美网络安全威胁能力分析报告

360 数字安全集团 二〇二四年制

目　录

在当今日益紧张的全球地缘政治形势下，作为世界唯一超级大国的美国，将传统威慑理念引入网络安全战略领域，以网络威慑作为其追求安全利益、扩大竞争优势、重塑国际霸权的重要手段，造成了国际社会的种种动荡和不稳定。

网络威慑自 2011 年被正式引入美国网络安全战略以来，始终以战略形式贯穿美国网络空间政策的发展过程。**美国政府过度发展网络安全威胁能力，在全球推进网络威慑战略，并倒打一耙持续炒作他国网络威胁论，激化国际紧张态势。**尤其是近年美国频频利用局限性的情报和猜测拼接式的逻辑归因形成各种安全分析报告来污蔑他国政府，造成“莫须有”的网络空间对抗形势，来为自己发展网络安全威胁能力构建依据。

当前，美国正在将网络安全威胁能力更多融入现实，在军事冲突、国际纠纷和反恐等行动中使用，以达成其政治、经济、军事企图。从相关报道和曝光可以看到，这对各国发展和稳定造成了重大影响，比如针对特定国家政府制造的大规模网络舆情来实施政治攻击、针对特定国家互联网设施进行破坏或阻断而造成网络大面积中断和瘫痪、以及秘密培植高级黑客组织来对他国实施大规模持续性的网络入侵等等。

目前，美国已在全球监听、信息获取、后门植入、漏洞储备、网络武器等方面建立了一套网络安全威胁能力，成为其推行网络霸权的重要支撑：

- **全球监听**

能力一：利用海缆汇聚优势具有监控全球数据流动的能力

能力二：利用掌控全球互联网根服务器和 CA 证书的地位来干扰各国互联网公平发展的能力

- **信息获取**

能力三：利用全球销售和运营的操作系统和互联网服务具有直接获取用户敏感数据的能力

- **后门植入**

能力四：利用掌控开源软件社区优势具有实施供应链攻击的便利

能力五：利用掌控商用信息化标准和协议的优势具有调配关键产品安全性的能力

- **漏洞储备**

能力六：利用全球通用漏洞披露标准及运营机构等具有优先获取安全漏洞的条件

- **网络武器**

能力七：通过多年网络武器开发具有对他国基础设施进行攻击窃密的标准化工具

能力一：利用海缆汇聚优势具有监控全球数据流动的能力

（一） 能力的基础和构成

美国利用海缆汇聚优势具有监控全球数据流动的能力，基础在于美国是全球海缆的汇聚中心。通信海缆作为全球信息互联互通的关键基础设施，在国际通信中占据主导地位，承载着全球超95%跨国数据传输。由于IPv4的根域名服务器主要在美国，辅之Facebook、Google、亚马逊等美国互联网企业的核心地位，造就了美国的全球海底光缆中心地位。美国东西海岸分别连接欧洲和亚洲，南美的网络也多路由北美，因此太平洋和大西洋海底光缆几乎都以美国为起止点，或途经美国领土，**因此美国也成为世界流量中心，欧洲-美国、亚洲-美国、拉美-美国是国际带宽最大的三个方向，即使中东、非洲也要经欧洲转接美国。**这意味着美国可以通过海缆，对全球互联网的数据流量、信息传输、网络访问等进行监控和干扰。

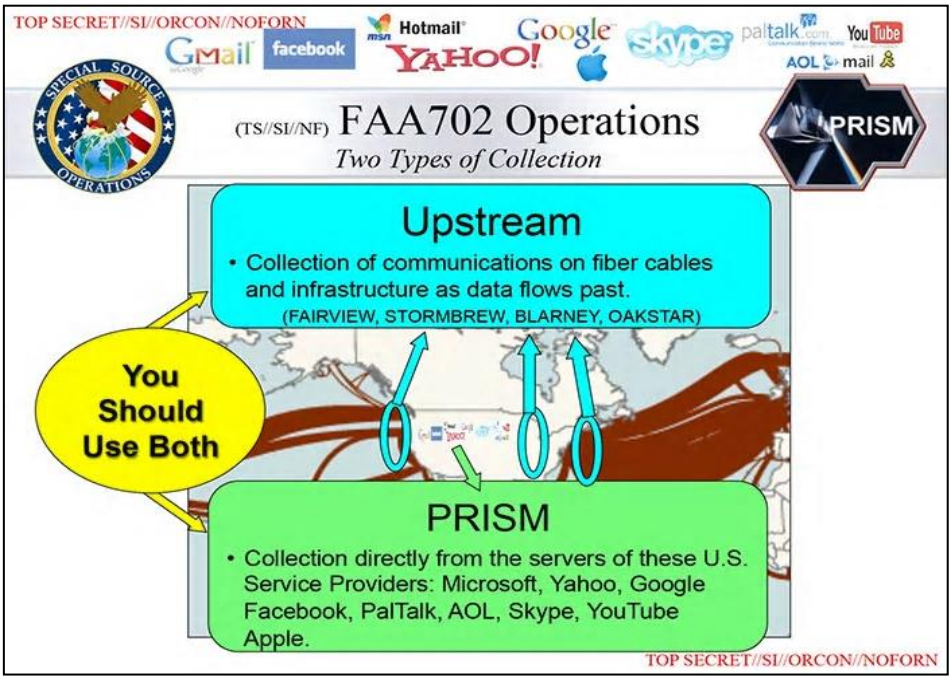
此外，美国2023年2月通过了《海底电缆管制法案》，旨在依据《出口管制改革法案》中的具体出口管制措施，限制“外国竞争对手国家”获取与海底电缆相关的产品和技术，进而巩固并增强美国在关键经济领域和电信基础设施的控制权。

（二） 能力的应用和负面影响

美国是大规模监控全球的“惯犯”，监视他国的做法可追溯到两次世界大战期间。第一次世界大战前夕，美国作为国际权力与政治舞台的新成员，在全球范围内开始进行战略情报生产，二战时，美国重建了战略情报能力，生产了大量的全球战略情报。第一次世界大战和

第二次世界大战之后，新武器、新技术的快速发展也促进了情报收集工具的发展，相应的，美国制定了 Black Chamber（黑室）和 Project SHAMROCK（三叶草）等情报收集计划，继续进行监视。此外，美国政府还提出了数个国家安全法案，包括《爱国者法案》和《国外情报监控法案》的修正案及其中的棱镜（PRISM）计划。

Upstream 计划是棱镜计划的上游项目，从“海底光缆等基础设施的收集数据，而棱镜计划则相当于“下游”项目。美国国家安全局和国防部等机构在 2003 年与美国环球电讯公司签署《网络安全协议》，与电信公司签署合作协议实则为保障“上游”项目的顺利实施。这项协议中规定，环球电讯公司需要在美国本土建立一个“网络运行中心”，美国政府官员可以在发出警告后的半小时内进入查访。据悉，环球电讯公司的海底光缆覆盖全球 4 个大洲的 27 个国家和地区。



能力二：利用掌控全球互联网根服务器和 CA 证书的地位来干扰各国互联网公平发展的能力

（一） 能力的基础和构成

美国能够长期保持对全球的网络威慑，关键在于美国控制了互联网骨干网的管理权和国际数字证书体系。

互联网是冷战期间美国为与苏联进行军事竞争而推动发展的技术，主要支持者是美国国防部。冷战结束后，互联网域名的分配和管理，始终掌握在最初编写互联网协议的 13 个根服务器的控制者手中，其中 10 个在美国。美国政府通过与国防部、CIA 等机构密切相关的公司掌控了根服务器，也强化了对互联网地址和根区的管理权、监督权。小布什总统曾宣布，美国永久保留这一权限，这意味着美国可以切断某些国家或地区的网络连接。

虽然由于 2013 年“斯诺登事件”的暴发并引起世界各国公愤，导致美国政府被迫于 2015 年正式将互联网域名和数字地址的分配权、控制权移交给 ICANN，但 ICANN 所享有的权力直到今天也并没有脱离美国政府的监管。其中，互联网 A 主根服务器的运营管理权，及其对 12 个根服务器的分发控制权，只是由 ICANN 转包给威瑞信这家美国政府的信息技术承包商，继续由其担任根区维护者。美国的单边主权，并没有受到实质触动，互联网已经成为后冷战时代美国世界权力的重要支点。

数字证书是网络空间信任体系的基石，好比是网络上的身份证或者营业执照，是网络上每一个网站、硬件、软件、芯片和文件的身份

证明。数字证书有两大功能，一个是身份认证，一个是数据加密，没有数字证书，网络上的网站、设备、软件就不可信，导致被欺骗或者数据被窃取，如果数字证书失效，就会导致重要系统不能工作，网络就会面临一场灾难。**美国通过两方面控制了国际数字证书体系，**一方面牵头成立联盟，利用谷歌牵头在国际上成立了数字证书联盟（CA/Browser Forum），成员涵盖浏览器、Web 服务器、审计、密码算法、硬件网关等相关企业。另一方面制定备案制度，设立了证书透明系统（Certificate Transparency，简称“CT”），国际上所有数字证书机构在发出任何一张数字证书之前，都需要首先在此系统备案，否则联盟会对其进行封杀。

（二） 能力的应用和负面影响

美国利用互联网骨干网的管理权发起断网突袭，造成目标网络大面积中断和瘫痪，严重破坏他国社会稳定运行。

- 2003 年期间，美国停止对伊拉克的域名解析，让伊拉克从互联网消失；
- 2004 年，美国终止对利比亚网络的解析服务，让利比亚从互联网上消失了 3 天。

美国利用对国际数字证书体系的掌控，对他国进行“卡脖子”，造成严重安全风险。

- **以贸易制裁为理由，拒绝颁发数字证书。**针对电信、交通等关键基础设施和重要信息系统，美有能力不予颁发数字证书，使得这些系统在网络上无法运行，产品不能用，网络安全防

护能力下降，引发社会动荡。目前在美国的主导下，全球数字证书机构都不允许给朝鲜、古巴、伊朗等国家发数字证书。

- **利用数字证书发动网络攻击。**通过给网络攻击软件颁发数字证书，助其潜伏进入关键系统。比如2010年破坏伊朗核工厂的震网病毒，就是获得了台湾硬件厂商瑞昱公司（RealTek）的数字签名，使其看起来是合法程序。

以上直接或间接的网络事件都展示了美国在网络空间里“单边主权”的任性和力量，也让全世界人民看到网络封锁战具有明显的国家行为特征，而未来网络霸权国家非常有可能继续利用这一手段打击现实世界的对手。

能力三：利用全球销售和运营的操作系统和互联网服务具有直接获取用户敏感数据的能力

（一） 能力的基础和构成

美国是全球软件产业和互联网长夜的领导者，掌握了许多核心技术和标准，在智能终端领域具有全球性优势，掌控了全球移动通信网络发展，对全球软件和互联网市场和创新有着巨大的影响力。

首先，美国通过开发大平台产品，垄断了操作系统和数据库等领域，利用其在软件和互联网产业的先发优势，牢牢控制了产业的高端业务，并通过制定一系列软件产品和互联网服务的标准，维持其在软件和互联网产业的领袖地位，常常举起商业制裁“大棒”，给软件和互联网产业多边治理和国际合作造成了严重阻碍。

其次，从 3G 到 5G，美国都在通过技术创新、市场竞争、政策制定来维护其在通信领域的技术优势和监听能力，通过制裁和排斥华为中兴等竞争对手，对全球 5G 供应商和市场进行干预和破坏，以维护其竞争优势。

最后，美国在智能终端领域具有全球性优势，主要体现在以下几个方面：一是硬件方面，美国拥有多家世界领先的移动终端芯片企业，如高通、博通、英伟达、苹果等，可以提供从基带芯片到射频芯片到应用处理器到图形处理器等各种芯片的解决方案。二是终端操作系统方面，美国的终端操作系统 iOS 和 Android 占据的全球智能终端市场的大部分份额。三是 5G 网络方面，美国是世界上首批商用 5G 的国家之一，通过频谱拍卖、政策支持、技术演进等方式，不断推动 5G 网络的发展，为智能终端提供更高的带宽、更低的时延、更多的应用场景。四是终端应用方面，美国拥有全球最多的知名互联网企业、社交媒体平台、电子商务网站、视频流媒体服务等，为终端用户提供丰富的内容和服务。在这些优势的基础上，美国在全球拥有最大的智能终端用户群体。

上述优势为美国通过全球销售和运营的操作系统和互联网服务来获取用户敏感数据奠定了基础，而在实施层面，美国基于这些优势构筑了以下情报获取手段：

- **通过互联网服务供应商收集情报。**据斯诺登曝光，美国国安局（NSA）和联邦调查局通过“棱镜”计划可直接接入 9 家美国互联网公司中心服务器，挖掘数据以搜集情报。微软、雅

虎、谷歌、Facebook、PalTalk、美国在线、Skype、YouTube、苹果等美国互联网公司均参与了这一计划，并在不同程度上与 NSA 合作，有的提供了直接的后门接入，有的提供了加密密钥，有的提供了特定的数据请求。可见，美国通过 Intel、微软、苹果、谷歌等互联网巨头构建了全球大数据和情报收集系统。

- **通过电话监听手段收集情报。**目前已曝光的手段包括：一是借助移动运营商或者其他终端，通过植入软件、截获通话信号等方式，侵入用户的信息通信通道截取信息。全球最大的手机 SIM 卡生产商金雅拓(Gemalto)就曾表示，美英情报机构很有可能入侵了该公司的网络，以便监听全球移动电话通信。二是采取建立假基站的方式，骗取用户终端自动接入，进而获取通话信息。三是美国在全球大约 80 个地点的驻外使领馆设有秘密监听站，窃听所在地区高官通信信息，而 NSA 利用这些监听站可以收集、解析和记录当地政府工作区上空穿梭往来的电子通讯信号。
- **通过在移动终端产业的软硬件产品中进行“埋雷”，实现对供应链企业的网络渗透和情报收集。**例如，“维基解密”显示，中央情报局(CIA)从 2008 年开始就派人渗透至苹果供应链，通过其供应链渠道将特定恶意软件安装到苹果手机中，实现对 IOS 设备的监控。

（二） 能力的应用和负面影响

9·11 事件之后，**美国政府通过的法律允许国安局开展大规模的监控，几乎可以为所欲为、不加甄别的监控别人。**斯诺登曾披露了一份美国国家安全局(NSA)的绝密文件《信号情报任务战略规划(2008-2013)》，由 NSA 组织 250 多个单位共同参与完成，目的是提高信号情报重点任务的性能，并将情报及时地转化为重大的国家成果。另一份绝密文件《信号情报战略（2012-2016)》旨在“确保信号情报为全面提升美国国家安全利益提供决定性的优势”。美国开展了大量的信号情报获取项目和计划，以实现其“监听一切”的目的。**这类项目或计划多由 NSA 负责具体实施，涵盖了网络、卫星、电话等多种信号情报源，共同支撑起了 NSA 强大的全球信号情报获取能力。**

- **“棱镜”（PRISM）计划**

棱镜计划，内部编号 US-984N，是从世界上各大互联网公司的服务器上搜集信息的大规模监控计划。“棱镜”是明确且特定的外国目标的通信信息收集计划 Error! Reference source not found.，“棱镜”计划每年总共收集了约 2.27 亿次互联网通信，为有关反情报、恐怖主义和武器扩散的报告提供了数据来源。美国国家安全局分析师每年撰写超过 2 万份基于 PRISM 数据的报告，约占该机构所有情报报告的 15%。NSA 通过“棱镜”计划，可以在不经过法院审批的情况下，直接从美国互联网公司的服务器上获取用户的网络通信内容和元数据，包括用户的身份、位置、联系人、时间、时长、频率等。NSA 还可以利用“棱镜”计划，对用户的网络行为进行分析和挖掘，识别出潜在的威胁和目标，进行进一步的监视和追踪。

“棱镜”计划的揭露，引发了全球的关注和抗议，被认为是美国对全球网络空间的侵犯和控制，损害了全球用户的隐私权和人权，破坏了全球网络空间的安全和信任，威胁了全球网络空间的公平和开放。美国互联网公司因为参与“棱镜”计划，遭到了全球用户的质疑和抵制，损失了市场信誉，面临了法律诉讼和监管压力。

“棱镜门”丑闻令美国的欧洲盟友大为震惊。时任欧盟外交与安全政策高级代表阿什顿要求美方就监听事件立即进行澄清。时任法国总统奥朗德要求美国立即停止监听行为。德国媒体披露，时任德国总理默克尔当时已被美国情报机构监听长达十几年，引发德国强烈不满。

- **MUSCULAR 项目**

MUSCULAR 项目（DS-200B）是美国国家安全局（NSA）在海外窃听谷歌和雅虎未加密的内部网络数据的一个搜集项目。项目始于 2009 年 7 月，是英国政府通信总部（GCHQ）和美国国家安全局（NSA）联合运营的全球监视计划。据华盛顿邮报报道，MUSCULARR 收集的数据量是棱镜计划的两倍。

其中，代表性的情报收集项目包括 Fairview、MYSTIC 和 MAINWAY。Fairview 是一个秘密计划，内部编号 US-990，NSA 根据该计划与美国电信公司 AT&T 合作，通过电缆、路由器和交换机收集美国境内的外国公民的电话、互联网和电子邮件数据，尤其是通过接触外国的电讯系统获得情报。MYSTIC 项目创建于 2009 年，由特别来源行动处(SSO)实施，MYSTIC 是美国国家安全局（NSA）使用的全球语音拦截程序。MAINWAY 收集来自多个来源的国内外电话和互联网元数据，包含通过

美国四大电话运营商进行的数千亿电话的元数据：AT＆T，SBC，BellSouth（现在全部三个称为 AT&T），和 Verizon，并具备数据质量管理、准备和排序功能。根据普利策奖获奖记者 James Risen 的说法，MAINWAY 是构成 20 世纪 90 年代 ThinThread 计划的四个组成部分中最重要的一个。国家安全局声称 MAINWAY 计划中只保留了五年的国内电话数据，但显然公众对这种说法并不买账。

- **三角测量（Operation Triangulation）行动**

2023 年 6 月 1 日，卡巴斯基实验室发布了一份未知 APT 组织的攻击报告，称其发现了一起定向攻击苹果 IOS 设备的高级威胁活动，该行动被命名为三角测量（Operation Triangulation）行动。此次攻击利用了苹果 IOS 设备中 iMessage 服务附件的 0day 漏洞获得目标 iOS 设备的 root 权限，再将恶意代码注入设备，之后通过 C&C 服务器下载多个后续恶意代码，最终实现对设备的完全控制。其中，后门植入物不会在受害者的手机中落地，只在受害者手机中的内存驻留，当手机重启后，所有后门植入物的痕迹都会丢失，具备很强的隐蔽性。

根据卡巴斯基的报告描述，三角测量（Operation Triangulation）行动开始于 2019 年，此次攻击涉及的 IOS 设备系统版本疑似为 IOS 15 版本，卡巴斯基实验室提供了攻击过程中可能遗留下的文件和网络活动信息情报，可以用来帮助识别受害者。针对此次漏洞情报，苹果公司在 2023 年 6 月 21 日为 iOS 15.7.7 发布了安全补丁，其中两个漏洞致谢了卡巴斯基实验室，这两个漏洞为三角测量（Operation Triangulation）行动所使用的零点击漏洞组合链中的核心部分，分

别是 CVE-2023-32435 - WebKit 远程代码执行漏洞,苹果公司官方确认在 iOS 15.7 之前，该漏洞已被在野利用，以及 CVE-2023-32434 - IOS 内核整数溢出漏洞，配合远程代码执行漏洞进行本地提权。

可见,苹果手机的 0day 漏洞存在相当长时间的无情报/无补丁真空期，同时也可能由于情报信息差导致苹果官方只修复了部分漏洞，导致攻击者在原有利用链上再组合备选漏洞后仍然长期可用。**这点让人疑惑,iPhone 后门的长期存在与美国 APT 攻击有某种相关性关系。**

能力四：利用掌控开源软件社区优势具有实施供应链攻击的便利

（一） 能力的基础和构成

美国具备完整的开源产业体系与生态环境,并通过其把控的商业科技巨头、开源基金会、开源社区及代码托管平台实质控制着全球开源软件供应链。美国政府也早已全面布局开源软件，尤其以 Linux、Apache、Android、Git、Hadoop、MySQL、Python 等为代表的开源软件在全球广泛普及，成为全球软件开发的基础。快速发展的云计算、大数据和人工智能等也得益于 ROS、Tensorflow、Pytorch 等开源软件的发展。同时，在开源基金会方面，Apache 基金会明确表明遵循美国出口管制条例，Mozilla 基金会则表示其司法管辖权归属美国加利福尼亚州，RISC-V 基金会也声明其司法管辖权在美国特拉华州。在开源平台方面，GitHub、SourceForge 及 Google Code 等代码托管平台均明确遵守美国出口管制条例，且司法管辖权在美国加利福尼亚州。

美国具备完整的开源产业体系与生态环境，是国际开源产业的主导，这种主导力也成为其利用掌控开源软件社区达成实施供应链攻击，并对全球开源软件供应链中自主性较差、依附性较强、处于弱势地位的国家随时断供制裁的悬顶之剑。

（二） 能力的应用和负面影响

相关资料显示，美国 CIA 所属投资机构 In-Q-Tel 于 1999 年成立。该机构的高层汇聚了商业、投资、情报、国防、技术和政府领域拥有丰富经验的革命性领导者，在其 20 多年间投资控制了人工智能、数据分析、工业 4.0、生物技术、IT 平台、通信领域等无数领域的重要核心项目。比如，CEO Christopher Darby，曾任职于英特尔公司副总裁，负责管理中间键产品部，也是国家人工智能安全委员会成员。可见，In-Q-Tel 是 NSA 控制各行业领域核心关键基础设施资源的中间件组织，方便 NSA 开展情报收集和网络攻击。

因此，**需要非常警惕一种全球性风险，即美国在棱镜事件中通过科技公司获取情报的惯性思维，而美国也存在借用开源社区的主导优势来注入漏洞和发起供应链攻击的可能性。**

一项重要的证据就是 Heartbleed(“心脏滴血”)漏洞，这是开源软件 OpenSSL 在 2014 年 4 月曝光的一个漏洞，出现在数千个网络服务器上，包括那些运行像雅虎这样的主要网站的服务器。据彭博社(Bloomberg)消息，两名不愿透露姓名的内部人士爆料，美国国家安全局 NSA 早已在两年前就得知 Heartbleed 漏洞的存在，且一直隐蔽地利用漏洞来窃取密码和收集数据，也就说明 NSA 利用开源软件

OpenSSL 中的漏洞，可以轻易入侵包括 Gmail 和亚马逊在内的众多服务器，这使得 NSA 几乎可以访问网络上三分之二的加密服务器。

能力五：利用掌控商用信息化标准和协议的优势具有调配关键产品安全性的能力

（一） 能力的基础和构成

美国借助技术先发优势，长期主导网络领域相关的技术标准和规则制定的话语权。一是美国通过其市场导向的标准体系，以企业为主体，参与和主导国际标准组织和机构，如国际电信联盟（ITU）、国际标准化组织（ISO）、国际电工委员会（IEC）等，推动制定符合其利益和需求的网络领域的技术标准和规则。二是美国通过其法律法规和政策措施，保护其网络技术的知识产权和安全，对网络领域的供应链和市场进行监管和干预，对网络领域的竞争对手和威胁进行制裁和排斥，以维护其在网络空间的优势和利益。三是美国通过其与盟友和伙伴的合作和协调，建立和推动基于规则的网络空间国际秩序，以其价值观和理念为指导，对网络领域的技术标准和规则的制定进行影响和塑造，以实现其在网络空间的领导和主导。

美国不断争取国际标准的主导权，其目的就是借助美国芯片、密码算法和 IT 安全的优势，试图将其根技术推向全球标准，从而构建美国对全球 ICT 产业的掌控力。为了增强影响力，美国政府持续加强国际网络安全标准的投入，其中，代表性的手段包括：2015 年成立跨部门国际网络安全标准工作组(IICSWG)，推动美国政府参加网络安全

相关国际标准制定，促进全球接受美国理念；2017 年美国商务部制定网络安全国际标准的优先事项，确保网络安全方法和政策具有全球相关性，在国际上倡导美国网络安全产品和服务；2022 年 CHIPS 法案授权 NIST 开展网络安全研究、提升美国在国际标准的竞争力。

实施层面，美国也通过大肆招揽“门客信徒”，通过国际信息化标准和协议的制定和推广，给全球加密系统打上后门破坏，以此达到自身企图。2013 年 9 月，英国《卫报》和美国《纽约时报》报道了斯诺登披露的 NSA“奔牛”计划（BULLRUN），曝光 NSA 能够破解广泛使用的在线协议，包括 HTTPS、VoIP 和安全套接层（SSL）等。NSA 的备忘录显示，NSA 每年花费 2.5 亿美元在软件和硬件中插入后门，且其破解特定网络通信技术加密的能力涉及多个非常敏感的来源。NSA 将该破解加密项目描述为“美国保持不受限制地访问和使用网络空间的入场券”。

（二） 能力的应用和负面影响

“奔牛”（BULLRUN）计划是美国情报界“信号情报赋能计划”（SIGINT Enabling Project）的重要组成部分。根据被曝光的该项目绝密预算文件显示，与科技公司“合作”是该计划的重要手段，**通过积极与国内和国外 IT 企业合作，暗中影响或公开利用其商业产品的设计，将漏洞插入商业加密系统**。参与此类合作的公司均未具名，这些细节具有更高级别密级。

BULLRUN 是美国国家安全局（NSA）与英国情报机构共同合作进行的旨在破解互联网加密技术的高度机密（TOP SECRET，extremely

sensitive）的计划，实施部门为 Deputy Director for Penetrating Target Defences(PTD)，计划的实施包括对硬件、软件、固件安全的攻击；对国家和国际标准的破坏；在特定的美国或跨国公司中插入关键的情报人员；还有一些其他途径。其中涉及的加密通讯技术包括 SSL/TLS 网页邮件、SSH、加密聊天、VPN、加密 VoIP。手段涉及 CNE、采购高精设备、高级数学技术、影响行业标准等。其中通过影响和削弱加密标准，获取主加密密钥，以及通过协议，通过强制加密数据之前或之后获得对数据的访问来保持其窃听加密通信的能力法律，或通过计算机网络利用（黑客）。

2013 年 12 月，路透社刊文《连接 NSA 与安全产业先锋的秘密合同》称，美国国家标准与技术研究院（NIST）2006 年正式发布的 SP 800-90 标准中推荐的确定性随机位发生器（Dual_EC_DRBG），确实存在 NSA 的后门。在 NIST 将 Dual_EC_DRBG 加密算法纳入标准之前的 2004 年，NSA 支付 1000 万美元与加密技术公司 RSA 达成秘密协议，使具有 NSA 漏洞的 Dual_EC_DRBG 作为 BSafe 加密库中首选的默认随机数据生成算法，助其开展大规模监控。美国研究人员证实，因为该算法漏洞的存在，“利用单个 CPU 或计算集群只需花费数秒或数十秒，就可以获得通信密钥”。英国《卫报》2013 年评论称，“NSA 的做法已经动摇了整个互联网的信任基础”。

能力六：利用全球通用漏洞披露标准及运营机构等具有优先获取安全漏洞的条件

（一） 能力的基础和构成

美国一直将漏洞管理作为网络安全国家战略的关键要素，其在未知漏报保护和利用上的处理等级完全不亚于实体军事武器。早在2013年12月，《瓦森纳协定》就将漏洞和一些入侵软件列入军用物资进行管制，随后，美国商务部也出台相关实施规则草案，将漏洞纳入美国《出口管理条例（EAR)》的管控范围。

首先，美国持续投入力量建立开放灵活的漏洞收集、发布等管控机制，力求在漏洞披露上平衡“安全防护”、“情报收集”和“网络反恐”等多方需求，做出“对整体利益最好的决策”。比如，VEP裁决委员就是由国家安全局、国土安全部、联邦特勤局、国家情报总监办公室、财政部、国务院、司法部、联邦调查局、能源部、白宫行政管理和预算办公室、国防部、商务部、中央情报局等众多机构组成，几乎囊括了主要的政府、军方等利益相关方，通过这种多方协调磋商形成国家统一的漏洞披露准则。同时，美国还致力于细化漏洞披露裁决程序，提高政策的可操作性。比如，VEP程序章程详细规定了漏洞裁决的六个步骤，形成了可操作的最佳实践。

2017年11月15日，美国政府发布年度报告漏洞公平判决程序章程（Vulnerabilities Equities Process，VEP），表明了美国政府对漏洞披露利弊的综合权衡。**VEP的基本做法是将美国各机构获得的漏洞信息在政府内部进行分享和评估，然后根据漏洞具体情况来决定**

是否告知企业，以便它们发布安全补丁和保护用户安全，还是保留该漏洞用于情报活动，以谋求更大利益。美国政府宣称最终他们会披露约 90%的软件漏洞。2018 年 1 月，美国众议院通过了《网络漏洞披露报告法案》(H.R.3202-Cyber Vulnerability Disclosure Reporting Act)，为美国政府 VEP 程序章程提供了法律保障。**该法案要求国土安全部提交网络漏洞披露报告，对漏洞做国家安全评估，决定是否向制造商和公众披露漏洞，还是利用新发现的漏洞攻击潜在对手。**

其次，美国基于公私合作的标准项目 CVE 和漏洞库 NVD 建设，完成了美国漏洞资源持续收集和储备的基础布局。一方面，美国资助非营利组织制定通用漏洞披露（CVE）并推广为全球通用标准。通用漏洞披露（CVE）是漏洞标识标准也是漏洞字典库，负责收集漏洞并给予编号以便于公众查阅。CVE 由美国国土安全部资助的非营利组织 MITRE 公司于 1999 年推出，后由其下属的国土安全系统工程与发展研究所（HSSEDI）运营维护，并在 2002 年被美国国家标准与技术研究院（NIST）推荐到美国全联邦机构使用，在 2004 年被美国国防信息系统局（DISA）推荐到安全产品中使用。通过建立 CVE 编码委员会（CNA)，充分吸纳了全球的商业公司、学术研究机构、开源组织、漏洞奖励平台以及知名安全专家，已被全球广泛采纳。**另一方面美国以标准先发优势建设了国家级漏洞库 NVD。**随着 CVE 国际影响力不断提升，为了进一步扩大在漏洞管理领域的影响力和掌控力，美国国土安全部委托 NIST 在 CVE 基础上建立了国家级漏洞库 NVD。NVD 与 CVE 同步更新，同时 NVD 还兼容了包含“通用漏洞评估系统”(CVSS)、“通

用平台列举”（CPE）等漏洞相关标准在内的安全内容自动化协议（SCAP），能够提供更为详细和全面的漏洞分类、分级、影响产品等标准化、格式化信息，数据应用性更强，使用范围更广。截至 2022 年 5 月，NVD 公开发表的漏洞数量合计 176207 条，居世界前列。

（二） 能力的应用和负面影响

在上述漏洞资源积累的基础上，美国通过保留诸多例外具备谋求漏洞资源（尤其零日漏洞）利用的优先权。尽管表面上美国漏洞披露管理的一系列政策法规，似乎在漏洞披露的透明度方面有所提高，改变了过去单纯由情报机构主导进行“暗箱操作”的做法，这也与近年来美方面临漏洞操控指责的公众压力有关，比如，2017 年 5 月“WannaCry”勒索病毒席卷全球让美国利用漏洞囤积网络武器的行为备受质疑。

然而，美国在漏洞披露方面仍有许多保留。以 VEP 程序章程为例，一是 VEP 可能受到第三方保密协议、谅解备忘录或其它条件限制，阻止漏洞信息及时披露。二是缺乏漏洞风险评级，难以评估 VEP 政策的实际效果，比如国家安全局可能公开披露 999 个低危和中危漏洞，但却手握 5 个高危漏洞而不披露。三是国家安全局作为美国军方情报机构，承担 VEP 执行秘书职责，能够主导 VEP 裁决相关事宜。众所周知，国家安全局拥有大量未知漏洞，许多漏洞已被用于制作网络武器，因此很难保证披露的公正性。四是 VEP 审核过程不受产业界的监督，预留了较多例外项，比如只向某些机构披露漏洞缓解信息，而不披露具体漏洞等。

对零日漏洞的利用则最能体现美国在漏洞资源方面的优势以及基于这种优势对全球网络空间稳定产生的破坏力。NSA、CIA 利用其持有的覆盖各类设备、平台、系统、软件的零日漏洞对各类高价值目标实施网络空间作业，有效支撑了美方的计算机网络利用（CNE）和计算机网络攻击（CNA)。伊朗核设施被攻击的“震网”(Stuxnet）事件就是一个典型的例子，在攻击行动中，攻击者一共使用了 5 个 Windows 的零日漏洞和 1 个西门子的零日漏洞，以一种看似近乎挥霍实则精妙组合利用零日漏洞的方式，实现了通过网络空间作业对伊朗核设施造成物理破坏的效果，几乎永久地迟滞了伊朗核计划，达成了美方的战略意图。

“震网”病毒是一种十分高级的蠕虫病毒，并且是一种定向的网络攻击武器，专门针对工业控制系统进行破坏。“震网”（Stuxnet）病毒内包含漏洞入侵技术，能够对 Windows 系统以及 SIMATIC WinCC 系统的漏洞实施攻击。“震网”（Stuxnet）病毒的结构极为复杂，且隐蔽性强，当被病毒感染的优盘插入电脑后，该病毒无须在外力作用下，即可对工业电脑系统进行攻击和控制。不同于传统计算机病毒，“震网”(Stuxnet）病毒并不会通过窥探个人隐私的方式来谋取不法利益，而是需要投入资金进行研制。

从漏洞利用角度来看，“震网”行动体现出了从技术层面零日漏洞到战略层面压制优势的价值转换。

能力七：通过多年网络武器开发具有对他国基础设施进行攻击窃密的标准化工具

（一） 能力的基础和构成

由于网络攻防两端长期存在严重失衡，美国认为光靠防守很难彻底抵御对手攻击，必须打造攻防兼备、侦打防评一体的网络威慑武器体系，能够支撑其发起大规模网络攻击。为此，美长期致力于推动政策支持，2019 年 9 月 24 日，美国、英国、澳大利亚、新西兰、加拿大、日本、韩国等 27 国签订《关于推进网络空间负责任国家行为的联合声明》将进攻性网络攻击合法化，把网络空间变为新战场——“针对间谍目标以及军事目标的网络攻击，应该被视为正当行为。”另一方面，美国通过大力开展网络空间攻防核心技术及武器装备研发，以获得“先发制人”的优势。

美国对先进网络攻防武器装备的追求孜孜不倦，明确提出“美国优先”原则，而这种“优先”在网络安全领域的表现，就是再度拉大与挑战对手间的绝对差距，以保证在需要时可以动用美国压倒性的技术装备优势来迫使对手妥协。

美国的网络武器研发主体主要分为三类：

一是洛克希德.马丁、雷神、通用等传统军工巨头，这些公司以传统、新型技术装备的网络化作战运用为基本起点，向网络空间攻防领域发展。例如，DARPA 将包括“X 计划”在内的多个网络领域研发合同授予雷神公司推动和负责。

二是思科、微软、甲骨文、IBM、亚马逊等大型信息科技公司，以

及其他盟国的科技公司，承担国家信息基础设施、关键业务网领域等网络项目。例如，2018 年 8 月，英国 BAE 系统公司被 DARPA 选中承担 CHASE 项目，开展新的人工智能网络安全技术原型设计，以应对高度复杂的网络攻击。

三是火眼、赛门铁克、CROWDSTRIKE、派拓等网络安全企业，承担网络攻防前沿技术装备研发。例如，2018 年 9 月，DARPA 授予 Packet Forensics 公司价值 120 万美元的合同，以开发一种新的僵尸网络防御系统。

（二） 能力的应用和负面影响

目前，美国在网络武器装备研发方面已遥遥领先，利用技术优势打造了平台化、自动化、定制化的网络武器系统。通过多年研发，美国已经建立了庞大的网络武器库，具备了超强的网络攻击能力。

2017 年席卷全球的“WannaCry”勒索病毒事件，就是攻击者利用了黑客泄露的美国 NSA 网络武器，造成了巨大影响。维基解密曝光的美军网络武器库，涵盖了信息窃取、持久化能力、隐蔽信息传输、边信道传输、直接漏洞利用、突破物理隔离等众多方面，包括了 Windows、Linux、苹果 OS X、iOS、Android 等常见操作系统，攻击目标覆盖智能电视、手机、个人电脑、服务器、路由器、交换机等各类设备。

2017 年 3 月 7 日，维基解密首次在其网站对外曝光了美国中央情报局（CIA）相关资料，并且代号为 Vault7，并且从当月直至 9 月 7 日每周都会对外披露其中一个项目的相关资料内容。在这批泄露资料中，主要涉及其相关网络武器库和行动项目的代号和对应文档介绍。

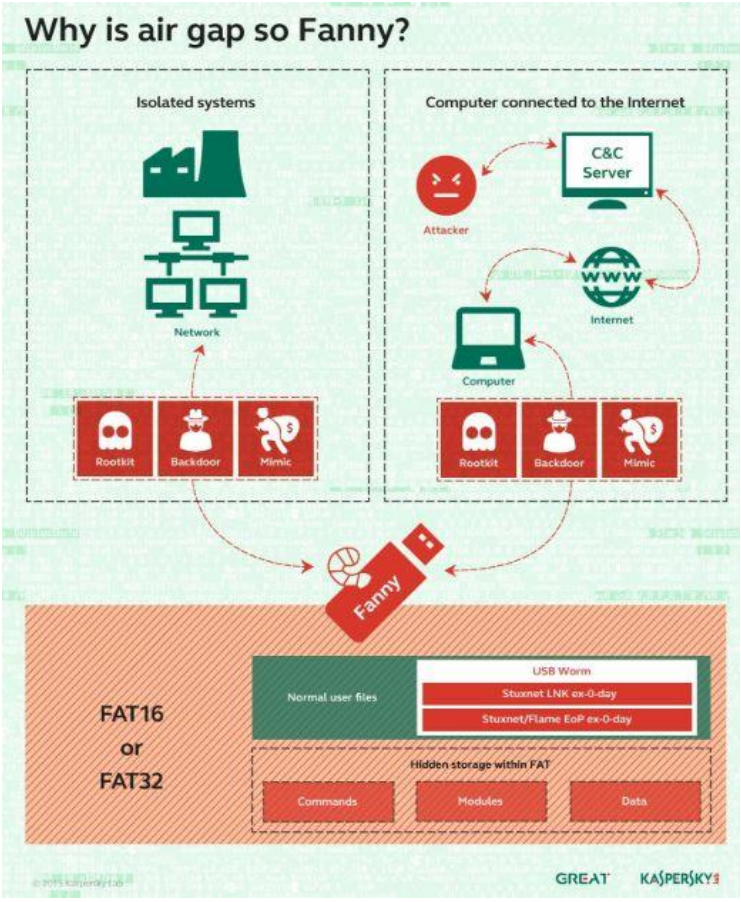
在此，列举一些该网络武器库中的代表性工具：

- **Athena（雅典娜），**在潜伏的情况下帮助黑客秘密远程访问装有 Window 操作系统(覆盖从 Windows XP 到 Windows 10 的大多数版本)的目标计算机。
- **Weeping Angel（哭泣天使），**该工具能够将智能电视的麦克风转变为监控工具。利用此工具，黑客能够将打开居民家中的智能电视（而且是在用户以为电视关闭的情况下），并窃听人们的对话。
- **Hive(蜂巢),**针对 Windows、Solaris、MikroTik(路由器 OS)、Linux 和 AVTech 网络视频监控等系统进行定制程序植入，协助黑客从植入恶意软件的目标机器中以 HTTPS 协议和数据加密方式执行命令和窃取数据。
- **AfterMidnight（午夜之后），**帮助黑客在目标机器上动态加载和执行恶意软件。
- **Archimedes（阿基米德），**是针对局域网(LAN)的一款中间人攻击工具，帮助黑客攻击局域网（LAN）内部计算机，通常用于办公室场景。
- **BrutalKangaroo（野蛮袋鼠），**是一个用于攻击 Microsoft windows 的工具套件，它通过 U 盘入侵使用隔离网闸的封闭网络。“野蛮袋鼠”组件同时还会创建一个隐蔽的网络，并且可以提供探测主机、列目录、执行可执行文件等功能。

此外，针对在线网络武器不能达到效果的情况，美国还研发了突

破物理隔离的系列武器。从无线战场、指挥控制中心到个人计算机，从雷达、战术通信终端、计算机到各种移动设备，从网络设备到 IoT 设备都不能幸免。例如，针对服务器和 PC 设备的配件与外设如主板、无线网卡、硬盘、U 盘、光盘、键盘、显示器、局域网插座等，都有对应的攻击工具。这些工具通过供应链感染、物流链劫持、无线 WIFI 攻击，物理摆渡（U 盘/光盘/移动设备）、物理入侵等各种手段植入目标，获取情报或者发起攻击。早在 2015 年，卡巴斯基实验室就公布了一份研究报告，指出 NSA 自 2001 年以来内部就存在一个称之为方程式的黑客组织，以各行各业为目标发起网络情报刺探活动。该黑客组织在网络攻击中善于使用蠕虫病毒、硬盘病毒、间谍软件等多种攻击手法，其中 Fanny 蠕虫病毒是该组织的利器之一。

Fanny 蠕虫病毒是一款威力极大的蠕虫病毒，可以对具备网闸隔离的网络进行攻击和侵入。这一蠕虫采用了基于通用串行总线（Universal Serial Bus，USB）的特殊控制机制，可通过优盘的感染与连接来进行侵入。当被感染 Fanny 蠕虫病毒的优盘被插入计算机后，该优盘中有一个极为隐秘的存储空间可用来对隔离网络的信息进行收集。被侵入的计算机在网络连接状态下，Fanny 蠕虫病毒可将收集到的相关信息实时传输给攻击者。若攻击者除了刺探相关情报信息外，还需要对被隔离的网络进行指令运行时，可通过 Fanny 蠕虫病毒事先将指令存储于优盘的隐匿空间中。当该优盘被连入计算机后，Fanny 蠕虫病毒会自动进行指令的运行。



Fanny 蠕虫病毒工作流程图

然而，这些网络武器可能仅是冰山一角，美国或掌握着更多更高度工程化的网络攻击平台，其在网络武器研发方面的不可控发展，将可能为全球网络安全带来无穷隐忧。

总结

美国作为网络空间的技术和规则领导者，一直试图维持其在网络空间的霸权地位，对其他国家和地区施加压力和干涉，严重损害了网络空间发展的公平性和多样性。美国对网络安全威胁能力的过度追求，不仅导致了网络空间的军事化和政治化，也威胁了全球网络空间的安全和稳定，引发了网络空间的对抗和冲突，损害了全球网络空间的信

任与合作。

美国在网络安全威胁能力方面的不受控发展和单方国家安全意图导向，诱发了其他国家的安全担忧和应对措施，导致网络空间的军事化程度不断提高，造成了全球网络对抗的“军事竞赛”趋势。此举不符合网络空间的共同、综合、合作、可持续的安全理念，也不符合网络空间的开放、合作、和平、安全、有序的发展方向。全球网络空间的稳定与发展需要警惕这种基于威慑的网络霸权主义，通过构建网络空间命运共同体，推动网络空间的国际规则和治理机制的完善和改革，促进网络空间的平等、互利、共赢的合作。

参考文献

1. 大国博弈背景下，我国通信海缆产业发展机遇和挑战.

https://www.secrss.com/articles/56658

2. 美国全球监听行动纪录显示 多达 35 国领导人被监听

http://www.xinhuanet.com/world/2014-05/27/c_126550886.htm

3. 15 年前美国用这招让伊拉克“消失”，现在对中国还好使吗？

https://m.huanqiu.com/article/9CaKrnK9QBr

4. 俄罗斯断网演习 2023，断的究竟是什么？

https://www.secrss.com/articles/56553

5. GlobalSign Causes Mass HTTPS Revocation

https://blog.trustico.com/cyber-security/globalsign-https-revocation-spotify-wikipedia-guardian-dropbox.php

6. 独家连载 | 零日漏洞：震网病毒全揭秘

https://www.aqniu.com/vendor/10160.html

7. 美国“棱镜门”持续发酵

https://qnck.cyol.com/html/2013-06/19/nw.D110000qnck_20130619_1-08.htm

8. 美英或曾黑入 SIM 卡巨头试图监听全球手机

https://cn.nytimes.com/technology/20150226/c26gemalto/zh-hant/

9. 维基解密:iPhone 刚出厂就可能被 CIA 监听

https://www.sohu.com/a/130044947_608245

10. 媒体历年披露的近四十个美国政府大规模监控项目

https://www.secrss.com/articles/8186

11. Operation Triangulation: iOS devices targeted with previously unknown malware

https://securelist.com/operation-triangulation/109842/

12. 内幕：NSA 已经利用 Heartbleed 漏洞多年

https://linux.cn/article-2837-1.html

13. “棱镜”十年：美国强化网空情报获取能力活动及其策略分析

https://www.secrss.com/articles/58518

14. 美军网络空间装备技术发展途径探析

https://www.secrss.com/articles/12760

15. DARPA 投资 120 万美元开发僵尸网络识别系统

https://www.secrss.com/articles/5135

16. Vault 7：CIA 黑客工具曝光

https://wikileaks.org/ciav7p1/

17. Kaspersky Lab Discovers Equation Group

https://usa.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage