软件化、虚拟化等特点带来的新安全威胁。

▶云计算带来的边界变化

云计算技术让网络的传统边界发生了变化，软件定义网络（SDN）、虚拟私有云（VPC）、弹性扩展、动态迁移等技术打破了传统的网络架构，过去基于传统网络和划分安全域，在出口上堆叠防火墙等防御设备的时代已经一去不复返了。公有云、混合云的出现，彻底将企业的安全边界扩展至企业内网之外。为了应对这种新的变化，我们首先要做的事情，就是重新构建弹性安全，重建云上的安全边界。

▶虚拟化漏洞的三大危害

虚拟化漏洞在目前主流虚拟化系统中广泛存在，黑客利用虚拟化漏洞不但可以偷取重要信息，甚至可以从一台虚拟机的普通用户发起攻击控制宿主机，最终控制整个云环境的所有用户。

虚拟化漏洞导致的危害主要有三个方面：一是造成宿主机崩溃，从而影响同一宿主机上其他虚拟机的正常运行；二是宿主机被控制，即虚拟机逃逸攻击，获取宿主机的控制权，使用宿主机发动更加深入的攻击；三是侧信道攻击，就是获取同一宿主机的其他虚拟机的敏感信息。

例如，2015年爆发的毒液漏洞，危害极大。这个漏洞能让攻击者越过虚拟化技术的限制，访问并监视控制宿主机，并通过宿主机的权限来

访问控制其他虚拟主机。一旦控制宿主机，利用宿主机强大的性能，攻击者就可以进行比特币挖矿、密码暴力破解，或者获取宿主机所有的虚拟机上的RSA私匙、数据库等。这个漏洞2004年就已经存在，被发现时已经过去了11年之久。

毒液漏洞拉开了云计算安全威胁的序幕，紧接着2015年下半年，更多的存在于云计算系统中的通用性虚拟化安全漏洞相继出现。这些漏洞一旦被黑客利用，轻则造成云计算系统崩溃，重则黑客直接控制云系统。

▶数据与资产的集中使攻击面更大

云让数据资产更集中，形成了一个个数据金矿，同时，也必然更容易吸引黑客的攻击。世界经济论坛（WEF）发布《全球风险报告》称，对主流云计算公司的网络攻击所造成的经济损失，堪比桑迪或卡特里娜飓风所带来的巨大灾难。如果攻击者拿下一家主流云提供商，其带来的损失可能在500亿到1200亿美元之间，正好与飓风桑迪和卡特里娜所致的损失相当。

▶云计算带来的管理上的变化

云计算将过去分散、孤立的IT系统进行了集中，这势必带来运维和管理的集中，原来的角色和责任分工也受到冲击。例如，租户、云平台运营方、安全防护方、云平台拥有方的责任分工目前不清晰，租户系统发生安全问题经常找不到责任方。

▶云计算带来的复杂度

在云环境中，变化是常态，静态的部署和策略配置基本无效，安全

也要能够随着云的变化而动态调整。此外，复杂的IT融合环境、SDN技术带来的控制和数据平面分开、弹性调度与动态迁移等，都使安全的配置与管理变得更加复杂。

云建设需要形成三方制衡机制

云的引入，对现行的IT技术和IT管理都产生了深刻影响。在本章的开篇，我提到了一个云安全“黑洞”，这需要引起我们的高度重视。

云和大数据平台存储的都是数字化信息，对甲方来说像“黑洞”，要想“看见”需要借助云厂商提供的工具。设想一下，如果云厂商技不如人，甲方数据“被丢失”，但甲方是没有感知的，也很难通过什么手段去核查。

甲方获知数据泄露的途径只有两种：一是数据泄露的危害显现出来，从而推导出数据被窃；二是依赖云厂商的良心，主动报告。如果厂商发现了这个事故就报告，一定会受到甲方的处罚，而他不报告，甲方又很难发现核查，他就可以免受甲方的处罚。在这个“二选一”的抉择里，如果没有任何监督手段，完全凭厂商的良心，其实是对事业的不负责任。

不管是电子政务，还是地铁、水电等公共服务，或是银行、航空等专业服务，云中的数据被偷、被篡改、被破坏，都会给甲方带来重大损失。

可以确定的是，云厂商的产品，无论水平多高都会有漏洞。像微软、谷歌、苹果、Adobe这样的大公司，每个月都会有几十个漏洞被发

现被提交，需要公告天下并打补丁。这些都是需要专业的安全团队才能完成的事情。

我们还要考虑到，云厂商的代码，要么是自己写的，要么是开源的，要么是供应商提供的，除了代码本身会有漏洞这个不可避免的因素，供应链安全问题、内部人员可靠性问题等，都是可能造成安全事故的巨大隐患。

目前，云在互联网之上已经成为全球攻击的重要目标，云的防护、应急、安全服务都需要和顶级的黑客对抗，乙方是不具备能力完成的。这与甲方的利益息息相关，需要引起高度重视。

在新时代，我们需要建立一个三方制衡机制，建设、运营和安全服务三个角色分开，这和建筑工程需要建设方、施工方和监理方三方制衡是一个道理。

一个建筑工程需要建设方、施工方和监理方。这是因为建房子有很多隐蔽工程，比如这个地基到底挖了多深，房子盖好就看不见了；用的钢筋是多粗，砖头一砌好也看不见了；用的水泥、电线、管道等材料，都需要在工程实施的过程中就进行有效监督。如果没有监督，再好的建设施工方，也有偷工减料的可能。

现在我国各地都在大力建设云平台、大数据中心，安全是政务云的生命线，需要明晰各方的分工和责任，甲方是建设方，要严格要求，乙方云厂商，要提高标准，还需要第三方安全服务查漏补缺。这三方互相制衡，才能从最大程度上杜绝漏洞，长治久安。

▶云厂商与云安全厂商要独立分开

云安全管理的要素之一，是要明晰云环境下的角色定义和安全责任分工界面。

以电子政务云为例，它可以分为云建设、云监管、云使用、云承建、云安全服务五个角色。哪个角色是监管责任，哪个角色是使用责任，哪个角色应该负责安全，其责任分别是什么，这些都要明确，并落实到日常工作中。

关于云安全服务方，目前在云的建设中存在两种观点：一种是云建设方是总集，负责协调云安全服务方；一种是云建设和云安全分开，两个角色相互独立。我认为，后一个观点更为合理。因为云安全服务方作为一个特殊角色，只有独立于云建设方，双方相互监督，相互制衡，才能避免在出现安全问题的时候“捂盖子”。

毕竟，当一家云厂商自己身兼数职，出现安全事故又很可能只有他自己才知道的时候，很难相信他会顶着巨大的压力，广而告之自己出了问题，并主动承担责任。

我们不以最坏的恶意揣测任何人，但云厂商如果没有独立第三方的安全厂商来监督与制约，那它就等于拥有了一只“上帝之手”，可能会毫无顾忌，这也是一个非常大的安全隐患。

▶云安全要重视常态化运营

云安全管理的另一个要素，是常态化运营。在云平台的生命周期中，大规模建设和扩容通常时间较短，更多的是长期运营。运营如何能做到统一、完整、及时，这要从多方面考虑。

比如，安全运维包括资产管理、网络安全管理、系统安全管理等，但云上的资产管理比传统资产管理难度更大，因为云上的弹性扩展与动态迁移会带来资产频繁的动态变化。常态化安全运营需要通过安全管理中心覆盖安全运维、威胁发现、持续监测问题溯源及联动控制几个方面，而这其中，人是运营的核心。

360在处理多起云环境应急时，发现了一个普遍的问题：用户对于后期云安全的运营重视程度不够，不能形成体系化、闭环的运营体系。有一个用户运营的云环境中，多次大面积中招挖矿程序。溯源分析发现这是由于该客户云环境中的租户，在云主机的登录口令设置上经常使用弱口令，并且多台云主机的口令可能是相同的，结合云主机的东西向攻击，导致很容易大面积出现问题。我们通过帮助客户梳理云主机开通时的安全设置和基线要求，以及设立云安全巡检，成功地消除了这个问题。

第四节　人工智能技术在安全中的应用

让我们再回到本章第一节所提到的影视作品中的各种科幻情节。

《疑犯追踪》第四季第11集讲述了芬奇在公园训练TM下国际象棋的故事。现实中，从阿尔法狗（AlphaGo）与世界围棋冠军李世石的人机大战到与我国中国围棋职业九段棋手柯洁的正面交锋，这都说明了人工智能与人的大脑的角逐一直在持续。

什么是人工智能

人工智能是计算机科学的一个分支，它企图了解智能的实质，并生产出一种新的、能以人类智能相似的方式做出反应的智能机器。该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。

人工智能（Artificial　Intelligence）英文缩写为AI，它是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。

随着人工智能理论和技术日益成熟，应用领域也不断扩大。人工智能可以模拟人的意识、思维的信息过程。人工智能不是人的智能，但能像人那样思考，也可能超过人的智能。

值得注意的是，尽管人工智能技术可以应用于安全防御，但也可能会被黑客利用。正如一些科幻电影中所展现的，一些黑客利用人工智能进行语音合成，模拟成其他人物进行精准欺诈；利用面部识别技术和无人驾驶飞机，进行识别并攻击特定的人类目标；或者利用培训过的机器，开展网络钓鱼等网络攻击。

2018年2月，来自牛津大学人类未来研究所、剑桥大学存在风险研究中心和OpenAI公司的二十多位专家共同发布了《人工智能的恶意使用：预测、预防和缓解》报告，指出未来五年人工智能可能带来的潜在社会威胁及其化解方式。报告写道：“随着人工智能越来越强大，越来越普及，我们预计人工智能系统的广泛应用将导致现有威胁的扩大，还会引发新的威胁，甚至改变典型的威胁特征。”

任何科技都有其双面性，新兴的人工智能也不例外。因此，在大力发展技术的时候，我们有必要注意防止该技术被滥用的可能性。

▶挖掘大数据进行精准攻击

黑客利用人工智能技术，可以通过挖取网络大数据得到每个人包括出生日期、电话等在内的几乎所有身份信息，也可以监控邮件、发送的信息，甚至是量身打造个性化的“鱼饵”，来进行精准的网络攻击。

例如，黑客组织Lazarus利用脸书、信使（Messenger）、领英（LinkedIn）、推特等社交平台上的信息，用人工智能的分析方法梳理出值得攻击的目标，然后跟踪分析，寻找机会。他们全球作案，涉案金额高达数亿美元，索尼数据泄露、加密货币交易所遭攻击、SWIFT银行网络遭攻击等事件都与该组织有关。

此外，黑客还利用人工智能技术进行自动化漏洞检测、构建恶意软

件等，不仅大规模降低了攻击成本，更提升了复杂攻击的速度与执行效率。不仅如此，人工智能还拥有超强适应性、自动智能判断等优势，当网络攻击遇到阻力，或者网络安全专家修复了原有漏洞时，人工智能会快速做出反应，提醒黑客利用另一项漏洞，发动入侵行为，让网络攻击的成功率更高。

▶更高级的鱼叉式钓鱼攻击

很多数据泄露事件都始于鱼叉式网络攻击，比如本书第一章中提到的希拉里“邮件门”事件就是一个典型代表案例。当黑客利用人工智能发起鱼叉式攻击时，将会增强网络钓鱼邮件的真实性与可信性。

在2016年的美国黑帽会议上，约翰·西摩（John Seymour）和菲利普·塔利（Philip Tully）发表了一篇名为《社会工程的武器数据科学推特上实现自动E2E鱼叉式网络钓鱼》的论文。该论文提出了一种时间递归神经网络，它可以学习如何向特定用户发布网络钓鱼帖子，通过把用户发布的帖子作为训练测试数据，并根据目标用户时间轴帖子中的主题动态播种，使钓鱼帖子更有可能被点击。通过在推特社交平台上的测试他们发现，为用户量身定做的钓鱼帖子，其点击率是有史以来所报道过大规模钓鱼攻击活动中最高的。

迈克菲实验室在2017年的预测中表示，犯罪分子将越来越多地利用机器学习来分析大量被盗记录，以识别潜在受害者，并能更加有效地构建针对这些人的、内容详尽的钓鱼类电子邮件。

▶混入“污染”样本逃过查杀

人类需要通过学习才能掌握知识，之后再通过实践来验证知识和扩展知识。人工智能技术也同样必须通过海量样本的学习和训练，再进行

人工校验才能生成可实用的系统。如果人类小时候学习了错误的知识，就有可能在长大以后做出错误的行为。

同样地，人工智能系统如果在做机器学习时，被恶意混入了错误的样本，或者是样本标识错误，这也就会导致人工智能系统最终识别的误判。这些错误的样本就是“污染”样本。

大量研究发现，“污染”样本的混入，往往会对人工智能系统产生致命的干扰。因此，一些黑客试图通过在人工智能系统的学习过程中混入“污染”样本的方法，来实现自己的攻击目的。

以上这三个方面只是黑客借助人工智能实施攻击的冰山一角。和大数据、云计算、物联网等新兴技术一样，人工智能也是一把“双刃剑”。我们不应该神话它，认为它无所不能。如果它被合理利用，那就可以发挥它的正面功能，造福社会；如果被不法分子利用，则后患无穷。

人工智能在安全防护中的应用

2017年，“人工智能”第一次被写入十三届全国人大一次会议政府工作报告，表明国家对人工智能的重视程度不断加大，人工智能已上升为国家战略。人工智能在安全漏洞防护中的应用将是未来的趋势之一。

目前，人工智能已经在多个领域得到了应用。比如，预测犯罪、杀毒引擎和漏洞攻防就是人工智能运用于网络安全防御方面的创新。

▶人工智能在预测犯罪中的应用

随着全球犯罪率的加剧和恐怖袭击的频繁发生，各国的安全部门正

引进大数据技术来帮助预测犯罪及恐怖袭击地点。科幻剧里预测犯罪的例子，现在已经成为现实。

早在2011年，美国洛杉矶警察局和英国曼彻斯特警察署合作，做了一次测试，试图通过算法预测犯罪地点，进而提前部署相应的警力和预防措施，来化解或应急处理犯罪。事实证明，这样的方法极为有效。当年洛杉矶的入室抢劫犯罪案件大幅度减小，曼彻斯特市特拉福德区的抢劫案与之前一年同期相比下降了26.6%，而整个曼彻斯特市的抢劫案件发生率相较之前一年同期减少了9.8%。

现在，人工智能分析技术被广泛地运用在重大活动或者会议的安全保障工作中。警方以历史案件信息的数据为基础，运用人工智能分析模型，建立犯罪数据分析系统，有效预测犯罪趋势，提高警力的投入效率。

▶人工智能在漏洞攻防中的应用

CGC（Cyber Grand Challenge）是2013年由美国国防部高级计划研究院（DARPA）发起的全球性网络安全挑战赛，是第一个在CTF竞赛中没有人类参与、完全由计算机完成的竞赛。CGC开启了网络自动攻防竞赛的先河，其目标是建立自动攻防系统对软件漏洞进行检测、验证和修补，提升利用人工智能进行网络攻防的能力。比赛的所有过程和步骤都要求做到全程自动化，现场只能看到7台机器的无声较量。

2016年，360网络安全北美研究院负责人李康和360企业安全集团顾问张超副教授，分别作为两个队伍的负责人和组织者，参加了CGC机器人竞赛项目，并闯入决赛。

从CGC的人工智能系统初期表现来看，还没有迹象表明它有能够全

面超越人类黑客的能力，但自动系统用于安全攻防的实践将加快到来。

▶人工智能在杀毒引擎中的应用

人工智能引擎的代表是奇虎支持向量机（Qihoo Support Vector Machine，QVM）人工智能引擎，这个引擎在2010年5月研发成功，当年正式应用于360杀毒产品中。它采用人工智能算法，具备自学习和自进化的能力，无须频繁升级特征库，不但查杀能力显著提升，而且从根本上攻克了前两代杀毒引擎“不升级病毒库就杀不了新病毒”的技术难题，这在全球范围内属于首创。

人工智能杀毒引擎的实质是将从海量样本中“找规律”的繁重工作交给机器来完成，而人的主要工作就是抽样分析一部分黑白样本，之后告诉机器：哪些是黑的，哪些是白的。当然，找规律的方法以及要从哪些方面来找规律，还是由人类工程师来设计。但具体找到的是什么规律，则完全是由计算机通过机器学习来自动完成的。

这种方法可以摆脱对病毒特征库的依赖，通过从海量病毒样本数据中归纳出一套智能算法，自己来发现和学习病毒变化规律。它无须频繁更新特征库、无须分析病毒静态特征、无须分析病毒行为，但是病毒检出率却远远超过了传统引擎，并且查杀速度比传统引擎至少快一倍。

打个比方，老神探教小侦探如何甄别好人和坏人，但老神探并不告诉小侦探具体的方法，而是只给了小侦探1000张好人的照片和1000张坏人的照片，让小侦探自己从照片中找规律。当小侦探看的照片足够多，并且真的能从这些照片中找出某些隐藏的规律时，那么他再看到其他人的照片时，也能像福尔摩斯那样，一眼就看出照片上的人是好人还是坏人。

不过，机器在学习过程中，对于学习样本的典型性和纯粹性都有比较高的要求。如果交给机器学习的样本缺乏代表性，那么学习结果就可能有偏颇；如果在白样本中掺入少量黑样本，或者在黑样本中掺入少量白样本，都会导致学习结果的彻底失效。所以，不同的人工智能杀毒引擎，其水平高低的本质差别，主要不在算法本身，而是在于机器背后的人类安全专家的素质和水平。

据我所知，现在很多公司都在利用人工智能进行网络攻防对抗。360也一直致力于用人工智能的方法解决智能时代的网络安全问题，除了将人工智能应用于杀毒引擎中，我们在用户行为识别发现中也采用了人工智能的方法，以用户行为、应用系统的日志等大量数据为基础，确定正常用户的基线，从而找出异常。在本书后续的章节中，我将更详细地介绍我们在人工智能应用方面的创新。

智能时代解决安全问题的方法论

在人工智能时代，一切都可编程，我们将进入万物互联的世界。无论是传统的网络安全技术，还是人工智能技术，这些都是手段，我们不能单纯依靠某种技术或者某个单一的项目来解决如此庞大、复杂和系统的问题，我们还需要有一个方法论层面的思想来指引我们。

更严格：构建整体安全体系，做到规划、建设和运营“三同步”

人工智能时代，信息化建设与以往的信息化建设有一个很大的不同：发展与安全的关系发生了变化。在信息化建设时代，发展是主，安

全是辅。但在今天，安全成为发展的前提。

2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上明确提出：“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。”

智能时代给了我们一个重建网络安全体系的机会，这要求我们必须具备同步意识，做到规划、建设和运营“三同步”，甚至在新建一个机房的时候，就应该考虑它的安全问题。这种系统化的思维方式是保障国家和社会安全的基本前提。

更创新：充分利用人工智能等新兴技术，构建积极防御能力

面对越来越智能的网络攻击，我们需要充分利用人工智能等新兴技术，构建网络安全积极防御能力体系。

比如，延缓或阻止与特定威胁相关的活动，甚至可将恶意的人、系统或设备隔离开来，快速降低攻击造成的损失。同时，积极采用动态防御，迫使攻击者不断重新适应并对动态转移的薄弱点做出反应，从而有效防止攻击者使用自动化程序，让廉价的攻击无法瞄准目标。

更全面：加强内部人员的安全意识，设置足够的安全运营人员

在本书第一章中，我提到内部威胁是最大的危害，所以，企业机构内部人员的安全意识很重要。在一些传统企业中，很多内部人员对网络安全的知识相对缺乏，因此，对现有人员进行交流和培训是比较经济有效的方法。企业可以进行内部交流培训，也可以同其他企业、安全服务和咨询公司进行外部交流和培训。

除了提高安全意识，我们还需要大量专业的安全技术和运维服务人

员来从事分析、研判和响应处置工作。据我了解，我国大部分政企单位的安全管理和技术团队力量严重不足，比如有的信息安全部门通常只有两三个人，很难做好日常安全运营工作，更无法快速地进行应急响应。在网络安全形势日益严峻的今天，一支“技术扎实、能力过硬、善打硬仗”网络安全运维队伍是守护国家和社会安全的根本保障。

智能时代带来更便捷的体验，我们享受着智能科技带给我们的便利，人工智能想我们所想，做我们想做。但正如老子所言：“祸兮福之所倚，福兮祸之所伏。”人工智能和万物互联，也是滋生漏洞的沃土，智能时代的漏洞防不胜防。

对个人而言，智能时代的漏洞影响的是个人隐私、日常生活，甚至是生命。但智能时代的各种技术并非只为个人服务，企业、社会，乃至一些政府机构都沉浸在智能技术带来的便利中。

可以预见，网络空间的攻防对抗将愈演愈烈，对抗的主体不再仅仅是某些个体或组织，而是上升到国家间的对抗。这种对抗的主要形态就是我即将在下一章中讲述的网络战。

Chapter 5
第五章
网络战场漏洞是癣疥之疾，还是堪比核武器

网络战，将是未来国家间竞争的主要形态。利用网络信息技术掌握其他国家的政治、经济和军事绝密情报，瘫痪其通信网络、金融信息系统和军事指挥系统，发动舆论攻势，实现不战而屈人之兵。

美国在1991年的海湾战争中对伊拉克实施的网络战，被普遍认为是网络战的开端。网络信息技术不断进步，开始在战争中发挥更重要的作用。现在，漏洞已经具备了武器属性，其威力被认为仅次于核武器。

和传统战争不同，在这个战场上，闻不见硝烟，看不到刺刀见红，也听不见战马人声，但它比传统战争残酷千百倍。网络渗透和控制将成为国际争斗中最常用、最危险的手段，网络战的攻击力事实上远大于传统战争。

第一节　网络战：愈发重要的战争类型

正如生产力的发展必然带来生产关系的变化，信息时代网络技术的飞速发展及其在各个领域的广泛应用，引发了经济、社会、文化和军事的深刻演变，网络空间已经成为世界各国战略博弈的新领域、军事斗争的新战场，网络战已经成为影响国家安全形势的关键因素。

中国2015年版国防白皮书《中国的军事战略》就已经指出：“世界新军事革命深入发展，武器装备远程精确化、智能化、隐身化、无人化趋势明显，太空和网络空间成为各方战略竞争新的制高点，战争形态加速向信息化战争演变。”

美国网络司令部升格获权“先发制人”

2018年5月4日，日裔美军上将保罗·中曾根（Paul　Nakasone）就任网络司令部司令，兼任美国国家安全局局长，成为美军网络司令部升级之后的首任司令。

此前的2017年8月，美国总统唐纳德·特朗普（Donald　John Trump）宣布，将网络司令部升级为美军第十个独立的联合作战司令部，地位与之前的九个联合作战司令部拉齐，分别是中央司令部、北方司令部、南方司令部、欧洲司令部、印太司令部、非洲司令部、特种司令部、战略司令部和运输司令部。

美国网络司令部是于2009年6月23日，由时任美国国防部长罗伯特·盖茨（Robert　Gates）下令创建的，隶属于战略司令部之下的二级司令部，以协调网络安全以及指挥网络战。总部编制700人，下辖6支战役级总部分队，以及由133支任务小组组成的规模约6200人的网络任务部队。

2017财年的国防授权法首次授权军方在网络安全领域使用特招入伍权限，允许地方专业人才最高以上校军衔直接入伍。

《纽约时报》2018年6月17日的报道称，美国国防部将在2018年秋天授权网络司令部采取更具进攻性的途径抵御网络攻击。报道援引国防部一份内部文件说，新政策的目的是让美国军力“尽可能接近对手活动的源头以扩展我们的影响范围，从而暴露对手的弱点、了解他们的意图和能力，并从袭击源头附近实施对抗，迫使他们增加国防资源，并减少袭击”。对网络司令部的新授权政策更为激进，目的就是通过报复性活动，迫使敌人重新审视发动袭击的价值。**美国多方认为，俄罗斯、朝鲜、伊朗和中国是其网络空间领域的潜在敌人。**

什么是网络战

网络战是指在网络空间或通过网络空间而进行的军事活动、情报活动和日常业务活动。美国独立分析机构皇家国际事务研究所更是把网络战直接定义为：在网络空间，出于政治、经济、领土目的，使用精确和合理的兵力攻击军事和工业目标的一种国家间冲突形式。

过去，我们说战争是一种集体、集团、组织、民族、派别、国家、政府之间互相使用暴力、攻击、杀戮的行为，是敌对双方为了达到一定

的政治、经济、领土的完整性等目的而进行的武装战斗。然而，随着漏洞不断成为一种被广泛争夺的资源，围绕争夺漏洞的网络战争开始打响，网络上出现了一种真正看不见硝烟的战争。

网络战在未来会取代传统的战争行动，因为，依靠现今的信息系统和人工智能、大数据、物联网、云计算等技术，高度网络化的社会表现出了一些新的战术和战略弱点，而且一些好战组织已经掌握了利用网络发动不同级别战争的能力。我们不难发现，网络战的核心是一个国家利用网络攻击来扰乱另一个国家的信息系统，从而对其造成显著的损失或破坏。其中，获取信息控制权是致胜关键，包括在指挥、控制、通信、情报和搜索等方面全面超过对手，抢在敌人之前了解敌人、欺骗敌人并发动奇袭。

具体来讲，网络战的博弈可以存在三种方式：一是网络盗窃战，即找到对方网络漏洞，破解文件密码，盗出机密信息；二是网络舆论战，即通过媒体网络，编造谎言、制造恐慌和分裂，破坏对方民心士气；三是网络摧毁战，即运用各种网络攻击武器，进行饱和式攻击，摧毁对方政府、军队等机构的信息网络。

曾经发生过的网络战

可以预见的是，网络渗透和控制将成为国际争斗中最常用、最危险的手段，网络战的攻击力，事实上不逊于，甚至远大于传统战争。

▶海湾战争：网络战争的开端

美国在1991年的海湾战争中对伊拉克实施的网络战，被普遍认为是

网络战的开端。网络信息技术不断进步，也开始在战争中发挥更重要的作用。

海湾战争爆发于1991年1月17日，历时42天，是美国领导的联盟军队，为恢复科威特领土完整而对伊拉克进行的一场战争，是冷战结束后第一场大规模武器冲突。**多国部队充分应用了信息化作战方式，以较小的伤亡代价重创伊拉克军队，体现了信息技术的发展所引起的作战特点的革命性变化。**

早在开战前，美国中央情报局就派特工到伊拉克，将含有计算机病毒的芯片换到了伊方从法国购买的防空系统中所使用的打印机芯片上。在战略空袭前，美方使用遥控手段激活了病毒，致使伊防空指挥中心主计算机系统程序错乱，防空C3I系统失灵。

不仅如此，多国部队集结了固定翼飞机、旋翼飞机、火箭发射车等多种现代化武器，尤其是在精确制导武器上，多国部队拥有绝对优势。美国还动用了50多颗各种军用和商用卫星构成战略侦察网，为多国部队提供了战略情报。

我在一篇对美国前情报总监迈克·麦康奈尔（Mike Mc Conell）的专访里看到，麦康奈尔认为，这次战争展现了美国使用计算机技术施行精确打击的能力：“在二战中要投1000枚炸弹才能有效摧毁目标，在越战中要几百枚，现在只需要一枚……”

在拥有网络信息技术优势的部队面前，单纯的数量对比已失去了意义。网络信息技术对战争的强烈影响使海湾战争成为一个新时代的开端。网络战不再是神话，它已经在现实生活中真实上演。

▶科索沃战争：第一次较大规模网络战

海湾战争中网络技术的应用颠覆了人们关于战争的传统观念，是机械化战争向信息化战争时代的转折，而1999年的科索沃战争，则被认为是史上第一次较大规模的网络战争。在此战争中，网络攻防战已成为交战双方的另一个前线战场。

1999年3月24日，北约发动了对南联盟的军事空袭，首先便将打击目标指向了南军的指挥联络网络。在前几轮空袭中，北约集中用“战斧”巡航导弹和能携带精确制导武器的战斗机对南军的控制网络进行毁灭性的打击，使其指挥控制、信息系统遭受重创，难以组织有效的反空袭和反击。同时以美国为首的北约利用互联网对南联盟发起强大舆论攻击，歪曲战争真相。

面对北约的种种打击，南联盟也不示弱，相应发动了网络攻击。南联盟的网络攻击主要是侵入北约军事相关部门计算机系统，对其指挥通信系统大肆破坏。北约开始轰炸的第三天，贝尔格莱德的黑客利用自己的计算机自动反复连接北约站点，造成网络阻塞。另一位黑客每天向北约电子邮件系统发送约2000份电子邮件，投放了5种计算机病毒。

1999年3月29日，俄罗斯黑客入侵美国白宫网站，造成该网站无法工作。当天英国与西班牙的多处官方网站也遭到破坏，北约国家轰炸行动中最依赖的英国气象局网站损失惨重。美国国防部称，在北约空袭南联盟期间，重要军事网站几乎每天都受到来自黑客的攻击。

4月4日，南联盟黑客又使用“梅丽莎”“疯牛”等病毒使北约通信网陷入瘫痪，美海军陆战队所有作战单元的电子邮件均被“梅丽莎”病毒阻塞。北约在贝尔格莱德的B—92无线电广播网，以及在布鲁塞尔总部的网络服务器和电子邮件服务器，均连续受到电脑病毒的破坏。电脑病毒还造成美海军“尼米兹”号航空母舰计算机系统瘫痪三个多小时。黑客高

手对英国“天空”卫星系统中的一颗卫星进行了劫持，使其反应迟钝，基本丧失效能。

科索沃战争是网络战的经典案例，被各大军校写入了教材。互联网使战争进入了一个全新时代，任何人都可以利用网络参战，甚至可能达到传统军事手段都无法实现的规模和效果。

▶伊拉克战争：开辟网络战新阶段

2003年的伊拉克战争开辟了网络战新时代，这次战争中所使用信息技术之多是历史上从来没有过的，又被称为“网络中心战”。

早在2002年7月，美国时任总统小布什签署了一份“国家安全第16号总统令”，要求政府部门制定有关网络袭击的战略，就向伊拉克这样的“敌对国家”展开网络攻击提出指导性原则。网络司令部给当时的网络部队三项任务：一是试验各种网络武器的有效性；二是制定使用网络武器的各种条例；三是培训出实战型的网上攻击部队。美方设想，在不出动飞机和部队的情况下，美国士兵可以坐在电脑终端前，悄无声息地侵入外国电脑系统，将敌人的雷达关闭，造成其电子指挥系统和电话服务失灵。

对伊拉克的网络战分为两个阶段。**第一阶段是在战争爆发前一周的（2013年）3月14日，伊拉克重要计算机系统遭到长时间、大规模的攻击。**伊拉克技术防范措施落后，计算机网络不是瘫痪就是被接管，军队指挥与通信系统陷入混乱，这种网络空间“先期作战”效果远胜传统的火力准备。**第二阶段美国先头部队携带各种网络设备，与潜伏的网络特别部队一起，入侵伊军指挥与通信系统，使伊军陷入一种被割裂的无指挥状态。**

网络舆论战成为推垮萨达姆政权的秘密武器。媒体报道称，很多伊拉克军官都收到过美军劝降的电子邮件，大意是：你们只要把坦克停到外面，就可以平安回家。美国情报系统不断地向伊拉克国内具有社会影响力的主流阶层发送电子邮件，这些邮件列数了伊拉克总统萨达姆执政20年来的种种罪状，散布萨达姆及其两个儿子被“铲除”的消息，极力劝降社会主流人物。

巴格达陷落半个月后，美国广播公司驻巴格达记者采访了三名伊军军官，这几名伊军军官承认，美军的舆论战和心理战的确动摇了伊军抵抗的信心，真正起到作用的并不是数以千万计的传单和专门开通的广播，而是美军向伊拉克指挥官发去的文传和电子邮件。

▶以色列空袭叙利亚：举世震惊的网络战

2007年9月6日，以色列空军10余架F15和F16非隐身战斗机突入叙利亚领空，对代尔祖尔市附近名为艾其巴（Al-Kibar）的疑似核设施实施了手术刀式轰炸。叙利亚的防空导弹旅和大量防空雷达竟然完全没有发现。最后，以军战机从原路安全返航，整个过程当中，都没有受到叙军的任何攻击，这让世界为之震惊。

据美国电气电子工程师学会（IEEE）出版物《科技综览》（*IEEE Spectrum*）分析，以色列人使用了美国的一种网络战攻击武器“舒特系统”。典型的“舒特系统”一般由电子侦察机、专用电子战飞机和战斗机组成，可以通过通讯信号找到对方雷达系统，然后将自己编造的数据传输进去，最后成功侵入对方防空雷达网，“接管”控制权，使其防空系统处于失效状态。

这次袭击又被称为“果园行动”，可以说是将网络战与常规战完美结

合的一次典范。20世纪90年代以来，以色列给予了网络技术领域前所未有的重视。据媒体报道，以色列社会主流精英将网络视为“第三次革命”，强调必须牢牢把握“第三次革命”的主动权。通过在人才培养、资金投入、技术创新等方面的大力投入，以色列已具备较强的网络空间作战能力。

▶爱沙尼亚大战：第一场国家间网络战

2007年的爱沙尼亚大战，被称为第一场国家间网络战。2007年4月，爱沙尼亚政府把苏军纪念碑“青铜战士”迁往他处，这一举动引发了占全国人口25%的俄罗斯族的不满。从4月下旬开始，各种爱沙尼亚政府机构、国内最大的银行、多家媒体的网站等都成为俄罗斯所资助特工们采用DDoS攻击的主要目标，致使网络传输中止。

爱沙尼亚被称为互联网普及率最高的欧洲国家，所有公民都能享受免费Wi-Fi无线网络，互联网在爱沙尼亚人的日常生活和各种活动中扮演着重要角色，人们投票、交税、转账几乎全部使用网络完成。所以，针对爱沙尼亚进行网络攻击就像一次数字化入侵，诸多基础设施和民生服务都陷入了瘫痪。

从拆迁铜像开始的一周内，第一波网络攻击高峰形成。大规模攻击导致政府、银行、报社、电视台、企业的网站陷入瘫痪，一些网站的首页甚至被换上俄罗斯宣传口号和伪造的道歉声明。接下来一周的第二波攻击高峰中，人们的日常生活受到了严重威胁。大量电脑遭恶意软件侵入，人们无法使用信用卡付账，最后爱沙尼亚外交部、国防部不得不紧急向北约求助。

爱沙尼亚国防部长称，攻击针对的是必不可少的电子基础设施，所

有的商业银行、电信运营商、媒体网点、域名服务器均受影响。攻击所造成的最大影响便是数以百万计的经济损失，爱沙尼亚最大银行汉莎银行报告其损失超过了100万美元。

▶俄罗斯与格鲁吉亚冲突：一场网络人民战争

网络战作为国家间冲突的组成部分已经不是一件新鲜事，2008年的俄罗斯与格鲁吉亚冲突把网络战提高到了一个新等级。

2008年8月，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。最终，格鲁吉亚的电视媒体、金融和交通等重要系统瘫痪，政府机构运作陷于混乱，机场物流和通讯等信息网络崩溃，急需的战争物资无法及时运送至指定位置，战争潜力被严重削弱。这种社会各要素在战争状态难以做好补充供给的情况，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，安装之后只要点击“开始攻击”按钮即可参与作战行动，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”。**

▶“震网”事件：对现实产生破坏的军用级网络攻击武器诞生

“震网”病毒有很多个全球公认的“第一”——世界上第一款军用级网络攻击武器，世界上第一款针对工业控制系统的木马病毒，世界上第一款能够对现实世界产生破坏性影响的木马病毒。

它是一款蠕虫病毒，赛门铁克（Symantec Corporation）和卡巴斯基

（Kaspersky）等知名安全公司都曾先后对该病毒进行过深入的追踪与研究。其英文名称是Stuxnet，最早于2010年6月由白俄罗斯安全公司Virus Blok Ada发现并披露，它最早的攻击可以追溯到2009年。

从扩散的地区来看，“震网”病毒显然是一款以伊朗为主要攻击目标的木马病毒。赛门铁克和微软的相关研究显示，在全球已确认被震网病毒感染的超过45000个工业控制系统中，近60％出现在伊朗，其次为印尼（约20％）和印度（约10％）。

“震网”无须通过互联网便可传播，用户用U盘就可以把这个病毒从一台计算机传播到另一台计算机。然后“震网”便会使用窃取的数字签名，顺利绕过安全检测，自动找寻及攻击工业控制系统软件，以控制设施冷却系统或涡轮机运作，甚至让设备失控自毁，而工作人员却毫不知情。可以说，“震网”是有史以来首个超级网络武器。

从攻击结果来看，伊朗的损失最为惨重。美国《纽约时报》在2011年1月16日发表文章称，“震网”电脑蠕虫病毒于2010年7月攻击了伊朗核设施，导致其浓缩铀工厂内约1/5的离心机报废，从而大大延迟了伊朗的核计划。有分析人士认为，“震网”病毒的攻击至少使伊朗的核计划倒退两年。

2011年2月，伊朗突然宣布暂时卸载布什尔核电站的核燃料。同年9月，伊朗原子能组织宣布布什尔核电站于当天并网发电，但联网的功率只有约60兆瓦，仅为核电站总装机容量的6％。

▶乌克兰断电：攻击关键信息基础设施的典型案例

攻击关键信息基础设施可以让工厂停工、能源停供、交通瘫痪、人员伤亡，其破坏力不亚于传统战争。电力、电信、能源、金融、交通、

海关、国防等关键信息基础设施，既是国家经济社会有序运行的“神经中枢”，也是战争状态下对手重点打击的战略目标。

乌克兰断电是攻击关键信息基础设施的一个典型案例。网络攻击者连续在2015年和2016年两年的圣诞节前夕得手，让人感到既讽刺又无奈。

第一次大规模停电事件发生在2015年12月23日。乌克兰一家电力公司的办公电脑和数据采集与监视控制系统遭第三方非法入侵。**事故导致伊万诺·弗兰科夫斯克地区将近一半的家庭经历了数小时的电力中断。起初，电力公司估计受灾用户大约8万户，后来发现受灾用户远远不止8万户，因为有三种不同配电站的能源公司都遭受了攻击，各领域共约有22.5万用户的电力中断。**

攻击事件发生后不久，乌克兰政府官员声称电力中断是由网络攻击引起的，并指责俄罗斯国家安全部门应为此事负责。

2016年12月，乌克兰某电力企业再次被攻击，造成规模性停电事故。

▶勒索病毒：一场全球网络战的演习

2017年5月12日爆发的“永恒之蓝”勒索病毒事件勒索了全球，震惊了全球。在本书中，我多次提到了这次事件，这不仅是因为它迅速感染一百多个国家、瘫痪多个关键信息基础设施所展现出的惊人的传播速度和破坏力，最重要的是，这次事件完全可以称为一场全球网络战的演习。

这次勒索病毒事件生动地展现了第三种网络战形式：网络摧毁战

——攻击者运用网络攻击武器进行饱和式攻击，以摧毁对方政府、军队等机构的信息网络。

攻击者所利用的网络武器是此前被泄露的NSA研制的“永恒之蓝”。“小蟊贼”低劣地使用就造成了如此巨大的影响和破坏，如果是由“正规军”来使用，后果难以想象。由此，美国网络武器的先进性可见一斑。我们从被曝光的NSA网络武器库资料来判断，其网络武器的研发已经实现了系统化、平台化、定制化和批量化。

▶索尼影业遭攻击：奥巴马称其为国家赞助的网络恐吓

2014年11月，索尼影业遭遇史上最大规模的网络攻击，5部未上映的电影资源遭泄露，公司的高管薪酬、员工的个人信息、企业的内部合同等各种高度机密信息一同被盗。

这次攻击被FBI调查断定为国家赞助的“恐吓”行为，这是美国首次指控一个国家在美国的土地上从事大规模的网络攻击活动。

在2014年12月19日举行的新闻发布会上，时任美国总统奥巴马称，索尼影业不应该屈服于朝鲜的这类犯罪攻击的恐吓，针对朝鲜造成的损失，美国将以牙还牙，选择一个地点、时间和方式予以回应。美国政府已经开始与日本、中国、韩国和俄罗斯展开磋商，希望寻求合作，以控制朝鲜的网络攻击活动。

美国时任众议院议长纽特·金里奇（Newt　Gingrich）更是直接把这次网络攻击认为是“战争行为”。他说：“索尼的崩溃意味着美国在第一次网络战中败北，这是一个非常危险的先例。”共和党参议员约翰·麦凯恩（John Mc Cain）也认为：“这会给坏人壮胆，使他们在将来更加积极地把网络作为一种攻击性武器。”

我选取的上述10起事件，勾勒出了网络战的整体趋势。我们可以看到，尽管网络战的历史并不长，但其发展速度、规模和对社会、对世界的影响都在发生指数级的变化。现在，网络战正在展现出一系列新态势、新问题。

网络军备竞赛向全球蔓延

网络无处不在，谁拥有网络的控制权，谁就无所不能。控制了社交网络，能控制洗脑术；控制了大数据，能控制智能决策；控制了通信，就能控制神经系统。

20世纪，网络威胁的行为主体是黑客和黑客团体等非国家行为体，到了21世纪，网络威胁的行为主体正在转向国家专业力量。以美国网络司令部升格为第10个联合作战司令部为标志，网络空间正式与海洋、陆地、天空和太空并列成为美军的第五战场。令人担忧的网络空间军事化趋势进一步加剧，军备竞赛已经蔓延至全球。

▶美国：133支网络任务部队已全部实现作战能力

2018年5月17日，美国国防部网络司令部官员称，美网络司令部下的133支网络任务部队（CMF，包括陆军41支、海军40支、空军39支、海军陆战队13支）已全部实现全面作战能力。美国军方所定义的全面作战能力，指的是国家网络部队经过充分训练和武装后，具备保卫国家网络空间安全的能力。

2018年1月，美国国防部信息网络联合部队总部（JFHQ—DODIN）也

实现了全面作战能力，提供全球范围内美国国防部信息网络行动、防御性网络行动和内部防御措施的指挥和控制，以实现所有作战领域的武装投射和行动自由。

让我们盘点一下美国网军的发展史。1993年，由国防部信息资源管理学院首批16名学员组成“第一代计算机网络战士”。

2002年12月，美国海军在弗吉尼亚比奇的小溪流两栖作战基地成立海军网络战司令部，指挥全球7000人的海军网络部队，2010年1月升格为独立建制。

2006年，组建了网络媒体战部队，2006年11月，成立网络战临时司令部，管辖65个网络战中队、预备役和国民警卫队，还有包括由近8000人组成的第67联队在内的4个网络战联队。

2009年，美军通过“挑战网络”竞赛项目发现10000名网络人才。

2010年5月，正式成立网络司令部，并斥资32亿美元建设总部工程。

2014年3月5日，美国防部发布《四年防务评估报告》，在精简部队结构、实行国防投入“自动消减机制”的大背景下，明确提出“投资新扩展的网络能力，建设133支网络任务部队”。

2017年8月18日，美国宣布将美军网络司令部升级为第10个一级联合作战司令部。

美国参谋长联席会议称，希望美军网络部队拥有把对方电脑网络搞瘫痪的能力，阻断敌人对关键信息和系统的访问和使用，并且能用假信息欺骗对手，让其做出误判。

紧随美国之后，全球46个国家制定了网络空间国家战略或组建了相应的网络空间力量，推动全球网络空间军备竞赛不断升级，这必将进一步造成全球网络空间的不稳定性。

▶英国：首个公开宣布建立具备攻击能力网络战部队的国家

尽管美国、以色列、俄罗斯等军事大国都有能力、有计划乃至已经建设了具备攻击能力的网络战部队，但首个公开宣布的国家却是英国。

2013年，时任英国国防大臣菲利普·哈蒙德（Philip Hammond）宣布，英国将耗资5亿英镑建立一支网络军队，以应对并在必要时实施网络攻击。时任英国首相卡梅伦说，这支新军将使英国军方具备“网络反击”能力。同军队其他作战人员一样，他们随时随地全天候为国家效力，作战地点不仅是英国本土，也有可能潜入英国境外的其他国家，从而保护重要的计算机网络和敏感数据。

英国的网络力量主要由两部分组成。一是网络安全行动中心，归属于国家通信情报总局管辖，主要负责监控互联网、通信系统安全，并为军方网络战提供相应的情报；二是网络作战部队，隶属于英国国防部，主要负责进攻其他国家的网络。

早在2001年，英国军情六处就秘密组建了一支由数百名计算机精英组成的黑客部队。他们年轻，背景多样，有的曾经是黑客，甚至有轻度网络犯罪行为。

2009年6月25日，英国政府宣布成立网络安全办公室和网络安全行动中心，分别负责协调政府各部门网络安全和协调政府与民间机构主要电脑系统安全保护工作。

2010年以来，英国相继发布了《战略防务与安全评估报告》《未来部队2020》《2012—2022年武器装备规划》《国防改革：国防部结构与管理的独立报告》《国家海洋安全战略报告》等重要文件，进行军队改革，其中的一项重要措施就是提高部队信息化建设水平，以适应未来战争新样式。

2013年5月，英国成立联合作战网络小组，隶属于国防部联合作战司令部。10月启动网络预备役计划，开始征召军队离职人员、具备必要技能的现任或曾任预备役军人，以及无从军经历但具备一定能力的人才，利用他们的专业技能为英国的网络安全提供保护。

至2014年初，英军基本建成了能够同时处置陆、海、空、天等各种信息的综合性网络，实现了数据的快速处理与分发。2015年4月，英国又正式启动了拥有1500人的新锐网络战部队“第77旅”，通过“脸书”平台专攻“非常规信息战”。

▶德国：网军成为第六军种，2021年完全做好应战准备

2017年4月，德国宣布成立网络与信息空间司令部，着手组建国防军负责网络安全的独立军种。这支部队将兼具网络攻击与防御能力，24小时不间断运行，捍卫德国信息基础设施、需计算机支持的武器系统等目标，是“创新、创造和网络信息空间高端技术的中心”，预计到2021年将“完全做好应战准备”。

根据国防部发布的声明，新组建的“网军”将与联邦国防军平级，成为陆军、海军、空军、联合支援军、联合医疗军之外的第六军种。德国因此成为首个拥有“独立”网络战司令部的北大西洋公约组织成员。德国此举或将掀起一轮北约的网络军备竞赛。

网军司令部设在德国西南部城市波恩，部队现有编制为260名士兵，将逐渐整合联邦国防军原有的网络攻防力量，包括战略侦察、作战通信和地理信息等部门，到2021年扩充至1.35万士兵与1500名文职雇员。其主要任务包括：确保联邦国防军信息系统在国内外的安全运作、加强在网络信息空间的侦察和影响力、在网络空间实施计算机网络军事行动以及在复杂电磁环境下进行电子战等。

值得注意的是，网军中设有“计算机网络行动部队”，现有编制60人，未来将扩充至80人，它将承担包含网络攻击在内的一些作战任务。德国国防部长乌尔苏拉·冯·德莱恩（Ursulavonder　Leyen）说：“如果德国军方遭到网络攻击，我们有能力自卫。一旦相关攻击危及德国作战力量的运行和作战准备，我们将还以进攻。”

德国联邦国防军是较早开始建设建制网络空间作战力量的军队之一。其中，最典型的部门为战略侦察指挥部和国防军信息技术中心。战略侦察指挥部由联邦国防军大学的信息专家组成，专门负责在联邦宪法规定的任务框架内执行网络空间作战任务。国防军信息技术中心则主要维护国防军通信安全，确保指挥通信系统正常运转，归属于联邦国防军信息技术局。此外，还有负责部队IT系统的联邦国防军信息技术指挥部、负责为军事行动提供地理信息支援保障的联邦国防军地理信息中心等。

这些专业机构与部门都将逐渐整合到新成立的网络与信息空间司令部中去。负责监察国防军的议会议员汉斯佩特·巴特尔斯（Hanspeter Bartels）说，德国在网军领域不是先行者，将向美国和以色列等具有网络攻防经验的国家取经。

▶俄罗斯：网络战是未来的“第六代战争”

俄罗斯总统普京曾在俄联邦安全委员会会议上表示，信息攻击已经被用来完成军事和政治任务，它的杀伤力可能超过常规武器。俄罗斯必须提高有效反击网络威胁的能力，提高保护战略设施信息系统的水平。

作为军事大国，俄罗斯在20世纪90年代就设立了信息安全委员会，专门负责信息安全。1995年，俄联邦宪法将信息安全正式纳入国家安全管理范畴。

2002年，俄颁布了《俄联邦信息安全学说》，该文件将网络战提升到新的高度，称作未来的“第六代战争”，全面阐述了国家信息网络安全面临的问题，以及网络空间作战武器装备现状、发展前景和防御方法等。

《俄联邦信息安全学说》颁布后，俄军在总参谋部下成立了信息与自动化管理局，各军兵种也相应成立了信息和自动化管理处，主管军队网络信息战建设；2003年，上述单位设立了专门主管信息化建设的副总参谋长，进一步强化对此项工作的组织领导。2007年，俄军专门设立了主管军队信息化建设的国防部副部长职位，负责领导全军信息化力量建设。

俄联邦一些强力部门都设有网络威胁应对机构，譬如，内务部设有“K”局负责调查境内网络犯罪活动；安全局设有信息安全中心，负责对抗利用虚拟空间危害俄国家和经济安全的外国情报机构、极端组织和犯罪组织。

2013年2月，俄罗斯新任国防部长绍伊古（Sergei Shoigu）下令总参作战总局、组织动员总局及相关部门制定网络司令部的组建方案，提交论证及实施报告，但此后的组建进展不详。

根据目前公开的资料显示，俄军担负网络空间作战的部队人数在7000人以上，大致分为专业和非专业两类。专业类大约组建于1998年，重点担负国家政治、经济领域的网络安全防御任务，同时担负网络信息领域的攻防任务。非专业类是俄军信息战部队中与网络空间作战相关的技术部队，主要包括用于网络攻击战的诸兵种合成无线电电子对抗部队以及负责宣传战、舆论战的信息战技术兵种。上述部队广泛配属于俄军各军兵种部队中。

▶日本：计划组建自卫队之外的新兵种“网络战高级部队”

2018年1月，日本国内媒体发表了一篇名为“日本政府新设太空和网络司令部”的报道，提出日本要建立一支太空和网络战的高级部队，这将是一支在自卫队之外的新兵种，由新成立的太空网络司令部直接管辖。由于这是一类新兵种，所以将不受日本战后相关条约的影响，也就是说它不再是只能自卫，而是可以实施进攻，可以说这是其迈向恢复军事正常化的关键性一步。

据报道，日本已经从军费中划拨出经费筹建这一兵种，目前已派遣了数百名技术人员前往美国战略司令部空间联合作战指挥中心学习相关技能。其网络防卫队的规模也将从现在的110人增加到1000人以上，用来专门应对来自其他国家的网络攻击。日本的具体目标是，与美国和欧洲一起管控来自太空的威胁，必要的时候在第一时间摧毁他国的作战卫星。

同时，日本防务省还决定，为了强化应对网络攻击的能力，在自卫队网军中引入人工智能，还计划将人工智能广泛应用于所有政府部门的网络防御。据日本《产经新闻》2018年1月7日报道，日本防卫省计划用两年时间开展调查研究，2019年度起着手开发相关软件，2021年度正式

投入使用。在2018年度预算案中，日本已经编入了8000万日元的调研经费，参考对象是在网络空间防御和人工智能方面领先的美国、以色列等国的技术。

2001年，日本政府就意识到信息网络安全的重要意义，提出了“电子日本”战略，此后逐步将网络安全建设提升到国家战略层面。

日本在构建网络作战系统中强调“攻守兼备”。日本防卫省在2011年建立了一支由5000人组成的“网络空间防卫队”，研制开发网络作战“进攻武器”和网络防御系统，目前已经具备了较强的网络进攻作战实力，力图通过掌握“制网权”瘫痪敌人的作战系统。

2014年3月，日本防务省正式建立网络空间防御部队。名为防御，实则具备较强的网络攻击能力，其武器不仅包括“过去曾经攻击日本的电脑病毒”，还包括新研发的专用木马。同年11月，日本国会众议院表决通过《网络安全基本法》，加强日本政府与民间在网络安全领域的协调和运用。此外，日本还积极开展国际合作，同北约、欧盟建立网络安全对话机制，通过集中训练、模拟演习等手段强化网络部队的作战能力。

2015年5月，日本组建“网络安全战略本部”；2016年4月又宣布成立“网络安全对策总部”。据日本《新华侨报》的报道，日本计划到2020年建成信息安全强国。

▶以色列：网络战能力比肩世界超级大国

2007年9月6日，以色列空军使用美国提供的“舒特”机载网络攻击系统，成功侵入叙利亚雷达、通信和计算机网络，使其庞大、抗干扰和识别能力突出的防空体系处于失效状态，对叙利亚纵深100公里的预定目

标实施了毁灭性打击，被认为是战争史上网络攻击战浓墨重彩的一笔。

在巴以冲突、黎以冲突中，以色列利用网络进攻的方式篡改网页、攻击电视台，以达到影响舆论导向的目的；侵入军方电脑窃取机密，以确定火力打击的重点目标和精确坐标；阻断敌人通信指挥系统，以掌握最佳的作战时机，这一切都是以军进行网络战的真实写照。

2012年6月，以色列国防军网站上公布了军方对“网络战”的定义及作战目标，军方首次正式承认把网络战作为攻击手段。当月，以色列网络安全国际会议在特拉维夫召开，国防部长巴拉克（Ehud Barak）表示，以色列要用互联网进行攻防，“我们正准备成为世界网络战的前沿阵地”。

以色列网军指挥官称，尽管以军网络战能力能够比肩世界超级大国，但“以色列太脆弱，经不起一场失败”，网络能力在未来战争中的重要性将愈发凸显，不仅会是战争爆发的“先手棋”。更将成为贯穿战争全程，甚至决定战争走向的“胜负手”，大型网络攻击将产生致命效果。

说起以色列的网络战部队，就不得不提著名的“8200部队”。以色列的“8200部队”相当于美国的国安局，是以色列国防军中规模最大的独立军事单位，被情报专家认为是世界上最令人敬畏的黑客部队之一。

在以军内部，有主管网络攻击的“8200部队”、主管网络防御的C4I分部，还有10多个网战小组，几乎都是无人知晓的秘密机构。这些小组为各种军事、情报和政府机构服务。以军定期举办全军“移动黑客马拉松大赛”，让各军兵种的“网络大神”一展绝活。据报道，每个参赛团队由6到7名成员组成，运用自研程序轮番上阵连续攻防48小时，既考验技术也考验团队协作和意志品质。

2017年5月14日，以色列国防军的一名高级网络官员称，以色列国防军正在筹建一个新的网络司令部。该司令部将与现有的指挥、控制、通信、计算机和情报部进行整合，并负责所有防御性网络作战和情报收集的工作。

以色列国防军总参谋部将负责在“8200部队”和新的网络司令部之间进行协调。网络司令部将由指挥、控制、通信、计算机和情报部现在的负责人纳达夫·帕詹（Nadav Pachan）少将领导，下辖技术部、联合网络防御部和数字作战中心；技术部负责设计数字域并使其生效；联合网络防御部门将进行计划、指挥控制和防御作战；数字作战中心又称“防火墙”，将负责整合情报描述并就实施行动做出决定。数字作战中心包括一个情报中心，这个情报中心将提供不间断的情报评估，并会有来自网络作战部队、联合网络防御部及其他部门的代表参加工作。

除了上述所列举的7个国家，印度、韩国、朝鲜等国都在组建自己的网络部队上下了大力气。以印度为例，它不仅将网络进攻写入作战条例，明确指出要建立能够瘫痪敌方指挥与控制系统以及武器系统的网络体系，在陆军总部、各军区以及重要军事部门分别设立网络安全机构，还一直坚持自主研发、军民合作的原则，投入了大量人力物力，力求在网络技术、密码技术、芯片技术以及操作系统方面自成体系。“闪光信使”高速宽带网络以及被称为“第三只眼”的海军保密数据信息传输网络的建成使用，进一步增强了印度军方应对未来网络战争的不对称优势。韩国则于2009年宣布组建“网络司令部”，并于2010年1月正式启动。目前，韩国已经拥有了约20万接受过专业训练的庞大的人才队伍，而且每年国防经费的5%被用来研发和改进实施网络战的核心技术。

网络战的六大特点

毫无疑问，网络空间已经成为陆、海、空以及太空以外的“第五作战空间”。网络武器扩散导致的网络灾难正在不断发生，网络空间安全与社会空间安全已经高度一体化。这并非耸人听闻，2017年5月12日爆发的“永恒之蓝”勒索病毒就是网络战的一次预演。

攻击者利用了据称是NSA泄露的网络武器，虽然攻击者使用该武器的技术手段低劣，但仍然造成了巨大的影响和破坏。当然，这次事件也侧面反映出美国遥遥领先的网络战能力，其网络武器的研发已经实现了系统化、平台化、定制化和批量化，而这将形成全球军事领域新的不平衡格局，并刺激世界各国竞相开展网络武器的军备竞赛。更需警惕的是，此次事件也打开了网络恐怖主义的“潘多拉盒子”，预示着网络恐怖袭击可能成为常态。

更具体来说，我认为网络战具有以下六个特点和趋势。

▶网络战是“不宣而战”

如果说，陆战是以天或者周为单位的，空战是以小时为单位的，那么网络战则是以秒和分钟为单位的。不同于传统战争有明显的开始和结束，网络攻击往往“不宣而战”，悄然发生。因此，我们在和平时期就必须未雨绸缪，提前做好防御。

1981年以色列空袭伊拉克核设施的主要方式是“空战+电子战+战术欺骗”；2007年以色列空袭叙利亚核设施的主要方式是“电子战+网络战+空战”；到了2010年，针对伊朗核设施实施的“震网”攻击就已经是纯网络战了，兵不血刃，但造成的损失极其惨重。

美国利用其网络战能力的优势在全球开展了长期的潜伏和渗透。维基解密公布的文件显示，CIA从2008年开始就深入苹果iPhone供应链，通过其供应链渠道将特定恶意软件安装到iPhone手机中，甚至感染其固件，实现对MacOS和iOS设备的监听。

2017年5月16日，曝光“方程式组织”（被普遍认为是NSA下属的APT机构）网络武器库的“影子经纪人”组织宣称，它将逐步披露更多窃取自NSA网络武器库的黑客工具和情报，其中包括针对中国、俄罗斯等国核设施的计划。

可以看出，网络战往往需要经过数以年计的长期渗透、潜伏和准备，然后在特定的时刻发动，实现瞬间一击制敌的效果。网络战必将成为战争的首选。

▶网络战是“整体战”

网络攻防是一场整体战，对每个个人、每台终端以及每个目标的安全保护都非常重要。在国家网络空间博弈防御体系的建设中，就需要统筹考虑军事网络和民间网络。

在传统战争中，军事目标和民用目标有较明确的区分。理论上讲，战争双方军队都应尽可能地避免攻击民用目标和普通百姓，即便是要攻击民用设施，也主要是攻击大坝、电厂等具有军事意义的重要民用设施。

但在网络空间博弈中，这一原则恰恰是被抛弃的。因为网络是一个相互连接的整体，任何单位或个人所使用的终端设备或者系统都是网络的一部分，任何个人设备被攻破，整个网络可能就会被攻陷。而且，网络攻击一般都是首先入侵个人或企业单位的电脑、手机等终端设备，再

以终端设备为跳板，横向扩散渗透攻击更重要的目标。

美国一直把其国家关键信息基础设施作为网络战保护的最主要目标，因此从克林顿政府以来，美国出台了诸多保护关键信息基础设施的法律文件。2017年，美国总统国家基础设施咨询委员会发布的《保护网络资产：应对紧急基础设施网络威胁》报告指出，必须采取行动防止针对基础设施的网络攻击，尤其是针对美国能源机构的攻击，美国军队2018年的几次演习也均以能源机构为目标。

2003年开始，中国也陆续制定了一系列针对关键信息基础设施进行保护的政策和法规，2017年颁布实施的《网络安全法》更是将关键信息基础设施的保护提升到了法律层面。

▶网络战是“超限战”

国家级网络空间博弈中，攻击手段将越来越剑走偏锋，没有底线和规则，无所不用其极。

维基解密曝光的文件资料显示，CIA可对三星F系列智能电视植入恶意软件，伪装电视进入“假关机”状态，利用电视内置的麦克风进行窃听和录制音频，并将音频文件通过互联网发送至隐蔽的CIA服务器。

“方程式组织”也可以将病毒植入硬盘制造商出厂的硬盘控制器中。一旦这些硬盘被特定的目标单位所使用，电脑联网后病毒即可将窃取的硬盘机密信息发送至黑客的服务器。

可见，网络攻击方法不一定正规，也没有公约的限制，大家都在用超常规的、出乎意料的手段达到其目的。同样地，我们应对网络攻击也需要超常规思维人才。

▶网络战是“漏洞战”

没有漏洞，就不要谈网络战。

从“震网病毒”“乌克兰电厂攻击”到此次“永恒之蓝”勒索病毒攻击，它们均利用了各种已知、未知漏洞。如果没有漏洞，就无法建立网络战的进攻和防御体系，可见，一个重要漏洞的价值不亚于一枚导弹。像石油、稀土等战略资源一样，漏洞是制造网络武器的战略资源。

美欧对漏洞资源极其重视。美国主导的“瓦森那协定”将漏洞列入军用资源限制出口，CIA、NSA等机构一直在斥巨资收购各种漏洞。此外，美国还通过各种比赛（如Pwn2Own黑客大赛）或以众包、众测方式的网络攻击大赛（如“黑掉五角大楼”“黑掉陆军”等行动），借助民间力量来获取漏洞资源。

除了对漏洞资源的掌握，美国网络战的能力还体现在建立了一整套针对网络武器的研发，网络攻击的组织、实施、验证、评估等的工程技术体系上，这实现了网络武器的系统化、平台化、批量化和定制化的制造。

▶网络战是“猎杀战”

人是网络战的最大漏洞。我总结过关于人性的两大“失效定律”：一切忽略人性的管理手段都会失效；一切没有技术手段作为保障的管理措施都会失效。

我在第一章就提到，内部威胁是最大的危害。通过美国国家安全局在“斯诺登”事件中的教训，我们可以看到，一个“内鬼”会给国家安全造成多大的伤害。

人性的弱点是导致内鬼的主要原因。

首先，这归咎于人无完人的思维缺陷。任何网络系统，无论软件还是硬件，都是由计算机程序组成。有研究显示：程序员平均每写1000行代码，就会有1个缺陷，缺陷一旦被发现被利用，就成为漏洞。而现在一个中型的软件系统（比如智能手机）动辄就要百万行代码，“千疮百孔”是难免的，其中任何一个严重漏洞都可能成为系统的软肋。

其次，不守规矩、不受约束、过度谋利是人性的又一大弱点。在我们的安全措施里，规章制度起着重要作用，制度一旦被违反，就出现无法堵住的漏洞。

举个例子，在希拉里“邮件门”事件中，希拉里非要在自己家地下室里偷偷架一个服务器，这相当于在美国政府网络里开了一个口子，美国国安局、中情局即便拥有再强大的网络安全保护能力也是枉然。

▶网络战是“情报战”

信息不等于情报。我认为，能够改变决策者决策的信息才是真正意义的情报。尤其在当前这样一个海量信息的时代，如何从海量的信息里辨识有用的情报，是一个难题。从这些海量信息里获取情报是网络战的重要目标。

从有战争起，就有情报。《孙子兵法·用间篇》谈道：“故明君贤将，所以动而胜人，成功出于众者，先知也。”这里的先知就是情报工作。飞鸽传书、鸡毛信，传递的都是情报。

随着人类文明的发展、新技术的不断涌现，战争的领域和复杂化程度发生了巨大变化，情报的内容、形式和作用也越来越丰富。互联网技

术开始在军事领域广泛应用，未来战争中，掌握制网权就意味着掌握了制空权、制海权，也就是战争的决胜权。人类对网络空间这个第五疆域的争夺已经开始，情报工作也随之延展到这个疆域。

情报意识需要建立在对国际关系、国际政治、本国发展需求以及敌对国家内部情况深刻了解的基础之上。

2017年6月，美国网络司令部新组建了一支情报与行动融合小组，将情报人员与技术人员融合，旨在快速形成一定水平的情报解读，国防信息系统局局长艾伦·林恩（Allen Lynn）表示，他们意识到网络行动需要大量情报支持，因此需要更多的情报人才。

这样我们就不难理解，为什么美国的历任网军司令都有着丰富的情报工作经验。这样的官员知道哪些情报是传统人力渠道无法获取，或无法保证质量的，知道网军的发力点和工作方向，这样才能让网军的情报工作更有效地服务于政府决策。

美国网络司令部升级后的首任司令保罗·中曾根是情报领域专业人士，从军开始就在情报战线工作。领导陆军网络战线时他组建起了多支年轻有为的网络战部队，曾领导过驻阿富汗美军情报部队，伊拉克战场也呆过，情报连、情报营、情报旅都带过，从他的经历可以看到，美国已经将情报与网络战密切结合起来。除美国外，俄罗斯、英国等国都已通过机构调整，将情报与网络战更紧密地结合起来。

第二节　APT攻击——网络战争最常用的攻击方法

360第一次系统地跟踪APT攻击是在2013年。当时我们截获了一个特种木马样本，后来经过研究人员大数据筛查、同源样本计算、定位追踪等，两年之后，也就是2015年我们发布了“海莲花APT报告”。这也是中国的第一个APT报告，引起了很大震动。在隔日的外交部例行新闻发布会上，这成为外国媒体追问的话题。

针对性、持续性是APT的显著特点

APT中文直译为高级持续性威胁，按照维基百科的说法，这个名词最初来源于2006年美国空军的格雷格·拉特雷上校。

维基百科描述道：“APT是一系列秘密而持续的计算机攻击活动，通常由个人或团体针对特定的对象组织实施。”这个概念的描述简单却很模糊，相较而言，戴尔网络安全部门（Dell Secure Works）对APT给出了一些特点描述：特定目标的针对性、资源丰富、复杂的方法和技术手段、受到资助。

根据长期研究和跟踪，360威胁情报中心也给出了自己对APT的定义：针对特定目标长期持续地进行攻击渗透以获取金钱、控制信息甚至潜伏破坏的组织或活动，背后的执行者往往是具有国家背景和丰富资源支持的专业团队。这里的定义刻意削弱了对高级手段的要求，强调了定向性与持续性，这与我们所观察到的实际活动和组织情况相符。

APT攻击与普通网络攻击的本质区别在于其特有的针对性。普通攻击为择弱的、非针对性的攻击，它主要基于感染量的获利模式，比如构建僵尸网络（Botnet）用于SPAM、DDoS、搜索引擎优化（SEO）、流氓推广、数字资产的盗窃、勒索、挖矿等。APT攻击则表现为不顾目标强弱的针对性攻击，基于目标自身价值的获利模式，通过获取关键系统的访问和控制，窃取敏感机密信息，进行控制潜伏破坏。

APT攻击有自己的军火库：既有常规武器（专用木马），也有生化武器（漏洞利用）和核武器（0day漏洞利用）；从多种不同的搭载系统上看，既有能精确制导的导弹系统（鱼叉攻击），也有攻击力强但可能误伤“平民”的轰炸机（水坑攻击）。不同的武器搭载系统与不同的武器类型相结合，就能产生不同的网络攻击。

多数情况下，APT攻击就是一场发生在互联网上的情报战争。攻防双方的焦点是情报和信息。当然，在某些特定情况下，APT攻击也会瞄准金融机构、工业系统和地缘政治，某些APT攻击的影响甚至是世界性的。

中国正是APT攻击的主要受害国之一。截至2018年中，360威胁情报中心已累计监测到针对中国境内目标发动攻击的境内外APT组织38个。

绝大多数的APT组织具有一定的政府背景，其攻击的战略目标以政府、军队、科研机构和大型商业机构为主，战术目标则是被攻击组织网络中的敏感情报信息。统计显示，疑似被APT攻击的境内组织机构有近200个。其中，大学占比最高，为40.0％，其次是企业占比25.0％，再次是政府及事业单位占比18.3％，还有科研机构占比11.1％，其他机构或个人占比5.6％。

我们所经历的APT

我们目睹的APT不在少数。我们发现的大多数APT组织的目标都是为了窃取敏感、机密的信息，因此，可以说这是传统国家间谍活动在网络空间的延伸。近些年来，我国遭遇了一些窃密类攻击团伙的袭击，我们一直在坚持与这些非法势力斗争，维护国家的网络主权。

▶海莲花

属　　性	详　　情
APT组织	APT-C-00（海莲花，OceanLotus）
攻击方式	鱼叉攻击和水坑攻击
行业	政府、科研院所、海事机构、海域建设、航运企业
负责地区	东南亚某国
影响国家	中国、东亚、北美等各类国家
涉及漏洞	CVE-2012-0158
最早发现时间	2013年
最近发现时间	2018年

2015年5月29日，360威胁情报中心首次披露了一起针对中国的国家级黑客组织的攻击细节。根据各方情报和我们的分析，这个黑客组织来源于某东南亚国家，有国家背景，我们把它命名为“海莲花”。

通过长期对该组织发起攻击事件的监测和分析，结合其在攻击中使用的战术、技术特点以及使用的恶意代码和攻击工具的同源性分析，我们发现“海莲花”组织是以专门攻击中国境内的核心政府、能源、科研等政企机构为目标的APT组织，其攻击目标包括我国的海事机构、海域建设部门、科研院所和航运企业等，并且以收集机密情报信息和窃取机密文档为主要攻击意图。

“海莲花”最早针对我国境内的攻击活动可以追溯到2011年，并且从2013年起该组织针对境内的攻击活动变得异常频繁。不仅如此，此后我们发现该组织还对东南亚其他国家发起过定向攻击渗透行动。

“海莲花”被公布后，仍然活动频繁。360威胁情报中心发现，“海莲花”使用过7个独立的恶意代码家族，样本100余个，感染者遍布中国29个省级行政区和境外的36个国家。为了隐蔽行踪，海莲花组织还先后在至少6个国家注册了服务器域名35个，相关服务器IP地址19个，分布在全球13个以上的不同国家。

通过360威胁情报中心对“海莲花”组织的持续监测和感知，2017年全年，境内仍然有大量重点政企机构的网站遭其攻击，这其中还有国内大型能源央企和核心科研机构。我们公司的人员在某重要部门的处置现场发现，其单位内部的网络已经被“海莲花”组织全面渗透，网络中的Windows域控制器已经失陷多月。我们发现，一些大型央企在部署了我们基于威胁情报的天眼产品后，几乎都会马上发现“海莲花”的远控活动，而实际的受感染和受控活动一般已持续几个月到半年。

2018年3月14日，国外某安全公司发现“海莲花”攻击近期又使用了新后门。经过持续追踪我们发现，这个组织大部分分布在越南、菲律宾、老挝和柬埔寨。以前间谍行为主要通过人工实现，现在很多信息可以通过网络获取，网络间谍行为越来越多，这将是未来的趋势。

▶摩诃草

属　性	详　情
APT组织	APT-C-09（摩诃草、Patchwork、白象）
攻击方式	鱼叉攻击为主，少量水坑
行业	政府机构、科研教育领域，军事，商业，新闻媒体
负责地区	南亚某国
影响国家	中国、巴基斯坦
涉及漏洞	CVE-2010-3333，CVE-2012-0158，CVE-2012-0422 CVE-2012-4792，CVE-2013-3906，CVE-2010-3333 CVE-2012-0158，CVE-2014-6352，CVE-2015-1641 CVE-2014-1761，CVE-2012-0158，CVE-2014-4114 CVE-2015-2545，CVE-2017-0261
最早发现时间	2009年
最近发现时间	2018年

“摩诃草”组织，又称Hangover，Viceroy Tiger，Patchwork，Dropping Elephant，MONSOON，国内其他安全厂商也称其为“白象”“丰收行动”，来源怀疑为南亚某国。

这是一个长期针对中国、巴基斯坦及其他部分南亚国家从事网络间谍活动的APT组织。自从2013年5月16日国外安全厂商Norman将它首次曝光以来，该组织的网络攻击活动异常活跃，国内外不少安全厂商相继发现其攻击事件和使用的恶意代码。

360威胁情报中心在2016年8月4日发布了“摩诃草组织（APT—C—09）来自南亚的定向攻击威胁”，详细介绍了该组织发起过的4次攻击行动，并对其以往使用的攻击工具和基础设施的关联性进行了比较和总结。

“摩诃草”组织主要针对我国的政府机构、科研教育领域以及军事领域的目标人员进行攻击，主要使用鱼叉攻击，也将基于即时通讯工具和

社交网络作为恶意代码的投递途径。其攻击使用的恶意代码主要针对Windows系统，也出现过针对其他平台的恶意代码。

根据国内外安全厂商在过去对“摩诃草”组织的历史攻击行动的披露情况分析，我们发现，在各家安全厂商披露的报告主要集中在两个时间段，一个是2013年5月至2014年至6月，另一个是2016年7月至今。这从一定程度反映了该组织在过去发起的两次大规模集中式的攻击行动。

2018年2月，我们到实际现场处理了一起鱼叉邮件攻击得手事件。2月14日，某科研单位的天眼产品输出摩诃草团伙相关的告警，应急团队到达现场处理，在相关的机器上发现木马文件，修改时间为2月14日11时23分。据受影响用户回忆，在此时间段附近，他打开过邮件来源的WORD文档附件。通过排查我们发现了名为“US_China.rtf”的文档，分析显示该文档大小异常，且创建时间与木马文件时间符合，确认为木马的投递文档，打开后会释放木马文件至系统并加载执行。通过搜索附近时间邮箱记录，发现了包含此文档下载链接的邮件。

至此，“摩诃草”组织的木马的进入途径得到了确认。使用天眼产品搜索下载域名请求记录，发现镜像的流量中除当前受害者外并无其他机器的访问记录。通过对该邮件的搜索发现，该科研单位邮箱系统中共计32个邮箱收到了此钓鱼邮件，虽然该邮件被邮件系统划分为垃圾邮件，但还是有个别用户尝试打开处理，导致机器受到感染。

▶蔓灵花

属　　性	详　　情
APT组织	蔓灵花（BITTER）
攻击方式	鱼叉邮件
行业	政府、电力和工业相关单位
负责地区	南亚某国
影响国家	中国、巴基斯坦
涉及漏洞	无
最早发现时间	2013
最近发现时间	2017

“蔓灵花”也是由360团队在国内首次公布的海外黑客攻击团伙，疑似来源于南亚某国。受影响单位主要涉及政府、电力和工业相关单位，该组织至今依然处于活跃状态。与“摩诃草”团伙相比，“蔓灵花”团伙的攻击目标更为聚焦。

美国网络安全公司Forcepoint曾在2016年11月发布一篇报告，主要披露了巴基斯坦政府官员最近遭到来源不明的网络间谍活动。该报告描述了攻击者使用鱼叉邮件、利用系统漏洞等方式，在受害者计算机中植入了定制的AndroRAT，意图窃取敏感信息和资料。

360基于大数据资源对该事件做了进一步分析，发现中国地区也遭受到了相关攻击的影响。截至目前我们已捕获到了超过33个恶意样本，恶意样本涉及Windows和Android多个平台，恶意样本的回连域名（C&C）超过26个。

对于“蔓灵花”团伙活动，我们最近处理的案例为2017年12月某军工集团受到的钓鱼攻击。这个集团收到了一封看似来源于mailservicegroup@126.com邮箱发送的钓鱼邮件，钓鱼邮件里面包含一个指向仿冒邮箱登录页面的链接。

用户访问了链接，就被收集到了用户名及密码，攻击者再以这个钓鱼得到的邮箱发送带有恶意附件的邮件给单位里的其他用户，这个附件是一个带有系统信息收集功能的Downloader，样本通过修改程序图标及在文件名中加入大量空格将自身伪装为DOCX文档文件，诱导用户打开。该样本为RAR生成的自解压程序，样本运行后会在c:\intel\logs目录下释放mobisynce.exe及一个与样本相同名称的正常DOCX，然后打开EXE及DOCX，从而迷惑受害者。Downloader程序连接外部的C&C服务器后可以接收执行指定程序，最终实现持久化或执行攻击者的恶意功能。

基于这些信息，360威胁情报中心做了拓展分析，发现了更多非常可能被用来执行钓鱼攻击的域名。

第三节　漏洞的储备与利用是军事现代化的必备能力

当前，国际局势较为复杂，面临的挑战更加多元，网络战已经开始取代部分常规战争，不仅如此，在网络基础设施、数据资源和空间治理规则上的争夺也变得如火如荼。

各国的军事现代化建设都在快速推进，其中至关重要的就是武器装备的现代化。我们看到，网络信息技术已经广泛应用于陆海空天武器平台，甚至出现了“数字化士兵系统”；美国NSA和CIA遭泄露的机密显示，他们已经建设起完备的网络武器平台，漏洞已经具备了武器属性。

在这样的大环境下，一个国家要想站得稳，势必要在武器装备现代化这场比拼中占据先机，落到实际操作层面，就是要强化对漏洞的储备和利用能力。

漏洞已经具备武器属性：网络武器仅次于核武器

网络战武器可集情报收集、指挥控制、功能毁伤、信息欺骗等多种功能于一体，对不同类型网络目标具有一定普适性，对目标的侦察、控制、破坏行动具有较长的潜伏期，实现了“从看到打”“从打到慑”的有机统一。

人类进入热兵器战争以来，炮弹、导弹、核弹等毁伤型武器的机理

多是基于能量的冲击波效应。但网络武器的机理却是基于漏洞的网络冲击波效应，与毁伤型武器基于能量的空气或电磁冲击波效应截然不同。

近年来，由国家开发的基于网络漏洞的网络战武器造成的破坏和规模越来越大，并向实战化不断演进。2017年美国网络战武器泄露引发的勒索软件持续攻击造成了全球性的威胁，“永恒之蓝”给上百个国家带来了巨大损失，影响空前。

目前西方网络强国正不断加强网络武器的开发建设，企图形成新的网络战优势。

俄罗斯军事预测中心主任、莫斯科国立大学世界政治系副教授阿纳托利·茨冈诺克（Anatoly Triroco）曾在接受俄《观点报》采访时指出：“使用网络武器的概念早已提出，并已被积极应用于军事冲突。目前这一武器的重要性仅次于核武器。”

2017年3月，维基解密发布的近9000份CIA机密文件显示，CIA网络情报中心拥有超过5000名员工，他们利用硬件和软件系统的漏洞，总共设计了超过1000个黑客工具。利用这些工具CIA可秘密侵入手机、电脑、智能电视等众多智能设备，这反映出CIA在网络攻击、监控和武器研发等方面具备了相当先进的水平，对其他国家的网络安全构成了严重威胁。

这是CIA迄今为止最大规模的机密文件泄露事件，但维基解密表示，公布的这些文件只是第一部分，不到CIA文件的1%。维基解密还披露，这些“黑客武器”面临着失控风险。最近CIA称“对其黑客武器库中的大部分工具失去控制”，这些工具“似乎正在美国前政府的黑客与承包商中传播”，存在“极大的扩散风险”。

2016年8月，黑客组织“影子经纪人”声称攻破了为NSA开发网络武器的黑客团队“方程式组织”的系统，获取了其用于网络攻击的网络武器库。要知道，“方程式组织”聚集了全球技术最强的黑客，有“网络武器王冠的制造者”的称号。从2001年开始，这个组织就在帮助NSA开发网络武器，利用软件漏洞作为网络武器，协助美国政府在全球各地进行网络攻击。

漏洞的储备利用之战已经打响

网络安全已经上升到国家高度，网络漏洞将会和飞机、导弹一样成为国之重器。在这样的大背景下，掌握漏洞的能力本身，即漏洞的发现与响应，也形成了产业链，比如漏洞响应平台和安全众测。通过漏洞响应平台，我们要把安全人才、技术和资源与全社会共享，协同企业和政府主管部门共同保护网络安全。谁主宰了漏洞，谁就是未来时代的上帝。

美国从2007年开始投入巨资实施“曼哈顿”国家网络防御计划，此后又积极发展“X计划”“数字大炮”“网络飞行器”“爱因斯坦主动防御系统”等尖端网络战手段。必须承认的是，美国建设的网络战武器已经形成了极强的攻防作战能力。

▶美国：实战化的网络风暴演习，发现军方漏洞免刑责

美国每两年举行一次网络风暴演习，演习分为攻、防两组进行模拟网络攻防战。攻方通过网络技术、物理破坏手段，攻击能源、金融、交通等关键信息基础设施，模拟仿真环境。守方负责搜集攻击部门的反映信息，及时协调，共同评估并强化网络筹备工作、检查事件响应流程并

提升信息共享能力。

2006年2月，美国国土安全部开展了第一次网络风暴行动，包括美国白宫国家安全委员会、国家安全署、中央情报局等在内的超过115个的政府机构、公司及组织参与演习。英国、加拿大和澳大利亚也参与到了演习中。

2010年9月举行第三次“网络风暴”演习时，参演国数量达到了2006年演习时的4倍，澳大利亚、加拿大、法国、英国等都参加了演习，美国11个州和来自金融、化学等行业的60家私营企业也参与其中。

2016年4月，美国国防部举行了首次黑客大比武，悬赏邀请民间高手寻找五角大楼网站漏洞，结果找到超过上百处隐患。五角大楼还制定了一系列后续计划，他们打算把这类活动扩大到部队，还将鼓励军方承包商效仿。另外，任何人今后如果在军方网络中发现漏洞，都可以报告而不用担心受到起诉。

2016年11月，美国国防部又展开了“黑掉陆军”项目。与“黑掉五角大楼”不同，“黑掉陆军”不仅邀请黑客评估静态网站，它的关注重点还放在征兵网站以及申请者和现役军官的个人信息数据库上。该项目没有对所有人开放，只有通过审查的黑客才会受到邀请。

从2017年5月30日持续到6月23日的“黑掉空军”奖励项目，让272名黑客针对精选出的公开美国空军（USAF）网站资源下手，寻找并负责任地公开漏洞，共有207个漏洞被发现并秘密报告。作为项目的一部分，USAF根据所报告漏洞的严重性和影响，为每个漏洞付出100美元到5000美元不等的酬金。这些安全漏洞的详细信息并没有公开。

尽管领赏黑客的姓名和具体奖金数额没有公开，USAF和漏洞悬赏

平台HackerOne还是提供了该漏洞奖励项目参与幅度的某些一般性细节。一位17岁的安全研究员提交了30份有效漏洞报告，摘得最高总赏金额。

该项目也从两名现役军方人员处收获了漏洞信息。值得注意的是，272名参与者中有33名外籍人士。此前的“黑掉国防部”漏洞奖励项目限定了参与者只能是美国人，而“黑掉空军”是首个非美籍黑客可参与的官方漏洞奖励项目，来自英国、加拿大、新西兰和澳大利亚的黑客提交了50多个有效漏洞。

2018年4月，美国国防部举行了第六次网络风暴演习，重点检测影响美国关键信息基础设施的大规模网络攻击，评估网络安全状态，检验事件响应过程、程序和信息共享情况，并确定需要改进的方面。

▶加拿大电商Shopify持续悬赏接受漏洞报告

Shopify是加拿大的一个电子商务的公司。该公司的Shopify网上商店平台适合跨境电商建立独立站，用户支付一定费用即可利用各种主题/模板建立自己的网上商店。目前该网站拥有超过500000个商家，总商品交易总额超过460亿美元。

从2015年起，加拿大电商Shopify开始在HackerOne上发起漏洞众测，持续到现在仍在接受漏洞报告。

根据HackerOne网站上的统计数据，Shopify已经接收并处理了的漏洞报告数为435个，为此发出的奖金数额超过208700美元，并致谢了272位“白帽”专家。Shopify提供的漏洞报告奖金最少为500美元，大额奖金在1000美元到20000美元之间。

▶芬兰保险巨头LocalTapiola在漏洞平台启动众测

2016年，芬兰保险巨头Local　Tapiola在HackerOne上启动了漏洞众测，为黑客提供最具竞争力的悬赏平台。一名安全研究人员因发现关键系统漏洞成功获得18000美元。此外，该公司表示，任何黑客只要能够找到严重的、项目规定范围内的漏洞，都有机会获得50000美元的奖励。LocalTapiola公司安全团队将根据提交的漏洞的严重程度为漏洞发现者颁发奖金，奖金额度为50美元到50000美元不等。最终，LocalTapiola至少接收了38份漏洞报告，并对40名黑客表达了感谢。

2017年3月18日，LocalTapiola在HackerOne上启动了不公开的漏洞众测活动。此次测试活动邀请了曾经参加过针对LocalTapiola进行漏洞众测的专家参加，根据声望、漏洞报告质量等因素选择参与的专家，选择过程由LocalTapiola公司安全团队全权负责，不接受电话咨询，组织者将直接与专家电话联系。

▶俄罗斯电子邮件Mail.ru向406位“白帽子”致谢

Mail.ru是俄罗斯最大的电子信箱服务网站之一，也是俄罗斯发展最快的网络资源。每天访问网站人数超过千万人。

从2014年起，俄罗斯电子信箱开始在HackerOne上发起漏洞众测，持续到现在仍在接受漏洞报告。

根据HackerOne网站上的统计数据，Mail.ru已经接收并处理了的漏洞报告数为1710个，为此发出的奖金数额超过100000美元，并致谢了406位“白帽”专家。Mail.ru提供的漏洞报告奖金最少为100美元，大额奖金在500美元到5000美元之间。

▶新加坡政府测试国防部8个网站

新加坡政府于2018年初首次邀请来自全球的“白帽黑客”攻击国防部的电脑网络系统，以测试系统是否有漏洞。

受雇的漏洞众测公司HackerOne在2018年1月15日至2月4日间攻击新加坡国防部八个连接网络的电脑系统，包括国防部网站、国民服役网站，以及国防部和新加坡武装部队人员的公共电邮服务。

据新加坡《联合早报》报道，200多名海内外高手“入侵”新加坡国防部属下的网络系统，其中100名来自本地的“白帽黑客”社群。这些“白帽黑客”在三个星期里抓到35个漏洞，共获得约两万美元奖金。

实战与演练：网络安全靶场

2008年1月8日，时任美国总统布什签署“国家网络安全综合计划”，“国家网络靶场”（National Network Range，NCR）是该项目的重要组成部分。项目由国防部先进研究项目局（Defense Advanced Research Projects Agency，DARPA）负责管理，靶场建成后将为美国国防部、陆海空三军和其他政府机构服务。NCR项目是美国国会70年来向DARPA直接下达的唯一项目。

随着信息技术的迅速发展，网络安全已成为各国政府关注的重点。为了对抗日益增长的针对政府、国防和工业控制领域的网络关键信息基础设施的攻击，世界各国都纷纷开展网络靶场的技术研究和应用。美国政府为了增强信息化作战的能力，确立其在网络安全中的“霸主”地位，率先开始了网络靶场的设计与运营。

网络靶场和传统的网络虚拟仿真技术有区别吗？答案是：有！网络靶场在试验规模、对象、环境、安全与复杂度等方面都有别于传统的网络虚拟仿真技术。

一般来讲，建设网络靶场时我们需要解决的关键技术难点主要有：大规模网络仿真环境构建技术、靶场试验时钟同步技术、靶场试验运行控制技术等。现阶段的美国在这些技术的积累方面处于全球领先的水平。

NCR建成后将具备的能力包括：大规模军用网络、政府网络、商用网络及国家级网络攻防对抗的仿真能力；支持成千上万的物理节点和虚拟节点的部署与测试，并提供自动测试的能力；支持不同安全等级条件下的大规模网络以及信息通讯的攻击与防御测试的能力；根据实际需求和资源情况，测试网络安全、主机系统安全工具和套件的能力；加速或减缓相关测试时间的能力；封闭或隔离测试数据的能力；真实复制相关用户行为及弱点的能力；开创与部署创新性网络测试的能力。

网络靶场可为用户构建网络安全攻防知识体系，并依托平台形成课件体系进行知识传递；为网络攻防专业人才培养提供方法论培养、知识学习、技能演练的统一平台。

NCR将成为美国测试各种网络研发项目的国家级资源，为美国网络战斗能力的提升带来革命性飞跃，为网络研发技术提供真实、定量的评估，保护国家的重要信息系统和关键信息基础设施，为新的研究项目提供试验环境，提高国家的网络作战能力，训练网络战士。

英国已正式启动本国相当于网络战靶场的国家级网络试验场。该试验场由美国军火商诺斯罗普·格鲁门公司（Northop Grumman）搭建，系

统非常复杂，足以模拟互联网的运作，但同时由于与真实互联网相互隔绝，英国军方、政府和学术机构都可以在安全、可控的试验环境中展开各种演练。该试验场将与诺斯罗普·格鲁门公司在美国马里兰州建立的美军“网络空间解决方案中心”以及全球其他网络实验室互联，以增强网络模拟能力，进行全球范围内的网络攻防试验。该试验场在路由器、交换机、服务器、防火墙、监测设备、无线系统等方面都尽可能重现真实互联网，网络战士可以方便地在这个环境中反复演练入侵和防御手段，并把攻击和防御日志生成报表，便于学习总结。这个试验场不久之后将与美国NCR连接，进行世界范围的高强度网络作战演习。

2009年，澳大利亚政府发布了《信息安全战略》，详细描述了政府将如何保护经济组织、关键信息基础设施、政府机构、企业和家庭用户免受网络威胁。2012年10月，美国诺斯罗普·格鲁门公司宣布已获得一份合同，为澳大利亚新南威尔士大学、澳大利亚国防学院堪培拉校园建立网络测试靶场。澳大利亚国防学院是澳大利亚国防部队和澳大利亚新南威尔士大学的合作伙伴，主要任务是为澳大利亚军队训练和培养军官。新成立的网络测试靶场将有助于澳大利亚军事网络技术的发展、测试和评估。

最后，我们来看看国内网络安全靶场的建设情况。当前国内网络靶场的主流设计涵盖三大板块：技能培训、模拟演练、练兵比武。

技能培训通常包括线上技能培训及线下培训两个部分，对网络安全技能、典型漏洞环境进行靶场复现还原。

模拟演练通过对常见的网络设备进行模拟，将网络情况进行沙盘方式地还原、模拟，从中研究突破策略。

练兵比武主要是对主流漏洞环境进行搭建模拟，并具备多种主流竞赛模式，以竞赛的方式发现不足，以赛促学、以赛促战。

军民融合：凝聚网络空间多元力量

军民融合是应对全球网络安全复杂形势挑战的需要，是国家重要发展战略。习近平总书记在2018年4月全国网络安全与信息化工作会议上指出，网信军民融合是军民融合的重点领域和前沿领域，也是军民融合最具活力和潜力的领域。

经验表明，网络安全产业是网络国防力量的基础，建设一流网络空间防御力量离不开网络安全产业支持，同时建设一流网络空间防御力量的军事需求，又将催生网络安全企业快速壮大，并带动中小企业产业生态链形成。

美国、以色列等网络强国在这方面一直走在前列。比如美国国家安全局安排大量的信息安全项目，由民间网络安全企业承担，如帕兰提尔技术公司（Palantir）、火眼公司（FireEye）等。以色列“8200部队”里退伍的很多人成了高科技企业的精英，孵化了37家以色列网络安全公司，并推动了整个网络安全市场的发展。经过以色列军队系统训练和网络实战锻炼的以色列青年人，在军中是为国效力的顶级网络高手，转业后是创业的领头羊；以色列网络安全军事需求和军工科研项目直接牵引民营企业和创业公司的发展，不少军工项目的理念也自然融合到网络安全产业之中，比如“网穹”防护系统就取名于以色列著名的反导防御系统“铁穹”。目前，以色列已经成为仅次于美国的全球第二大网络安全产品和服务出口国。

我们一直说，未知攻焉知防。网络空间是无限的，网络应用数不胜数。从安全角度来说，互联网是平的，没有高地，而从战争的角度来说，一个没有高地的战场注定易攻难守。这就决定了我们和攻击者之间的战争是不对称、不平衡的，必须对攻击者进行有针对性、匹配性的对抗，才有可能保护安全。因此，在网络安全形势日益严峻的今天，我们需要大力推进军民融合，凝聚网络空间多元力量，保护网络空间安全。

360在网信军民融合方面做了很多探索。2017年12月，在中央军民融合发展委员会办公室和军队相关部门的指导下，我们牵头承建了首个军地联手搭建的“网络空间安全军民融合创新中心”。创新中心以大数据协同安全技术国家工程实验室为依托，聚焦网络空间国防安全领域，探索军民深度融合的创新发展模式，服务建设我军一流网络空间国防装备目标，提供与国际前沿接轨的网络国防安全智库服务和创新技术产业服务。

2018年3月，我们在绵阳落地了网络空间安全军民融合创新中心绵阳分中心、安全运营服务总部、网络安全人才培养绵阳基地。其中，网络空间安全军民融合创新中心绵阳分中心的设立将进一步落实国家网络空间安全和军民融合两大国家战略，推动网络安全能力建设和产业发展，助力网络空间国防建设。

当前，网络战威胁泛化，既有来自敌对国家的网络入侵，也有各类组织的APT网络威胁，还有个人的网络攻击等。面对如此复杂的网络安全局面，单靠军队或地方的网络安全力量无法有效应对。网络战形势发展驱动着网络国防理念不断创新，维护国家网络空间安全不仅需要锋利的军队网络之矛，也需要坚实的地方网络之盾。

恩格斯指出，“人类以什么方式生产，就会以什么方式作战”。金戈铁马驰骋疆场时，人们难以感知海洋的深邃；坚船利炮劈波斩浪时，人们难以预见蓝天的高远……

随着信息时代的到来，人类制造和开发了一个全新的，将政治、经济、军事、文化、外交等活动一网打尽的网络空间，极大地改变了人类的生产生活。实体空间发生的一切，在虚拟世界都有千丝万缕的联系和映射，因此这个网络空间中蕴藏着巨大的国家利益，也开辟了全面覆盖人们现实生活的新战场。

在当前人类的生活环境中，网络空间既是一个国家生产、生活秩序的重要保障，也是支撑整个战争体系运转的核心要素。这就导致了现代战争无时无刻不伴随着网络战的身影——经济领域的网络战暗涛汹涌，军事领域的网络战锋芒显现，政治领域的网络战愈演愈烈，利用互联网攻击敌国、颠覆政权，已经成为战争手段的必然选择。

Chapter 6
第六章
新战力数据驱动安全

“无危则安，无损则全。”出自《易传》中的这句话应该是我国最早对安全的阐释。在国家标准里，安全的定义是这样表述的：安全是指免除了不可接受的损害风险的状态。

安全，是人类的本能欲望，是人生命中最基础、最本质的追求。“居安思危”“安不忘危”“防微杜渐”.....在人们的观念中，安全往往和危险相对，要想长久实现安全，就需要对危机保持警惕。但遗憾的是，在网络世界里，安全就像盐一样——不被重视，存在时，你没有感觉，但当它消失时，你才会寝食难安。

当前，大数据已经融入我们的生活和生产之中，其安全问题也成为一个绕不开、必须谈的话题。大数据安全应该包含两个层面。一个层面是运用大数据技术，来解决大数据时代的安全问题，用数据驱动安全，这一理念将是未来网络安全发展的方向；另一个层面是大数据作为重要资产，用其本身的安全来驱动数据产业开花结果，良性发展。

第一节　不断被刷新的网络安全定义

这一章，我们要讲网络安全。老规矩，我们先要完成破题的工作，回答什么是网络安全。我们要从学理上先把这些概念性、原则性的内容理清楚，才能更加深刻地探讨安全问题。

网络安全的定义需要不断刷新

从技术上理解网络安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。从广义上来说，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全的研究领域。

但网络的定义和内涵是随着技术的发展而不断丰富的。以前提起网络，大家默认是以太网，以及TCP/IP等网络层的内容。但现在随着无线网、SDN与虚拟网络、物联网、工业互联网等新内容的出现，未来的网络已经成为虚拟世界与物理世界的融合体。

因此，网络安全的定义也必须同步刷新，否则，这会极大约束和影响我们的判断力和想象力，导致前瞻性不够，创新不足，难以抓住事物发展的主要矛盾。

我认为，现在对网络安全比较合适的定义是，通过采取各种技术和

管理措施，提高全社会的网络安全意识和水平，监测、防御、处置来源于网络空间的各类安全风险和威胁，保护基础网络、重要信息系统、工业控制系统等各类信息基础设施免受攻击、侵入、干扰和破坏，保护网络空间的数据安全和个人隐私信息安全，依法惩治网络违法犯罪活动，规范网络空间秩序，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。

其中，大数据、云计算、物联网、车联网、工业网络、人工智能等新技术手段，既起到创新发展催化剂的作用，也对网络安全问题的变异、显著化起到极大的推波助澜作用。

网络安全的判断标准

人对自己的境况是否安全，能通过对环境的感知和理解来确定，但是对网络信息却很难以直觉感知的方式完成判断。因此，我们需要对网络和信息的安全建立一个基本的标准，以此来判断网络和信息的安全性。

具体而言，我认为至少要确保网络和信息的“七性”，即真实性、机密性、完整性、不可否认性、可用性、可核查性和可控性。当具备这“七性”时，我们才能说网络和信息是安全的。

根据中央网信办印发的《国家网络安全事件应急预案》，网络安全事件是指“由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件”。

具体来讲，会破坏网络和信息“七性”的安全事件主要包括：有害程

序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

通常看来，当有自然灾害及物理环境威胁、信息系统自身脆弱性、系统设置或用户操作不当，以及恶意程序与网络攻击泛滥等安全威胁存在时，便会被引发网络安全事件，网络和信息的安全难以保证。

网络安全相关的理论发展

网络安全是一门涉及诸多领域的交叉学科，如计算机科学、通信、密码学、应用数学等。近年来，我国也出现了一些新兴理论，如可信计算、拟态防御和安全通论等。以下是对这些理论的一个简要介绍。

密码学：密码学是研究编制密码和破译密码的科学技术。近年来，密码学技术的发展与互联网应用的发展紧密相连。比如现在备受追捧的区块链技术就大量依赖了密码学技术的研究成果。再比如，数据放在云上，既要计算，还要放心，于是同态加密技术备受关注。还有现实中出现的软件、硬件，以及不安全的多元化攻击环境，又催生出了诸如盒密码、灰盒密码、代码混淆、抗泄露密码等一系列的新型密码理论。

可信计算：可信计算是一种信息系统安全新技术，包括可信硬件、可信软件、可信网络和可信计算应用等。中国工程院院士沈昌祥认为，可信计算是指在计算的同时进行安全防护，计算全程可测可控，不被干扰，使计算结果总是与预期一样，只有这样才能改变只讲求计算效率，而不讲安全防护的片面计算模式，是一种运算和防护并存的主动免疫的新计算模式。

拟态防御：拟态防御是一种主动防御行为，主要应用于网络空间安全领域，因此常作为网络空间拟态防御的简称。2008年，中国工程院院士邬江兴从条纹章鱼能模仿十几种海洋生物的形态和行为中受到启发，提出了研发拟态计算机的构想。2016年，国内9家权威评测机构组成联合测试验证团队，对拟态防御原理验证系统进行了为期6个月的验证测试。测评专家委员会发布的《拟态防御原理验证系统测评意见》认为，拟态防御机制能够独立且有效地应对或抵御基于漏洞、后门等已知风险或不确定威胁。

安全通论：世界范围内，网络空间安全的各个分支领域都还处于彼此独立的状态，缺乏全面系统的网络空间安全统一理论。安全通论试图建立一套网络空间安全的基础理论，以统一网络空间安全各分支学科为最高目标，帮助指导网络空间安全领域的相关人员，在统一的基础理论指导下，协同一致地建设网络空间安全体系架构。

第二节　网络安全的新常态

在本书中，我一直在反复强调一个观念：网络安全本质是一种和漏洞攻击者的对抗。当前网络安全的状态和发展趋势是值得我们深入研究的重要课题。

随着信息化的不断普及和深入，网络安全已经和国家安全、经济稳定、人民的衣食住行融为一体，难分彼此。2018年4月的全国网络安全和信息化工作会议专门提出了要以自主创新推进网络强国建设。

网络安全进入了一个新的时代。和以往相比，当前的技术更加发达，网络安全所面临的局势和状况也更加复杂。我一直在总结网络安全的常态和趋势，认真思考后，我认为网络安全新常态主要表现在以下六个方面。

漏洞军火化、军火民用化

当漏洞变成了像稀土、原油一样的国家战略资源后，一个重要漏洞的价值不亚于一枚导弹。因此，哪个国家和企业拥有漏洞能力，就意味着它拥有在网络战中的领先实力。

评价漏洞能力的高低，通常有两个指标：一个是给美国微软、苹果、谷歌、Adobe、VMWare等厂商提交的漏洞数量，360在2017年发现漏洞519个，2016年发现漏洞408个，连续两年位列世界第一；另一个是微软公布的全球最有影响力的、做出杰出贡献的安全专家排名，前100

名中有10位是360的，其中有3位排在前10名。未来，360还会在漏洞能力上加大投入，进一步提升这种能力，巩固我们作为第一大安全公司的地位。

军火民用化的趋势体现在2015年的美国网络军火库被盗事件中，“小蟊贼”能利用网络重武器，在全球进行网络敲诈勒索。所以，未来的网络军火不仅会民用化，同时民用的网络攻击也会借用网络军火。

网络攻击产业化、犯罪集团化

网络攻击的方法为什么不断地推陈出新、变出花样，就是因为有黑色产业的支撑。

关于网络攻击的产业我已经开辟了专门的章节来讲解，在此只想要强调，网络“黑产”的规模是相当大的。2017年，我国互联网广告的市场规模近3000亿元，而网络“黑产”的规模至少有1000亿元。只要这个规模一天不下降，网络攻击就一天不会消停。此外，国家与国家的网络战更是形成了一种产业链条。

因此，作为一个网络安全公司，保护客户的安全已经不再是和一些小偷小摸作战斗，我们是在和一系列有组织的集团斗争。如果没有足够的本事，能行吗？

态势感知智能化

“全天候全方位感知网络安全态势”是习近平总书记在2016年4月

19日全国网络安全与信息化座谈会上对网络安全提出的明确要求。要让态势感知更准、更快，漏报率更低，需要加入更多的智能化分析方法，所以态势感知的智能化也是一个趋势。

2015年，在第三届中国互联网安全大会（ISC）上，360提出“数据驱动安全”的网络安全技术体系，宣告传统的围墙式的网络安全技术过时了，人工智能、大数据、物联网时代的安全问题只有通过大数据技术解决，即收集一切可能的数据，用威胁情报、人工智能、人工运营结合方法，对网络安全时间及时告警，快速响应。

目前，我们的态势感知系统已经实现从感知到应急的一体化，进入了一个很实用化的阶段，并且得到了国家有关部门的认可。为什么？就是因为我们报得准、报得快。

应急响应小时化

我们的安全理念不只在于要在漏洞产生后及时修补，还强调在敌人干坏事的时候，把他抓到，这就是响应速度的问题，所以应急响应小时化非常重要。

为什么要用小时为单位来衡量应急响应的效果？举一个例子，2017年“一带一路”峰会期间，360参与了重保活动，我们当时做出了承诺：二线专家半小时到场，一线专家3分钟到现场。其间，我们也遭到并经受住了一次考验。在勒索病毒事件中，奥运村附近的一个客户需要安全专家，刚好我们在那里有部署，所以3分钟就到了。我不得不承认这次事件在3分钟内解决具有运气成分，但是二线专家半小时到场，我们确实是做到了。

大数据和安全是背道而驰的，“不把全部鸡蛋放在一个篮子里”，就是说明分布式最安全，集中有风险。而大数据越集中就越有价值、越智能。所以网络安全只能迎难而上。但大数据的海量，也让网络攻击者会花更多的时间去寻找目标数据，这为我们采取应急措施留出了宝贵的时间。

“等保”法制化

未来的网络安全体系建设里，我们会遇到越来越复杂的问题，要想更加条理清晰地、快速地解决问题，把安全保护纳入到法制化是未来的趋势。

现在，当责任制在各个单位和部门中反复强调的时候，信息安全等级保护成了最基础的要求，因为将信息和信息载体按照重要性等级分级别进行保护，不仅能够便于管理，而且能更有针对性地调配人力、物力，推动国家网络安全水平的提升。

人工智能时代，网络攻击开始破坏物理世界。从大处说，电网、通信网、航空、铁路、水、煤气、银行等基础设施一旦被成功攻击，就会导致灾难性后果；从小处讲，工厂车间的智能控制系统、自动驾驶汽车的云端大脑、智能家居的控制中心被成功攻击，损失也不可估量。

“重保”常态化

近年来，网络“重保”的任务越来越重。“重保”是对我们的安全保障能力、危机响应能力、日常运维能力等的综合考验。

美国总统出访的时候，都会随时带安保人员，目的就是为了保证在重大活动期间总统的人身安全。我们也经常看到在G8、G20首脑峰会期间，主办国都是“大敌来临”般地进行严格的安保措施，这些看得见的都是传统的“重保”。

360企业安全多次积极参与国家重大活动期间的网络安全保卫工作并圆满完成任务。

从2017年到2018年上半年，360企业安全先后完成了春晚、“两会”、博鳌论坛、“一带一路”高峰论坛、达沃斯论坛、贵阳大数据博览会、香港回归20周年、全运会、金砖国家峰会、国际刑警大会、“十九大”、上合青岛峰会等国家级网络安全保卫任务，以及北京、辽宁、四川、河南、湖南、浙江、广东、福建等多省市的重大网络安全保卫活动，先后投入3000多人次，昼夜奋战24000小时，处理了上万次应急事件，用自己的能力和行动捍卫着国家和企业的网络安全。

第三节　网络安全的终极目标是保护大数据

“天下熙熙，皆为利来。”在大数据时代，海量数据背后隐藏着大量的经济和政治利益。总有一些不法分子试图利用各种手段谋取利益。

前文中，我已经详细论述过，大数据管理和传统网络安全管理其实是背道而驰的，大数据是越集中越有价值、越智能，而网络安全则是越集中风险越高，因为攻击只要成功一次，就得手了。

因此，在当前这样的时代背景下，网络安全的终极目标，就是要保护大数据的安全。

大数据代表着未来

从2014年大数据首次进入政府工作报告起，大数据产业开始得到国家层面的支持。自十八届五中全会的“十三五”规划提出“大数据发展”战略以来，各地都在大数据建设上取得了不少成就，深刻改变着我们的思维、生产、生活和学习方式。大数据代表着未来，在未来10年、20年以及更长的时间里一定会引领市场和潮流。

▶大数据比金钱更重要

我们还是以2017年5月12日爆发的“永恒之蓝”勒索蠕虫事件为例。两天时间内，英国国家健康服务网络、美国联邦快递、西班牙电信巨头

Telefonica、法国雷诺汽车、德国的联邦铁路系统、俄罗斯内政部先后有系统被攻陷，重要数据被加密破坏，造成部分业务中断或无法正常运行。英国医院里大量病患诊断被延误，有病人因此无法及时接受心脏手术。我国很多高校毕业生的论文被加密，部分公共服务系统暂停服务，政府机构系统无法正常使用。加油站、火车站、ATM机、政府办事终端等设备以及邮政、医院、电信运营商、部分工业设施都有“中招”。

一直到现在，加密数据以中断机构或企业的正常业务，并以此要挟勒索的网络攻击事件还在不断发生。

这些事件充分证明了，在大数据时代，数据远比金钱重要。对数据的攻击和破坏不仅带来经济利益上的损失，还会严重影响我们的日常生活，影响城市的运转和人的生命安全，每一个人都不可避免地成为网络安全威胁的受害者。

▶大数据是新经济的“石油”

最近十年，互联网经济飞速发展，创造了一个又一个神话，几乎所有世界级互联网企业都得益于大数据的应用，得益于用大数据的方法颠覆了传统产业。

近几年，互联网流行的精准营销、用户画像都是通过大数据实现的。很多人认为大数据是指大数据技术，这是一个误区，技术只是手段，核心是数据。互联网公司的产品连接每个用户的鼠标和手指，能完整地把用户的所思所为变成数据。将海量的数据“提纯”并迅速处理成有用信息，就像掌握了一把能打开另一个世界的钥匙。

我在参加国资委的一次关于企业改革的会议上谈过一个观点，大数据是新经济的“石油”，它对新经济的驱动力可以用“加减乘除”来概括。

加法就是要更精细的质量、更高的效率，以及更多的扩展业务；减法就是要降低成本，降低消耗，减少次品；乘法就是要通过大数据驱动人工智能，让产品的性能和价值实现几倍甚至百倍的蹿升；除法就是通过网络化让供应链精准分工，实现轻资产的运营。

▶大数据是工业互联网的大脑

现在，全球都在讨论工业互联网，它必将成为未来20年的风口。美国把它叫“智能制造”，德国叫“工业4.0”，也称为第四次工业革命。

可以说，第一次工业革命创造了蒸汽时代，第二次工业革命创造了电气时代，第三次工业革命创造了信息时代，第四次工业革命将创造智能时代或者工业互联网时代。

我总结，工业互联网的主题有四个：一是智能工厂，二是智能生产，三是智能物流，四是智能产品，并将实现“四化”：设计个性化、生产无人化、产品智能化、销售网络化。

以前一架飞行中的飞机引擎要是出了故障，依靠的是飞行员的判断。但现在，飞机自带的感应器具备分析功能，航空公司的控制中心就能基于传感器提供的数据，利用数据分析技术先于飞行员知道这个情况，马上给飞行员发指令，并能提前在目的地安排好维修保养人员。谷歌最近声称，你的下一件衣服可以通过大数据来制造。富士康已经逐渐开始建造无人化工厂，用机器人替代工人，无人化工厂甚至不需要照明。

对大数据的收集、存储、处理造就了对传统工业的颠覆。大数据是工业互联网的大脑，通过对大数据的机器深度学习，使工业互联网拥有了智慧和意识，拥有了对事物的识别、决策的判断和行动的执行能力。

大数据是“大熊猫”，需要被重点保护

大数据在给我们带来智慧和便利的同时，也带来了新的网络威胁。现在各地都在建数据中心、智慧城市、政务云，大数据和云计算技术已经在政务、企业、金融、电信、能源各大行业广泛应用，承载着大量敏感信息。这些涉及个人、企业、政府的敏感信息一旦泄露，网络安全问题会对城市建设造成直接的、实质性的影响，对公民个人权益、企业商业利益、政府信息安全带来不可估量的危害。大数据安全一旦出问题，后果是灾难性的。

▶大数据成为黑客更显著的攻击目标

在网络空间里，大数据更容易被“发现”。大量的数据意味着更复杂、更敏感的数据，而敏感信息会吸引更多的攻击者。同时，大量数据汇集使黑客攻击一次就能获得更多数据，降低了黑客的攻击成本。

▶大数据技术成为黑客的攻击手段

黑客和不法分子也在与时俱进。在企业利用大数据、人工智能和机器学习等技术获取商业价值的同时，黑客也在使用这些技术向企业和国家发起攻击。黑客会最大限度地收集更多有用信息，例如邮件、电话、电子商务、社交网络等。此外，黑客利用大数据发起僵尸网络攻击，可能会同时控制上万台傀儡主机并发动攻击。

▶隐私泄露风险增加

个人隐私泄露会给不法分子带来便利，便于其采用社会工程学等手段，进行电话诈骗、广告推销等，给我们的财产、精神带来损失，现在

越来越多的骚扰电话、垃圾短信即是明证。另一方面，一些敏感数据的所有权和使用权并没有明确界定，很多大数据应用的分析都未考虑其中的个人隐私问题。

▶影响社会稳定运转

现在是大数据与万物互联的时代，智能交通、智慧医疗、智慧城市的建设如火如荼，对数据的破坏将可能直接导致关键信息基础设施的瘫痪，安全问题已经威胁到城市的正常运转与人民的生命安全。

▶威胁现有的防护设施

大数据技术还会对安全控制的措施产生一定的影响。其主要原因是由于安全防护手段的更新升级速度无法跟上数据量非线性增长的步伐，这会暴露大数据安全防护的漏洞。

大数据的到来为安全产业的发展带来了新的契机，大数据正在为安全分析提供新的可能性。在未来的安全架构体系中，如何通过大数据智能分析有效地将原来分割的安全产品更好地融合起来，成为不同的安全智能节点，并驱动这个体系高效运转，将是大数据时代安全产业研究突破的重点。

第四节　数据驱动的安全创新

数据驱动安全已经成为大数据时代安全行业的一个共识。通过对各类网络行为数据的记录、存储和分析，结合安全技术和防护经验，我们可以从更高的视野和角度、更广的维度上去发现异常，捕获威胁，实现威胁与入侵的快速监测、快速发现和快速响应，更好地应对未来不断变化、日益增长的安全威胁。

大数据驱动安全可“预期”

不安全感很多时候来自对现状的无法掌控和未来的不可预知，尤其是网络安全。近年来知名企业被黑的事件层出不穷，没有绝对的安全，没有攻不破的系统，这些观点已经成为共识，很多企业对自身信息系统和安全数据的健康没有安全感。

安全现状的掌控可以简单划分为内部和外部两方面。从内部来说，安全工作做了很多，安全措施上了很多，系统运行数据也采集了很多，但哪个核心指标能代表当前安全现状？短板到底在哪里？是否需要加强？

衡量一个国家的经济现状，可以用国民生产总值（GDP）、采购经理指标（PMI）等指标进行持续不断的监测，既能发现问题，又能看到趋势，依此判断经济是否健康，是过热还是低迷。

针对企业内部的网络安全状况，我们沿用“电脑体检”的思路，开发

了一个“网络体检”，综合360对安全的认识和积累，加上业务的需求和数据共享，依托大数据，制定出某行业、某类型甚至某单个组织的安全现状监测指标体系，包括漏洞、补丁、被攻击、被渗透等细项，综合打分，这样内部安全现状就可衡量了。

从外部来说，以前我们缺乏手段来跟踪外部威胁，现在的技术和数据源的可获得性大大提高，我们可以利用大数据技术更好地发现外部威胁，同时监测可能发生的网络攻击事件，甚至预制重大安全事件。从这个意义上来说，利用大数据技术来保护网络安全显然是未来的必然选项，甚至是唯一选项。

大数据是解决安全漏洞的“药方”

说大数据是未来解决安全漏洞的“药方”，主要是从两个方面来考虑的：一是数据源。云计算、物联网、车联网、工业网络等，以及基础的网络，都是网络安全的大数据源。相关数据被采集后，都可作为大数据分析的源泉。二是数据分析与挖掘能力。大数据存储、计算、建模（规则、机器学习、深度学习、人工智能）、可视化是大数据能够真正被利用来解决网络安全问题的保障和支撑。

下面我将选取几个方面，详细论述大数据驱动的安全创新。

▶网络安全态势感知（Situation Awareness，SA）

2016年4月19日，习近平总书记在全国网络安全与信息化工作座谈会上指出：“要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。”这是我国确立“网络强国”战略之后，首次在国内提出

应用态势感知、大数据这样的非对称技术、撒手锏技术，并以此来解决我们面临的网络安全威胁的问题。

“态势感知”并不是一个新名词，它最早用在军事领域。20世纪80年代，美国空军开始态势感知的研究，用来分析空战环境信息，快速判断当前及未来形势并做出正确反应。

到了20世纪90年代，这个概念开始进入信息安全领域。我们所说的“网络安全态势感知”是一种基于环境的，动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。

所以，态势感知是网络安全运营的感知中心、数据中心、决策中心和响应中心。

网络安全态势感知系统的构成

态势感知不是宏观层面的大屏展示或“地图炮”，更应该是结合微观与中观层面的安全数据与安全能力的融合平台，是一个体系。

一个完整的态势感知系统需要包含以下几个大核心部分。

一是数据中心的分布式、跨越、多维的数据采集能力。可实现对周边安全态势要素的获取，也就是对海量数据、日志数据、告警数据的采集、解析和识别能力。像传统安全一样，以前破案靠神探，现在网络发达了，破案靠遍布马路等公共场所的摄像头时刻采集图像，靠酒店、火车、飞机的实名登记，这些都可以归结为数据的采集能力。

网络也一样，把来自不同源头、不同类型的数据融合在一起、产生

关联，通过进一步分析去发现问题。这也要求承担数据中心作用的大数据平台能把海量数据高效地存储与计算，为在此基础上做安全检测、事件捕猎、调查分析，并发现、定位、溯源安全事件创造条件。

二是感知中心的多维与智联安全分析能力。可实现捕获威胁与攻击，甚至溯源攻击背后的情况。我们目前最熟悉的数据分析应用是搜索引擎，要查找什么就把关键词输入到搜索框里，会出来成百上千条相关的搜索结果，前三条的质量决定用户的满意度。但搜索引擎是简单的数据分析，因为它只是一个维度的关键词关联。而网络安全数据分析更复杂，是多维的，与上下文有关，与时序有关。

比如，黑客利用一种漏洞对我们进行攻击，如果我们恰好没有掌握这个漏洞的情报，就不能检测出这个攻击行为。但如果把时间轴推到攻击之前，黑客一定会通过扫描和多种攻击方法试探系统漏洞。我们把这种上下文串联起来，就可能检测出网络攻击。

所以，我们不仅要看见安全问题的发生，更要知道攻击目的、攻击方式、会产生什么后果、是什么组织进行的，做到知己知彼。深度的多维度数据关联分析、基于语义分析的检测引擎、可进行人机交互式的调查研判平台、可视化分析、威胁情报技术、特定问题的机器学习都能成为有力的武器。

三是决策中心整合感知结果与威胁情报、攻防专家资源的整合能力。感知结果是知己，威胁情报是知彼。外部数据是威胁情报的重要来源，是指从互联网（以及工业网络、物联网、车联网等）层面上看到的数据。企业看到内部的一些单点事件，在外部其他单位可能曾经发生过，并有各种关联。

即使一些技术高超的攻击者，包括APT攻击组织，在进行攻击的时候，也多数使用过去别人曾经用过的手法，它在互联网的过往历史上都会有一些痕迹，再通过不同的数据维度、时间维度把这些线索串联起来，就能形成威胁情报体系。在生产、研究这些威胁情报的时候，我们会用到很多诸如样本数据、DNS数据等的基础数据，它们都是上百亿的数据量。威胁情报与感知结果融合就能对多数网络攻击行为作出判断；还有一部分感知结果，需要攻防专家研判后给出结果。这些结果就是决策指令，需要实时输出给响应中心。

四是响应中心的落地执行能力。应急响应是网络安全防护的最终目标，其他都是工具手段。它包括通知、通报、启动预案、隔离问题资产与网络、切断攻击路径和传播路径、启动溯源分析等，还有更重要的内容就是立即调集第三方专业安全服务公司进场进行更全面的清查和防御。没有系统性的应急响应能力，就没有网络安全；没有全方位全天候的态势感知能力，就没有系统的应急响应能力。

建立态势感知系统首先要明确目标、范围和目的，对需要监测与防护的最关键业务网络资产和运营机构进行梳理，然后从微观层面获取完整的安全要素数据，其中的一个原则是，数据越全，威胁发生的过程、攻击链条就越清楚。之后再结合来自外部安全大数据的情报能力，从中观层面来分析数据，发现威胁与异常，做到结合安全服务来落地安全能力。

网络安全态势感知的应用

网络安全态势感知的应用很广泛，小到企业、行业，大到城市安全、国家监管层面，都可以通过建立网络安全态势感知提升安全能力，这也是我们在新时代必须具备的能力。

从狭义的角度来说，对于具体的某个企业或者行业，网络安全态势感知能够帮助它们全面了解自身的安全状况，提升各类外部安全威胁来临时响应能力，成为帮助它们构建能力型安全运营系统的基础。

放大到城市的态势感知系统，能帮助监管机构加强对关键信息基础设施的安全监控与防护，从而监管与维护各个重要行业的日常安全运行，随时掌握辖区内重点保护单位的安全威胁态势，随时通报和处置各类安全事件。一旦威胁趋势呈扩大迹象，监管机构能立即启动不同等级的应急响应策略，与各个行业单位形成协同联动，在网络边界、终端、云端进行协同防御，将辖区内的安全风险控制在尽可能小的范围内。

从国家监管层面来说，监管机构能够利用大数据方法，将各个城市、行业的安全态势感知系统进行协同，汇总信息，共享情报，从而以更宏观的视角来指挥调度，协调资源，掌控全局。

比如，在2017年抗击“永恒之蓝”勒索病毒的应急处置过程中，360通过安全态势感知与威胁情报系统，实时了解到病毒在全国的感染和传播态势，每个地区、每个行业的感染状况，细化到感染时间、地点和IP，这样指挥中心就可以协调全国各地的技术团队及时为被感染机构提供支持，也大大提高了相关机构排查的效率。72小时内，我们推送给政企机构的预警通告更新了8个版本，提供了7个修复指南，6个修复工具；出动了三千多人，提供了上万次的上门支持服务和超两万次电话支持服务。可以说，这套系统为公安、网信等领导部门指挥全国应急发挥了重要作用。

在国家网络空间安全监管领域，我们为公安部、网信办建立了针对关键信息基础设施的态势感知系统，通过特有的安全大数据分析技术以及具有领先优势的威胁情报技术，建立国家—省—市多级的网络空间安

全的“监管大脑”，并利用大数据分析及人工智能技术，在反恐、案件侦破等特殊领域做出卓越贡献，尤其在“十九大”“两会”等重大会议期间，此系统被有关部门用于网络安全保卫工作的应急指挥技术系统。

网络安全态势感知的未来

未来，态势感知平台可以考虑通过有管理的公开共享，打通数据、部门、行业甚至厂商壁垒，做到数据互联互通，真正实现数据驱动安全，让更多的部门、数据提供商以及数据分析、安全从业者依托态势感知平台实现自身价值，形成安全生态。

如果将网络安全与现实安全作类比去思考，我们可以这样理解：我们不能因为安装了摄像头就说可以发现全部偷盗，就类似于我们不能因为在关键信息基础设施单位装了流量探针，就说可以发现所有网络攻击一样。但是安装了摄像头和流量探针，能在一定程度上提高发现问题的概率。

再进一步分析。如果社会治理中将摄像头当做一个单点，如果安装这么多摄像头只是为了发现万一可能发生的刑事案件，那么投入产出价值绝对是不划算的。但如果通过摄像头的部署，能够提升社会管理水平，让我们生活更便利，那就可以让一个小摄像头产生更大的价值。有了摄像头实时数据的积累和分析，我们能获悉和预判交通拥堵情况，优化出行，降低交通事故发生概率，提高出行安全；能通过多摄像头的监控，图像提取，进行可疑人员的轨迹追踪，预判和预防重大事件。

类比网络安全世界，态势感知是一个很广阔的概念。首先，网络安全是手段，业务安全、生产安全才是终极目标，当业务、生产全面互联网化后，态势感知自然从单一网络攻击感知上升为业务、生产安全感

知；其次，不同行业、不同地域、不同企业的态势感知互通，这样才能产生更大的价值；最后，态势感知平台开放共享，让各种第三方应用的专家都能在态势感知平台上增加APP，感知将更广泛。

依托态势感知平台实现自身价值，形成安全生态的核心理念是，打造一种机制，成就别人的同时也最大限度成就自己。我们考虑可以主动邀请各数据源提供厂商、部门、人员参与各自数据的使用设计，让专业的人做专业的事情。同时，实现平台不同维度数据、场景创新；实现数据价值深挖；提高交付效率；真正站在平台和集成商的视角，数据和应用提供者均为“店铺”，客户有选择权；快速实现生态式发展，当平台成就越来越多的人员、厂商之后，平台就越来越无法取代。

▶网络安全领域的威胁情报

威胁情报，作为新的网络安全威胁发现与分析的技术手段与数据资源，被越来越多地运用到网络安全领域，在安全检测、研判分析、防御、响应、预测方面发挥积极的作用。从APT发现到勒索蠕虫处置，威胁情报都发挥了奇效。

威胁情报在安全中的价值

威胁情报已经广泛应用到安全产品中，包括防火墙、入侵防御系统、终端防护、Web应用防护系统、安全运营中心（SOC/SIEM）、漏洞管理系统等。它们开始使用可机读的威胁情报信息，用来增强系统的检测与防护能力。

情报自身的质量以及使用对象决定了威胁情报的价值。从总体来说，现阶段安全行业还是缺乏足够的安全分析、事件响应人员。我们注意到失陷检测入侵威胁指标（IoC）类的威胁情报事实上已经成为驱动

安全事件响应的核心，这类情报用以发现内部被APT团伙、木马后门、僵尸网络控制的失陷主机，类型上往往是域名、统一资源定位符（URL）等。

目前，对用户价值最大的可能是IoC类的机读情报和设备自动化交互，它们可以帮助用户快速检测、发现内部的失陷主机，并提供详细的攻击目的、危害、处置建议等信息，让安全运营人员可以快速地进行处置，有效地化解风险。

经过一段时间的市场发展，综合类情报关联分析平台日益受到关注，这说明安全分析、响应日益受到重视，专业人员也在逐步增加，这是一个非常好的趋势。

360威胁情报中心建立之初的重心就包括IoC类型的情报。现阶段360的大多数产品，包括APT检测设备、下一代防火墙、终端安全软件等都具备利用IoC检测或阻截黑客远控服务器的能力，能够在不同的用户处检测发现APT攻击、后门木马、蠕虫病毒等威胁。未来360企业安全将会提供多种形式，让更多其他厂商的安全产品和用户可以利用360的威胁情报能力。

威胁情报分析平台

在利用威胁情报进行安全事件分析研判的过程中，安全分析师需要有相应的工具进行误报识别、攻击类型判别，并能够对攻击意图、团伙背景等情况做进一步的分析。威胁情报分析平台就是以此为目的提供的专用工具。

以360威胁情报分析平台（ti.360.net）为例，针对一个域名可以提供下列的信息：

不同安全情报源对域名的判别信息；

域名关联的样本及恶意链接信息；

域名本身的访问量和最早存在时间、最近访问时间等；

已知和域名相关的攻击家族或者攻击团伙，以及对应的详情；

曾经提到这个域名的安全日志或分析报告；

域名曾经指向哪些IP；

域名的注册者信息；

……

利用这些信息我们可以掌握全球范围内主要情报源中查询域名的信息，判断域名是黑是白，被什么样的攻击者使用，使用的时间段和影响，并可以通过关联分析挖掘更多的内容。

比如，我们通过平台查询在一次攻击中发现的IP，发现这些IP在近期曾被“黑产”用来做过SPAM攻击，就可以初步排除定向攻击的可能性；如果希望知道一次攻击中的几个IP是否属于同一团伙，除了可以通过参照情报平台的攻击历史信息外，我们还可以获得IP的地理位置、主机类型（网关、IDC主机、终端等）、操作系统等信息，这些都是快速判断的有力依据。

威胁情报除了有利于安全事件的研判并提出进一步防护方案外，还有着更为广泛的应用，包括恶意样本分析、红蓝对抗、漏洞管理加强、外部网络资产的发现、业务欺诈的分析与响应、暗网监控等。

当情报具备了与被动防护、积极防御产品技术体系融合的能力，更进一步的情报安全分析才成为可能。

APT攻击的捕获和溯源

从我们捕获的APT攻击可以看到，在进行威胁的发现定位以及研判处置的过程中，威胁情报都发挥了极其重要的作用。

360威胁情报中心陆续捕获了多个APT组织的攻击。自2015年在国内首次发现并披露境外黑客组织“海莲花”对中国的APT攻击至今，我们已经累计发现了38个APT组织。

例如，我们从威胁情报入手，逐步揭开了专门针对金融行业进行APT攻击的团伙“黄金眼”，他们在国内长达8年针对金融进行高级威胁攻击。这个组织至少从2004年就开始活动，专门攻击证券行业，渗透了大量证券、基金、保险相关的组织机构网络，其中包括市场上几个主要的证券服务公司。攻击团伙对所渗透的网络资产进行长期、秘密的控制，读取数据牟利。攻击者分工明确，手段复杂，结合了免杀木马的构建，通过供应链环节进行投递，在被攻击单位内部横向移动渗透，在获取内部信息后进行市场获利操作。这样精心构造、潜藏多年的攻击链条，随着威胁情报技术的应用，终于被发现定位。被攻击机构的威胁被全面检查、清除，攻击者也被绳之以法。

再例如“海莲花”。这个组织在2015年就被我们发现并公布，直到现在还在活动。它也是我们通过强大的威胁情报能力捕获到的。

一直以来，外界只知道360发布了“海莲花”的APT报告，挖出了一个“海莲花”组织，引起了很大轰动，连外交部也在新闻发布会上对这件事情做了回答，但并不知道我们发现和持续跟踪的细节。

我们到底是怎么发现这个“海莲花”，并且持续跟踪的呢？我总结了一个五步法。

第一步，获取特种木马。我们在一个敏感单位里捕捉到了一个特种木马，它在半夜连接一个境外IP，如果在传统安全公司，发现了这个木马就及时杀掉，把它对外连接的通道阻断掉，然后排查一下哪些电脑受了感染，清除干净，这样就算完成防护了。

但是我们抓到这个特种木马以后，做的事情要多得多。

大家都知道，我们有全世界最大的用户量，所以我们拥有全世界最大的样本库，现在已经达到了200亿个，每天还在不断增长。在这200亿里有20％是已知的黑样本和白样本，但还有80％，也就是超过100亿个是灰的，这100多亿个灰样本价值非常大，它是我们能掌握到的对中国的几乎所有攻击的全集，包括特种木马。

为什么说它是全集呢？因为所有对中国进行特种木马攻击的犯罪分子，包括国外的APT团伙，一定要做一个用行话讲叫“免杀”的行为。这个行为说白了就是将木马程序放在中国普及率最高的杀毒软件上测试，看看会不会被报警。如果过不了，就意味着它的攻击会失败。由于测试的时候，它还是个小众样本，我们可能识别不出来，但是库里一定会记录下这个样本，所以我们百分之百有这些特种木马的样本，这样就形成了一个非常宝贵的情报库。

第二步，关联同源家族。把最初拿到的这个样本放到360的200亿全集样本库里，利用机器学习生成的特征匹配，我们就能发现许多同源（也就是说同一家族）的样本，以及采集这个样本的具体时间。这时候，再查这个家族做过的案子，我们就会发现，很多重要单位都被感染了。通过分析样本的语言特征和做“免杀”测试机器的IP，我们很快找出了它的源头。

第三步，提取网络行为。除了基于样本做关联分析，我们还会通过攻击过程的网络活动来拓展分析视野。360运行自己的DNS递归解析服务器，可以看到国内10％以上的DNS解析请求，并提取关键信息做记录。根据积累的多年数据，我们可以知道历史上某个域名曾经绑定过哪个IP，哪个IP曾经解析成哪个域名。

为什么说收集和分析被动DNS的能力很重要呢？因为它就是一个“时间机器”。当我们在分析“海莲花”样本连接的域名时，可能已经不知道攻击发生的时候这个域名解析到哪个IP，但有了这个时间机器则一目了然。知道的意义在于，“海莲花”团伙会在一个IP上绑定多个他们用到的域名，这些域名可能还会解析其他团伙使用过的IP，一层层地反复关联，我们就能把团伙使用的网络基础设施来个大起底。

第四步，回查更多家族。也就是再回过头来，在样本库里找连接过那些IP和域名的样本，我们可以从中找到更多的独立家族。就这样通过关联样本和网络活动，可以还原整个攻击活动的历史，以及所有涉及的恶意代码、发生的时间、受影响的机构等。

目前360确认了“海莲花”团伙使用过7个独立的恶意代码家族，上百个机构受攻击，影响了数千个用户，其中有不少是敏感单位。

到这里还没完，**第五步，重复第二、三、四步。**我们用数据库再查被“海莲花”攻击的电脑，就会发现更多的特种木马。因为攻击这些敏感单位的不可能只有一个组织。我们用新发现的特种木马就能发现更多境外主控IP，再用新的主控IP发现更多的木马。

这就形成了一个循环链，它的独特之处在于，如果没有我们长年积累的大量威胁相关基础数据，是没有办法做到完全溯源、排查和处置

的。

《马太福音》中耶稣对众门徒说：“你们是世上的盐。”

这个比喻，平凡但却发人深省。盐，食之有味，又能保持食物的清洁，防止食物腐坏。基督想以此教诲他的门徒，应该肩负什么样的使命，发挥什么样的影响——他们来到这个世界，就是要净化、美化他们所在的世界，让这个世界免于腐败，并为世人创造更新鲜、更健康的生活气息。

我们要做世上的盐，要积极地服务于社会，为世人造福。这是我们第一个也是最后一个社会责任。网络安全亦如是，更如是。

对于每一位网络安全从业者而言，我们现在的责任就是全身心地投入到时刻发生的网络攻防战中去，投入到为人民造福中去。我想没有什么比这更伟大的了。

Chapter 7
第七章
新战具第三代网络安全技术

爱因斯坦说：“如果不改变思维模式，就无法解决我们用当前的思维模式所创建的问题。”如果我们还用老思路、老办法去做安全，显然解决不了现在的安全问题。

从2015年起，360就开始研究适用于新信息技术发展的新一代网络安全技术理念。随着大数据、云计算、物联网等新兴技术的不断发展，数据安全威胁的感知和捕捉变得越来越困难。传统的围墙式安全防御体系已经失效，需要我们用新战具建立全新的网络安全体系。

我们认为，这个新战具是“查行为”的第三代网络安全技术。它通过大数据智能分析，有效地将原来分割的安全产品更好地融合起来，基于大数据分析、人工智能和协同技术，代表着国际网络安全界的最新发展动向。

第一节　互联网的“基因病变现象”：漏洞的四个假设

本书前几章中，我反复强调，缺陷是天生的，漏洞是不可避免的，网络安全归根结底就是漏洞的事。

缺陷是互联网的基因，与生俱来。漏洞就像病变了的基因，给我们带来危害和痛苦，就像人们不能确切地知道自己的哪个基因会病变，会怎么病变，以及是否已经病变了。所以我从2017年开始就在多个场合反复提到了关于漏洞的“四个假设”。

假设系统一定有未被发现的漏洞

这些年，360都在给微软、苹果、谷歌、Adobe、VMware这些知名的、用户覆盖全球、使用率居行业第一的软件公司提交漏洞。仅2017年一年，我们就提交了519个漏洞，居安全厂商之首，创了世界纪录。

所以，系统一定有漏洞，只是有没有被发现而已。据360研究人员统计，程序员每写1000行代码，会出现1个缺陷，其中的一部分就成了漏洞，还是我反复说的那句话：“缺陷是天生的，漏洞是必然的。”因此，及时发现漏洞利用行为、及时检测被攻击非常重要。

目前，各个行业已经逐步形成了横向、纵向全国互联的广域网，每张子网、每个安全域、每台终端都是一个可能被攻击的突破口。一些网络虽然与其他公共信息网络物理隔离，但是像APT这样的高级攻击仍旧

可以利用病毒木马、零日漏洞社会工程学等手段突破。这类型的高级攻击都具有定向性，在被发现揭露出来之前，都有一定潜伏和秘密活动期，从几个月到几年不等，像“震网”病毒就在伊朗潜伏并执行破坏持续几个月，而“海莲花”在发现时，也已经在我国潜伏活动了3年。一旦发生数据被窃密，无法追溯、定位、取证，国家秘密就会受到严重威胁。

传统的安全设备和产品像入侵检测系统（IDS）、入侵防御系统（IPS）及审计类产品，主要采用经典的通用入侵检测框架（CIDF）模型，这个模型最核心的思想是依靠特征库匹配的方式，完成对攻击行为的检测。但APT采用的攻击方法和技术都是未知行为，依靠已知特征、已知行为模式进行检测，理论上无法检测到APT攻击。因此我们需要使用新方法，例如：

1．使用源代码审计等设备对拟上线的系统进行安全缺陷漏洞检查。无数的案例证明，通过上线前做的安全监测发现的漏洞的修复成本远低于上线后。

2．用实网攻击方法，寻找系统漏洞。“360众测平台”是在严格系统监测下，引入“白帽子”网络攻防专家对系统进行攻击型漏洞检测。同时，渗透测试、漏洞扫描评估也要坚持做。

假设一定有已发现但仍未修补的漏洞

说起这一点，没有什么比“永恒之蓝”勒索病毒的例子更有说服力的了。这个肆虐全球的病毒利用的是NSA黑客组织泄露的漏洞武器“永恒之蓝”以及Windows系统中的一个漏洞进行传播，虽然微软在病毒爆发前就发布了针对Windows 7及以上版本操作系统的安全漏洞补丁，但很

多单位都没有及时安装更新，这些单位都成了病毒“重灾区”。对Windows XP、Windows 2003等老操作系统，微软已不再提供安全更新，而国内大量的教育机构、政务办公系统、业务应用终端仍旧在使用，也是造成本次蠕虫爆发的重要原因，隔离网也没有幸免。

根据补天平台的统计（图7-1），2014年漏洞的平均修补时间是362天，2015年是164天，2016年是132天。到了2017年，由于《网络安全法》的发布和大众重视安全，平均修复时间缩短到了57天。到2018年上半年，平均仅需21天即可完成漏洞修复。虽然漏洞修复的时间已经大大缩短，但是依然有将近一个月的时间可以被黑客随意攻击。因此，及时发现漏洞和强制修补漏洞非常重要。

我们认为至少需要做以下四项工作：状态判定、损失评估、追踪溯源和对策设计。

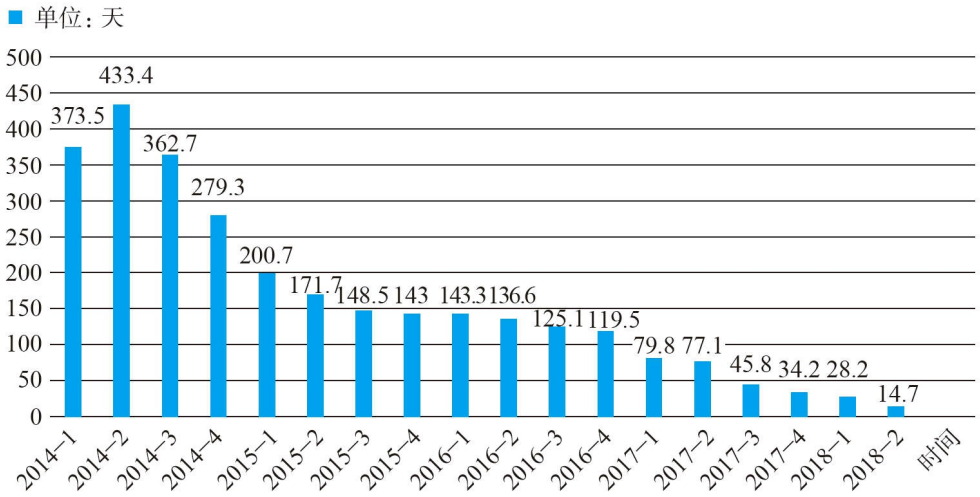

图7-1 2014年1月—2018年2月漏洞平均修复时间

360有一个威胁情报中心，拥有全球最大的样本库，总样本数超过200亿个，并且每天新增数量为900万个。分析每天新增的样本、恶意URL等海量数据并结合多方社区、组织、第三方报告等资源，360每天

形成超过百份的威胁及漏洞情报，通过在线或离线方式推送到客户侧的产品、服务和平台。

这些威胁情报能准确地提供状态判定。比如，360推送的后门C&C（Command and Control）域名信息匹配到了内网的某个主机正在解析相应的域名，这就可以确定这台机器已经被植入了后门，要立刻对机器采取隔离、检测和清除操作以消除后门。

只要发现一台内网的机器遭到入侵，我们就可以断定一定还有其他机器也被入侵。360威胁情报还能提供已知后门程序的多个同源样本信息，在网络的其他机器中搜索这些同源样本文件的散列（HASH），有可能发现更多被攻击的机器。在这个场景下，威胁情报就能对损失评估提供支持。

威胁情报还能支持追踪溯源。比如，发现的某一个后门的使用者来自南边某国，他利用微软WORD软件的某一个漏洞，使用鱼叉邮件的方式投递恶意代码。有了这些，我们就可以定位到导致攻击的邮件，提取特征，再到邮件服务器上搜索，就能发现更多受害邮箱，找到更多潜在受感染者。

这样，以威胁情报为核心的态势感知与安全运营模式就形成了，它能够更好地为网络安全体系建设提供支撑。

假设系统已经被渗透

过去，物理隔离的方式一度被认为是安全的。由于隔离了恶意代码部分入侵途径，因此隔离网在恶意代码防护方面具有天然的优势。

但随着攻击手段的发展，在短短的几年时间内，恶意威胁的复杂性和多样性有显著变化和提升，从过去的直接、随机、粗暴的恶意攻击手段转变为有目标、精确、持久隐藏的恶意攻击。攻击入侵的路径也不局限于互联网，还可以通过移动介质、内部网络横向传播，并和社会工程学等手段相结合。

之前提到的“震网”病毒就是一个很典型的案例。伊朗的核设施是一个物理隔离、高度防护的网络，但是在APT攻击下，核设施参数被修改的事件还是发生了。攻击者用USB移动介质作为跳板，植入了木马文件，成功绕过安全产品的检测，再利用Windows和西门子系统的漏洞，成功入侵了离心机的控制系统，修改了离心机参数，干扰正常运行，但控制系统却显示一切正常。

还有很多被长期渗透控制的例子，因为保密的原因，大多不便于披露。“黑链”就是网站渗透的一种形式，也是一种搜索引擎优化的“技巧”。我们都知道，当搜索引擎排序时，评级越高的网站，排序越靠前；被五星评级的网站引用的文章也会被排在前面。于是，有很多小网站雇佣黑客团队，用违规方式提高网站搜索排名，以非公正性的手段影响和干预搜索引擎结果排名，以牟取非法利益。

相比直接暴露在互联网上的终端，隔离网内的终端面临的恶意代码入侵途径相对少一些，但一些突出的安全问题依然存在。

首先是本地恶意代码防御能力比较弱。大多数的终端杀毒软件受本地存储资源的限制，特征库的数量与恶意样本总量相比几乎只有1%，而传统的恶意样本的检测方式基本依赖于这种本地特征库。目前业内比较先进的云查杀技术，建立在云端庞大的黑、白名单数据库的基础上，具有病毒检出率高、系统资源占用率低等特点，能够大大提升终端的查

杀能力。但是在隔离网环境下，终端无法直接与云端通信，云端的大数据资源不能有效发挥作用。因此，我们需要尽快解决新型查杀技术在隔离网环境的适配问题。

其次是病毒库更新的问题。由于恶意代码演变的速度很快，传统的防病毒软件必须保证病毒特征库的及时更新，才能保证防护效果。而在隔离网环境下，由于病毒库的更新需要人工导入，更新的频率一般都不高。所以，我们一方面需要更先进的隔离网病毒库更新工具，另一方面也需要采用不依赖特征库的智能杀毒技术。

“360天擎”就采用了这种智能查杀技术。它通过机器学习技术把360云端查杀能力变成了人工智能引擎，再在本地建“鉴定中心”平台，为用户提供立体防护体系。

假设经过层层防护的系统已经被渗透了，那我们就应该快速地定位问题，减少损失。但是，很多单位受人员和资金的限制，安全人员的技术、经验和工具都比较薄弱，缺乏对安全事件的分析能力、事件发生后的应急响应能力，在关键时刻没有采取措施，导致损失的发生和扩大。

针对这种情况，我们研发了一套网络安全态势感知系统，先是建立本地的安全大数据中心，通过智能关联计算模型，挖掘漏洞线索，再将网络中的原始流量、设备运行日志、设备告警日志及终端日志等各种信息经过归一化处理，存储到本地搭建的大数据中心，最后利用收集到的数据，基于多维度数据的智能分析模型，发现可疑流量。同时，经过攻防人员的进一步分析，我们可以提升对未知漏洞攻击的发现、阻断、取证、回溯、研判和拓展的能力。

假设内部人员不可靠

第一章中我就提到内部威胁是最大的危害。供应链、外包商、员工等都可能变成“内鬼”，窃取机密信息，造成不可估量的危害。从无数个真实发生的案例中，我们总结了关于人的两大“失效定律”。

▶一切忽略人性的管理手段都会失效

还是以“永恒之蓝”勒索病毒为例。在这次事件中我国很多高校校园网、能源企业、政府机构被大范围感染，即使是处于隔离网的设备也大量中招。

360对国内上百家政企机构进行抽样调研发现，病毒渗透内网的首要原因是员工私自搭建了网络，导致只要有一台设备被攻击，就会造成内网系统中的其他设备也被感染。

在我们处理的另一起事件中，执行任务的人员因为保密需要被要求24小时不得离开酒店房间，但是他们实际工作的时间只有8个小时，有一个耐不住寂寞的人偷偷将内网机器连了外网，所有执行任务人员的电脑全部中招。

后来，我们在排查中发现了多起私自用网线把内网机和互联网插口连到一起，或用手机建Wi-Fi热点，然后将内网设备连接到Wi-Fi热点上的行为，给内网带来了极大的安全风险。

2016年初，某大型能源企业的地质勘探部门发现，某些同行小公司手中居然拥有他们内部使用的地质地理数据库，而且信息非常全面。调查确认，这些数据库信息很有可能是从该企业勘探部门下属的一家子公

司泄露出去的。

经过全面调查后我们发现，为了方便外出勘探时使用，这家子公司的很多员工随身携带的U盘中都存储了大量核心数据资源。我们还发现有少数员工使用公司的地质地理数据库暗中接私活，其中雇主就包括很多同行小公司，甚至有个别员工私下直接盗卖公司核心数据库中的数据资源。后来，这家企业不得不找我们买了大量带有身份认证功能的加密U盘。这种U盘只有插在经过集中授权的电脑上才能正常使用，同时，这种U盘上存储的数据也经过了高强度加密。

这些事件说明，即使有严格的规定，我们也无法保证每个人都会严格遵守，尤其是忽略人性的管理手段，在信息安全保密的实际工作中，一定会失效。

▶一切没有技术手段保障的管理措施都会失效

虽然很多保密规定要求内网机器不得连接外网，不得私自使用移动存储设备，但在实际工作中，连接外网、私自存储的事情经常发生。

如果应用有效的技术手段，让内网机器连接不了外网，或者无法识别私用的移动存储设备，就可以有效保障这些保密规定的实施。比如，360要求每个员工的电脑密码必须是十五位高级密码，并且每三个月就需要更换一次。

但是十五位的复杂密码，每三个月还得换，输入麻烦，也难记，哪怕我们是做安全的公司，还是会有很多员工嫌麻烦，不愿意遵守。刚才说过第一条定律了，忽略人性的管理手段一定会失效。所以，我们必须

靠技术手段来保障这个要求被完全执行。

360有一个信息安全部，每天都会用弱密码库来不断碰撞员工的电脑，一旦发现不符合要求的简单密码或者超过三个月没有更改密码时，他们就会让这个员工的电脑无法开机。我们还开发出了更先进的认证系统——移动终端生物指纹认证。它可以省去输入密码的环节，彻底解决因密码泄露而导致的攻击。所以，没有强有力的技术手段保障，管理措施就会形同虚设。

在这两大失效定律的前提下，我们认为，要从内部消除数据安全的威胁，首先要做的就是在安全体系设计中考虑人的因素，要能够及时发现内部人员的异常行为，并及时检测和阻断来自内部的攻击。360推出了两种方法来解决这个问题：一种方法叫业务安全网关，在产品上叫SSG，另一种方法叫用户实体行为分析，产品上叫UEBA。

业务安全网关（SSG）好比“数据探针”，可以识别人的违规或恶意操作。SSG负责收集访问各种业务系统、数据库和服务器的数据，从业务系统、业务操作和内部人员三个维度构建评分，帮助掌握各种网络系统的整体态势。

360曾帮助查处了一起政府单位信息泄露事件。员工张某利用测试账号进入系统，一次批量查询了10000条客户信息，进行了多次查询操作。SSG通过抽取用户和业务操作等数据，比对了操作特征、数据特征、行为特征和本地安全策略，发现这是一次恶意操作，及时阻断了这名内部人员的操作。

用户实体行为分析（UEBA）就是用大数据分析发现“内鬼”。UEBA通过机器学习来发现高级威胁，在发现用户异常方面具备非常高

的“命中率”。我们推出的这个平台可以通过多维数据关联与用户行为分析，及时发现和定位高风险用户。这样就能及时阻止不可靠内部人员的异常操作，避免重大安全事件的发生。

第二节　网络安全技术的变革：从“查黑”到“查行为”

在社会信息化和网络化三十多年的发展过程中，网络安全技术伴随着网络攻击的变化不断变革。我总结，在这三十多年里出现了网络攻击的三次浪潮，也随之诞生了三代网络安全核心技术。其中，“查白”的第二代网络安全核心技术就是360发明的。现在网络攻击进入第三次浪潮，我们又创新地提出了“查行为”的第三代网络安全创新技术。

第一代技术：“查黑”

世界上第一个被广泛传播的计算机病毒出现在1987年，叫做C-BRAIN。这个病毒的作者是一对巴基斯坦兄弟，他们开了一家电脑公司。为了防止软件被任意盗拷，他们编写了第一款防盗拷程序——C-BRAIN，意思是“大脑”。

只要有人盗拷他们的软件，C-BRAIN就会发作，将盗拷者的剩余硬盘空间“吃掉”。尽管这个程序的诞生并不是出于恶意，但由于它对电脑的破坏性以及会像病毒一样不断地传染，它被业界公认为真正具备完整特征的计算机病毒始祖。

随着互联网的发展，一些新的病毒纷纷出笼。比如，1988年我国出现的第一例感染型病毒“小球病毒”；1995年第一例感染中文WORD的宏病毒“台湾1号”以及1997年宏病毒泛滥成灾；1998年出现、1999年大规模爆发的第一例造成计算机硬件故障的CIH病毒；1999年第一例通过邮

件传播的“梅丽莎”病毒，以及2000年“爱虫”病毒爆发。

经过十几年的发展，病毒样本数量从1986年的8种发展到1995年的1000种，再到2000年突破1万种，最多时每天以几百种的速度增加。由于当时病毒的传播速度很慢，且多数病毒并不是感染之后立刻发作——像1998年出现的CIH病毒，1.2版是每年4月26日发作，1.3版是每年6月26日发作，1.4版是每月26日发作——所以，当时应对这些病毒的方式是根据他们的特征码，做一个程序，在电脑里匹配出病毒，然后再清理掉。

当时的杀毒软件有两个核心：查杀引擎和每天运营升级的病毒特征库。查杀引擎逐一扫描电脑硬盘上的文件，实时与特征库比对。文件中某一段代码与病毒特征匹配上了，就杀掉，否则就放过。这就是俗称的“黑名单”机制，我称其为“查黑”的第一代网络安全技术。这类技术主要有三点特征：第一，只能管已知的病毒；第二，查杀是滞后的；第三，当时的病毒传播方式主要是以介质感染、文件感染、邮件传播为主，比较缓慢。

随后，病毒制造者和杀毒厂商展开攻防对抗，出现了加壳技术和变种病毒，通俗地说，就是给病毒穿上马甲或者换身衣裳。应对这种新病毒，杀毒厂商推出了“启发式”杀毒引擎，可以理解为1.5代网络安全技术。“启发式”能够通过一些行为规则或静态特征来识别一些未知的病毒，对未知病毒有一定的检测能力，但误报率一般超过10%，需要用户配合去除误报，不适宜小白用户，所以并没有得到广泛使用。

第二代技术：“查白”

2001年以后，随着互联网的快速发展，蠕虫病毒开始大规模出现，比如2001年的“红色代码”、2003年的“冲击波”、2004年的“震荡波”、2005年的“狙击波”、2006年的“熊猫烧香”等。

最需要重点提出的是2001年出现的尼姆达病毒，它被普遍认为是第一个快速传播的网络病毒，是首个利用系统漏洞对互联网发起攻击的病毒。尼姆达病毒首先于2001年9月18日上午9：08在美国被发现，半个小时之内就传遍了世界，当天下午就蔓延到了中国。它不但可以感染Windows 95、Windows 98、Windows Me和Windows 2000的PC机，还可以感染运行Windows 2000的服务器，是第一个可以在四种不同的操作系统上传播的蠕虫病毒。

蠕虫病毒和以往普通病毒的区别在于，它可以不通过感染文件的方式而独立存在，有的只存在于内存中，而且它能够自动扫描系统漏洞、端口实现自我复制和传播。蠕虫能借助互联网、企业内网、电子邮件、网站挂马等方式进行传播，因此破坏性比普通病毒大得多。普通病毒的传染能力主要是针对计算机内的系统，而蠕虫的传染目标是互联网内的所有计算机，短时间内就能蔓延至整个网络。

2006年，流氓软件的爆发进一步把木马数量推高。因此，这一时期木马病毒呈指数级爆发，每日新样本数量从1万个上涨到峰值时期的近1000万个。传统安全公司的样本分析运营部门再也无力及时分析每日上千万个样本，导致病毒库无法及时更新。另外，网络病毒的传播速度变得极快，短短几分钟就可能感染上百万台设备，传统杀毒软件因需滞后几天甚至几周才能杀掉病毒而变得毫无作用。黑名单机制宣告失效，网络安全产业迎来了第二代技术创新。

在这样的背景下，360创新发明了第二代网络安全技术“查白”，

首次把搜索引擎、云技术、人工智能等互联网技术应用于安全领域，建立了全球最大的白名单文件数据库，覆盖了99%以上网民常用的操作系统和应用软件。由于覆盖面足够广，所以，只要这个文件不在白名单中，它就很可能是新的木马病毒，也称为“非白即黑”。360的云查杀引擎就会限制它的敏感操作，而且尽快进行安全性鉴定，一般在30秒以内就能捕获网上新出现的木马病毒。

从“非黑即白”变成了“非白即黑”，效果是很显著的，它攻克了当时黑名单瞬息万变不可捕捉的难题。

360推出以“查白”为核心的第二代技术后，网络攻击者也不得不采用新的方法进行攻击。所以，360在2010年前后推出了主动防御引擎，我称之为2.5代网络安全技术。主动防御在白名单样本的基础上增加了行为黑名单，在黑名单上的程序直接报毒，在白名单上的直接放行，不在黑、白名单的未知程序则转由云端的行为分析器来判断这个程序的动作是否有危害。

第二代安全技术取得的成绩有目共睹，很好地解决了当时的安全问题。在微软每年发布的全球安全报告中，中国连续五年排名第一，恶意软件感染率仅为全球平均的六分之一。

第三代技术“：查行为”

2015年前后，APT攻击成为主流，出现了大量“白利用”攻击手段，即利用已知或未知的系统漏洞，把恶意程序注入系统白文件中，操纵系统文件进行攻击，让安全软件看上去是一个系统文件的正常操作，好比我们守着安检门，但黑客跟随有免检证的人走了VIP通道，安全技

术再次进入颠覆期。因为无论是“查黑”还是“查白”技术，前提是能看样本，如果木马病毒走侧门，安全设备看不见，当然也就检测不出安全威胁。

比如，2017年5月12日爆发的“永恒之蓝”勒索病毒事件，黑客就使用了“白文件利用”攻击手段，他们通过系统的远程代码执行漏洞——永恒之蓝（MS17-010），将恶意代码注入系统进程中，又利用cmd.exe、attrib.exe、icacls.exe、wbadmin.exe、reg.exe等7个操作系统本身的功能程序，实现隐藏、自启动、删除系统备份、获取文件操作权限、遍历全盘文件、加密特定类型文件等恶意目的，最后弹出窗口向用户勒索赎金。如果不结合行为特征，光靠白名单、黑名单，病毒是无法查杀的，这也是“白利用”泛滥的原因。

所以，我们又创新地提出了第三代网络安全技术框架，用数据驱动安全，从关注样本黑与白上升到关注网络行为。白名单只能作为参考依据，而不再是无原则地信任清单。第三代技术突破了终端和边界的限制，通过尽可能全地收集大数据，对每个样本ID、IP、流量进行计算，判断行为是否合法，把可疑行为找出来告警，行为分析至关重要。

在本章的第一节，我提出了网络安全的“四个假设”。这四个假设充分表明，过去我们把安全二元化地分为黑和白，把黑的拦截住，把白的放进来的方式已经失效了。只要有黑白的标准，就意味着能依据这个标准，躲过黑的检测或者把自己伪装成白。因此，我们需要探索不再按黑白来解决安全问题的办法，行为分析变得至关重要。

所以，第三代网络安全技术的核心是“查行为”。“查行为”主要分为三个方面的内容：第一，通过威胁情报，确定攻击行为；第二，通过机器学习，建立行为基线；第三，对超出基线的可疑行为，进行响应。

第三节　第三代网络安全技术的大数据观

第三代网络安全技术以尽可能全面的大数据采集为基础，以机器学习、人工智能的行为分析为核心，其关键是威胁检测与应急响应。

以空间换时间

网络渗透和攻击都会留下痕迹，在无法判断哪些行为是攻击的情况下，我们需要尽量多地对行为和数据进行记录。数据掌握的越多，维度越广泛，检测的信息就越全，发现攻击的速度就会越快，这就是“以空间换时间”。

没有充分的数据采集，就谈不上任何的数据能力。数据采集的能力又可以分为四个方面：一是安全数据的历史积累，如过去若干年的恶意样本库、恶意网址库、查杀记录等。这对于很多传统的安全企业和新入行的安全企业来说，是一个极大的挑战。

二是最新安全数据的采集能力。这种能力主要取决于安全企业的终端用户数以及安全服务业务的覆盖面。

三是相关领域的多维度数据采集能力。因为安全事件并不是孤立的网络事件，它与网络服务器、DNS解析、网站页面内容等很多其他方面的网络信息密切相关，所以是否能够在最大程度上采集相关领域的数据，决定了安全服务分析的范围以及有多大的可扩展空间。

四是数据采集的维度与粒度。只有足够丰富的维度和足够细密的粒度才能保证数据对真实攻击的呈现是充分的、完整的。

360目前有全球6亿PC端和8亿移动端用户，拥有世界最大的样本库，是全球最大的针对中国攻击的木马全集，同时拥有被动DNS“时光机器”，可解析十余年境内外IP与域名历史痕迹。

以算力提战力

怎么确定一个人的正常和异常行为呢？我们认为，如果通过大数据获取一个人在相当长一段时间内的数据，就可以给这个人设立行为基线。当他做坏事的时候，甚至当他刚有变坏的想法时，他就超出了自己的行为基线。

同时，我们给曾经出现在黑名单上的电脑、IP地址、用户也建立一个基线，叫黑基线；给从来没有出现在黑名单的行为再建一个基线，叫白基线。通过建立这三条基线，我们就能实现最快速的威胁检测、最准确的告警和最及时的措施。

数据之间往往存在着内在的关联性，将数据进行有价值的关联分析，是发现未知威胁和高级攻击的关键所在。例如，当防火墙监测到一个流量异常时，其对应的攻击可能是终端上感染了一个木马。如果终端与防火墙的数据能够进行实时关联分析，我们就有可能形成联动效果和快速的威胁发现能力——这也是下一代防火墙的重要能力之一。

对于网络中实时产生的海量数据，完全使用人工分析显然是不可能的。这时，机器学习就特别重要，机器学习与人工智能技术是大数据分

析的必备能力。

以往，我们会使用机器学习技术来进行恶意程序的样本分析。360自主研发的QVM引擎就是全球第一个通过机器学习技术实现的人工智能杀毒引擎，它很好地解决了海量样本的快速分析与识别问题。

现在，机器学习在其他安全大数据领域已经取得了很大突破。比如，流量识别在传统安全技术领域一直是一个让人头疼的问题，特别是协议还原技术，既考验分析系统对层出不穷的各种网络协议的解析能力，同时也会对服务器造成巨大的计算压力，成本很高。但通过机器学习技术，我们可以在不解包数据流、不进行任何协议还原，甚至完全不知道流量包采用的是什么通信协议的情况下，直接通过分析数据包本身特征，对流量进行快速识别和分类，其准确性、识别效率和可扩展性都远远优于传统的方法。

以已知求未知

什么是威胁情报？今天黑客组织最新的攻击目标是什么？他们发现了哪些漏洞？发明了哪些新的攻击方式？我们利用机器学习、人工智能的行为分析，从每天新增的样本、第三方报告等海量数据资源中，形成超过百份的威胁和漏洞情报，通过在线或离线方式推送到客户侧的产品、服务、平台。

对安全状态的掌控，我认为可以大致分为内部和外部威胁两个方面。对于内部威胁，360依托大数据，综合对安全的认识和积累，加上客户对业务的需求和数据共享，制定出某行业、某类型甚至某客户的安全现状监测体系，让内部安全现状可衡量。

相对于内部威胁，外部威胁更难跟踪发现。但现在，技术和数据源的可获得性大大提高，利用大数据技术，我们可以较好地掌控外部威胁的情况。例如，阿里为了解决举办活动时被“黑产”薅羊毛的问题，专门收集网上“黑产”发布信息常用的论坛和交易QQ群，并逐一落实跟踪，使用各种数据抓取工具抓取相关数据。通过关键字匹配找到与自己相关的信息，第一时间跟踪“黑产”对阿里特殊活动的“兴趣”。如发布活动前，“黑产”控制的手机号开始大量提前注册账号，意向非常明显，需要提前预防。

此外，从安全监测的角度看，以前安全监测的视野比较窄，基本都聚焦于被保护对象，如关键信息基础设施、党政机关网站等，对于被保护对象以外的范畴关注较少。通过大数据技术，我们其实可以把感知到的安全威胁、攻击通过攻击溯源等方法，找出值得关注的攻击源或者关键路径上的关键节点，并对这些节点也进行监测，同时建立异常发现模型。一旦这些节点有异常行为，就意味着可能有比较严重的攻击要发生，从而预测、预判和预防。

一般来说，能够监测到的各种告警、事件往往是被孤立看待的，而客观上，这些事件其实存在潜在的关联。如果能够把这些散布在不同时期、不同位置的线索通过大数据建模关联起来，就很可能预判重大安全事件。关于威胁情报，我将在下一章中进一步阐述。

目前，360已经建成了比较完备的第三代“查行为”的核心技术体系，推出了态势感知系统、威胁情报分析、安全运营平台等一系列解决方案。

漏洞的四个假设充分证明，安全产业已经进入了颠覆、创新的时间窗口。我们认为，

第三代“查行为”的网络安全核心技术是应对当前网络安全形势较为理想的解决方案。

当然，随着网络安全态势不断演进，网络安全技术必将需要新的创新和突破，360也将不断提高自身能力，紧跟技术前沿，做网络安全行业的引领者。

Chapter 8
第八章
新战术安全从0开始

当前，影响全球的安全事件此起彼伏，数字化时代让安全价值回归，应对网络威胁的战术也必须同步发展。我们认为，要回到安全的本源和原点思考，安全应该从0开始。

安全从0开始，意味着“0信任”。简言之，“0信任”的策略就是默认不相信任何人、任何设备，哪怕曾经给予它授权，因为历历在目的往事中，被攻击、被渗透的设备几乎无一例外都是我们授权的可信设备。这背后的安全理念和我在上一章中提到的网络安全的“四个假设”是一样的。这四个假设并不是对未来的设想，而是已经在我们现实生活中真实地上演。对网络安全而言，信任应该和时间、应用紧密相关，而不是无限。

安全从0开始，意味着必须从0开始规划网络安全体系的整体架构，包括之前我们坚守的所谓网络边界、授权认证、隔离措施；意味着从0开始部署网络安全设备和产品，让它们具备向云端传送日志的能力，供安全大数据中心全面分析、审计；意味着从0开始搭建网络安全运营人才队伍。

安全从0开始，还意味着必须从0开始做到安全与项目的规划、建

设、运营“三同步”，将安全管理和防护措施前移到项目的初始阶段。尤其是对漏洞的治理，以往我们认为这是运营的活儿，甚至认为治理漏洞就是打补丁，可如果有补丁打不上，或者没有补丁，就只能放之任之，这是最大的漏洞。所以，治理漏洞也要从0开始“三同步”。

第一节　从“五段论”看网络安全市场前景

在网络安全领域，有一个著名的滑动标尺模型，我喜欢叫它“五段论”。这个理论把网络安全的行动措施和资源投入进行了分类，可以让机构很方便地辨识自己所处的阶段，以及应该采取的措施和投入。对网络安全从业者来说，它可以帮助我们审视自己产品和服务的布局。

网络安全滑动标尺模型是SANS公司研究员罗伯特·M.李（Robert M.Lee）在2015年8月发表的一份白皮书《网络安全滑动模型》（*The Sliding Scale of Cyber Security*）中建立的一个网络安全的滑动标尺模型。它共包含五大类别，分别为架构安全（Architecture）、被动防御（Passive Defense）、积极防御（Active Defense）、威胁情报（Intelligence）和进攻反制（Offense）。

图8-1非常好地展现了这五大类别的特征：每个阶段直接具有连续性关系，并且处于动态，不容易界定。

图8-1也很好地体现了习近平总书记在2016年4月19日的网络与信息安全工作座谈会上谈到正确的网络安全观时指出的五个网络安全的特点：网络安全是整体的而不是割裂的，是动态的而不是静态的，是开放的而不是封闭的，是相对的而不是绝对的，是共同的而不是孤立的。

图8-1　网络安全的滑动标尺模型

架构安全

架构安全指的是在系统规划、建设和维护的过程中我们应该充分考虑安全要素，确保这些安全要素被设计到系统中，从而构建一个安全要素齐全的基础架构。就像建造一栋房子，需要打好地基、筑好框架，建好楼板，房子才会安全、坚固。

在安全的各个方面中，最重要的一个方面就是确保系统能够建立正确的架构安全体系，其中包含与组织业务目标的一致性、投入费用的充足性以及人员配置的合理性。

如果我们在搭建系统的时候，没有正确划分安全区域，建好补丁管理系统，就会出现大量低级错误，如偶发恶意软件感染、网络安全配置等问题，产生大量低级告警。这些问题就像巨大的“噪声”，真正的网络攻击者的行为埋没在这巨大的“噪声”里，给自己在网络防护的时候识别真实威胁带来巨大的障碍。

架构安全并不能仅仅定位于抵御攻击者，而是必须使系统既能够支撑组织的业务需求，又能够应对紧急事件发生时的运行情况。系统安全措施应该让系统有能力应对各种紧急事件，如意外的恶意软件感染、系统配置不当导致的网络流量峰值以及多系统因放置在同一网络而导致的彼此干扰等。在设计系统时充分考虑这些情况并设计相应措施，这将有助于维持系统的机密性、可用性和完整性，从而支持实现组织机构的业务需求。

因此，组织机构应该首先确定其IT系统所支撑的业务目标，这些业务目标在不同组织和行业中会存在差异，系统的安全防护必须能够支撑这些业务目标，并在对系统进行规划、工程管理和设计时，就开始引入架构安全措施。

系统的安全开发、采购和实施是架构安全类别措施的另一个关键组成部分。要确保供应链中每个环节的安全性，并结合相应的系统维护措施（如打安全补丁等），使系统防护变得更容易。

架构安全只是基础，并不足以实现网络安全。但有了这个基础，我们就可以在此之上以较低的成本构建安全措施，所以我说架构安全是“以不变应万变”。

被动防御

被动防御是建立在架构安全基础上的，目的是假设攻击者存在的前提下，保护系统的安全。我在本书中一直重申，缺陷是天生的，漏洞是不可避免的，网络攻击是必然的。有机会、有意愿和有能力的攻击者或威胁最终一定会找到方法绕过完善的架构安全体系，所以，被动防御是

必需的。

美国国防部对“被动防御”的定义是“在无意于采取主动行动的前提下，为降低敌对行动造成的损害可能性以及损害影响所采取的措施。”虽然这个定义本身看起来很容易理解，但当把它应用到网络空间的正常操作环境中时，仅仅根据字面意思理解是不够的。

在军事上，被动防御是指在不需要军方介入的情况下提供一定程度的防御。在建筑物周围加固屏障、增加诱饵、进行军事伪装以及添加附加物的措施都属于被动防御。

我们知道，在物理世界中资源会有损耗，就像炸弹扔完一颗就少一颗，我们总说的一个词叫“弹尽粮绝”，谁撑到对方打完最后一颗子弹，谁就获胜了。但在网络世界中，一旦某一个恶意软件得手，只要它没有被发现，或者没有针对它的对抗措施，它就可以在许多其他攻击活动中重复使用。那么攻击者消耗的资源是什么呢？是时间、所用人员等资源。因此，消耗攻击者的这些资源（包括其用于制定计划和达到目标所需的时间）就变得非常重要。“被动防御”正是在实现这一目标上发挥大的作用。

我们可以推导出一个概念：在已有的结构上，可以通过添加附加物达到保护已有结构的目的。物理世界中的被动防御不需要防御人员的不断介入。同样的，在网络世界中，在没有人员介入的情况下，附加在系统架构之上，可以提供持续的威胁防御或威胁洞察力的系统，就是“被动防御”。

添加到架构安全上的系统可以起到保护资产、阻止或限制已知安全漏洞被利用等作用，这些系统包括防火墙、反恶意软件系统、入侵防御

系统、反病毒、入侵检测系统和类似的传统安全系统。

积极防御

面对“意志坚定”、资源充足的攻击者，被动防御机制终将失效。因此，对抗此类攻击者时，我们需要采取主动的防御措施。打一个比方，主动防御就是在洲际弹道导弹（ICBM）击中目标前，我们使用综合防空手段对这枚导弹进行跟踪和摧毁。

实施主动防御的前提是需要训练有素的安全人员来对抗训练有素的攻击者。其中很重要的一点是，我们要给予这些训练有素的安全人员充足的授权，让他们能在已经构建了被动防御系统的架构安全体系上展开防御工作。

“主动防御”强调的是机动能力，包含整合军事情报和识别攻击的能力、在己方区域或对抗区域内对攻击行动或攻击方能力进行响应攻击的能力，以及交战后总结经验的能力。

从网络安全角度看，我们可以将基于主动防御模式的“积极防御”理解为分析人员对处于所防御网络内的威胁进行监控、响应、获取经验和应用行动的过程。

在积极防御这个阶段，我们重点关注的是人，而不是工具，因为积极防御要求的是机动能力和适应性。防御体系的软硬件系统扮演的角色是积极防御者的工具。这里说的人，指的是能够利用环境寻找攻击者并做出响应的各类安全人员，包括事件响应人员、恶意软件逆向工程师、威胁分析师、网络安全监控分析师和其他相关安全人员。

有一点要特别强调的是，在网络安全领域中的积极防御只适用于防守区域内，而且只是针对攻击者的能力展开对抗，而不是直接针对攻击者。这句话说起来有点绕口，我们还是可以用洲际弹道导弹的例子来理解。这就好比综合防空作战中，洲际弹道导弹主动防御机制只损毁导弹，并不会攻击导弹发射阵地所在地的人员或设施。

威胁情报

要实现有效的积极防御，很关键的一点是要具备针对攻击者的情报使用能力。威胁情报是一种特定类型的情报，旨在为防御者提供有关攻击者的知识，帮助防御者了解攻击者在防御者环境中的行动、攻击者的能力和TTP（战术、技术和规程）信息，让我们从攻击者身上获得相关经验教训，从而更好地识别威胁和做出响应。

在滑动标尺模型里，情报的生产是一种情报行动，属于情报阶段，而情报的使用则是积极防御类别中的一个角色，属于积极防御阶段。在情报这一阶段，分析人员通过各种方法，从各种来源中产生关于攻击者的数据、信息和情报。情报生产和情报使用所需要的分析人员、过程和工具方面都存在着显著差异。情报生产通常需要大量的资源投入、广泛的数据收集机会，以及聚焦目标了解所有的信息；情报使用则要求分析人员熟悉威胁情报作用的环境，了解可能受到影响的业务操作和技术，并且能够将情报以可用的形式呈现。

情报是一个常用词，也是常常被误解的概念。美军将情报定义为“通过对有关外国公民、敌对或潜在敌对的势力或元素，或真实或潜在行动区域的可用信息的收集、处理、整合、评估、分析以及解释所得（信息）产品”。该术语也适用于生成产品的活动及参与这项活动的组

织。简单地说，情报被同时定义为产品和过程。在网络安全领域，“情报”是“收集数据、将数据利用转换为信息，并将信息生产加工为评估结果，以填补已知知识缺口的过程”。

网络安全领域中的情报涉及一系列活动。例如，某些组织通过访问攻击者所处的网络从而收集和分析信息，这就是一种网络情报行动；被窃取的文件会执行自动回连行为，这种文件存储在攻击者的网络内部，会向防御者传送攻击者环境的确切位置信息。所收集的这些信息将成为对国家政策制定者、军队或其他人员非常有价值的情报。

再比如，从蜜罐技术角度分析攻击行为的研究人员，可以在不对攻击者采取行动的情况下，收集相关信息并进行分析，创建出有关攻击者的情报。

分析人员从已被攻击者攻陷的系统中收集数据，从而得出关于所面临威胁的情报。这个情报在网络安全社区中被定义为“威胁情报”。

威胁情报非常有用，但由于缺乏深入理解，许多组织都没有充分利用它，因此导致了许多错误认知。正确利用威胁情报至少要做到以下三点：

1．必须知道什么能够对自己构成威胁（有机会、能力和意图伤害他们的攻击者）；

2．必须能够使用情报来有效驱动行动措施；

3．必须了解生产情报和使用情报之间的区别。

目前，大多数组织并不了解他们所面临的威胁，无法准确地确定哪些攻击者和攻击手段会对他们构成实际威胁。

如果没有做好组织的架构安全和被动防御，我们就确定不了机构的系统中是否存在某一已识别的漏洞，也无法确定哪些漏洞能被修复，因此对风险把握不准。只有熟悉系统所承载的业务流程、安全状态、网络与系统的架构安全体系的人，才能有效利用威胁情报。此外，他们还必须熟悉组织内部的运作机制，拥有来自组织管理层的支持，这样才能根据情报采取行动。

简单地说，组织必须了解自己、了解威胁，并授权人员使用情报信息采取行动，才能正确使用威胁情报。由于情报必须建立在标尺模型中提出的其他三个阶段的基础之上，所以情报的实际应用会更加复杂。但也正是上述这些基础，才使威胁情报具有极大的价值。

进攻反制

进攻反制阶段位于网络安全滑动标尺模型的最右位置，指的是在友好网络之外，以自卫为目的，对攻击者采取的合法反制措施和反击行动。

执行“进攻”行为的人需要理解其他阶段的内容及相关技能，并且经常需要其他类别的基础支撑。例如，对环境中威胁的识别通常发生在积极防御阶段；在被动防御和架构安全的基础上才能正确执行积极防御；识别攻击者信息、积累操作行动所需的知识，发生在情报阶段。

从独立行动的角度来看，“进攻”的代价很高。综合考虑进攻行动所需的基础投入后我们认为，“进攻”是组织机构所能采取的最昂贵的行为。

“进攻”覆盖广泛的多种行为，所以我们用的是“进攻”这个术语，而不用“网络攻击”。美国国防部关于这类术语的联合出版物没有定义进攻性网络行为，但以“在或通过网络空间施加武力来投射力量”的方式讨论了进攻性网络行为。

在国际法框架下，国家实施的网络空间进攻行为是否合法，是具有高度争议的。迄今为止，针对该争议记录和解释得最为全面的参考文献是被称为第一部网络战争规范法典的《塔林手册》（*Tallinn Manual*）。无论国内法和国际法如何演变，民间或国家组织实施的进攻性行为必须具有合法性质，这才能被视为网络安全行为而不是侵略行为。出于复仇或打击报复所实施的进攻性行为，既不符合国际法，也从来不会被视为自卫行为。

未来的网络安全市场

在本节的一开始，我就说过，“五段论”对于网络安全从业者的重要意义。它可以帮助我们很好地审视自己的产品和服务的布局，对未来的网络安全市场有比较清晰的判断和把握。

当前，随着各国政府对网络空间安全的高度重视，我国也在持续加大在网络安全建设方面的投入，各政府单位及企事业部门的网络安全建设规模都在快速增长。未来，网络安全市场的重点会是什么？产品和服务如何布局才是合理的？**我认为，从“五段论”可以很明确地看到，我们需要重点考虑的是如何形成一个综合的、高效的安全体系，以支撑持续的安全监测、响应和运营。**

市场数据也能证明这个判断。近年来，安全集中分析和管理品类的

产品销售额高速增长，这反映了市场对于安全运营与安全分析的迫切需求。全球知名的IT咨询公司高德纳（Gartner）在2017年发布的报告中，也明确提出了现代化安全运营中心的概念。

从实际应用效果来看，过去的安全运营方式难以实现全面的威胁发现、分析和监测运营。原因是其主要依赖于网络安全运维管理（SOC/SIEM）类产品平台所能提供的能力，数据维度相对不足，分析方法比较单一。

现代化的安全运营中心强调以全面的智能威胁分析为基础，扩展用于分析的数据维度，借助多种检测引擎、高级分析方法，同时结合威胁捕猎，实现集中的安全监测，再通过响应形成处置的闭环。

在我国，信息化系统的建设和业务发展在不断进步，业务信息系统的规模和复杂度不断增加，安全威胁的防护压力日益加大。从市场的角度看，我们最迫切需要的是具有较完整威胁分析监测能力、“可运营”的安全运营支撑型平台。这并不是一件容易的事，因为它不但对技术层面提出了更广泛的要求（如大数据平台与计算能力、威胁情报、行为分析等），还要求从业务理解到技术的转化，以及在人员与运营能力方面有深厚的积累和储备。

我认为，下一代安全运营体系要做到以下几点：

▶弹性大数据安全分析平台

底层平台一定要强调开放性与弹性扩展，方便人们将各类数据源进行配置接入，能针对多元异构数据进行合理的采集、处理、存储，并配合适当的数据计算分析引擎，从而支撑上层的各类网络安全与业务安全的应用。

▶应用更多的高级分析方法

数据驱动的安全分析体系中，越来越多的高级分析方法在近两年被落地使用，并且借助大数据安全分析的技术能力，为企业及机构的威胁发现、安全分析、安全运营提供更多的变革。

比如从传统的基于规则的威胁检测演进到基于全流量的深度威胁分析，并将流量探针更多地落入企业内部网络的关键检查点；从传统的SOC/SIEM中的关联分析方法，逐步演进到结合用户与实体行为的分析系统（UEBA）；从终端的多维度数据源头进行探查并提供分析基础；以及在分析能力中内建机器学习能力等。

▶深度整合的威胁情报能力

安全是个攻防的动态过程，从积极防御阶段开始，我们对威胁情报的需求开始迫切。

深度整合的威胁情报能力能摆脱只采集用户内网安全数据的信息孤岛局面，实时掌握互联网空间最新的威胁动态，并进行深度的威胁情报分析和追踪溯源，以此来判断识别其对受保护网络的危害和渗透。

▶终端检测与响应

由于用户数量众多、应用环境复杂、人员使用管理成本高，终端是最容易出现不安全使用行为的部分，一直以来都被认为是安全隐患高发的环节。因此，终端层面的威胁检测与响应也成为未来安全体系中的重要组成部分。

我们需要记录大量终端与网络事件，并将这些数据存储在终端本地或者集中数据库中，然后对这些数据进行特征比对、行为分析和机器学

习，用以持续对这些数据进行分析，识别信息泄露等内部威胁，并快速对攻击进行响应。

▶平台与人的结合

实践证明，单一的依靠平台、产品是行不通的。“五段论”中，从积极防御阶段开始，人发挥的作用越来越大。

任何一个平台或产品都无法完全避免漏报、误报，也不可能完全覆盖分析需求。换句话说，平台不可能完全脱离人单独运转，不论是日常的一线运维人员，还是重点事件的专家分析研判。我们需要做的是建立一个完整、有效的安全体系，这个体系能结合平台的分析工具能力，以及云端的数据、情报能力，赋予人更强的能力。

第二节　“三位能力”系统是安全从0开始的最佳实践

“五段论”是我们审视安全产品和服务布局的依据，是打开未来网络安全市场之门的钥匙。在从基础架构到反制进攻的演进过程中，我们从能力的维度构建了一个低位、中位、高位“三位能力”系统。我们需要基于这个“三位能力”系统，不断进行网络安全技术的创新，构建低位、中位和高位的数据能力，这是安全从0开始的最佳实践。

我先打个比方。假设我们有1万个关键信息基础设施和4万个网络安全防护人员，平均到某个关键信息基础设施上的防守力量是4个人。如果敌方的军力也是4万人，他们并不需要同时攻击这1万个基础设施，打瘫一个就可以达到目的，那就是4个人与4万人的对抗，这显然是守不住的。所以我们总说，网络攻防对抗是不对等的。

怎么解决这种不对等呢？如果我们把这1万个基础设施、4万个人的能力数字化集中到一个中心里来，有任何一个点被攻击，我们都能实时感知并调度其他点的人力来应对，就是4万人对4万人，一盘散沙变成了一支能被灵活调配的集团军，不对等就变成了势均力敌。

4万人分散开来守卫1万个目标，这就是架构安全和被动防御阶段要做的事，也是我们根据“五段论”构建“三位能力”系统里的低位能力；这种把分散能力数字化，集中起来形成能力中心的做法，相当于传统作战时的参谋部和前线指挥部，是“三位能力”系统里的中位能力；“五段论”中的情报和进攻反制是“三位能力”系统里的高位能力。

低位能力——安全体系的“五官和四肢”

低位能力是传统的安全防御能力，即通过部署终端、边界等安全产品，实现数据的生产和采集。它就好比一个人的“五官和四肢”，负责听、看、闻、尝、取，以及在大脑指挥下采取动作行动。

和人体一样，低位能力采集到的数据是多维的，而不仅仅是网络空间的数据，也包含物理世界的数据。举个简单的例子，如果你办公室的电脑正在传输一些数据，但是我们同时发现你还没有打卡进入办公室，这就可以初步判断，不是你在操作电脑。这是很简单的物理和虚拟世界的数据对应，这两方面的数据都是低位数据，对于很多内部检测场景非常重要，是构建人工智能时代网络安全体系的基础。

再举个例子。做APT检测时，如果低位数据能力不足，没有终端和网络的全量数据，就会非常麻烦。因为APT是安全对抗中比较高级别的层次，数据粒度不够会直接影响溯源、分析、调查、研判和未来的取证，所以低位是非常重要的能力。

中位能力——安全体系的“心脏”

中位能力包含态势感知、安全运营、应急响应、威胁发现、安全治理等，是对海量数据的建模与分析能力，就像人的“心脏”，它不断输送血液，为人体供应氧和各种营养物质。

习近平总书记在2018年4月的全国网络安全和信息化工作会议上强

调：“加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。”

什么是“关口前移”呢？“关口前移”就是把网络安全防护的关口前移到一线。比如，“0信任”安全架构把信任的边界“关口前移”到了用户和终端，将“身份”作为新的安全边界，遵循先验证设备和用户的身份、后访问业务的原则，只有在充分的用户、设备验证和授权之后，业务资源才对用户“可见”。所有的业务资源访问必须进行加密和细粒度的动态授权访问控制。

“0信任”架构对身份管理和授权管理提出了精细化、动态化的要求，同时要求具备数据级防控安全等级的场景，主要是关键行业的特定域网，比如公安、政府、运营商、能源、医疗等行业，以及基础运营网络和国家重要信息系统的网络、国家安全等。

态势感知也是非常重要的中位能力。那么，什么是态势感知呢？

我认为，首先要建沙盘系统，摸清家底，并实现数据的可视化分析。人的肉眼是很难直接读取海量的数据符号的，安全数据的可视化技术可以帮助安全人员更加迅速而有效地分析安全问题，捕获安全线索，发现未知威胁。

在数据可视化分析的基础上，我们通过安全大数据中心，知道什么人来了，干了什么，然后用威胁情报做出决策智能审计，找出坏人坏事，最后驱动应急指挥，实施安全事件的响应和处置。

高位能力——安全体系的“大脑”

高位能力是云端威胁情报与分析能力，能对中位和低位提供支撑和决策。它就像人的“大脑”，负责复杂的思考和下达行为指令。

以威胁情报为例。传统的威胁情报往往只关注本单位的网络里发生了什么，关注如何把本单位的网络防范得像铁桶一样安全。但现在互联网上的攻击手段，很容易复制到具有相同弱点的单位，其他单位刚刚发生的网络安全事件很可能不久后在本单位也会发生。

高位能力利用低、中位反馈的数据和安全线索，产生精准的威胁情报，第一时间调整本单位的防护措施和策略，及时弥补攻击所利用的漏洞，提前化解威胁。同时，高位能力还可以结合云端的威胁情报分析成果，对APT攻击、新型木马、特种免杀木马进行规则化描述，从多维度特征还原攻击者全貌。

这三位能力是一个系统，相辅相成，低位能力不断提供数据给中、高位，产生威胁情报。反过来，中、高位的能力能解决低位能力的一些不足，并将安全能力和措施下发下去。

数据驱动安全的“三位能力”联动系统

2015年，我们在第三届中国互联网安全大会（ISC2015）上创新地提出了“数据驱动安全”这个理念。如今它已经成为安全行业的一个共识。多位院士和业内专家都认同，围墙式防护过时了，基于数据驱动的协同联动防御是安全防御的未来方向。

基于这个理念，我们认为，安全体系是高位能力、中位能力和低位能力的“三位能力”联动。高、中、低“三位能力”是描述三种能力在

层次结构体系中的位置，并不是说这三种能力有高有低。这“三位能力”互相不可替代，互相补充，协同联动：低位能力相当于一线作战联队，中位能力相当于参谋部、前线指挥部，高位能力相当于情报部、战略支援部队和战略导弹部队。

这个系统主要有以下几个特点：

▶运维数据全量记录

对各类安全产品及网络流量的运维数据进行全量记录，用以进行态势感知、异常发现以及攻击事件还原等安全分析。

▶多维数据关联分析

对不同来源、不同维度的本地安全大数据，如终端杀毒、防火墙、服务器流量、设备资产等数据进行快速汇集、深度关联，以及自动化的高级智能分析。

▶威胁情报辅助决策

将本地安全大数据与云端威胁情报中心推送的专属威胁情报相结合，实现对未知威胁与高级攻击的快速发现、精准定位和攻击溯源。

▶协同联动快速响应

根据大数据分析系统的分析结果，对政府部门、企业内网系统实现持续的安全监测、快速响应、事件调查及安全态势感知，并能够联动网络检测响应（NDR）和终端检测响应（EDR），进行快速协同响应处置。

随着安全威胁的不断演化，数据驱动安全的理念也在与时俱进。正如我在第五章中所强调的，人是安全的核心。无论是“高大上”的研判分析和追踪溯源，还是态势感知和威胁情报，都离不开人的运营，基础架构、被动防御同样需要人去做“脏活累活”。

因此，在2017年的中国互联网安全大会上，我们提出了“数据驱动安全2.0”理念，这是“数据驱动安全”技术理念经过两年实践后的创新演进。其核心理念是建立一套以人为核心的协同联动安全运营体系，用大数据让分析研判和追踪溯源的人更智能，让安全一线运维的人更加智能。通过充分利用云端能力，结合本地设备协同联动，提升研判分析、追踪溯源、响应处置和运行维护水平，全面保护网络空间安全。

第三节　漏洞的“一体化”治理之道

安全的本质是和漏洞攻击者的对抗。我们之前对漏洞的重视还停留在漏洞扫描、漏洞补丁的阶段，这是非常初级的水平。我们需要从0开始改进，因为：首先许多系统漏洞补丁存在千分之几乃至更大概率的兼容性错误。一旦碰上兼容性错误，系统故障就会产生，严重时甚至宕机。对于重要的、一刻也不能中断的在线运行系统，我们不得不为了“安全运行”而被迫放弃打补丁。其次，对放弃打补丁习以为常后，对漏洞的重视就会“挂在口、记在心、疏于行动”，以至于漏洞不清、补丁不清。

在与漏洞攻击者进行博弈的过程中，我们需要评估漏洞的优先级，对不同优先级的漏洞进行不同等级的处理，掌握漏洞的治理之道。

漏洞是有优先级的

由于漏洞本身是风险的一种，因此，信息系统的管理员需要给漏洞分优先级，以便识别风险最大的漏洞并进行对应的处置。在漏洞的治理中，最忌讳眉毛胡子一把抓，导致高优先级的漏洞和低优先级的漏洞被一视同仁地处理，这一方面增加了信息系统的维护工作量，另一方面也往往耽误了真正高优先级的漏洞的处理。

漏洞的优先级需要借助几个不同的维度来评估：基于漏洞本身的评估、基于资产的评估和基于风险的评估。

基于漏洞本身的评估方法常见于厂商提供的安全公告，如发布每个月微软例行的漏洞安全公告等。以微软为例，其每月的漏洞报告都包括以下几个信息：漏洞类型（远程代码利用、本地提权、拒绝服务等）、被利用的难度（必然、很可能、比较可能、比较不可能、很难），并基于这些信息给出一个等级（严重、重要、普通）。这种做法标记出的属性可以作为优先级的一个输入，代表了漏洞本身潜在会造成的威胁有多大。

基于资产的评估是指根据漏洞在什么系统、什么服务器、什么终端上存在而决定漏洞的优先级。例如，对于非常重要的系统比如用户中心，即使是一个信息泄露的漏洞也需要尽快修补。同理，对于关键业务系统的终端的漏洞，每月微软的关键补丁应该尽快打上。

基于风险的评估是基于某个漏洞被利用的情况来决定优先级，比如，一个漏洞如果是安全研究人员发现报告给厂商的，并没有黑客组织在实际使用，其优先级可以适度放低。若已经是在野的利用，尤其是捕获到的针对自己企业所在行业的利用，就需要被重点关注、高优先级处理。

漏洞治理的四个环节

漏洞本身是一种风险，因此漏洞管理属于风险管理的范畴，也适用于普遍的风险管理流程。针对漏洞的治理工作一般分为以下四个环节：发现、评估、修复和缓解。

▶漏洞的发现

漏洞的发现是指针对企业内部的资产进行扫描，发现其中潜在的漏洞的过程。这个过程当中需要将外部的漏洞数据库与内部的资产配置进行匹配，根据软件的版本号等信息进行“是否有漏洞”的判定。这个通常是漏洞扫描产品的工作。

针对匹配的结果，有的产品会进行攻防性的扫描确认，以便确认此漏洞是否可以利用。漏洞的发现是后续所有环节的基础，因此需要保证完整性和准确性。要想完整扫描出资产上存在的漏洞，需要完整的资产排查作为基础，并针对资产的细节进行进一步的归集，包括CPU、固件版本、虚拟化软件、操作系统、软件、驱动程序等。由于每一种资产都有可能产生漏洞，因此对于这些资产数据的归集应该越细越好。除了资产数据之外，我们还需要准确的漏洞库输入。漏洞库通常由安全厂商提供，根据系统上的软件版本进行比对是最简单也是最准确的漏洞判定方法。此外，也有部分漏洞扫描程序将攻击的POC进行无害化处理，并以此来对实际系统进行攻击，以确认是否存在漏洞，这种方式能够从利用的角度给出漏洞是否存在的证据，对于已经使用了合适的缓解手段的系统，此方式可以降低误报率。

由于漏洞多是信息系统或软件的编码引入的，因此也存在一系列的针对信息系统或软件的代码和测试环节当中进行漏洞发现的尝试。源代码漏洞是可以检测的。近些年来我们一直推动甲方在验收系统时，除了做功能性测试外，增加代码缺陷测试。这个领域被称为应用安全测试（Application Security Testing，AST），又细分为静态应用安全测试（Static Application Security Testing，SAST）、动态应用安全测试（Dynamic Application Security Testing，DAST）和交互式应用安全测试（Interactive Application Security Testing，IAST）。由于应用安全测试是一个非常大的领域，漏洞的发现只是其特性集合当中的很小一部分，

因此在这里不进行展开。

另一个需要关注的点是开源软件的漏洞管理（Open Source Vulnerability Management，OSVM）。由于现代的应用软件当中已经大量包含开源软件组件，现代的软件开发工作更像是用一系列的开源软件进行“组合”，而不是从头开发，因此几乎所有的现代软件中都包含有开源的组件或模块。这种情况会导致一旦一些被广泛使用的基础开源软件出现漏洞，影响就会非常大，如OpenSSL的心脏滴血（HeartBleed）漏洞和近日持续不断出现的Struts2漏洞等。为了应对这种威胁，我们需要一种OSVM的机制。OSVM可以识别出应用代码库或者应用程序二进制包当中所有的开源组件，并将此清单和已知的漏洞进行比较。入门级的OSVM只是根据源代码当中的声明开源信息或者动态链接库的信息进行判定，高级的OSVM则会使用源代码分析或二进制文件扫描的方式来确保识别了被静态链接或修改后的开源软件。一定程度上，OSVM可以被理解为一种更细力度的资产管理手段，将资产的细分从软件细分到了软件模块级别。

▶漏洞的评估

漏洞的评估是漏洞治理工作的核心。它是针对发现的漏洞进行优先级判定、影响面评估、并决定后续动作的过程。这个过程往往与组织的性质、业务的特点、资产的优先级等信息紧密相关。

常见的漏洞评估手段包括基于漏洞、资产和风险的优先级划分方法（前面已经描述），包括渗透测试或红蓝对抗测试。这两种测试方式都需要人的参与，因此属于安全服务的类型。

用渗透测试方法评估漏洞有捷径可走。很多黑客在公布他们发现的

漏洞时，会附带一个利用这个漏洞进行攻击的程序，以此证明自己的发现。有一种被称为“脚本小子”的人，他们不是黑客，多数甚至没有写过一行攻击代码，但却梦想用黑客行为显示自己，于是他们辛勤地在网上收集所有这些黑客编写的小程序，熟悉它的使用方法，用别人开发的程序破坏他人系统。这种扫描基于黑客组织和“脚本小子”们使用的技术来对系统进行扫描评估，因此更接近实战。其基本逻辑是除了少量APT之外，大部分的网络在黑客和“脚本小子”面前都是无差别的。只要有办法避免这种大规模自动化攻击，就可以很大程度上提升系统的安全水平。这种思路对于普通的政企单位是非常务实的选择，值得关注。

▶漏洞的修补

漏洞评估的结论一般决定了后续的动作——用什么样的手段对漏洞进行响应。通常第一个问题是针对此漏洞是否有补丁。对于有补丁的漏洞，尽快打补丁是应该最优先考虑的漏洞修复手段，只有没有补丁的漏洞（通常是0day或停服的系统）才应该考虑使用其他的方式进行漏洞的缓解。

对于Windows、Adobe等常见的系统，厂商通常都会针对安全问题提供补丁，因此大多数政企需要做的就是尽快应用补丁。对于开源系统，开源社区通常也会快速跟进漏洞报告。

较为麻烦的是自行开发的业务应用，由于业务系统的维护方并不一定一直存在，或业务系统维护方的安全意识不足，可能不知道或不愿意针对系统进行修改，这就需要甲方的安全团队对业务部门和业务系统的供应商进行响应管理，帮助他们制定漏洞响应规范和流程。

▶漏洞的缓解

常见的漏洞缓解方案包括虚拟补丁、热补丁、利用缓解（Exploit Mitigation）等。虚拟补丁通常针对网络级的漏洞攻击，如Web、远程桌面或文件共享，通常使用的机制是在协议层进行的数据过滤，此功能往往集成在IPS、防火墙、Web应用防护系统（WAF）等网关类设备中，而在虚拟化环境中它则可能部署在虚拟IPS当中。

热补丁运行在系统上，使用动态加载的机制，对存在漏洞的代码进行动态修改或动态替换，或在漏洞触发边界上针对相应的数据进行过滤，避免漏洞代码被触发，这种机制通常用于对于浏览器和操作系统内核的修补工作。

利用缓解是一种较为高级的技术，这种技术通过对系统上的一些核心机制的修改，针对特定的利用方法（Exploit）进行处理，避免利用成功。由于大量漏洞都是同一种类别的，虽然漏洞出现的地方不同，但漏洞的利用方法相同，因此利用缓解的机制往往可以通过一个机制缓解掉一类漏洞的威胁。这种漏洞缓解机制在360推出的XP盾甲产品当中有大量的应用，微软的增强减灾体验工具（Enhanced Mitigation Experience Toolkit，EMET）是这种方式的集大成者，在Windows 10等现代操作系统中，也有大量的类似机制直接内建其中。

现在有一种较新的技术称为运行时应用自我保护（Runtime Application Self Protection，RASP），可以在应用系统的运行时（如PHP解释器、Java解释器、.NET容器等）增加相应的防护手段，对恶意的应用行为进行分析和拦截。这种方式针对类似Struts2的漏洞、PHP代码当中的注入漏洞等具有高效的防护效果，从分类上可以划归为漏洞缓解技术。这种技术最近几年发展较为快速，值得重点关注。

需要强调的是，漏洞响应究竟使用修复方案还是缓解方案，需要根

据系统的具体情况决定。通常官方发布修复补丁时，我们应该尽量尽快使用修复方案，但如果信息系统存在维护窗口问题，在无法立即使用修复方案的情况下，相应的缓解方案就变得非常重要。而这种缓解方案往往是需要事先在系统当中埋点的（如RASP、利用缓解、热补丁等都需要在系统当中埋点，虚拟补丁也需要在网络当中串联额外的设备），因此我们要在系统构建的过程中加以考虑，而不能在应急过程中使用。应急时多大程度上具备这样的机制作为储备，也是反映机构漏洞治理水平的一个重要指标。

无论是修复还是缓解，在相应的手段上线之后，都需要进行验证。验证的方法需要针对不同的漏洞针对性地制定。如果是简单的补丁，只要重新比对即可。如果是修改应用系统或应用缓解手段，则应该使用相应的利用程序（POC）进行重新的攻击验证，确保了机制的有效性。

漏洞治理的响应等级

有了漏洞的优先级划分和漏洞治理的框架体系，我们就可以针对不同优先级的漏洞进行不同等级的处理，这种等级的划分称为响应等级。

响应等级定义了针对不同类型和优先级的漏洞的具体响应过程，每个响应等级对应了一个响应过程，覆盖了漏洞治理的各个环节。不同运营等级的侧重点不同，需要人员参与的水平不同，对资源的占用也不同。它的基本原则是针对低优先级的漏洞处理使用较少的资源，对于优先级较高的漏洞处理使用较多的资源。根据流程的优先级和资源占用情况，我们将响应等级分为日常运营、重点优先、应急响应三种不同级别。

▶最低响应等级——“日常运营”

最低的响应等级是“日常运营”，即漏洞并不需要被特别关注，只要根据厂商给出的补丁信息进行例行的补丁即可。

终端上的微软、Adobe、浏览器补丁通常属于这个类别。由于这些厂商对于漏洞的处理流程已经非常成熟和稳定，对于相应的漏洞修复也有较为充分的测试，因此不需要政企网络的管理员进行过多的操作，根据厂商的要求进行补丁即可。目前，360针对此类补丁具有了非常完整的验证、测试和发布流程，且有大量的个人版用户提前对补丁推送进行“云测试”，这可作为厂商测试的重要补充，也是这种日常运营补丁流程的重要特性。

理论上补丁是需要尽快打上的，评估打补丁效率的指标一般是80％（或更高比例，但通常不是100％）的终端打上补丁需要的时间，通常称为修复时长。原则上修复时长越短越好，但是越短的修复时长需要越多的带宽储备，因此一般的企业都会在这个中间找到一个适合自己企业的平衡值，通常在一个月以内是比较健康的，超过一个月就不太健康，因为每个月的补丁如果不能在当月打完，意味着会有补丁积压的情况出现。

补丁的处理流程需要尽可能的自动化，尽量做到无人值守。要达到这个目的的关键在于以下几个方面：补丁系统的稳定性（表现为终端的可达性、下载成功率、安装成功率等）、补丁兼容性的提前测试、现场补丁的灰度测试和放量，以及流量的合理调度（以避免影响业务）。由于终端的情况复杂，补丁分发过程中可能出现多种异常情况，这种异常情况需要及时处理。对于补丁打失败的情况，我们推荐使用基于云端和AI的机制来进行自动化判定。

服务器和业务系统的打补丁工作与桌面终端有诸多不同，因此不一定能够实现完全的自动化。首先是服务器打补丁需要重启服务甚至重启系统，因此需要在维护窗口期间打补丁。其次是服务器上通常运行着业务系统，而打补丁属于业务系统变更的一种，需要严格按照业务系统的变更管理流程进行评估、测试、上线和验证。虽然如此，通过安全团队与运维团队的良好互动，服务器的补丁工作仍然可以做到日常运营级别，这需要的是运维人员实现月度规律的维护窗口和系统变更流程，更多的是管理流程问题而非技术问题。如果具备条件，安全团队只需要制定相应的日常运营的指标要求（如修复时长），而不需要在这个过程中深度参与。

作为日常运营的工作，例外管理是非常重要的。无论是桌面系统还是服务器系统，总是存在一些例外情况，包括补丁与业务系统的冲突、重点业务无法停机等。针对例外情况，安全管理团队应该将漏洞补丁无法打上的风险周知业务部门，得到业务部门的确认，并了解业务部门的整改时限。在整改完成之前的窗口期内，我们应该尽量使用缓解手段或监控手段对存在漏洞的业务系统进行重点关注。

▶第二个响应等级——“重点优先”

第二个响应等级是“重点优先”，处于这个等级的漏洞需要管理员重点关注，不能完全依赖自动化，需要在有限的时间内尽快修复。

对于可以实现远程攻击，尤其是可以远程执行代码的漏洞和不需要终端用户交互的漏洞，我们一定要把它们放入这个等级。如果外部已经出现了公开的POC攻击代码，甚至更严重的情况是漏洞利用工具包或其他恶意代码已经在使用这个漏洞（有在野利用），我们则不能把它放在这个等级，而是应该考虑放入“应急响应”等级。2017年3月发布的补丁

（修复了“永恒之蓝”漏洞）在4月份NSA网络武器库泄露之前，都是属于这个级别的，而在NSA网络武器库泄露之后，这几个漏洞补丁应该属于更高的“应急响应”级别。

处于这个级别的漏洞的修复时长应该比日常运营要短，因为相关的攻击一旦发生将很难得到遏制，但由于没有公开的POC，被攻击的可能性较低。通常建议这种漏洞的修复时长不超过2周。由于常态化的日常运营的补丁工作是按部就班的，而这类漏洞的威胁较大，因此需要安全管理人员重点关注，协调资源（如带宽）保障补丁的分发工作，提升相应的补丁在日常运营中的优先级。

针对服务器和业务系统，我们应该协调业务部门和运维部门认清工作的紧迫性，尽快完成相应的修复工作。在修复之前的窗口期，应该立即上线缓解措施。此时选择拥有较强安全响应能力的安全厂商非常重要，它们会比普通厂商发布更快速、更稳定的规避手段。站在安全厂商的角度，针对这种漏洞我们拼的是规则库运营的速度，比友商更加快速地推出缓解措施，尤其是以IPS、防火墙、WAF等提供虚拟补丁类型缓解措施的厂商。安全厂商应该尤其注重这种能力的建设。

由于微软存在MAPP计划，可以在每个月补丁发布之前与MAPP伙伴共享漏洞相关的信息，包括如何验证漏洞、如何进行缓解防护的手段，因此安全厂商应该努力加入MAPP计划，提升对于客户的响应速度。360就是中国的MAPP伙伴。

▶最高级别响应——“应急响应”

第三个响应等级是“应急响应”，是针对漏洞处理的最高级别流程。当一个漏洞不再是潜在的风险而成为实实在在的威胁的时候，我们

就应该进入这种状态。

典型的触发这种流程的条件是：这个漏洞是无须交互的远程攻击，已经有在野的恶意样本或漏洞利用工具包开始使用这个漏洞，已经有针对这个漏洞的公开POC，或者已经有政企由于这个漏洞被攻陷。由于公开的POC到实际可用的攻击手段之间往往只有数小时到一天的时间差，因此这种情况是实实在在地与漏洞赛跑。对于非远程攻击类的漏洞，由于利用门槛较高，可以不纳入这个级别，仍然作为“重点优先”级别处理。

在这种流程下，政企的网络安全管理员应该主动承担起责任，成为应急响应的指挥者。360应急响应中心会立即动员相应的安全服务工程师对客户进行通知、协助应急，甚至代替客户承担指挥工作。这种情况下以下几项工作尤其重要：

1．甲方安全管理人员得到高层领导的支持，与业务部门的协调工作，尤其是让业务部门理解工作的紧迫程度；

2．安全公司需要针对监管部门进行紧急通知，并协助监管部门推动工作；

3．安全公司需要紧急和持续地对事件进行通报，保证信息的透明性以帮助客户决策；

4．安全公司除了提供紧急的缓解措施（参考“重点优先”响应等级）之外，还需要提供相应的应急工具和方法，包括手工应急工具和自动化应急工具；

5．安全公司动员末梢安全服务人员，快速分发工具，为客户提供

服务。

回顾2017年的“永恒之蓝”，实际上从4月25日NSA网络武器库泄露开始，相应的漏洞响应等级就应该被提升到“应急响应”级别。而2017年的几次Struts2漏洞，也应该属于“应急响应”级别。

漏洞治理的关键

未经指标化的管理和运营工作是无法落地的，漏洞管理和运营也是如此。对于漏洞治理，企业的安全管理人员需要重点关注的指标包括：

1．**基础资产的覆盖度：**桌面终端、移动终端、服务器、IoT终端、网络设备等设备资产的覆盖度，以及设备资产内部细节的深度；

2．**漏洞评估的准确度：**针对漏洞的影响面、风险、威胁程度等方面的评估的准确性，尤其是影响资产的评估准确性；

3．**漏洞的修复或缓解时间差：**针对漏洞的不同级别，制定不同的漏洞修复或缓解的目标时间差，评估漏洞处置达到这个期望的比例；

4．**漏洞修复的时长：**虽然上线了缓解措施，但最终修复漏洞仍然是根治漏洞的重要工作。针对漏洞最终被修复的时长，安全团队应该对其进行评估，尤其是服务器和业务系统。应该基于不同的业务团队进行评估，将压力传递到最终的业务团队，而非由安全团队承担全部的压力。

漏洞治理中未来可能的问题和关注点

随着云、大数据、物联网和移动互联网的发展，现代的企业IT已经变得非常复杂，而且这些新技术的引入同时也带来了大量的漏洞。这些变化有可能成为漏洞运营工作中的问题，应该引起安全团队的注意。

员工个人自带设备问题，尤其是移动设备。由于移动设备的漏洞的修复过程并不如Windows这么成熟，且存在运营商、手机厂商等碎片化的问题，所以大量的移动设备是带漏洞运行的，这些设备的漏洞评估和处置工作会很难展开。安全团队需要考虑使用网络准入控制（NAC）、轻量级移动设备管理体系（MDM）结合VPN、隔离网络等方式对员工自带设备进行控制，避免带有高危漏洞的移动设备影响政企网络。

物联网设备问题，尤其是设计为家用的物联网设备。由于大量的物联网设备都是封闭的定制化系统，对于漏洞的发现、评估、修复等都缺少标准化的手段，有的物联网设备甚至无法进行漏洞修复，所以安全团队针对商用物联网设备，应该考虑制定安全准入规范，确保物联网设备厂商有能力和有机制修复漏洞。安全团队同时应该考虑物联网接入控制网关等设备，建立对物联网设备漏洞的缓解能力，避免带有漏洞的物联网设备伤害政企网络。

云的普及导致管理程序层的漏洞难以修补，往往需要停机修补。管理程序停机通常意味着大规模的客户停机，更难协调升级窗口时间，会导致修复时间拉长。大型的公有云厂商基本已经建立了针对管理程序层或客户系统层的热补丁机制，针对某些漏洞可以实现热补丁缓解，借助虚拟机漂移技术，可以实现灰度修补的机制。对于面向私有云的安全方案，我们也应该考虑提供此类能力。

公有云或行业云的使用导致漏洞的修补工作由云运营商而非自有的运维团队负责。政企的安全团队应该与云提供商约定漏洞的修补服务等

级协议（SLA）并对其进行约束，避免运营商变成漏洞修复的瓶颈。

DevOps机制（是一组过程、方法与系统的统称，用于促进开发、技术运营和质量保障部门之间的沟通、协作与整合），带来了快速开发、快速上线的互联网业务模式，对于漏洞治理提出了更加细致的要求。我们应该将漏洞治理工作融入开发过程当中，避免过晚介入导致的被动局面。

至此，我们已经从技术层面分析了应对网络安全威胁的新战术——从0开始构建数据驱动安全的“三位能力”联动系统，以及如何更好地治理漏洞。

但必须指出的是，网络安全的本质是人与人的攻防对抗。我在之前的章节中也多次明确指出，内部威胁是最大的危害。那么，在未来的网络攻防对抗中，人将发挥什么样的作用？在接下来的一章，我将详细阐述这个问题。

Chapter 9
第九章
新战法人是安全的尺度

我们说，网络安全的本质在于对抗，对抗的本质在于攻防两端能力的较量，说到底就是人与人之间的对抗。没有顶尖的一流人才，网络安全可以说是一句空话。

只有人才能最终解决人性的缺陷。在网络安全的低位、中位和高位“三位能力”系统中，人是保障网络安全最为重要的因素。

构建低位数据能力需要很多运维人员；构建中位数据能力需要很多分析师和调查员；构建高位数据能力需要很多对抗的专家，比如漏洞挖掘、情报分析领域的专家。因此，我们必须采用新战法，用精英战攻坚克难，用人海战普惠网络空间安全。

第一节　漏洞攻防是人海战

在前八章里，我们从各个角度展现了漏洞的危害。从网络攻防角度来说，漏洞是撒手锏，漏洞的挖掘需要高手。从防御角度来说，发现和修补漏洞需要经验，也是高手的角逐。

换句话说，漏洞攻防就是高手过招，人永远是网络攻防和网络安全的核心。所以，在2017年举办的中国互联网安全大会上，我们提出“万物皆变，人是安全的尺度”的观点。人，对网络安全起着决定性作用。

“数据驱动安全”不仅是致力于用大数据让设备更智能，而且更关注用大数据让分析研判和追踪溯源的人员更智能，让安全一线运维人员更加智能，提升研判分析、追踪溯源、响应处置和运行维护水平，全面保护网络空间安全。

再聪明的机器，也不能取代人

机器本身不完美，很容易受到攻击和欺骗，受到干扰。机器和人类各有优缺点，简单、技巧性的工作机器做得比较好，涉及专业、知识，人类就比较擅长。所以，再聪明的机器，也不能取代人。

这几年，人机大战有很多传奇，机器人“阿尔法狗”不断战胜围棋大师，使人工智能大热。但网络安全对抗是“不走寻常路”的智慧对抗。机器人的特长是对人类套路的模仿，靠的是超强的计算能力，而网络安全人才是实力和计谋的融合。

360在几年前就组建了机器智能自动攻防团队，目前在国际比赛上已经处于领先水平。我们也有一些自动漏洞挖掘的技术，但终究还是不能与高手专家相比，只能用于机器和机器的比赛。

近几年国内外很多公司都展示了一些用人工智能识别网络攻击的技术，但都还处于非常初级的水平。专家普遍认为，在未来相当长的一段时期内，机器还是很难超越人类。

比如，美国国防部组织的CGC网络自动攻防竞赛虽然验证了机器攻防的可能性，但其本质还是按照既定的方法和策略进行攻防，本质还是人的思维和方法的对抗，还没有迹象表明机器有能够全面超越人类黑客的能力。

再比如，机器人“阿尔法狗”之所以能战胜围棋大师，是因为它在两个星期内学习了全球围棋大师的三千万个优秀棋局，随后又通过人工智能的算法，模拟了几十亿个棋局。人类棋手一生最多下百万个棋局，与这几十亿的数据相比，输的可能性很大，但这不是机器人的胜利，而是数据的胜利。

只要有足够的样本，通过深度学习，充分的大数据确实可以产生智能，完全可以让机器自动找到所需的特征。正是这一点给我们带来了好处，但也因此产生了很多局限性：面对动态变化的环境、信息不完全或存在干扰与虚假信息时，性能就会显著下降。机器展现出不可解释和不可理解，就事论事，需要大量的训练样本，缺乏推广能力，遇到新的情况一筹莫展，很难正确处理，无人车就是一个典型的例子。

在网络安全领域更是如此，人们需要用基于特征标志的方法来检测的病毒或入侵。机器检测是没问题的，但它只能就事论事，也就是说它

只能针对已知的入侵。新的入侵只有在发生之后，机器才有可能去发现它的特征，所以它是个“事后诸葛亮”。因为这是它方法本身带来的问题，能解决的就是“知其然不知其所以然”的问题，模式识别一般属于这类问题。这种深度学习不需要专业知识，但需要大量的数据，且这些数据必须是完整的、确定的。

换句话讲，如果数据缺损，缺损的内容就学不到了。当机器学会判别若干攻击方法之后，如果攻击方法稍加变化，机器就判别不了了。如果在军事、打击犯罪等领域，仅仅依靠这样人工智能的机器做决策是会出大问题的。

人+机器，能极大提高战斗力

网络太复杂，互联网太庞大，尤其随着网络的扩大，可能被入侵的地方或被进攻的地方越来越多，漏洞也越来越多。如果单纯靠人工、靠高手手工作业，找出网络攻击就像大海捞针，是办不到的。所以，只能求助于人工智能，人+机器能极大提高战斗力。

在2017年举办的中国互联网安全大会上，多位院士和业内专家都认同，传统的检出率、误报率、漏报率的观点已经过时。以前，当网络攻击大面积发生、损害随机产生的时候，能防住99％的攻击，即使漏掉了1％，损失是可承受的。但是现在，当我们面对的是APT等高级攻击时，攻击的目标可能是毁掉一个基础设施，如水厂、电厂，或者盗窃一批关键数据，攻击发生在瞬息之间。哪怕是只漏掉万分之一，损失都是不可承受的，几个毫秒的差错就能够引起很大的危害。

以前对待误报的态度也是随意的，多数情况下都被忽略掉了，这在

现在，都是不可以的。所以，对机器拿不准的，我们必须用强大的人顶上去，用人做决定，用出色的人的努力，去争取100％的检出率和零漏报率。

但单纯靠人工、高手的手工作业，也是不可行的。我们只能借助大数据、人工智能，采用已知样本、已知攻击、已知漏洞特征等相关技术，来进行扫描、辨识和阻断网络攻击。而针对0day、1day未知漏洞，或者新的攻击方法，甚至点对点的APT攻击，则需要采用“人+机器”的方法，其中，人起到关键性作用。

我们的“数据驱动安全”理念实现的方式是“赋能”。赋能包括了两层含义：一是利用大数据赋能设备，提升设备的能力，增加设备的智能；二是赋能人，让人变得更聪明，让普通人具备安全专家的智慧和智能，像专家一样去工作。

在这个理念下，我们推出的威胁情报中心、安全运营中心、大数据分析平台、态势感知系统成为赋能中心，把人的知识驱动和机器的数据驱动结合起来，大大提升了安全运维人员的战斗力。

第二节　再先进的防护技术也不能代替运营和响应

在过去十年的网络安全防护过程中，我们经历了无数次的攻防较量、重点保障、应急处置和分析溯源的实践，积累了大量宝贵的成功经验与失败教训，也渐渐清晰地认识到，再先进的防护技术也不能代替运营和响应。

一个有效的安全体系必须具备四个基本要素：第一，数据是安全的基础与驱动力；第二，人是安全防护的核心与尺度；第三，安全运营与管理是安全最重要的手段；第四，围绕数据、人、工具、运营管理的积极防御体系是未来安全体系发展的方向。

安全运营需要更多干“脏活累活”的人

安全是个持续运营的活儿，不仅需要高大上的安全分析，更需要打补丁、配置安全策略、做基础架构、进行被动防御等干“脏活累活”的人。

在2017年5月12日“永恒之蓝”勒索蠕虫事件的处置过程中，处置措施就是要在最短的时间内给大量存在漏洞的服务器和电脑打补丁，就是这样一个简单的活儿却成了很多地区和企业的难题。

一个县级市专职负责网络安全运维的人员一般只有1～2个，他们面对的是需要打补丁的几千家机构的数万台电脑；即使人员配置相对比较

充足的大型央企，面对这样的突发状况能够干“脏活累活”的人也捉襟见肘。因此，在三天时间里，我们动员了3000多人，奔赴客户现场，协助他们快速培训打补丁的人，向全国分发了近数万份手册和操作指南，教政府机关和企业人员怎么打补丁。

目前，我国网络安全市场的运营人才面临着巨大缺口。2018年4月，网络安全与信息化产业联盟发布的报告显示，我国最近三年培养的安全专业人才仅有3万人，不足70万需求的5%。预计到2020年，需求量将达到140万人。但这部分的安全人才的培养成本是很高的，培养时间也很长，在短时间内这个缺口很难填补。

但我们现在一提到网络安全，无论是CTF还是其他各类竞赛，给学生传输的概念，都是要做“黑客”，要培养渗透、攻防、挖漏洞等这类看起来更“高大上”的技术人才。

所以，现在整体是个倒置的过程，我们需要网络安全人才，更需要做基本运营的人员。很多大专、职校的学生经过一段时间的培养就可以进入运维岗位，这也是现在网络安全行业缺失的。

用全新模式培养网络安全运营人才

为了尽快解决安全运营人员短缺问题，我们需要探索全新的网络安全人才培养模式。这个模式的本质是建立一个“管、产、学、用”一体化的协同生态平台，在这个平台上学校、企业、主管机构和用人单位可以实现从选才、培养到使用的人才培养全生命周期的紧密协同。

2018年3月，我们跟绵阳市政府合作，在绵阳建立了首个网络安全

人才培养基地。绵阳模式具体有以下几个内容：

采用订单班模式：360企业安全向合作院校提出生源需求，学校选择并提供生源，在360企业安全集团网络安全人才培养绵阳基地的学习过程采用课程置换学分机制，学生第二学期进入360企业安全上岗实践；

人才库模式：360企业安全建立线上培训教育平台，全国高校学生都可以在线上平台学习，考试通过后进入人才库，360企业安全根据用人需求从中选人培训上岗；

学分互认模式：360企业安全向院校输出课程和实验环境，学校负责教育培训，学分互认，学生认证后获得“360企业安全网络安全运营服务工程师”上岗资格。

此模式把学校的教育体系与企业基于实战的实践性强化培训结合。经过3个月，绵阳基地首批50名学员正式毕业，正式入职成为360企业安全集团网络安全运营服务工程师，被派往全国各地，服务于党政机关和企事业单位。实践证明“绵阳模式”是符合当前网络安全行业需求的、有效而成功的人才培养模式。我们期望绵阳基地继续努力，实现3年内培养5000人的战略目标。

目前我们正在复制“绵阳模式”，整合形成示范项目体系，向全国进行复制推广，共建人才培养生态体系平台，弥补目前整个行业网络安全人才培养体系的不足。

第三节　网络安全靠人民

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，对格鲁吉亚网络展开了全面的“蜂群”式网络阻瘫攻击。值得关注的是，俄罗斯为这次网络袭击进行了“全民”动员。俄罗斯网民可以从网上下载黑客工具，安装之后点击“开始攻击”按钮即可进行网络攻击。

这次网络战使用的人海战术，动员了大规模的网民群体和他们手上的电脑和网络资源，看似简单粗暴，但实现了攻击效果。

在我国，国家网络安全宣传周的主题是“网络安全为人民、网络安全靠人民”，这也同样反映了人人参与对于网络安全的重要性。在每个人的工作和生活都与网络息息相关的大背景下，每个人都不是网络安全的旁观者。

共治：发动人民群众治理网络安全问题

数字经济时代，需要有“多元共治”的新理念。随着网络“黑产”的发展壮大，仅仅靠公安机关的力量难以快速地打击“黑产”。在这样的背景下，我们需要发动人民群众的力量，用“群众路线”解决网络安全问题。

“群众路线”作为一种思维模式广泛应用在360的产品中，最典型有两个产品：一个是网购先赔，另一个是手机卫士。

▶网购先赔利用人民力量打击网络诈骗

2012年，360在全国率先推出了网购先赔服务。网购先赔的核心是通过“赔”，动员网民上报漏洞和攻击，获得海量样本，加快响应速度，大大缩短了“黑产”利用漏洞攻击的有效时间，沉重打击了黑色产业链。

我们向用户承诺，如果用户在使用了360安全卫士后仍然感染了木马病毒，或被钓鱼网站所骗，360可以先行赔付用户一定的损失。一开始我们设定的赔付限额是单次被骗最多赔1000元，单个用户一年最多赔偿36000元。后来，把单次赔付额度提升到了3000元，一年最多赔72000元。

原本我们认为，用户使用了安全卫士等产品后是不太可能中毒的。但我们没想到的是，真正使用户遭遇经济损失的，并不是什么技术特别高级的木马病毒，而是网络诈骗，甚至有被骗的用户根本就没有感染任何木马病毒或访问钓鱼网站，就主动把钱转给了骗子。

2013年5月，安徽省陈女士账户中近11万元存款几乎被全部转走，只剩下4.38元余额。这笔钱是她和男友辛苦打工三年的全部积蓄，准备结婚盖房子。被骗之后，她承受不住打击，病倒住进了医院。

经调查，陈女士遭遇的是一种新型网络诈骗：超级网银授权支付诈骗。骗子无须使用木马病毒、钓鱼网站，甚至也不需要知道受害者银行账户的密码，仅通过诱骗用户在网银上进行一个不起眼的授权操作，就能完全控制受害者账户。

由于陈女士的被骗过程没有遭遇木马病毒或钓鱼网站，所以并不符合360“网购先赔”的理赔条件。但陈女士在留言中写道：“我不知道我点

开的银行链接有危险，难道360这么专业，也不知道吗？”她的话点醒了我们：普通人很难判别出什么链接是危险的。于是，我们下定决心扩展网络安全产业的外延：向这种新型的高危网络骗术全面宣战。

我们通过安全卫士，全面拦截“超级网银授权支付链接”，并对用户提示风险。同时，我们对网民展开大规模宣传教育，通过各大媒体曝光这种骗术，提醒网民不要上当。

最后，通过与公安机关的全面配合，我们成功帮助陈女士追回了10万多元的损失。之后，我们进一步与银行等金融机构积极合作，用了大约半年时间，彻底“消灭”了这种高危网络诈骗形式。

在“网购先赔”服务经验的基础上，我们又研究了基于用户行为和场景的反诈骗技术，推出了“网购保镖”“网站照妖镜”等一系列专门针对网络诈骗的新型安全技术。在一次与公安机关的交流中，北京网安的同志对我们的工作给予了极大的肯定，并提出和我们一起做一个专门的反诈骗平台——猎网平台，把公安机关的刑侦优势和360的技术优势、平台优势结合起来，共同打击网络诈骗。

截至2018年5月，“猎网平台”已经累计接到用户各类网络诈骗举报26万多起，沉重打击了黑色产业链。同时，这也使360成为国内最大的大数据公司和拥有最大“白黑”样本的公司。

▶手机卫士利用人民力量治理骚扰电话和垃圾短信

骚扰电话和垃圾短信被称为手机上的牛皮癣，也是骗子实施网络诈骗的一个重要途径。治理骚扰电话和垃圾短信一直是网络治理的一个难题。

2013年，360手机卫士推出了一个骚扰电话标注和垃圾短信举报功能。手机用户在收到骚扰电话和垃圾短信时可以通过360手机卫士进行标注和举报。通过这样的方式我们发动8亿手机用户一起来发现、标注、举报骚扰电话和垃圾短信，然后经过后台技术手段进一步进行判别，确定拦截规则和机制，帮助所有用户进行拦截。

事实证明，这个技术含量并不高的“发明”有效遏制了电话骚扰和垃圾短信对手机用户的骚扰，这种“人人为我，我为人人”的网络安全群众路线取得了成功。2017年，360为用户拦截骚扰电话381亿次，平均每天1.1亿次；拦截垃圾短信99亿条，平均每天3000万条。如今这种治理方式已成为一种行业共同行动，在手机中广泛使用。

补天：汇聚和动员民间“白帽”黑客力量

在这场全民保卫网络安全战中，有一个我们不能忽视的力量——“白帽”黑客。

“白帽”黑客是指那些专门研究或者从事网络、计算机技术防御的人，他们通常受雇于各大公司，对产品进行模拟黑客攻击，以检测产品的可靠性。还有一些“白帽”并不受雇于大型企业，攻防成了他们的一种业余爱好或者是义务，他们希望通过黑客行为来告警一些网络或者系统漏洞，以达到警示别人的目的。

“白帽”黑客群体的天性是追求自由和无约束，这也决定了他们的组织性和群体性聚集的难度，所以除了部分服务于安全机构外，大量的“白帽”黑客散落在“民间”。动员和组织民间“白帽”黑客，利用他们的

力量来服务于网络安全，是世界各国探索的一个方向。

为了聚集“白帽”黑客的力量，360创办了补天漏洞平台，其初衷是为了尊重“白帽子”的劳动付出，让“白帽子”获得回报，同时建立实时高效的漏洞报告与响应机制，推动网络安全产业发展。

现在，“补天”已发展成为国内最大的漏洞响应平台。从数量上来看，目前在补天平台上注册的“白帽子”已达4万人，发现的漏洞数量超过25万个，注册企业达到5000余家，成为国家重要机构和企事业单位漏洞响应的保障。

补天平台最开始叫“库带计划”。当时，国内已经有一些漏洞收集平台，但是它们并不为漏洞付费，并且强制公开漏洞，让企业感到很大压力。面对这种矛盾，“补天”决定为漏洞付费，并且让企业可以自由选择是否公开漏洞。

为漏洞付费的另外一个好处是鼓励更多的“白帽子”向我们提交漏洞，并且对站在十字路口的年轻人起到了一个灯塔作用。我们都知道，凡是懂点安全技术的人，靠做“黑产”项目一年能轻轻松松赚到几百万元，甚至上千万元。

“黑产”圈子虽然充满诱惑，但也可能面临严厉的法律制裁。所以，对于那些不想触碰法律，但又想靠技术养活自己的年轻人来说，补天平台希望通过一定的奖励，在心理层面引导他们走上“白帽子”之路。

补天平台的“白帽子”增长很快，每年大约增长30％以上，其中很多都是刚毕业的大学生。活跃在补天平台上的“白帽子”不仅仅是年轻人，还有年近80岁的老人和五六年级的小学生。2015年，我们对补天“白帽子”的生存现状进行了一次调查，结果发现最年轻的“白帽子”只有12

岁，最年长的“白帽子”为78岁，最老“白帽子”与最小“白帽子”的年龄相差65岁。网络安全和黑客攻防技术正在成为全社会的关注重点。

“白帽”黑客这一群体已经成为我国网络安全的中坚力量。360互联网安全中心统计的数据显示，2017年上半年向补天平台提交漏洞的“白帽子”中，18～28岁之间的“白帽子”数量最多，约占总数的79.9％。

从年龄段来看，年轻的“90后”目前是“白帽子”的绝对主力，占“白帽子”。总量的75.2％；“80后”次之，占10.8％。值得注意的是，00后正在崛起。2016年“00后”“白帽子”的占比还只有2.6％，但仅过了一年时间，17岁及以下的“00后”“白帽子”已经占到了9.1％。

随着漏洞的收集、发现与响应越来越受到重视，类似的产品、平台和系统不断被开发出来，并逐步形成产业链。在第八章中我提到，安全众测能借用社会力量提升网络安全水平。因此，从2016年开始，“补天”就推出了漏洞众测服务，以帮助企业在第一时间发现漏洞，最大限度降低漏洞危害。

在企业授权后，“补天”会从平台中为客户量身挑选15～50名精英“白帽”，对企业进行专业漏洞检测，并提供修复方案，快速排除企业漏洞安全隐患，提升其安全防护能力。截至2017年底，补天平台一共完成了150多个众测服务项目，累计为用户发现漏洞5400多个，其中具备严重危害的漏洞占比50％以上。

从成立起，“补天”一直努力地为企业用户提供有温度、有深度的安全服务。未来，“补天”将进一步巩固和发扬民间安全力量的智慧，激励更多“白帽子”将自己的智力成果转化成生产力，以更智能的方式守护用户安全。同时，我们深入探索网络安全人才培养新模式，通过建立校企

联盟等方式，吸引更多人才进入网络安全领域。

俗话说“道高一尺，魔高一丈”，还有“出其不意，克敌制胜”，这都是在说人是制胜关键。网络安全问题不是仅靠购买和部署一批网络安全设备、产品就能解决的。就像我们要有研制武器的顶尖人才、善于排兵布阵的将军，也要有能熟练使用武器的军人和警察。

所以，未来的网络安全行业必须采取人海战术，建立“人+系统”的安全体系。我相信，海量的安全人才，加上不断发展的互联网技术，一定能营造更加安全的网络空间。

Chapter 10
第十章
新方略没有网络安全就没有国家安全

如果你认真看了前面九章的内容，我相信你现在已然能够脱口说出关于网络世界与现实世界边界消融的问题，以及关于漏洞的一系列问题。

漏洞攻击在网络社会无处不在，它出现在政治、经济、军事、民生等社会生活的核心领域，公共安全、金融安全、国防安全、政治安全等核心安全都和网络安全融为了一体。

2017年6月1日，我国开始正式实行《网络安全法》，标志着中国正式进入网络及信息安全的法制时代。随着政府高度重视网络空间安全，以及各企业单位持续加大在网络安全建设方面的投入，各政府单位及企事业部门的网络安全建设规模都在快速增长。随之而来的问题是，如何形成综合的安全监测、响应体系，以及如何在关键机构构建高效的安全运营体系。更为重要的是，政府该如何构建互联网安全监管机制。

在本章中，我将结合360企业安全深耕网络安全的实践，系统梳理我国当前在网络安全建设中重要举措，并从我们的角度给出国家网络安全建设方面的建议。

第一节　国家网络安全的外部威胁：网络恐怖主义

在本书撰写过程中，我在每一章节中几乎都会涉及很多国外网络安全的案例，这些关于漏洞被利用、修复，以及黑白之间斗争的故事构成了我国网络安全的外部生态。国家的网络安全建设需要认清当前发展面临的巨大挑战和威胁，这种威胁最直接、最大层面地来源于网络恐怖主义。

互联网成为恐怖主义的主战场

当前，恐怖主义虽然动机不变，但其模式正在改变，我们现在正面临新的陌生武器的威胁。各国多年砺炼出的反恐手段也可能无法有效应对这个武器。因为这个武器不是卡车装载炸药，不是装有沙林毒气的公文包，不是自杀式袭击，也不是行凶的砍刀。

这个武器是利用互联网发起的恐怖袭击。我们的敌人运用这个武器，在我们最脆弱的物理世界和虚拟世界汇聚的地方，寻找监管或技术上的“漏洞”，伺机向我们发起攻击。对于这一非常规但是具有毁灭性的武器，我们现有的安全情报体系、战术都可能无能为力。

2001年“9·11”恐怖袭击后，整个美国陷入恐慌，本·拉登（Hamza bin Laden）被锁定为制造恐怖袭击事件的头号嫌疑犯。美国众议院在事件发生三天后同意授权总统布什对恐怖分子使用武力。当年10月7日，时任美国总统布什宣布，美英两国已

开始对阿富汗塔利班当局军事目标和伊斯兰极端主义份子拉登在卡达的训练营进行军事打击，标志着一场以美国为首的反恐战争在全球范围内打响。

在这场持续13年的阿富汗反恐战争中，“基地”组织受到重创，其在阿富汗的训练营被美军摧毁殆尽，生存空间受到严重挤压，残余力量分别逃往其他中小国家。但“基地”组织并未被彻底摧毁，经过一段时间的蛰伏后，其力量进行了重整，尤其是伊拉克战争的爆发为“基地”组织的转圜创造了契机。

2013年4月9日，“基地”组织伊拉克分支“伊拉克伊斯兰国”（ISI）头目巴格达迪（Abu Bakral-Baghdadi）宣布与叙利亚反对派武装组织“救国阵线”合并，取消之前各自的称谓，宣布建立“伊拉克和黎凡特伊斯兰国”（ISIL），简称“伊斯兰国”。

“伊斯兰国”比“基地组织”具备更强的军事作战能力、更完备的组织领导体系、更丰厚的资金来源和更先进的通信技术。在此后的4年里，国际社会加大合作和打击力度，并取得了积极进展。2017年初以来，打击“伊斯兰国”等极端恐怖组织的斗争取得了令人鼓舞的胜利，伊拉克和叙利亚两大战场捷报频传。

然而，在“伊斯兰国”被击溃的形势下，新一波极端恐怖主义狂潮从中东向全球外溢。曾经从世界各地来到中东的“圣战分子”纷纷回流，对各国的安全和稳定构成严重的威胁。

例如，突尼斯一国就有7000多人在叙利亚、伊拉克、利比亚等地进行“圣战”，不少人陆续回国，这使当局面临严峻的挑战。在阿富汗，从中东回流的“伊斯兰国”人员已经建立了新的基地。在非洲和东南亚，博科圣地、索马里青年党、伊斯兰祈祷团、阿布萨耶夫等恐怖组织由于中东回流人员的加入也再次活跃起来。

互联网为恐怖分子提供了新手段与新平台，恐怖主义活动从物理空间延伸到网络空间。恐怖组织不再集中于某地，而是碎片化、分散化地向全球渗透，他们的行为方式和面貌也正在发生着改变。

这些渗透全球的恐怖组织结合快速发展的网络信息技术，逐步化身为比传统恐怖主义生命力、影响力、破坏力都更为惊人的网络恐怖主义。他们在互联网上发布恐怖音视频，宣扬圣战思想，利用网络招兵买马、募集资金、指挥行动。

互联网已经成为恐怖主义的主战场。在万物互联的时代，任何物体、机构、个人或者体系都有可能成为恐怖分子的攻击目标。如何在“工业4.0”时代防范网络恐怖主义，成为各国在应对非传统安全领域里所面临的新的迫切问题。

网络恐怖主义：把计算机与电信网络作为犯罪工具

网络恐怖主义（Cyber Terrorism）这个说法最早是1997年由美国加州安全情报研究院（Institute for Security and Intelligence）的巴里·C.科林（Barry C.Collin）提出的。“9·11”恐怖袭击之后，美国国会通过了反恐法案，该法案将网络恐怖主义列为新的法律术语，网络恐怖主义犯罪被纳入司法程序。

那么我们该如何定义网络恐怖主义呢？中外学界和反恐主责部门对此略有侧重不同。美国国防部对网络恐怖主义给出的定义是：“把计算机与电信设施作为犯罪工具，旨在造成社会恐慌与不安定，从而达到自

己的目的。”

我国学界认为，网络恐怖主义是基于一定政治、宗教或社会原因，以制造恐慌为目的，对社会通信网络设施进行破坏或威胁的活动。我国《反恐怖主义法》中没有明确定义网络恐怖主义，但是对恐怖主义的定义是，“通过暴力、破坏、恐吓等手段，制造社会恐慌、危害公共安全、侵犯人身财产，或者胁迫国家机关、国际组织，以实现其政治、意识形态等目的的主张和行为。”网络恐怖主义作为恐怖主义向互联网延伸的新形态，属于恐怖主义范畴。我国公安部对网络恐怖主义的认定是，把网络作为工具，散布恐怖消息、组织恐怖活动、攻击电脑程序或者信息系统等。

综上所述，网络恐怖主义应该是恐怖主义的一种形式，是恐怖主义向网络空间扩张的产物，是指非政府组织（或个人）以扰乱社会秩序为目的，有预谋地利用网络实施犯罪或者以网络为犯罪对象的恐怖行为。

网络恐怖主义活动类型：利用监管漏洞和技术漏洞

在360举办的第五届中国互联网安全大会上（ISC　2017），国家创新与发展战略研究会副会长郝叶力在观潮网络空间论坛上发表了题为“新安全威胁下的战略稳定之道”的主题演讲。她在如何定义和理解新安全威胁时首先谈到了网络恐怖袭击。

在她看来，“恐怖主义利用互联网制造全球恐慌出现新的趋势，构建了三大链条，即传播链、集资链和攻击链。所有互联网上强大、便利的技术工具，一旦为恐怖主义所利用，就产生了危害人类的恶性事

件。”

网络恐怖主义活动总体上分为两大类：第一类是利用监管方面的缺陷开展活动，第二类是利用技术漏洞开展恐怖活动。

▶利用监管方面的缺陷开展活动

恐怖分子通过互联网和社交媒体等招募人员，传播暴恐思想，传授暴恐技术，筹集恐怖活动资金，策划恐怖袭击活动，这是当前比较主流的活动类型。比如，网络社交媒体就对近年来“伊斯兰国”的迅速崛起发挥着重要作用。

一方面，“伊斯兰国”利用网络开展心理战。主要表现为发布虐杀或屠杀俘虏的视频，对对方部队造成极大的心理震慑，瓦解军心斗志，以及迫使其占领地区的平民“归顺”。他们在网上发布斩首西方人质的视频，对西方国家的反恐言论和反恐行动提出警告；他们还在网上传播极端思想，对同情者和支持者不断洗脑，招募战士，促使他们积极投身“圣战”。

另一方面，“伊斯兰国”善于利用发达的网络社交工具，打造现代化宣传新媒体，持续扩大影响力。他们在推特上注册了账号，并迅速收到良好效果。随后，其追随者和同情者们相继在脸书、优兔、汤博乐（Tumblr）等注册账号。“伊斯兰国”不仅通过社交媒体传递信息，还积极与支持者互动，加大信息传播速度和效果。在遭到部分社交媒体的封杀后，他们研发了一款APP——“黎明报喜”的阿拉伯语的手机应用，注册用户可以通过这个软件获取并转发“伊斯兰国”的最新动态。

“伊斯兰国”还会通过诸如在线文本编辑平台JustPaste等工具来总结自己的战斗情况，通过在线音频分享平台云录制（SoundCloud）公布音

频报告，并通过照片分享软件Instagram和用于智能手机之间通讯的跨平台应用程序WhatsApp来发布图片和视频内容。他们拥有一支专业高效的网络宣传队伍，其制作的视频画面精良，图片内容丰富且具有强烈的煽动性。

与此同时，在过去的十多年里，以“东伊运”为代表的“东突”恐怖势力也越来越多地运用互联网开展活动。他们借助自建网站、免费网络硬盘、境外恐怖组织网站、分享网站、社交平台以及电子书籍等途径进行音视频对外宣传，积极鼓励境内宗教极端和暴力恐怖分子组成暴力恐怖团伙，宣扬宗教极端思想、煽动民族仇恨、煽动进行圣战、传授制爆方法和技术。

此外，“伊斯兰国”还利用网络构建起完善的融资体系。他们利用提供匿名服务的新支付系统，将募集到的资金转给恐怖分子和他们的支持者，同时也利用社交媒体为自己募集资金。他们在绑架来自西方国家的人质后，会将相关视频上传到互联网上，制造强烈的社会舆论，从而勒索巨额赎金。“伊斯兰国”对人质的赎金从几万到上亿美金不等，比如曾对所绑架的2名日本人质提出高达2亿美金的赎金要求。

▶利用技术漏洞开展恐怖活动

这类恐怖活动可具体表现为四种形式。

一是向互联网中散播特定程序的病毒、木马，或是向特定设备、网络中投放病毒程序，破坏服务器、计算机等，使计算机丧失信息处理及控制功能。

二是针对电子邮件、电子商务、社交网络等人们常用的网络应用发动黑客攻击，目的是给网站运营商、公司企业造成经济损失，影响网络

应用提供商的企业信誉，动摇网民对互联网的信心，或通过入侵大型网站，释放大量虚假信息。

三是入侵政府机关或重要机构的网络，窃取机密信息或者篡改重要数据。他们利用这些信息，发动更具危害力的攻击，或者躲避政府的追踪监控，比如“斯诺登”事件后，“基地”组织武装分子改变了通信手段以避免监控，还制作了一段视频通知其他极端分子注意。

四是对关键信息基础设施发动攻击。虽然迄今为止尚未有恐怖主义组织或个人对关键信息基础设施和重要网络系统发动网络攻击、并造成重大经济损失和人员伤亡的实例，但在工业4.0时代，利用技术上的漏洞，攻击水电、通信、交通、金融、医疗、卫生、军事等关键信息基础设施并使其陷入瘫痪的网络恐怖主义威胁将变得十分现实。

美国从20世纪90年代起就开始重视对关键信息基础设施的保护，重点防止恐怖分子对关键信息基础设施发动攻击，同时最大限度地阻止恐怖主义分子获得先进的信息通信技术。美国1996年《参与和扩展的国家安全战略》指出，要尽力防止恐怖主义和大规模杀伤性武器等破坏性力量对美国的重要信息系统构成威胁。

任何系统都有漏洞，这是一个残酷的现实。恐怖分子可能攻入证券交易所破坏金融体系，攻入药厂改变药物的配方，攻入航空指挥系统让两架飞机相撞，攻入卫星、航母等关键军用设施……而且，在这一切发生前不会有预警，我们也无法阻止他们，因为我们不知道这个网络恐怖主义分子是谁、在哪里。

应对网络恐怖主义：技术、人才与合

作机制

从20世纪90年代中期以来，互联网的发展速度之快令人惊叹。1996年全球互联网用户不到4000万人，到2018年2月，全球互联网用户数已突破40亿人，这意味着当前全球76亿人口中有一半“触网”。同时，全球人口中约2/3已拥有手机，且超过半数为智能型设备，人们可以随时随地轻松地获取丰富的互联网体验。

我们对网络虚拟世界的依赖性越强，网络恐怖主义发生所能造成的危害就越大。目前，我们无法削减现实生活中对网络的依赖，也很难阻止恐怖分子获取网络恐怖活动的能力，因此，我们只能从机制、技术和人才方面着手，防范应对网络恐怖主义。

▶依靠更先进的网络安全技术

恐怖分子使用网络技术攻击的技术手段越高，发动恐怖袭击的成本就越低。防范和应对网络恐怖主义的根本在于能否掌握比恐怖分子更先进的技术。

美国和以色列都是网络强国，一直在网络安全技术的研发和应用中投入大量的人力和物力，在网络安全技术的开发和使用上居于领先地位。然而，他们的技术研发并不仅限于政府部门，而是与私营企业深度合作，鼓励企业不断创新，这在很大程度上削弱了恐怖组织发动网络恐怖袭击的能力。

我国可在此方面充分利用军民融合这个大舞台，鼓励网络安全企业积极参与科技创新，用更先进的网络安全技术应对网络恐怖主义，具体包括：①建立国家、省、市三级大数据监控网络，汇集物理世界和网络

世界的所有数据，锁定恐怖分子策划、串联、聚集和实施犯罪的过程；②破解通信协议、暗网追踪、围剿用于地下交易的比特货币，以及用人工智能方法自动识别智能分析视频、图像和语音。这些对于获取情报至关重要；③漏洞挖掘、进攻反制、远程控制是察敌制胜的撒手锏；④网络演习依法取缔网络恐怖分子的生存空间，能起到斩草除根的效果；⑤利用网络音视频系统，将城市视频监控系统、报警指挥调度、地理信息系统等无缝连接，实现同步指挥调度，充分挖掘和发挥各种系统协同作用，实现城市反恐从“事后控制”向“事前防范、事中制止”转变。

与此同时，工业互联网成为恐怖分子窥视的焦点，因此必须将工业互联网的安全上升到最高级。一方面我们要建立全天候全方位工业互联网安全态势感知能力，一个网络攻击者不会单纯地攻击某一家企业，我们要关注整个行业的网络安全状况；另一方面，我们要建立跨越物理世界、商业世界、工控网络（OT）和信息网络（IT）的一体化安全防御体系，改变割裂对待OT、IT安全的状况，提高工业互联网预警、检测、响应、追踪溯源的纵深防御能力。

此外，建立工业互联网大数据安全运营与分析中心也十分必要，对企业内工业大数据和安全大数据持续收集，建立企业的安全数据仓库，利用大数据方法发现工业生产异常，并通过数据协同、智能协同和产业协同建立安全生态和立体防御体系。

▶依靠人才

应对网络恐怖主义只靠政府是很难成功的，网络恐怖主义可以渗透到国家国防、民生和经济建设的各个领域，而且方式多种多样，所以必须依靠人才。

一方面，务必要提高民众整体的网络安全意识，对于特定行业和特定领域的人，还要增强对恐怖主义危害的认识；另一方面，务必要加强网络安全专业人才的培养，用人的专业能力将管理和技术上的漏洞因可能被恐怖分子利用而造成的损失降到最低。

例如，在2016年的美国东海岸断网事件中，360的蜜罐系统在事件发生两个月前就监测到了僵尸网络活动的苗头，我们的网络攻防人员通过伪装，诱骗犯罪分子向我们发送指令。在持续跟踪、分析这个僵尸网络的攻击特征后，360在2016年10月16日发布了研究报告，紧急向安全社区发布预警。

还可以利用人才对社交网络进行渗透，例如塑造安全可靠的网络身份，提高网络勾连的成功率，全面解决脸书、推特、领英等境外不可控大型社交媒体的数据萃取难题，构建各类成熟的情报业务模型和深度分析模型，帮助分析员从已知的种子线索拓展未知线索，辅助分析员迅速锁定高价值目标等。

▶依靠国际合作机制

虽然各国的互联网管理政策存在差异，但值得欣慰的是，国际社会在反对恐怖主义的问题上基本达成了共识，即加强交流合作，共同打击恐怖主义，这为我们防范和应对网络恐怖主义打下了良好的基础。

首先应加强全球反恐合作，支持联合国在国际反恐合作中发挥主导作用。2014年6月，第68届联合国大会进行《联合国全球反恐战略》第四次评审并通过决议，根据中国提出的修改意见，这份决议中首次写入了打击网络恐怖主义的内容。决议要求各国关注恐怖分子利用互联网等信息技术从事煽动、招募、资助或者策划恐怖活动，各国应携手打击网

络恐怖主义，决不能让互联网成为恐怖主义滋生蔓延的土壤。此举表明国际社会对网络恐怖主义危害和合作打击网络恐怖主义的共识日益广泛，也说明网络恐怖活动已经成为十分重大的世界范围的网络安全问题。只有通过在立法、司法、反恐情报的对等交流、切断恐怖犯罪资金支持渠道等多方面开展国际合作，进而为网络反恐提供支持，才能应对国际社会面临的新安全挑战。

其次是充分发挥现有多边反恐合作框架的作用。例如，在上海合作组织、二十国集团（G20）、金砖国家会议等多边机制中强化网络反恐合作，交换网络反恐情报、技术和经验。

最后，开展务实的双边网络反恐交流，增强国家间的互信，真正实现信息共享，互通有无。

第二节　我国网络安全建设的三大保卫战

外部环境是我国网络安全建设的重要参考，结合过去所遇到的网络安全问题以及形成的经验，我们国家也一直在网络安全领域加强建设。具体来讲，主要分为关键信息基础设施保护、安全态势感知能力建设和核心技术自主创新三个方面。

关键信息基础设施的保卫战

关键信息基础设施已经成为网络攻击的一个重要目标，甚至成为大国博弈、地区战争的工具。这些由国家支持的网络攻击往往会导致网络中断和系统的瘫痪，带来经济损失和生产、业务的中断，不仅影响人民的生活、企业的正常运行，严重的甚至会影响国家的政治活动。因此，对关键信息基础设施防护的认识需要提升到全新的高度。

▶关键信息基础设施保护已成法律义务：对主管部门进行责任追究

习近平总书记在2016年的“4·19”讲话中强调：“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。我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。”

2016年11月，第十二届全国人民代表大会常务委员会第二十四次会

议通过了《中华人民共和国网络安全法》（以下简称《网络安全法》）。随后，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布了《国家网络空间安全战略》（以下简称《战略》）。《网络安全法》和《战略》是国家层面对各类网络攻击的战略指导，其中都花费大量笔墨描述了关键信息基础设施的保障要求，可见其重要程度之高。

其中，《战略》从国家层面为国家关键信息基础设施下了定义：“国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施。”《战略》指出，“关键信息基础设施保护是政府、企业和全社会的共同责任”，并详细提出了关键信息基础设施保障的要务，包括采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏，这是对关键信息基础设施重要性、关键性的根本共识。

《网络安全法》在第三章第二节中规定了关键信息基础设施的运行安全，强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据强制本地存储等法律措施，确保关键信息基础设施的运行安全。

▶国内关键信息基础设施防护存在三大不足

经过多年的信息安全发展，国内关键信息基础设施的国家部门、企事业单位的安全技术支撑能力，与面对的新型安全挑战相比还存在三大不足。

我国成为APT攻击重灾区，但防护能力不足

根据360威胁情报中心的数据，我国是APT攻击的主要受害国，仅在2015-2018年，360天眼实验室和360追日团队就发现了多达38个针对我国的网络攻击组织。这些针对我国政府部门、重要企事业和科研机构的攻击已经造成了大量数据泄露。这说明，我国在防范APT攻击方面仍存在防护能力不足的问题。

关键网站漏洞修复率不足半数，且修复周期过长

根据360互联网安全中心发布的数据，通过对2016年补天平台的备案网站漏洞的抽样调查，我们发现，平均漏洞修复率仅为42.9%。即便是在能够修复漏洞的网站中，仍有近2/3的网站存在漏洞修复周期过长、修复很不及时（大于7天）的问题。

传统安全防护手段落后，彼此之间脱节，没有建成一体化态势感知、安全运营和响应中心，中位和高位能力缺失

传统的安全产品以配置安全策略规则、碰撞防护的思路为主，由于安全产品类型、厂商、型号和策略众多，在遭受威胁和攻击时，它们相互之间的识别、防护、检测、预警、响应和处置的协调能力较差，不能形成完整的安全闭环体系。

网络安全态势感知能力的保卫战

习近平总书记在2016年“4·19”网络安全和信息化工作座谈会上提出：“全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是‘谁进来了不知道、是

敌是友不知道、干了什么不知道’，长期‘潜伏’在里面，一旦有事就发作了。”

总书记将网络安全态势感知定位成网络安全最基本、最基础的工作，建立统一、高效的网络安全风险报告机制、情报共享机制是当前需要持续开发和完善的工作。

▶网络安全态势感知是网络安全的基础

《网络安全法》第五章将监测预警与应急处置工作制度化、法制化，明确国家建立网络安全监测预警和信息通报制度，建立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演练。这为建立统一、高效的网络安全风险报告机制、情报共享机制、研判处置机制提供了法律依据，为深化网络安全防护体系、实现全天候全方位感知网络安全态势提供了法律保障。

2016年12月27日，国务院全文刊发了《“十三五”国家信息化规划》，再次强调了态势感知的重要性。“十大任务”中的最后一项“健全网络安全保障体系”，提出了“全天候、全方位感知网络安全态势”。

从习总书记4·19讲话到《网络安全法》出台，再到《“十三五”国家信息化规划》，它们都强调了态势感知的重要性。我理解主要有两方面原因。

第一，传统战争易守难攻，而网络却相反，进攻容易防守难。重点网络、关键信息基础设施数量庞大，全国有数十万计，如果每个点的守军都孤军作战，瞬间就会被攻击者集中兵力各个击破。所以，要用态势感知能力提前预警和及时调兵遣将，协同联动。

第二，不断提高攻击者的成本。态势感知的情报告警机制可以让一个点被攻击暴露出的漏洞，在其余所有点上快速修复，以此循环下去，网络会越来越强壮。

▶基于多维大数据的威胁态势感知、预测和响应

建立网络安全态势感知体系的目标是全面提升识别、理解和处理威胁及各类异常的能力。通过建立态势感知体系我们可以提供网络安全持续监控能力，以及时发现各种攻击威胁；建立威胁可视化及分析能力，对威胁相关的影响范围、攻击路径、目的、手段进行快速判别以支撑有效的安全决策和响应；建立安全预警机制来完善风险控制、应急响应和整体安全防护的水平。

作为态势感知领域的先行者，360认为态势感知体现的是看见和预测安全威胁的能力，需要基于多维度大数据和多维度大数据挖掘、处理能力，同时协同安全人员和安全专家的安全能力、经验和智慧，实现对安全威胁的感知、分析和预测，然后做出响应决策。

那么在具体实践中，一个完整的态势感知体系必须具备哪些能力呢？我简要总结了以下几点。

多维态势基础数据收集、存储和处理能力

数据是态势感知的基础，所以建立态势感知体系首先要基于态势获取、理解、呈现和预测的具体目的，分析确定所需要采集的数据，并采取相应方法完成多元数据的汇聚、存储和管理。

基于安全态势感知的特定需求，使用的大数据平台应是以海量数据存储、索引、查询、统计为特点的系统，保障千亿级日志量的存储以及

数据的快速查询和统计。态势数据的收集与存储具备开放性，以便为后续更多的应用，如业务安全留有接口。

态势元素获取与持续安全监测能力

态势感知体系要提供较完善的持续安全监控能力。对于各类安全告警及内控异常，态势感知体系通过统计建模、威胁情报、事件关联分析、机器学习等方式进行二次分析，获取真实的攻击事件信息。

态势感知体系通过威胁情报对日志信息进行分析，及时发现内部已经被攻击者控制的主机与服务器；通过多层次异常分析，提供未知网络攻击发现能力；通过行为分析，发现各类内控异常行为；通过大数据分析及人机交互过程，增强安全“追踪”能力。

态势元素理解、智能分析和可视化能力

针对报警事件，态势感知体系采用多种方式进行理解、分析，然后研判、呈现必要信息来支撑决策和具体的安全响应活动。利用云威胁情报系统，对告警进行自动分析处理，获取安全威胁和攻击相关信息。

对于无法自动获取相应信息的报警，态势感知体系通过大数据可视化关联分析和人机交互方式进行调查分析，协助安全运维分析人员尽可能地还原攻击链条。同时，通过数据可视化，对不同安全场景进行态势展示，用以判断热点、重点或趋势，以辅助安全决策。

对态势预警与响应能力

态势感知体系通过自身安全事件分析、外部情报共享等方式，获得威胁相关的战略、战术情报，用以评估自身防护体系的完备性，同时指导安全防护体系建设及风险控制、应急预案的完善。

对于内部重要安全事件，态势感知体系通过回溯分析等方式，还原攻击者的技战术手法，掌握攻击者渗透时利用的内部脆弱点；通过情报关联分析，了解类似攻击团伙的技战术手法；通过情报共享或者商业情报等方式，订阅与行业相关的攻击团伙的技战术手法和攻击目的等情报。

核心技术自主创新的保卫战

2018年4月，美国商务部宣布对中兴通讯采取出口管制措施，折射出我国科技产业在底层技术上的薄弱。这次事件为我们敲响了警钟，企业一定要立足自主创新，把核心技术掌握在自己手上。尤其在网络安全领域，核心技术的自主创新是实现网络安全的重要保证。

习近平总书记在2016年“4·19”讲话中指出：“核心技术是国之重器，最关键最核心的技术要立足自主创新、自立自强。”《国家网络空间安全战略》也明确提出：“坚持创新驱动发展，积极创造有利于技术创新的政策环境，统筹资源和力量，以企业为主体，产学研用相结合，协同攻关、以点带面、整体推进，尽快在核心技术上取得突破。优化市场环境，鼓励网络安全企业做大、做强，为保障国家网络安全夯实产业基础。”

作为国内最大的网络安全企业，360经过十多年的积累和发展，自主研发和积累的安全能力和技术，在网络攻防、威胁识别、防护响应、威胁情报、态势感知、大数据、云安全和大数据安全等多个方面都处于全球领先水平。公司将继续与国内的政府主管单位、科研院校、安全行业协同合作，建立网络安全技术自主发展生态圈，加速国内关键技术自

主创新，从而提升我国的网络安全整体水平。

第三节　“一法二条例”保障国家网络安全措施落地

安全是给发展的列车装刹车和限速器，既要花钱又要降速，所以如果没有法律保障和责任追究制度，网络安全措施就无法高质量落实。

“一法二条例”为网络安全建设加装了新动力

《网络安全法》《关键信息基础设施安全保护条例（征求意见稿）》和《网络安全等级保护条例（征求意见稿）》被并称为国家网络安全措施落地的基石。

2017年6月正式施行的《网络安全法》不仅涵盖了政治、经济、军事、社会等各战略层面，也从支持与促进、运行安全、网络信息安全、监测与应急处置、法律罚则等方面给出了提纲挈领的概括性界定和规划性安排。

2017年7月，国家互联网信息办公室发布了《关键信息基础设施安全保护条例（征求意见稿）》，对关键信息基础设施的范围、各监管部门的职责、运营者的安全保护义务以及安全检测评估制度提出了更加具体、更具操作性的要求，为开展关键信息基础设施的安全保护工作提供了重要的法律支撑。

2018年6月，公安部发布了《网络安全等级保护条例（征求意见

稿）》，对网络安全等级保护的适用范围、各监管部门的职责、网络运营者的安全保护义务以及网络安全等级保护建设提出了更加具体、更具操作性的要求，为开展等级保护工作提供了重要的法律支撑。

▶网络运营者的安全责任是“发动机”

2016年，“网络运营者”这一概念在《网络安全法》中首次确立，其内涵是指网络的所有者、管理者和网络服务提供者。网络运营者的安全责任是保障国家网络安全措施落地的“发动机”。

网络运营者的安全责任在《网络安全法》第三、四、五章中有详细的描述，与此前各类相关法律法规相比，变化较大的方面包括但不限于以下几点：

第一，信息安全等级保护制度升级为网络安全等级保护制度，其主体内容预期将出现一些变化，特别是威胁情报、态势感知等概念可能会更多出现在高级别的安全保护等级规范中。

第二，在网络安全等级保护基础上，法律对网络运营者提出了一些新的要求。例如，网络日志必须留存6个月以上，确保运营业务或产品的连续性等问题。

第三，网络运营者要接受社会监督。发生网络安全事件除了需要立即启动应急预案、采取技术和其他必要措施，消除安全隐患防止危害扩大等之外，还必须及时向社会、公众发布有关警示信息。该条款体现出：法律要求网络运营者对社会、对广大网民担当企业责任。

第四，网络运营者要依法配合有关部门调查执法。重大安全事件需向主管部门报告，而且网络运营者有义务和责任为公安及国家安全机关

依法维护国家安全和侦察犯罪的活动提供技术支持和协助等。

▶监管部门通报制度是“涡轮增压机”

《网络安全法》第五章中强调了建立网络安全监测预警和信息通报制度的重要性，这是保障国家网络安全措施落地的“涡轮增压机”。具体来说，主要内容有以下几点：

第一，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。

第二，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。

第三，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。

第四，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。

第五，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。

▶追责产品服务提供者漏洞响应滞后和预留后门是“变速箱”

面对网络空间形形色色的威胁时，追责产品服务提供者的安全责任非常重要，这是保障国家网络安全措施落地的“变速箱”。

《网络安全法》第三章第二十二条明确规定：“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，应当及时告知用户并采取补救措施，并按照规定向有关主管部门报告。”

上述条款在2015年和2016年上半年的《网络安全法》前两版草案中还没有出现，但在下半年的三审稿中新增写入。这说明网络安全漏洞已经引起越来越多业内政府部门以及企业机构专家学者的关注和重视。

漏洞防护进入立法者视野，这从侧面反映出业内出现的第三方漏洞监测、通报收录平台，以及安全企业围绕漏洞修复而初步探索出的“自动扫描+人工挖掘”模式得到了业界认可。这种模式在帮助提升信息基础设施、企业网站、开放信息系统、公共服务系统的漏洞监测水平，降低潜在风险，消除漏洞威胁等方面，将发挥重要作用。

例如，补天平台发起的公益项目——公有安全应急响应中心（SRC），以及针对高安全标准需求提供的私有SRC以及“补天众测”项目，就是致力于落实法律对漏洞安全管理的相关规范原则，也给业界在如何更好地落实上述法律法规方面带来启发。

需要补充说明的是，从法治角度来讲，在现有法律规定不完善的情况下，立法从正向引导和限制边界这两个角度进一步明确“白帽子”挖掘漏洞行为。例如，从引导角度来看，法律应该真正将“白帽子”和众测平台通过适当的衡量标准纳入安全产业当中，切实给予他们合法地位。同时，对于不能触碰的关键信息基础设施和信息应用系统，也需给出较为清晰的界定，并明确“白帽子”的行为边界，让第三方漏洞收录平台及提交者在遵守法律法规时心中有数。

▶严格个人信息保护是“油门”

2016年的《网络安全法》有一个突出的亮点是，首次在国家层面开始高度重视对个人信息的保护，这是保障国家网络安全措施落地的“油门”。法案中给出了几个非常重要的原则：

第一，任何互联网企业在收集和使用公民信息时，必须遵循“合法、正当、必要”这三个原则。网络运营者不得收集与其提供的服务无关的公民个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用公民个人信息，而且网络运营者在收集、使用公民个人信息时应当公开其收集、使用规则。

第二，它间接承认了个人对自身的信息享有被遗忘权和更正权。《网络安全法》第三十七条中指出，“公民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”。

第三，在严格规范网络运营者的数据保护责任方面，法律也明确要求一旦发生泄露、毁损、丢失的情况（如网站注册用户信息遭拖库）时，网站方必须及时采取有效措施降低危害，或采取技术等手段及时补救，并且“按照规定及时告知用户并向有关主管部门报告”。

同时，在针对侵害、非法获取及出售个人信息的惩处罚责上也做出了严格的规定。例如，对于构成犯罪的交检察机关起诉，对于尚不构成犯罪的，在没收违法所得的同时还可最高罚款至一百万元。

▶日志留存推动数据驱动安全落地是“大容量油箱”

大量互联网信息安全隐患和基于此的违法犯罪行为，都是因为访问日志留存规范不健全，违法犯罪分子乘虚而入造成的，最终对用户合法权益造成了危害。日志留存推动数据驱动安全落地是保障国家网络安全措施落地的“大容量油箱”。

《网络安全法》第二十一条第三项规定：“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。”

网络日志是公安机关依法追查网络违法犯罪的重要基础和有效保证。对不法分子访问而产生的网络日志进行完整留存、准确记录和及时查询，可为下一步循线追踪，查获不法分子打下坚实基础，留下可靠依据。正因如此，《网络安全法》严格规定了网络运营者（必须）记录并留存网络日志的法定义务。

关键信息基础设施清单

世界各国都将关键信息基础设施列为重点保护对象，中国也不例外。《网络安全法》三易其稿，最终敲定了具有代表性的几大领域，即公共通信和广播电视传输等服务的基础信息服务网络、能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公共服务、电子政务作为关键信息基础设施，要求必须“在网络安全等级保护制度的基础上，实行重点保护”。

《国家网络空间安全战略》则进一步补充教育、科研、工业制造等三个领域，并将《网络安全法》中公共服务进一步具体化为医疗卫生和社会保障。此外《国家网络空间安全战略》还单独强调了重要互联网应

用系统（应当属于公共通信和信息服务中的一个组成部分），这一点也值得互联网从业者重点关注。

《关键信息基础设施安全保护条例（征求意见稿）》在《网络安全法》和《国家网络空间安全战略》的基础上，增加了环境保护以及国防科工、大型装备、化工、食品药品等科研领域的基础设施。某些方面还细化了具体内容，比如，针对“重要互联网应用系统”，上述条例中特别提到了“提供云计算、大数据和其他大型公共信息网络服务的单位”。

从安全业界实践层面看，网络安全需首要考虑的保护对象就是关键信息基础设施（CII）。国家在这一领域投入重大资金进行安全保护的同时，也在逐步建立国家级的CII清单——即纳入被保护对象的最为重要的基础网络或信息应用系统。

关键信息基础设施清单的明确和公布对安保责任主体提出了更严格和高标准的要求。《国家网络空间安全战略》提出“坚持技术与管理并重，保护与威慑并举”的原则，并且要求“着眼识别、防护、监测、预警、响应、处置等环节，建立关键信息基础设施保护制度”。

关键基础信息系统的安全保障建设，对一般性网络设施或信息应用系统的安全建设将起到示范和标杆作用，对于提高网络信息系统责任主体的安全意识、普遍提升整个互联网的安全水平具有积极效应。

新等级保护制度**2.0**的精彩之处

2018年6月27日，公安部发布关于《网络安全等级保护条例（征求意见稿）》（以下简称《保护条例》）公开征求意见的公告，旨在贯彻

落实《网络安全法》，深入推进实施国家网络安全等级保护制度。如果将之前的等保制度称为“等保1.0”，那么这次颁布的新等保制度可被形象地称为“等保2.0”。

“等保2.0”不是凭空出现的，是在网络空间与现实空间持续交织融合、网络威胁不断演变的安全形势下逐渐调整、优化、完善形成的。随着2013年“斯诺登”事件的爆发以及2014年中央网络安全与信息化领导小组的成立，网络安全开始上升为国家安全高度，《网络安全法》也于2017年开始正式实施。公安部此次发布的《网络安全等级保护条例（征求意见稿）》是对之前办法的修订和完善，结合了一些新的形势和要求。

“等保2.0”最大的特点是，总结保留“等保1.0”时代的实践经验，又最大程度吸收大数据分析、云计算、可视化等领域最新技术成果优势，从而更好地保护网络空间安全。

《保护条例》的适用范围扩大，所有网络运营者都要对相关网络开展等保工作。确立了各部门统筹协作、分工负责的监管机制，所涉及的监管部门包括中央网络安全和信息化领导机构、国家网信部门、国务院公安部门、国家保密行政管理部门、国家密码管理部门、国务院其他相关部门以及县级以上地方人民政府有关部门等。

《保护条例》根据网络在国家安全、经济建设、社会生活中的重要程度，以及遭受破坏之后的危害程度等因素，将网络分为五个安全保护等级。第十六条明确规定，“网络运营者应当在规划设计阶段确定网络的安全保护等级。意味着系统使用前必须先定级。与此同时，网络功能、服务范围、服务对象和处理的数据等发生重大变化时，需要根据情况调整定级”。

如果说《网络安全法》是维护国家网络安全和网络空间国家主权的重要制度保障，那么等保制度是贯彻落实《网络安全法》的关键支撑。等级保护的实施将和关键信息基础设施的划定相互结合，共同推进。

网络安全人才的春天

少年强，则中国强。网络强国战略之下，青少年网络安全人才培养与安全意识宣传受到空前重视。《网络安全法》总则第十三条明确规定，“国家支持研究开发有利于未成年健康成长的网络产品和服务”。

2016年9月，中央网信办起草的《未成年人网络保护条例（送审稿）》全文公布。它“鼓励中小学校通过开设校外课堂等方式指导未成年学生的监护人，帮助未成年学生养成良好上网习惯、提高网络素养”，显示了国家对未成年人网络安全的高度重视。

该条例的第二章第十条和第十二条进一步指出，“国家鼓励并支持研发、生产和推广未成年人上网保护软件”，“智能终端产品制造商在产品出厂时、智能终端产品进口商在产品销售前应当在产品上安装未成年人上网保护软件，或者为安装未成年人上网保护软件提供便利，并采用显著方式告知用户安装渠道和方法。”

在产业实践层面，已有部分社会机构或企业走在前列。共青团中央和360公司已经联合开发出适合青少年安全上网的奇未安全桌面（PC端）、奇未安全OS（移动端）等，并成功制作推出集科技和教育元素于一身的安全战车，在全国巡讲与科普网络安全知识，并且开展青少年网络安全知识竞赛活动，以及为青少年提供网络安全的实战“靶场”。

预计未来，越来越多的互联网安全企业将和教育相关部门继续探索更加新颖的模式，并借助一线安全企业的技术与应用优势，结合中小学校、科普文化基地等教育场所的自身优势，推出更加适合在中小学生中宣传安全意识的方式和方法，为打造安全成长环境、为社会储备和培养安全人才做出企业的贡献。

第四节　建立现代政企网络安全防护体系

在网络安全等级保护不断升级、网络安全制度不断完善的前提下，我们的目标应该是搭建一个现代政企网络安全防护体系。

过去，传统的政府部门、企业的安全防御体系特点是：单点防御、各自为战。它们分别从不同的厂商采购各种各样的安全产品或服务，尽管表面上“设施齐全”，但实际上不同的安全产品之间却独立运行，无法全面地把控自身网络安全问题，对于自身安全状况也处于一种完全不自知的状态。同时还普遍存在“重防御，轻响应”的问题，一旦发生安全事件往往无所适从，从而产生了很多不必要的损失。

通过前九章对漏洞的论述，我们已经知道，任何安全体系都不是无懈可击、完美无瑕的。我们要做的是基于漏洞的特征，把握漏洞的规律，搭建一个更科学、更具有规避风险能力的防护体系。

这个体系的核心思想是：建立数据驱动、协同联动、“云+端+边界”的立体纵深防御体系，以及迅捷有效的网络安全应急响应体系，及时应对各种突发的网络安全事件。

树立正确的现代网络安全观

据我观察，阻碍政府部门、企业建立现代网络安全防御体系的首要障碍，既不是成本问题，也不是技术问题，而是观念问题。这是一个很

有趣的现象，很多政府部门、企业的网络运营与管理者抱有错误的、过时的网络安全观。这主要表现在以下几个方面。

▶安全管理以免责为目标

以等保标准的实践为例，很多政府部门、企业管理者认为，只要达到了国家制定的信息安全等级保护制度要求的标准，政府部门、企业就已经实现了安全达标，如果再发生安全事件，不论事件造成多么大的损失，政府部门、企业自身都没有任何责任。

这种免责观念导致很多政府部门、企业只是为了达到等保要求而被动地采购标准指定的网络安全设备或系统，不仅对新兴安全技术与方法不闻不问，同时也不能正确有效地使用已经采购的网络安全设备或系统。最后，很多政府部门、企业采购的安全产品几乎都变成了无用的摆设，而这种情况实际上违背了等保制度设计的初衷。

▶害怕暴露问题，存在侥幸心理

很多政府部门、企业害怕安全人员对其网络系统进行安全检测，更害怕第三方报告其网络系统存在的安全漏洞。他们认为，被报告有问题就说明自己的工作没做好。这就好像一个人害怕体检一样，但不体检不等于身体就没有生病。这种错误的观念使很多政府部门、企业错过了最佳的“诊疗时机”，大量安全隐患长期存在，最后变成“要么不出事，要么出大事”。

▶关心自身损失，忽略社会责任

根据补天平台的统计，在已经被通告其系统存在安全漏洞的情况下，中国网站的平均漏洞修复率也仅为42.9%，半数以上的政府部门、

企业对自己的安全漏洞不闻不问。造成这种情况的一个重要原因就是，这些漏洞可能不会给网站自身带来直接的经济损失。比如，网站用户信息被泄露，用户可能因此面临网络诈骗等各种高危风险，但网站自身却可能没有任何直接经济损失，因此它们就对报告的漏洞睁一只眼闭一只眼。

但是，新出台的《网络安全法》给这种错误的观念敲响了警钟。其中第六十条规定，“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，政府部门、企业将有可能面临五万元以上五十万元以下罚款，直接负责的主管人员将可能面临一万元以上十万元以下罚款。”

▶缺乏动态防御与应急响应意识

时至今日，仍然有相当多的政府部门、企业管理者认为，所谓政府部门、企业安全就是给政府部门、企业的每台电脑装上杀毒软件，给政府部门、企业网络边界安装一套防火墙。这些管理者完全没有运营监控和动态防御的意识。但实际上，现代网络安全实践已经证明，任何静态部署的防御系统都不可能有效地防御现代网络攻击。

此外，传统安全观主要立足于防护，尽可能地避免安全事件的发生，而不太重视应急响应机制的建设。而新型的安全观认为，“防不住是一定的”，应当立足于一定防不住的假设来设计自己的防御、监控和运营系统。

综上所述，现代大中型政府部门、企业在网络安全管理方面需要树立这样的正确安全观：注重实际效果，主动查找问题，坚持动态监控，做好数据运维，完善应急响应，兼顾社会责任。

建立数据驱动的协同联动防御体系

在本书中，我从多个角度论述了传统的安全防御体系已经过时了。新型防御体系需要以数据为核心，调动网络系统中的各类安全产品及资源进行协同防御，从而实现对各类网络威胁特别是未知威胁的快速发现、快速响应与快速处置。

关于数据驱动的协同联动防御体系，本书的第八章第二节有详细展开，在此我不再赘述。

建立有效的网络安全应急响应体系

网络安全应急响应体系建设的不足，是现代政府部门、企业网络安全建设的主要缺陷之一。这主要是源于人们对“防不住是一定的”这一客观事实的认识不足。

政府部门、企业的网络安全应急响应体系建设是一个系统工程。在网络安全应急响应体系中，最核心的部分是网络安全应急响应小组，这一小组是应急响应处置的核心协调机构，其上还设有应急响应领导小组。

应急响应小组在处置网络安全应急事件过程中，需要进行大量的内外协调工作。其中，内部协调需要分别调动指挥与事件相关的业务线人员以及专门负责技术维护的IT技术支持人员。而外部协调的对象则主要包括政府机构、业务关联方、相关供应商及专业安全服务商等。

在“互联网+”时代，现代政府部门、企业是否能够建立一套技能专

业、反应迅速、领导有力的网络安全应急响应体系，是其网络安全综合管理水平的重要体现。

专业的安全服务是保障安全的关键

需要特别指出的是，即便政府部门和企业采购了世界上最先进的全套网络安全产品，并且建立了完善的网络安全应急响应体系，也未必能胜任政府部门、企业的网络安全日常运维与管理工作。因为这些政府部门、企业在采购安全产品时，很可能忽略了一项最具商业价值的内容——“安全服务”。

在国内政府部门、企业的安全采购过程中，他们往往能够接受为软硬件安全产品买单，却普遍不愿意为安全服务买单。甚至很多政府部门、企业认为，安全服务本应该就是安全产品的售后服务，应该是无偿的。

但无论是从运营成本还是商业价值来看，安全服务都要比安全产品高得多。这就好比是再豪华的汽车，如果没有司机开也不过是废铁一堆。由于安全人才全球性的极度短缺，在网络安全领域，好的司机比好的汽车难找得多，这也就使得安全服务的成本事实上要远大于安全产品的研发成本。对于政府部门、企业安全服务商来说，安全服务的质量和水平才是服务商实力差距和价值高低的根本体现。

所以，政府部门、企业在选择安全服务商时，不应该只看中其产品的功能和报价，而更应该把关注的焦点放在服务商专家队伍技能水平和服务水平上。选择一支优秀的安全服务队伍，才是保障政府部门、企业网络安全的关键。

反之，如果政府部门、企业在安全采购过程中轻视安全服务，则必然导致安全服务质量的大幅下降，同时企业采购的各类安全产品的使用价值也将大打折扣。

“天之道，损有余而补不足。”书写至此，关于漏洞的故事即将在我的笔下结束。但在现实中，对抗漏洞的战争必将是一场持久战，如果你要问时限，我的回答是：只要存在网络，漏洞便会永无止境；只要网络与物理世界的边界愈发消亡，这场战役就永远不会停歇。

“孰能有余以奉天下。”在这场关乎我们生存和安危的战争中，需要你、我、他每一个社会主体都能够积极参与保护国家网络安全，共同应对一项项挑战与危机。唯有如此，我们才能终将胜利。我将带领360企业安全集团，坚持初心，继续深耕，为保卫国家网络安全而奋斗，为维护人民群众利益而努力。

参考文献

1．解读CPU漏洞：熔断和幽灵．雷锋网．2018-01-08

https://www.leiphone.com/news/201801/TIV0ThWMtqMsyM3b.htr

2．OpenSSL曝重大漏洞　全球互联网心脏出血．中国青年网.2014-04-10

http://news.youth.cn/jsxw/201404/t20140410_5002492.htm

3．新加坡遭网络攻击　李显龙：全面加强相关防备和程序．中国新闻网．2018-07-21

http://www.chinanews.com/gj/2018/07-21/8574761.shtml

4．FTC对脸书进行非公开调查　最高处罚7.1万亿美元．新浪科技．2018-04-10

http://tech.sina.com.cn/it/2018-04-10/doc-ifyteqtq7331188.shtml

5．维基解密曝光CIA黑客工具：让电视“假关机”转成录音模式．参考消息网.2017-03-08

http://www.cankaoxiaoxi.com/world/20170308/1747454.shtml

6．维基解密，被泄密的美国总统大选．三联生活周刊．2016-08-08

http://www.lifeweek.com.cn/2016/0808/47982.shtml

7．墨西哥多家银行巨款神秘消失或遭“黑客”窃取．新华网．2018-05-16

http://www.xinhuanet.com/world/2018-05/16/c_129872969.htm

8．加拿大两家银行遭黑客攻击，被索要一百万美元XRP币．36kr．2018-05-31

http://36kr.com/p/5136648.html

9．内部威胁那些事儿．Freebuf．2016-05-12

http://www.freebuf.com/news/topnews/104030.html

10．特斯拉起诉前员工盗取并泄露公司内部数据．新浪科技．2018-06-21

https://tech.sina.com.cn/it/2018-06-21/doc-ihefphqk5971851.shtml

11．解读Verizon 2018数据泄漏调查报告．CSDN．2018-05-17

https://blog.csdn.net/Secboot/article/details/80355133

12．史上最严重数据车祸：通用丰田特斯拉统统中招．新浪网．2018-07-23

http://tech.sina.com.cn/csj/2018-07-23/doc-ihftenhy6618099.shtml

13．窃取50TB机密数据的前NSA承包商计划认罪．cn　Beta.2018-

01-05

https://www.cnbeta.com/articles/tech/686241.htm

14．我国尖端武器机密遭售卖　危及国防安全必须打击.央视网.2018-04-15

http://news.cctv.com/2018/04/15/ARTIw6Sq2q0VZBLZeRPenFxi1

15．科技公司员工盗取100个比特币　北京检方：依法批捕．新浪科技．2018-03-25

http://tech.sina.com.cn/i/2018-03-25/doc-ifysqpzz2606793.shtml

16．著名黑客巴纳比离奇死亡　曾曝光心脏起搏器漏洞可遥控杀人.中国广播网．2013-07-29

http://china.cnr.cn/xwwgf/201307/t20130729_513177730.shtml

17．2017年漏洞披露大爆发．搜狐科技．018-02-22

https://www.sohu.com/a/223451594_490113

18．《2017年度安全报告——漏洞势态》．360网络安全响应中心．2018-02-02

https://cert.360.cn/report/detail?id=616c0e2391cc69a547cfd4a414eb38ef

19．《2017勒索软件威胁形势分析报告》．360互联网安全中心．2017-12-20

http://zt.360.cn/1101061855.php?
dtid=1101062360&did=490927082

20．网络攻击危害远超想象　全球经济损失超千亿美元.环球网.2017-07-18

http://finance.huanqiu.com/gjcx/2017-07/10995169.html

21．零日漏洞：震网病毒全揭秘．安全牛．2015-09-08

http://www.aqniu.com/industry/10299.html

22．博士窃取贩卖500万条公民信息．楚天都市报．2018-04-13

http://ctdsb-cnhubei-com/html/ctdsb/20180413/ctdsb3239050-html

23．“网络黑产”市场规模高达千亿．法制日报．2017-07-28

http://epaper-legaldaily-com-
cn/fzrb/content/20170728/Articel06009GN-htm

24．临沂女孩被骗学费　郁结于心离世．齐鲁晚报．2016-08-23

http://linyi-qlwb-com-cn/2016/0823/704804-shtml

25．3个月非法获利2000多万元　广西贵港警方破获一起特大网络赌博案.新华网．2017-04-29

http://m-xinhuanet-com/2017-04/29/c_1120895100-htm

26．检察机关去年受理非法集资案9500余件“e租宝”涉案近600亿．

新华网．2017-03-01

http://www-xinhuanet-com/legal/2017-03/01/c_129498787-htm

27．编造央企背景推销虚拟货币　涉案38亿元特大网络传销案开审.新华网．2018-07-21

http://www.xinhuanet.com/2018-07/21/c_1123157409.htm

28．“云联惠”网络传销案主要疑犯被依法逮捕．广州日报．2018-07-02

http://gzdaily.dayoo.com/pc/html/2018-07/02/content_95942_520623.htm

29．钱宝网坠落　百分之六七十收益背后的庞氏骗局.新京报．2018-01-03

http://www.bjnews.com.cn/finance/2018/01/03/470966.html

30．昆明首例“善心汇”特大传销组织案8人获刑．新华网．2018-06-28

http://yn.xinhuanet.com/yqhy/2018-06/28/c_137286455.htm

31．比特币平台乱象：洗钱、虚假交易、被诉操纵市场．凤凰网．2017-07-18

http://finance-ifeng-com/a/20170718/15535952_0-shtml

32．美国警方希腊逮捕俄罗斯洗钱嫌犯：用比特币洗钱超40亿美

元.澎湃新闻．2017-07-27

https://www.thepaper.cn/newsDetail_forward_1744478

33．“暗网”有多“暗”？有人说，那里是网络世界的罪恶天堂．虎嗅网．2015-10-09

https://www-huxiu-com/article/127660-html

34．美国司法部破获特大网络犯罪案：涉案人员达36人．新浪科技．2018-02-08

http://tech.sina.com.cn/i/2018-02-08/doc-ifyrmfmc0001873.shtml

35．广告有毒！大规模播放器挂马攻击预警．凤凰网．2018-04-13

http://news-ifeng-com/a/20180413/57535909_0-shtml

36．男子利用铁路购票系统非法获取60余万组用户信息获刑．新华网．2016-10-26

http://www-xinhuanet-com/legal/2016-10/26/c_1119792830-htm

37．“美国断网”案告破三名嫌疑人控制全球89万台摄像头与路由器.南方网．2017-12-15

http://kb.southcn.com/content/2017-12/15/content_179643250.htm

38．“美国断网”案件告破，FBI致谢中国安全企业．雷锋网．2017-12-15

https://www-leiphone-com/news/201712/VKJrFbIZdvyDCI7y-html

39．速览丨勒索软件“简史”．光明网．2017-05-14

http://world-gmw-cn/2017-05/14/content_24475243-htm

40．以太坊钱包MyEtherWallet遭遇DNS劫持攻击．搜狐科技．2018-04-26

http://www-sohu-com/a/229475859_115060

41．市政府遭勒索软件袭击重回纸质办公时代．安全牛．2018-04-01

http://www.aqniu.com/news-views/32530.html

42．美国海恩斯维尔遭遇勒索软件攻击　致多项城市在线生活服务中断．网易新闻．2018-03-21

http://www.sohu.com/a/225994690_100066938

43．工程师蓄意报复致供水设施网络瘫痪，工控系统安全事件层出不穷．雷锋网．2018-02-02

https://www-leiphone-com/news/201802/75b6x6TlhWXKzYip-html

44．思科SMI协议中又现漏洞美国关键基础设施已遭攻击．安全客．2018-04-08

https://www.anquanke.com/post/id/103824

45．黑客演化史：从20世纪60年代至今．安全牛．2016-08-31

http://www.aqniu.com/hack-geek/19247.html

46．电脑史上10大黑客．果壳网．2011-09-14

https://www.guokr.com/article/63490/

47．黑客与英雄们：双国战记．极客视界．2016-03-11

http://geekview.cn/g11/15763.html

48．黑客十五年：寻找被黑金毁掉的黑客精神．新浪科技．2013-07-12

http://tech.sina.com.cn/i/2013-07-12/08188532501.shtml

49．凯文·米特尼克　最黑的黑客．新京报．2013-08-04

http://epaper.bjnews.com.cn/html/2013-08/04/content_455016.htm?div=-1

50．解密“维基解密”：专揭政府和企业腐败行为．腾讯科技．2010-08-01

http://tech.qq.com/a/20100801/000067.htm

51．厄瓜多尔外长称已授予阿桑奇厄公民身份．中国新闻网．2018-01-12

http://www.chinanews.com/gj/2018/01-12/8422539.shtml

52．向警方举报切尔西·曼宁的黑客阿德里安·拉莫去世　年仅37岁．cnBeta．2018-03-17

https://www.cnbeta.com/articles/tech/707769.htm

53．天才少年乔纳森·詹姆斯　既是黑客也是红客．搜狐新闻．2018-11-04

http://www.sohu.com/a/39714375_148329

54．外媒评史上5大最著名黑客：曾侵入五角大楼．腾讯科技．2009-04-03

http://tech.qq.com/a/20090403/000284.htm

55．美网络武器库都有什么凶器　“方程式组织”全球最牛．人民网．2015-05-17

http://media.people.com.cn/n1/2017/0517/c40606-29280035.html

56．美媒揭秘国际黑客团体“匿名者”面具后面是何人．网易新闻．2012-02-08

http://news.163.com/12/0208/12/7PO6GH5700014AEE.html

57．美剧《疑犯追踪》预言棱镜门　监控无处不在．腾讯科技．2013-07-12

http://tech.qq.com/a/20130712/010022.htm

58．智能合约频遭黑客攻击，谁来背锅？华尔街见闻．2018-05-24

https://wallstreetcn.com/articles/3320080

59．国内两家省级医院遭勒索病毒攻击：索要1个比特币．搜狐科技．2018-02-24

http://www.sohu.com/a/223828089_163726

60．麦肯锡：物联网九大应用潜力无限　2025年经济价值高达11.1万亿美元．搜狐科技．2018-01-14

http://www.sohu.com/a/216581924_500627

61．工业互联网：打破智慧与机器的边界．人民网．2015-06-29

http://history.people.com.cn/n/2015/0629/c386266-27225011.html

62．2018年能源行业工业控制系统网络安全态势报告．工业互联网安全应急响应中心.2018-06-25

https://www.ics-cert.org.cn/portal/page/121/3862170dea824bcebeb515a7154ecd13.h

63．Industroyer：自震网病毒以来对工控系统的最大威胁．E安全．2017-06-14

https://www.easyaq.com/news/1029984171.shtml

64．勒索病毒再攻击欧洲多国　乌克兰：规模前所未见．中国新闻网．2017-06-28

http://www.chinanews.com/gj/2017/06-28/8263093.shtml

65．Triton在施耐德Triconex SIS控制器中利用了零日漏洞．搜狐科技．2018-02-07

http://www.sohu.com/a/221412688_507120

66．基于机器学习发起网络攻击的六种方式．安全牛．2018-02-01

http://www.aqniu.com/news-views/31367.html

67．分析1300万起案件 洛杉矶警局如何用算法预测犯罪．搜狐科技．2016-05-09

http://www.sohu.com/a/74300201_116235

68．美网络司令部升级 日裔陆军上将中曾根就任新司令．环球网．2018-05-06

http://world.huanqiu.com/exclusive/2018-05/11980482.html

69．美前情报总监：中国网络实力不及美俄仅居第6．环球网．2010-02-09

http://mil.huanqiu.com/observation/2010-02/713926.html

70．深度：为什么这仗受到全球瞩目 海湾战争开创了现代空袭新纪元．新浪军事．2016-07-09

http://mil.news.sina.com.cn/jssd/2016-07-09/doc-ifxtwiht3433718.shtml

71．美国霸霸的杀威棒抡向叙利亚：盘点“战斧”经典战例．网易新闻．2017-04-77

http://news.163.com/17/0407/14/CHE63EIO000187VE.html

72．乌克兰称电网遭遇黑客攻击，能源网络安全再次引发关注．澎湃新闻．2016-01-07

https://www-thepaper-cn/newsDetail_forward_1417952

73．深度：震网病毒的秘密．Freebuf.2013-12-03

http://www.freebuf.com/articles/system/19059.html

74．伊朗宣布将卸载首座核电站核燃料.新浪新闻．2011-02-28

http://news.sina.com.cn/w/p/2011-02-28/042422024727.shtml

75．乌克兰再次称网络攻击来自俄罗斯：“同一个黑客”.澎湃新闻.2017-07-01

https://www-thepaper-cn/newsDetail_forward_1722754

76．我们为什么会战败——伊拉克军官反思战争．中国青年报．2003-04-24

http://zqb.cyol.com/content/2003-04/24/content_653649.htm

77．打赢网络战争　以色列在行动．中国青年报．2017-07-06

http://zqb.cyol.com/html/2017-

07/06/nw.D110000zgqnb_20170706_2-11.htm

78．奥巴马：索尼本不该撤映《刺杀金正恩》.环球网.2014-12-20

http://tech.huanqiu.com/news/2014-12/5269043.html

79．美网络部队独立成军．中国军网.2017-08-20

http://www.81.cn/jfjbmap/content/2017-08/20/content_185945.htm

80．网络空间军备竞赛正愈演愈烈．新浪网．2018-06-14

http://news.sina.com.cn/o/2018-06-14/doc-ihcwpcmq6159918.shtml

81．发展网络战，各国有招数．中国军网．2015-04-17

http://www.81.cn/jfjbmap/content/2015-04/17/content_108020.htm

82．新闻分析：德国打造攻防兼备的“网络军”．新华网．2017-04-12

http://www.xinhuanet.com/2017-04/12/c_1120796671.htm

83．俄军网络战，擅长打“人民战争”．中国青年网．2016-03-11

http://zqb.cyol.com/html/2016-03/11/nw.D110000zgqnb_20160311_2-05.htm

84．俄将建立强大“网军”．科技日报．2013-07-30

http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2013-

07/30/content_215488.htm?div=-1

85．日本自卫队“网军”花8000万引入人工智能　参考美以技术．参考消息．2018-01-08

http://www.cankaoxiaoxi.com/science/20180108/2250984.shtml

86．日本组建网战部队　看虚虚实实的日本“网军”．环球网．2013-12-05

http://mil.huanqiu.com/world/2013-12/4693604.html

87．以色列决定发展网络战实力　投数亿组建网军．环球网．2012-11-03

http://world.huanqiu.com/exclusive/2012-11/3239935.html

88．网络硝烟无声　大国博弈正酣．科技日报．2014-04-01

http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2014-04/01/content_254556.htm?div=-1

89．维基解密：美国中央情报局可以入侵任何设备．新华网．2017-03-09

http://www.xinhuanet.com/world/2017-03/09/c_129505094.htm

90．美国国防部举行黑客大比武　寻找五角大楼网站漏洞．中华网．2016-06-09

https://news.china.com/international/1000/20160619/22898706.htm

91．Hackerone：漏洞众测的未来会生机勃勃．安全牛．2016-12-03

http://www.aqniu.com/news-views/14278.html

92．“白帽”黑客“攻击”新加坡国防部网络　三周抓35漏洞．环球网．2018-02-22

http://world.huanqiu.com/exclusive/2018-02/11613487.html

93．从制定战略法规到全民安全教育——澳大利亚重视网络安全．新华网．2017-04-15

http://www.xinhuanet.com/world/2017-04/15/c_1120815667.htm

94．五角大楼为检查美空军网站安全性寻找天才黑客．中国新闻网．2017-04-28

http://www.chinanews.com/gj/2017/04-28/8211386.shtml

95．特别企划丨国内外顶级漏洞赏金计划．Freebuf．2017-08-19

http://www.freebuf.com/news/144135.html

96．沈昌祥：可信计算已成为国家网络空间主权的核心技术．新浪财经．2017-12-08

http://finance.sina.com.cn/money/bank/bank_hydt/2017-12-08/doc-ifyppemf5827364.shtml

97．社交网络的便利被ISIS歪曲利用　网络恐怖袭击已成又一反恐战场．搜狐新闻．2017-01-04

https://www.sohu.com/a/123431685_465554

98．2018年DHS“网络风暴6”：重点关注制造业与交通运输行业．E安全．2017-08-21

https://www.easyaq.com/news/1543473211.shtml

99．《中华人民共和国网络安全法》．中国人大网．2016-11-07

http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

100．国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知．中国网信网．2017-07-11

http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

101．公安部关于《网络安全等级保护条例（征求意见稿）》公开征求意见的公告．中国公安部网站.2018-06-27

http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.htr

102．国务院关于印发“十三五”国家信息化规划的通知．中国政府网．2016-12-27

http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm

103．《国家网络空间安全战略》全文．中国网信网．2016-12-27

http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

104．国家互联网信息办公室关于《未成年人网络保护条例（草案征求意见稿）》公开征求意见的通知．中国网信网．2016-09-30

http://www.cac.gov.cn/2016-09/30/c_1119656665.htm

后记

从2015年组建360企业安全集团至今，我们遇到了不计其数的挑战，在此过程中，这个集体迸发出的智慧，经常让我产生把它们写出来的冲动。因此，这本书是大家集体智慧的结晶。

同时，这本书也是360企业安全集团三年创业的奋斗史，是360人面对新时代、创新新安全的纪实。

在这本书落笔付印时，由360主办的一年一度的中国互联网安全大会（ISC）即将召开。从2013年开办至今，这已经是第六届了。每年，确定ISC大会的主题都是我们最重要的任务。周鸿祎和我作为大会联席主席，谭晓生作为大会执行主席，吴云坤作为专业委员会主任，在ISC召开前几个月就开始不断深刻地思考，从“数据驱动安全”“协同联动”到“人是安全的尺度”，再到2018年的“安全从0开始”。功夫不负苦心人，ISC每年的主题都成为了安全行业的趋势和主要技术方向。在此，要特别感谢韩笑和她所带领的市场部团队为ISC所付出的努力，也特别感谢ISC各分论坛的主办机构、企业和高校。

在网络世界中，我们一直说“未知攻，焉知防”，与攻击者对抗的核心就是漏洞挖掘能力。在此特别感谢360伏尔甘团队负责人郑文彬、微软Top100安全贡献榜中排名最高的华人古河、360独角兽安全团队创始人杨卿、第一位出现在世界黑客大会上的中国女黑客黄琳、知名反黑工具“狙剑”的作者徐贵斌、代码卫士团队负责人柳本金等优秀黑客对漏洞

挖掘的不断深入研究，是他们让360的产品和能力不断提高。

说到漏洞，不得不谈“补天”，这个国内最大的漏洞响应平台聚集了民间“白帽”黑客的力量。在此感谢白健和他带领的团队，更要感谢在补天平台上注册的4万余名“白帽子”，是他们一起推动了网络安全产业的发展。

过去三年间，360企业安全集团创新提出的“数据驱动安全”，已经成为了安全行业的一个共识。这三年，全公司上下一心、争分夺秒，日以继夜地攻关克难、不断创新，才有了这个安全体系的实践和落地。我要感谢网康创始人袁沈刚，他带领的网康开创了上网行为管理这一细分领域；感谢曲晓东、何新飞、冯新秀，他们实现了网神公司超预期地融入360企业安全大家庭；还要感谢张聪领导的终端安全团队，在终端安全检测与响应系统EDR上取得了卓越成绩；王伟、吴亚东领导的边界安全团队，创新了新一代智慧防火墙；韩永刚、李虎、张卓领导的大数据安全团队，先后推出了威胁情报中心、天眼新一代威胁感知系统、态势感知与安全运营平台，对我们整个数据安全体系至关重要；刘浩领导的云计算安全团队、欧怀谷领导的Web安全团队、张翀斌领导的安服团队、梁志勇领导的行为安全团队……是他们所付出的巨大努力，创新出的产品、服务和方案构建了基于数据驱动安全的、协同联动的纵深防御体系，为大数据时代的政企网络安全提供了全新的、完整的解决方案。

我还要感谢陈洪波、付君云、何瑞、李钠、倪俊、裴智勇、陶耀东、汪列军、王清、徐贵斌、许传朝、张勇、赵晋龙、左英男（按姓氏拼音排序）等人提供的研究和编辑资料，没有他们，本书不可能面世。

最后，在本书的策划和写作过程中，得到了很多朋友和同事的大力支持，在此特别感谢同济大学国家创新发展研究院副院长李舒教授，

360企业安全集团调研室尹乃潇、周丹，经过她们的数次修改完善，本书才得以顺利完成。

悉往知未来。过往发生的事能给我们启迪，希望经过本书的梳理、总结，能让你们看到未来网络安全领域的趋势，找到解决网络安全问题的钥匙。

齐向东

2018年8月6日