科技的黑暗面

克里斯·威利兹

数字时代所带来的好处受到了数据安全风险的影响

数字技术为我们所带来的舒适性和便利性是上一代人几乎无法想象的。互联网的出现为学生和学者们节省了大量的时间，他们不必花费数个小时在图书馆乏味地查阅资料，同时互联网还实现了即时的视觉通讯以及口头和书面的实时沟通，而且由此产生的成本几乎为零。在一座陌生的城市中，人们只要使用智能手机上的全球定位系统就不会迷路，或者也可以通过这一功能找到离自己最近的星巴克。消费者可以在线购物或者在线办理银行业务，医生可以通过计算机辅助功能为患者诊断病情。这些都是数字时代的神奇所在，学者埃里克·布吕诺尔夫松（Erik Brynjolfsson）和安德鲁·麦卡菲（Andrew McAfee）将这个数字时代称为“第二次机器革命时代”，他们认为计算机现在代替人脑所做的事情与第一次工业革命时期机器生产代替手工劳动的性质相同。

但是，科技进步的过程中也存在着弊端。一些批评人士对部分大型社交媒体利用数字时代左右公众舆论的行为表示失望。还有一些批评人士对于网络欺凌和网络色情之类的问题深表担忧。现在，几乎任何的活动、电话和电子邮件都会留下数字足迹，从而被好管闲事的邻居或者干预型的政府所利用，所以有人担心这些问题可能会暴露个人隐私，危害公民自由。

虽然这些担心都是合乎情理的，但人们无法对其进行量化。然而，数字技术在某些方面的确使公司和经济发展遭受了重大的损失，至少在一定程度上降低了第二次机器革命时代的生产效率。

黑客能够控制车辆或者关闭电网。网络窃贼在窃取个人信息后会取光个人银行账户中的存款或者在网上盗刷信用卡。虽然电子邮件、手机和社交媒体为人们的沟通带来了变革，但也降低了办公室员工的生产效率，因为他们着迷于推特或者即时通信。

网络安全风险

一群以色列 8200 信号情报部队的退役军官们共同创办了一家私人网络安全公司，他们认为联网汽车将是下一个热门事物。

阿古斯网络安全有限公司（Argus Cyber Security Ltd.）副总裁尤尼·海尔布隆 (Yoni Heibronn) 说，“他们只了解了一下市场行情，然后想，好吧，路上很快就会有数百万辆联网的汽车了。”

三年后，总部位于特拉维夫市的阿古斯公司分别在德国、日本和美国设立了办事处。随着黑客控制汽车的消息——还不算由此导致的交通事故——同特斯拉汽车的自动驾驶功能相关联后，阿古斯公司的业务发展更是如日中升，公众的关注点都转向了提升汽车网络安全的问题上。

欢迎来到物联网的时代——将物体同网络相联接后可进行数据的接收和发送——这一功能已经涵盖了从医院的诊断设备到咖啡机和其他家用电器等范围。根据著名 IT 研究与顾问咨询公司高德纳咨询公司的预测，今年网络驱动的设备数量将会增长 30%，达到 64 亿美元。全球在物联网安全上的花费将上涨 24%，达到 3.48 亿美元。

互联的世界为网络罪犯提供了新的机会，他们可以将收集到的个人信息用于欺骗性的交易或者勒索软件——这是一种恶意软件，能使用户的设备死机或者对数据进行加密，然后要求用户付款后才为其提供解密密码。

昆特网络安全公司（Kount）总部位于美国爱达荷州首府博伊西，该公司的首席执行官布拉德利·威斯克尔绅（Bradley J. Wiskirchen）说，“世界互联对于诈骗者是一个新的切入点。如果黑客能够通过入侵我的打印机或者冰箱收集到我的个人信息，那么他们就无需再入侵我的电脑了。”

入侵联网的家电设备通常比较容易，原因很简单，这些家电设备基本上没有什么自带的安全防护功能。但像耐斯特实验（Nest Labs）这样的公司所生产的智能家电却是例外。耐斯特实验公司总部位于美国加利福尼亚州帕洛阿尔托市，是一家生产带有尖端网络安全功能的智能家电制造商。

计算机安全应急响应组协调中心（CERT Coordination Center）属于美国卡内基梅隆大学软件工程研究院，该中心的计算机安全隐患分析师克里斯·金（Chris King）表示，“许多其他的公司把一些开源软件随便地安装到设备上，对网络安全问题根本没有给予太多的考虑。”甚至那种能联接无线网络的“哈啰芭比”娃娃都会受到黑客的攻击。

随着网络世界的扩大，易受黑客攻击的设备名单也在加长。克里斯·金称，曾有黑客关闭了医院的诊断系统，以此勒索钱财。去年在乌克兰西部，黑客入侵了一家电网公司，导致 20 多万人停电。还有德国的黑客攻击了一家炼钢厂，使该厂的一个铸造车间遭受了巨大损失。

网络罪犯将收集到的个人信息用于欺骗性的交易或者勒索软件。

被黑客入侵的汽车更加让人感到恐怖，因为这可能会造成致命的交通事故。据高德纳公司预测，到 2020 年，全球将大约有 2.5 亿辆汽车拥有车载无线联网功能。

几乎现代汽车的一切功能——制动、转向、胎压监测、灯光照明——都是由电脑控制器控制的，这些控制器通过通讯系统或者“总线”进行相互联接，这种“总线”是人们在 30 年前发明的，当时互联网还没有出现。和汽车的许多其他设备一样，这种总线本身并不安全。

克里斯·金表示，“以前没有被设计用于联网的系统现在也联接了网络，当时的设计者并未想到现在的所有问题，所以这种系统是非常脆弱的。”

在经历了两起黑客的高调攻击事件后，汽车和零配件制造商们也开始严肃地对待网络安全问题，并加强了防范措施。

在阿古斯公司，研究人员入侵了一款名叫祖笔（Zubie）的设备。这款设备可监测车辆的性能，并通过云端向驾驶员的智能手机实时传输无线数据，同时还发送保养提醒信息和改进驾驶习惯的小帖士。入侵这款设备后，研究人员便可控制车辆的转向装置、制动功能和发动机。阿古斯公司告知祖笔公司该漏洞后，祖笔公司随后表示已对此问题进行了修复。

去年，《连线杂志》（Wired）报道称研究人员利用笔记本电脑，通过车辆仪表盘电脑控制了一台吉普切诺基。随后，克莱斯勒汽车公司宣布对 140 万辆汽车实施召回。

海尔布隆（Heilbronn）称，“如果你的汽车能联网，你就需要为其采取安全防护措施。”■

网络盗窃

马格纳斯·卡尔森（Magnus Carlsson）正坐在位于美国马里兰州贝塞斯达一条繁华街道旁的 8 层办公室里，突然他的电脑上弹出一封电子邮件。他的老板——国际财资管理专业人士协会（Association for Financial Professionals）董事长，要求他转账一笔资金。

但是，当卡尔森点击回复按钮时，在他的邮箱窗口中弹出了一条陌生的地址。卡尔森说，“我从一开始就知道这是一条典型的诈骗信息。”他很清楚：作为一名负责财务和付款事宜的经理，代表着全球行业集团的财务高管，他的工作职责之一便是提醒协会成员警惕金融欺诈信息，其中包括网络诈骗。

卡尔森将这种攻击策略描述为“企业邮件受骇”

(business email compromise)，目前这种攻击方式正在迅速获得网络犯罪分子的偏爱，网络犯罪分子通常通过模仿上级领导的邮件，要求公司员工向假冒的供应商或者债权人进行电子转账。根据针对该协会成员的一项调研显示，64% 的受访者表示曾收到过这种诈骗邮件。

网络罪犯的蓄意破坏行为会导致全球金融系统的崩塌。

全球网络诈骗问题正在不断扩大，其中涵盖了各种新奇的策略和工具——名字听起来有些邪恶——勒索软件、鱼叉式网路钓鱼、特洛伊木马，而企业邮件受骇只不过是一个小伎俩。网络罪犯变得越来越狡猾、越来越活跃和大胆。他们首先会捕捉一些知名企业和组织，包括摩根大通、英国航空、菲律宾选举委员会以及美国联邦税务局，而当这些最大型企业及组织在网络安全上投入更多资源时，网络罪犯又会将目标下移至“企业食物链”的较底层——那些安全防范措施薄弱的“猎物”身上，这样他们会更容易得手。

詹姆斯·安德鲁·路易斯（James Andrew Lewis）是华盛顿国际战略研究中心的高级副总裁，他写了很多关于网络诈骗的文章。他表示，“网络犯罪不断增涨是因为有越来越多的国家和公司都开始使用互联网，而他们所采用的网络安全措施只是最初级的，所以他们很容易成为网络罪犯的攻击目标。此外，由于各国执法情况差异极大，所以如果你是一名聪明的黑客，你就会在那些执法不严的国家生活。”

据路易斯估计，网络犯罪每年给全球造成的损失高达 5 亿多美元，超过了瑞典的 GDP。这一数值包括被盗取的现金和知识产权的价值，弥补数据泄露造成的损失以及网络犯罪对创新、贸易和经济增长所造成的损失。

对网络罪犯而言，金融企业是极具吸引力的攻击目标。今年，孟加拉国央行失窃 8100 万美元巨款的事件就证明了这一点。黑客利用银行一名员工的认证信息向纽约联邦储备银行发送了 30 多次虚假的转账要求。

对于像孟加拉国这样的国家而言，这是一笔非常大的资金损失，但监管部门担心还有更为严重的风险：网络罪犯的蓄意破坏行为会导致全球金融系统的崩塌，引发一场堪比 2007—2008 年金融危机规模的经济灾难。

“这相当于潜在拒绝了市场参与者进入我们的主要市场，”澳大利亚证券投资委员会主席格雷格·梅德柯拉夫特（Greg Medcraft）说道，“网络攻击可能会成为全球下一个黑天鹅事件。”

美国存管信托和清算公司（Depository Trust & Clearing Corporation）针对全球金融稳定的威胁进行了一次调研，结果显示多数受访者（25%）将网络犯罪列为首要威胁因素。去年这一数值高达 46%，而今年出现下降，其中部分原因是金融机构加强了对网络安全防犯的投资，同时也受到其他风险因素的影响，如亚洲经济增长放缓等。

尽管如此，监管部门也不愿冒任何风险。根据国际清算银行和国际证监会组织在 6 月份发布的指导方针显示，付款和贸易结算系统以及全球金融体系中的重要部分已采取相关方案，对网络攻击进行防范和应对，同时指定一名管理人员对计划的执行情况进行监督。

普华永道会计师事务所的一项调查显示，网络犯罪是仅次于挪用资产的第二大常见商业犯罪。虽然有 61% 的首席执行官非常担忧网络安全问题，但仅有 37% 的公司针对网络安全问题制定了应对方案。

网络犯罪分为两大类。第一类是以获取金钱为目的的网络入侵，如盗取身份证和支付卡信息。第二类是网络间谍行为，如窃取商业机密、谈判策略和产品信息等。

据赛门铁克公司（Symantec Corporation）的年度《互联网安全威胁报告》（Internet Security Threat Report）统计显示，去年被泄露的身份信息总量上涨了 23%，达到 4.29 亿。而实际数量可能会超过 5 亿，因为许多公司没有上报数据泄露问题。

昆特网络安全公司首席执行官布拉德利·威斯克尔绅（Bradley J. Wiskirchen）估计，像健康保险公司美国安森保险（Anthem Inc.）和数码公司易趣（eBay Inc.）等出现大规模的数据泄露问题，几乎相当于美国每位居民的身份信息都被泄露了。昆特网络安全公司总部位于美国爱达荷州首府博伊西，是一家提供数字化风险管理解决方案的领先型供应商。

威斯克尔绅表示，“实际上每个人都受到了影响。”盗来的信息会被在网络黑市上进行交易，现在这种网络黑市正在迅速兴起，狡猾的国际商家在网上销售他们的商品，以同世界上最优秀的零售商们进行竞争，他们向客户提供退款保证、大宗购买折扣和使用辅导等服务。

近期，由 IBM 和波耐蒙研究所（Ponemon Institute）共同对分别来自 12 个国家的 383 家公司进行了一项调查。调查结果显示，数据泄露的平均损失已经从 379 万美元上升到了 400 万美元。数据泄露最常发生在巴西和南非，而在澳大利亚和德国则较少发生。

2014 年，总部位于纽约的摩根大通遭受网络攻击，导致 8300 万名客户信息泄露，其中包括客户姓名、邮箱地址、通信地址和手机号。这是美国历史上最大的一次针对金融机构的网络攻击。虽然摩根大通并未给出数据泄露所造成的具体损失金额，但该银行宣布每年将额外投资 2.5 亿美元用于网络安全措施。

窃取知识产权所造成的损失更难以估计，但其造成的经济损失可能更大。华盛顿国际战略研究中心的路易斯表示，“盗取从涂料配方到火箭的各种知识产权都会减少创新所带来的收益。人们在经济利益的激励下去发明新的事物，但如果他们无法得到利益回报，就会转做其他的事情了。”

结果会导致对新技术投资不足，工作机会减少，造成

经济增长下降。即使一些国家可以暂时获益，但从长远来看，最终也会以失败告终，因为对偷来的技术产生依赖后将会使其无法学会如何去开发自己的技术。路易斯表示，“这样会导致全球发展变缓。”

路易斯预计，网络犯罪的总成本，其中包括窃取知识产权，平均是世界 GDP 的 0.5%。在高收入国家中，创新在经济中占据更为重要的角色，所以那些经济体的所遭受的损失可能高达 GDP 的 0.9%。对发展中经济体而言，这一数据为 0.2% 左右。所有这一切都表明，人们对网络安全服务的需求极为迫切，根据调研和市场情报分析公司——网络安全投资公司(Cybersecurity Ventures) 的预测，网络安全市场规模将从去年的 750 亿美元扩大到 2020 年的 1700 亿美元。

昆特公司的年交易量增长已达到三位数，威斯克尔绅称，“我们还没有真正抓住潜在机会，很遗憾我们处在一个高增长的行业。”■

数字干扰

劳里·沃斯（Laurie Voss）年轻时是美国硅谷的一名程序员，当时他被安排花费一个月的时间去完成一项极其枯燥、毫无成就感的工作。现在回想起当时的情景，他说，“那是一份费力不讨好的任务。那个月我在推特上花了很多时间。”

现在，沃斯自己创办了一家名为 NPM 的公司，并担任公司首席技术官。对沃斯而言，通过推特发布工作信息就像 21 世纪版的死海现象：节奏拖沓。

数字干扰及其近亲——信息过载，对人们的生产率产生了日益严重的影响。

最新的应用程序和小工具当然为人们提供了新鲜的、无法抵抗的方式，让人们去浪费时间。在全世界，坐在工作隔间里的上班族们不断收到手机、电脑和平板电脑发出的信息。随着新技术在全球的普及以及知识经济的扩散，数字干扰及其近亲——信息过载，对人们的生产率产生了日益严重的影响。

凯业必达招聘网（CareerBuilder）是一家总部位于美国芝加哥的人力资源咨询公司。根据该公司于 6 月份发布的一项调查结果显示，美国有 3/4 的雇主称由于员工受到干扰，每天要浪费掉两个多小时。

雇主们表示，最浪费时间的是玩手机和发信息，其次是上网、办公室八卦和社交媒体。这些问题最终会导致工作质量下降，降低员工士气，因为一些员工不得不弥补其他员工由于分心所造成的工作松懈和错过截止日期的问题。

内森·扎德斯（Nathan Zeldes）是一家耶路撒冷公司的顾问。他认为邮件是最浪费时间的，责怪雇主们没有限制邮件的使用。他说，一名办公室员工每天可能会收到 50 到 300 条和工作相关的信息。

扎德斯称，“你没有办法很聪明地去读邮件或者处理邮件，而且你总是不停地收到邮件。”

扎德斯引用了他在 2006 年担任计算机芯片制造商英特尔公司工程师时所做的一项研究称，无用的邮件和一些不必要的干扰使普通知识工作者每周浪费一天的时间。这样算来，对于一个拥有 5 万名员工的公司而言，每年的损失将达到近 10 亿美元。

扎德斯称，人们很难抵制邮件。由于担心错过重要的沟通信息，或者是希望给同事或老板留下深刻的印象，员工不得不随时查收并回复邮件，无论是白天还是晚上。

他说，“我把这比作囚徒困境。每个人都希望少发邮件，早点下班回家。但没有人敢做第一个吃螃蟹的人。”

格洛丽亚·马克（Gloria Mark）是一名心理学博士，执教于加利福尼亚大学欧文分校信息学院，她将人们使用邮件的行为比喻成赌博。

她说，“我将其称为拉斯维加斯现象。”老虎机玩家偶尔会赢得派彩。而希望获得另外一次派彩的可能性足以让玩家继续在老虎机前玩下去。

“无意中强化的行为是最难改掉的，”马克称。

在 2012 年的一项研究中，马克发现：在转换到下一项工作前，员工的注意力集中到计算机屏幕上的平均时间仅为 75.5 秒。而截止到去年，这一数值下降到了 47 秒。

员工和雇主们已经制定了各种策略，应对干扰和信息量过载的问题。比如，有许多人会安排在一天中固定的时间去处理邮件，而在其他时间忽略邮箱信息。

NPM 公司的沃斯说，“我花了很多时间去优化邮件的处理。”沃斯的方法就是，“无情地过滤掉”所有重复的、日常的、他无需知道或者无需处理的信息。

隔壁公司（Nextdoor）总部位于旧金山，公司专注于创建“私密的社区邻里网站”。该公司资深设计师克利夫·威廉姆斯（Cliff Williams）建议人们，“关掉所有的系统通知功能。不要让信息弹出来。”

不过，威廉姆斯承认，避免干扰是一场“长期的斗争”。

他说，“这就像是减肥一样，你的体重下降一些后又会升上来。”■

克里斯·威利兹（Chris Wellisz）是一名驻华盛顿的金融记者。