第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

网络空间的敌情想定分析

安天创始人、首席技术架构师

肖新光

红旗漫卷

敌情想定是前提，网络安全实战化

- **所以，我们应该研究一般战争的规律；也应该研究革命战争的规律；最后，我们还是应该研究中国革命战争的规律。**

——毛泽东《中国革命战争的战略问题》

- **网络安全的本质在对抗，对抗的本质在攻防两端能力较量。**

——习近平《在网信安全和信息化工作座谈会上的讲话》

提纲

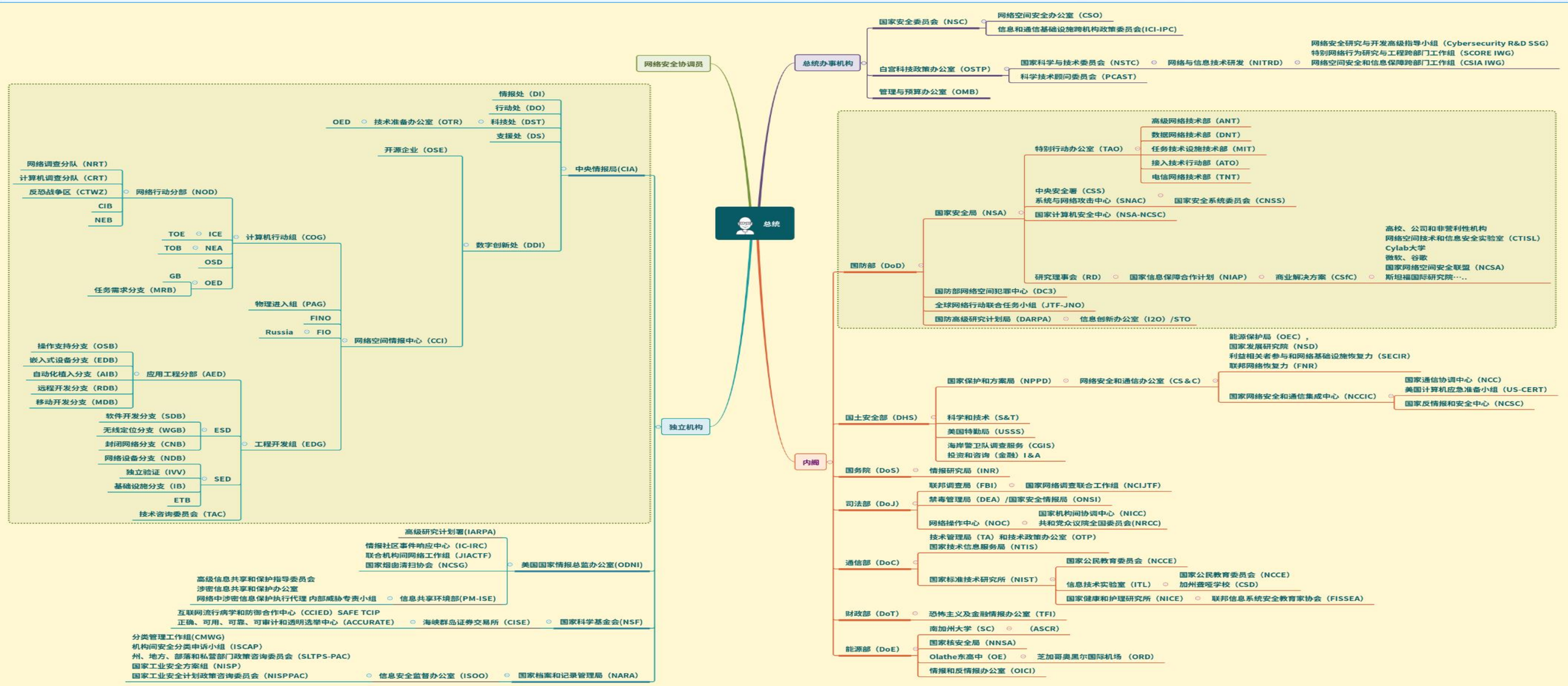
通过超级对手的认知对手极限能力和能力体系

新威胁、新装备、新手段

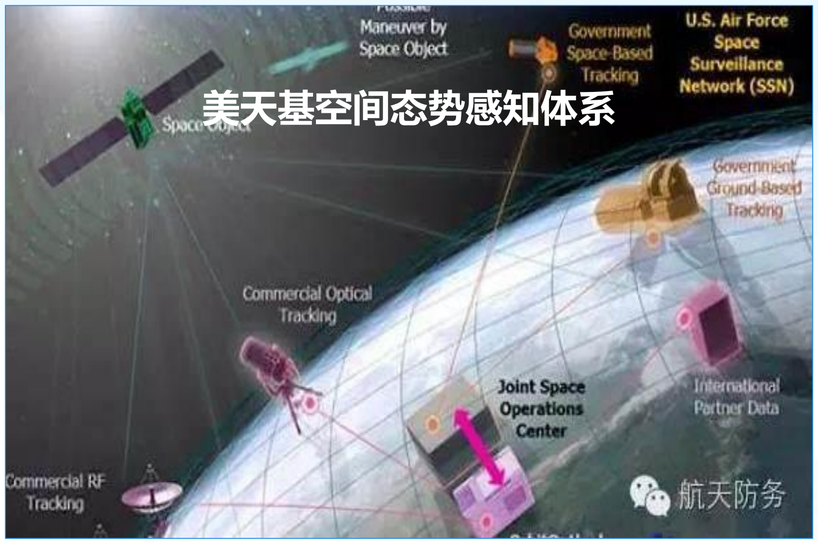
敌情想定的完善和具象化

1 通过超级对手的认知对手极限能力和能力体系

充沛的安全预算和组织人员规模



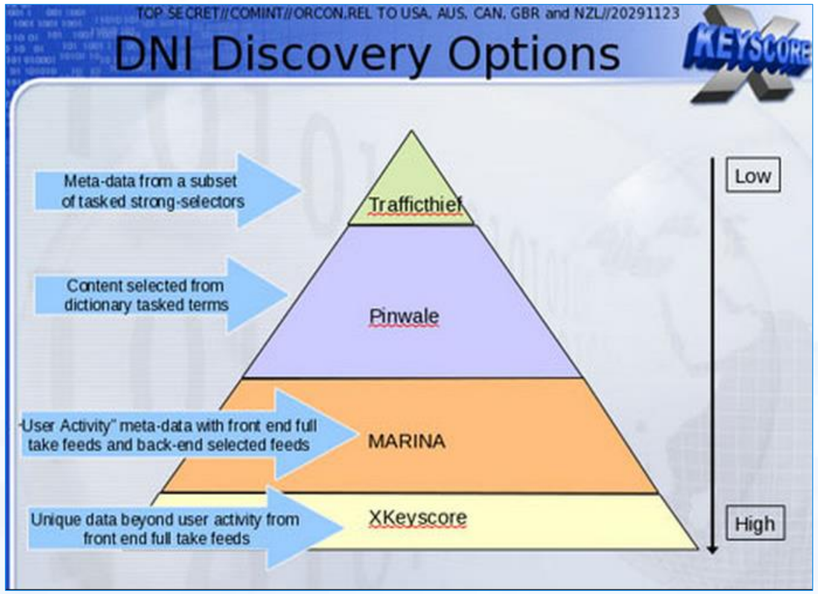
在大工程系统的支持下形成攻击作业能力

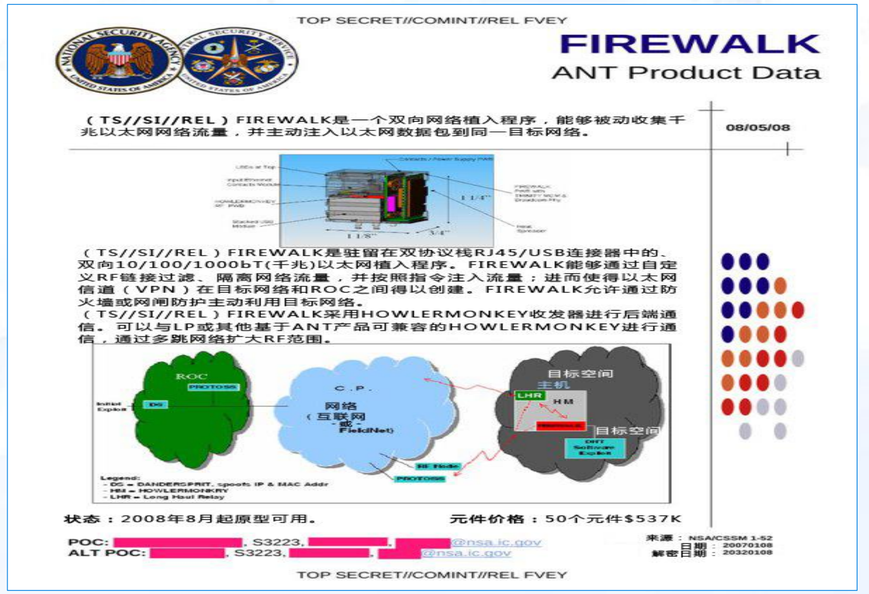


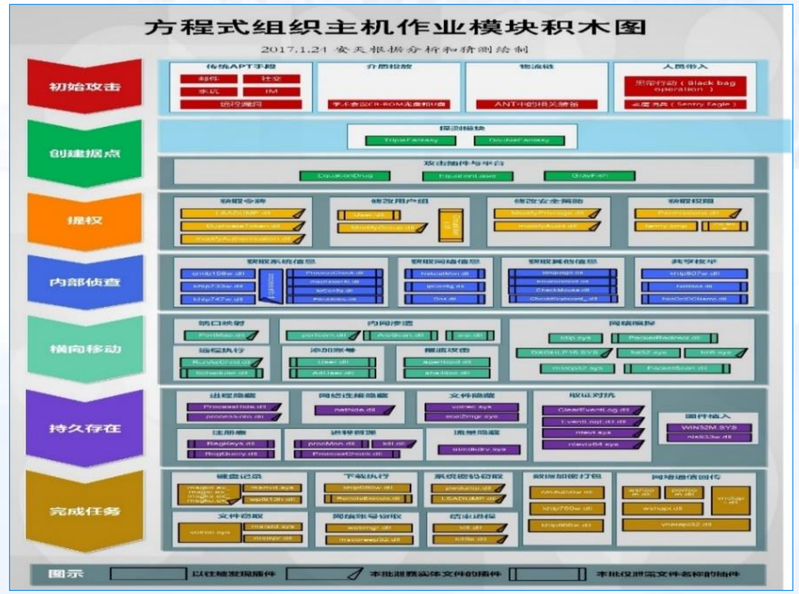
美天基空间态势感知体系

美B2隐形轰炸机

美军防区外空地导弹



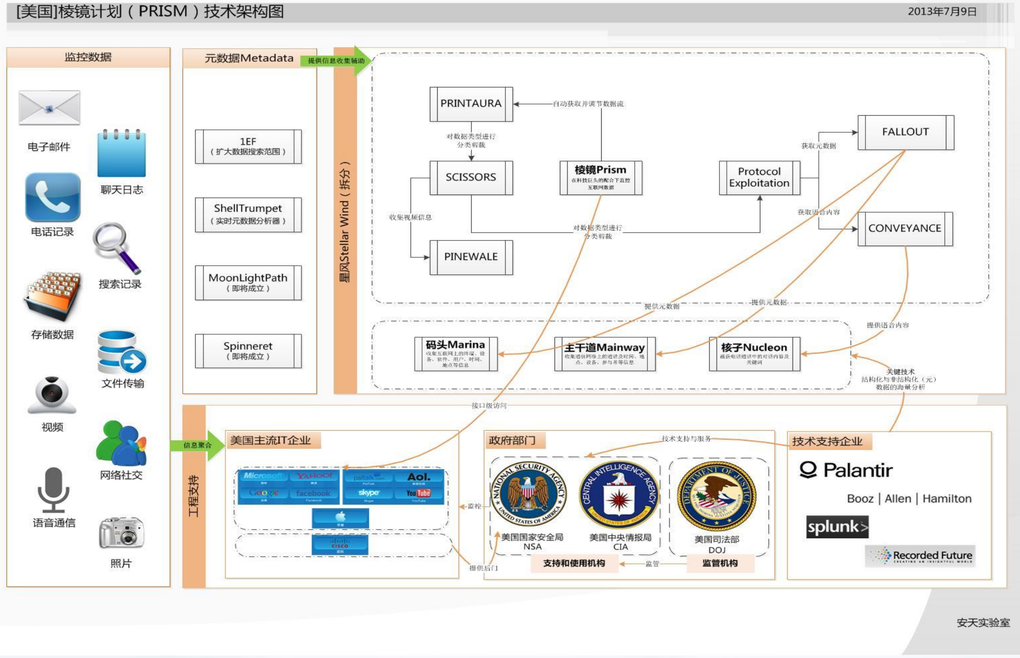




对对手作业方式和信息获得通道的梳理

信息获取

基于美国厂商互联网模式和IT服务的全球采集，形成全球用户、设备、身份、链路、言论、习惯、位置等大数据体系，基于“棱镜”等系统实现定位、溯源等。



数据整合

- 建制化的网络攻击团队
- 庞大的支撑工程体系
- 制式化的攻击装备库
- 漏洞采集和分析挖掘能力和关联资源储备
- 系统化的作业规程和手册

情报作业

装备体系覆盖全场景

漏洞利用工具和恶意代码载荷覆盖全平台

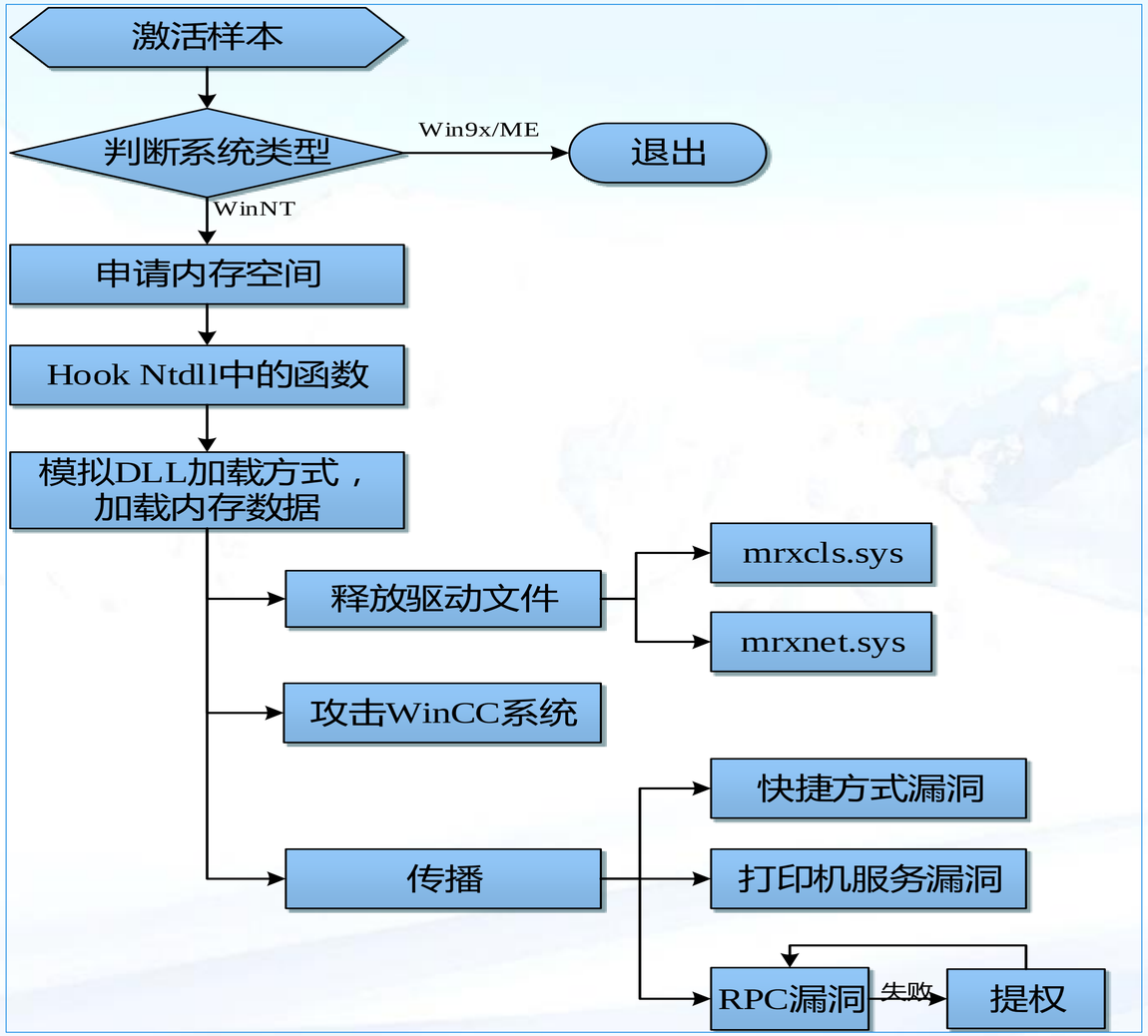
持久化能力覆盖全环节的特点

装备体系——制式化、清晰引导和渐进列装成型

A	B	C	D	E
所属组织	代 号	价格	描 述	备 注
ANT	CANDYGRAM	$40,000.00	横拟GSM蜂窝塔。数据包中还包括通过短信与本机通信Windows XP笔记本电脑和手机，可同时定位200个电话号码。	参见：DRTBOX、Stingray、CANDYGRAM、NEBULA、CYCLONE和TYPHON
ANT	COTTONMOUTH-1 (	$20,300.00	USB电缆w /转换射频发射器/接收器和恶意软件有效载荷	GENIE兼容，与STRAITBIZARRE，其他COTTOMNOUTH设备通信，可重新编程，可能与DEWSWEEPER相关（可能是相
ANT	COTTONMOUTH-II	$4,000.00	双栈USB端口（直接焊接到主板上），提供跨气隙系统的隐蔽“长途”继电器。像CM-I和许多其他系统一样，它用CHIMNEYPOOL框架编写，并通过STRAITBIZARRE进行通信。与CM-I和CM-III不同的是，它不包含HOWLERMONKEY或TRINITY。	参见：CM-I, CM-III, STRAITBIZARRE, CHIMNEYPOOL.可能是DEWSWEEPER的子类。
ANT	COTTONMOUTH-III	$24,960.00	双栈USB端口/ RJ45以太网插孔组合（直接焊接到主板上），提供跨网闸系统的隐蔽RF继电器。像CM-I和许多其他系统一样，也用CHIMNEYPOOL框架编写，并通过STRAITBIZARRE进行通信。 它可以使用SPECULATION协议与其他CM设备通信，还集成了TRINITY和HOWLERMONKEY RF收发器。	参见：CM-1、CM-II、TRINITY、HOWLERMONKEY、SPECULATION、CHIMNEYPOOL和STRAITBIZARRE。可能是DEWSWEEPER的子类。
ANT	CYCLONE Hx9	$70,000 (2 month rental)	EGSM基站路由器，用于收集GSM手机信号。笔记本电脑和配件用于命令和控制，使用与TYPHON相同的GUI。可通过802.11 WiFi控制。	参见：TYPHON、CANDYGRAM、DRTBOX和NEBULA
ANT	EBSR	$40,000.00	低功耗GSM基站路由器	参见：TYPHON、CANDYGRAM、DRTBOX、CYCLONE Hx9和NEBULA
ANT	ENTOURAGE	$70,000.00	应用于HOLLOWPOINT平台，包括特定频段的天线和用于命令和控制的笔记本电脑。 通过千兆以太网可控制未来计划（大约2008年）包括WiFi、WiMAX和LTE。	
ANT	FIREWALK	$10,740.00	“FIREWALK是一种双向网络植入，能够被动收集千兆以太网流量并将以太网数据包注入同一个目标网络。” 集成TRINITY和HOWLERMONKEY。通过VPN提供直接或间接隐蔽的RF链接到远程操作中心。 目录中的版本需要焊接到主板。	参见：HOWLERMONKEY、DANDERSPRITZ和TRINITY。注意：单元从物理上看似与CM-III几乎相同。 可能是RADON的一个子类。
NSA	FLUXBABBIT	$500.00	使用Xeon 5100和5300处理器的Dell PowerEdge 1950和2950服务器基于硬件的Bug。安装需要拦截服务器，同时路由到其目的地，进行后门并安装硬件	

A	B	C	D	E
ANT	HOWLERMONKEY	$750-$1,000	隐蔽中短程RF收发器，旨在与更大的设备集成。通过SPECULATION和CONJECTURE协议进行通信。包括HOWLERMONKEY的已知产品有：CM-I、CM-II、FIREWALK、SUTURESAILOR和YELLOWPIN。	参见：CM-I、CM-III、FIREWALK、YELLOWPIN、COTS、SPECULATION、CONJECTURE和STRIKEZONE。
ANT	LOUDAUTO	$30.00	一个房间的音频bug。实现为射频回复反射器（ANGRYNEIGHBOR系列）。它需要一个单元，如CTX4000以回传到基地。	参见：ANGRYNEIGHBOR、VARGANT、CTX4000、PHOTOANGLO和DROPMIRE
ANT	MAESTRO II	000 - $4,000	通用的可编程微型计算机，用于隐蔽的错误。规格：66Mhz ARM 7微控制器，4 MB闪存，8 MB SDRAM一个“XC2V500 500k门” FPGA。与一毛钱硬币大小相同。	参见：JUNIORMINT、TRINITY和SPARROW II
ANT	PHOTOANGLO	$40,000.00	替代CTX4000，连续的雷达波发生器，用于ANGRYNEIGHBOR系列复古反射器，包括VAGRANT，DROPMIRE和LOADAUTO。 然后将信号发送到处理系统，例如NIGHTWATCH或VIEWPLATE（处理和显示来自VAGRANT监视器电缆虫的信号）。LFS-2被列为另一种类型的处理系统。NSA / GCHQ联合项目。	
ANT	PICASSO	$2,000.00	由智能操作员携带的GSM手机，用于在其范围内窃听对话和通话。 包括操作员使用的紧急按钮。	
ANT	RAGEMASTER	$30.00	视频电缆错误。 实现为射频后向反射器。 用于VAGRANT集合。	参见： VAGRANT, CTX4000, PHOTOANGLO, DROPMIRE, LOADAUTO, NIGHTWATCH, VIEWPLATE.
ANT	SOMBERKNAVE	$50,000.00	基于软件的恶意软件，旨在通过使用未使用过的802.11无线接口来桥接空气间隙。适用于Windows XP。允许其他恶意软件“自动通报”。特别是VALIDATOR和OLYMPUS木马。	参见：VALIDATOR
ANT	SPARROW II	$6,000.00	专门用于无人机操作的微型计算机。包括集成WLAN，支持小型PCI插槽。IBM PowerPC 405GR、64MB SDRAM、16MB闪存。适用调查无线网络（Wifi / GSM等，取决于扩展卡）。	参见：TRINITY，MAESTRO II，JUNIORMINT
ANT	SURLYSPAWN	$30.00	执行嵌入在电缆中的RF反射器的键盘或鼠标漏洞。导致ANGRYNEIGHBOR家族漏洞。	参见：ANGRYNEIGHBOR，VAGRANT，DROPMIRE，SURLYSPAWN，CTX4000，PHOTOANGLO，
ANT	TAWDRYYARD	$30.00	ANGRYNEIGHBOR RF反射器的目的是作为一个信标，RF波发生器（CTX4000或PHOTOANGLO）可以找到RAGEMASTER视频电缆漏洞。并将注意力全部集中于此	参见：ANGRYNEIGHBOR，VAGRANT，DROPMIRE，SURLYSPAWN，CTX4000，PHOTOANGLO，

装备体系：弹药基数储备



MS08-067

- RPC远程执行漏洞

MS10-046

- 快捷方式文件解析漏洞

MS10-061

- 打印机后台程序服务漏洞

MS10-073

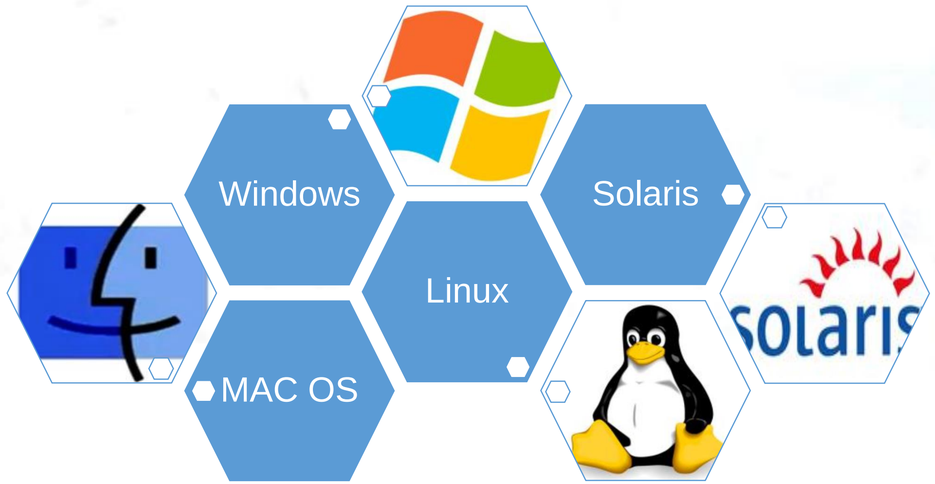
- 内核模式驱动程序漏洞

MS10-092

- 任务计划程序程序漏洞

来源：安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》，2012年9月首发

装备体系：立足于全平台无死角的平台覆盖



信息	Windows	Linux	Solaris	Oracle-owned Unix	FreeBSD	Mac OS
安天：修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件[3]	分析样本载荷和硬盘持久化能力					
安天：方程式（EQUATION）部分组件中的加密技巧分析[4]	分析加密算法					
安天：EQUATION 攻击组织的全平台载荷能力解析（本报告）		曝光存在，分析相关载荷	分析相关载荷			
The Hacker News：《Shadow Brokers reveals list of Servers Hacked by the NSA》			曝光存在	曝光存在	曝光存在	
卡巴斯基：Equation: The Death Star of Malware Galaxy[5]	揭秘方程式攻击组织					
卡巴斯基：A Fanny Equation: "I am your father, Stuxnet"[6]	Fanny 组件分析					
卡巴斯基：Equation Group: from Houston with love[[7]	Doublefantasy 分析					
卡巴斯基：《EQUATION GROUP: QUESTIONS AND ANSWERS》[8]	方程式组织问与答					根据网络特征提出猜测

注：安天在 Solaris 样本中分析出的 User Agent 具有 Solaris 标识，而卡巴斯基在“EQUATION GROUP: QUESTIONS AND ANSWERS”[8]中披露出曾捕获到 Mac OS X 的 User Agent 的信息，由此来看，尽管安天和卡巴斯基厂商目前都尚未捕获 Mac OS X 的样本，但方程式组织针对 MAC OS X 的攻击载荷是真实存在的。

来源：安天技术报告《从方程式到“方程组”EQUATION攻击组织高级恶意代码的全平台能力解析》，2016年11月首发

战场预制能力

供应链预制

- 标准污染（SP800/90）
- 开源污染
- ……

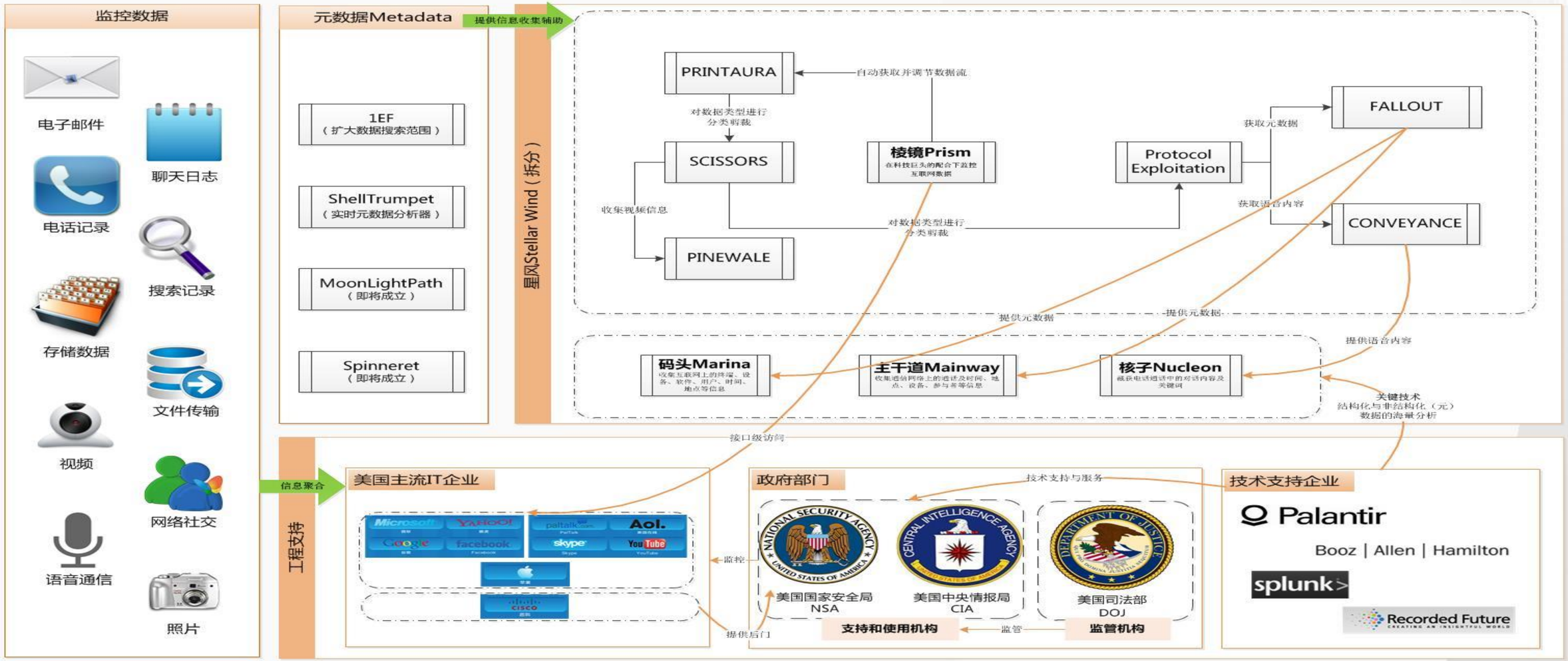
前出性预制

- 对全球运营商入侵劫持
- 海底光缆切割监听
- 工业场景多点预制工作
- ……

针对性预制

- 对目标人员的周边部署
- 物流链劫持

攻击基础——全球网络地形绘制和目标寻址能力



通过大规模采集建立形成了终端、设备、软件、用户身份的信息库，结合运营商入侵前出，形成了针对互联网目标的能力。

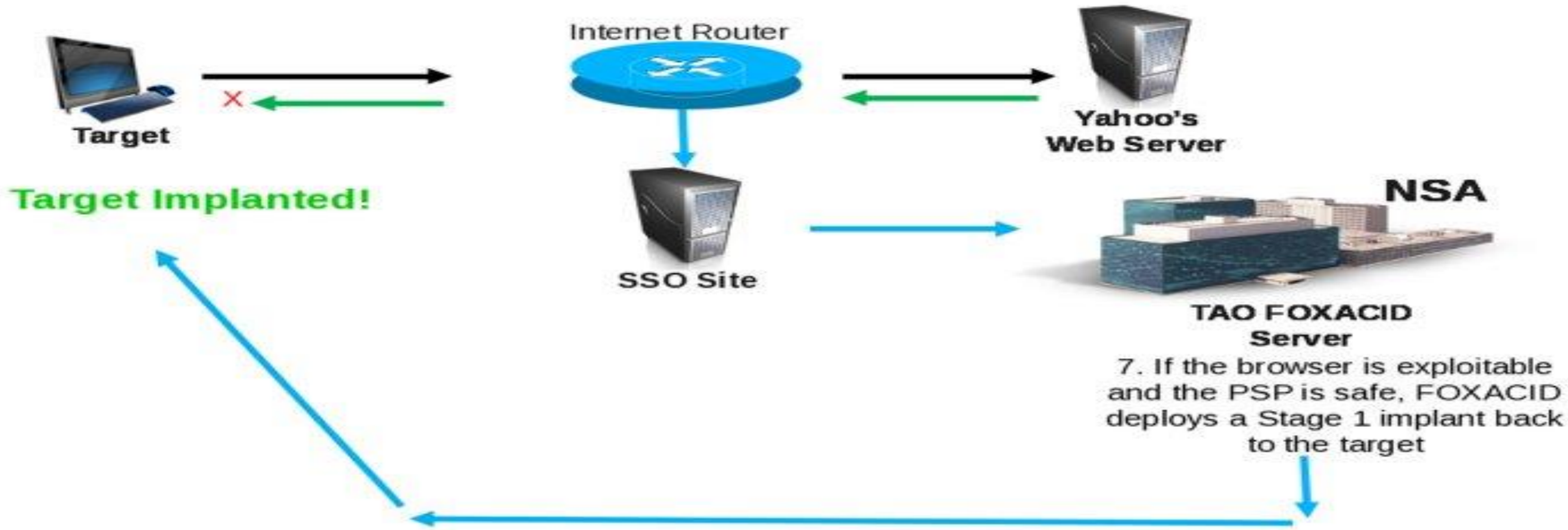
安天实验室

流量侧注入打点能力——浏览器入口

TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

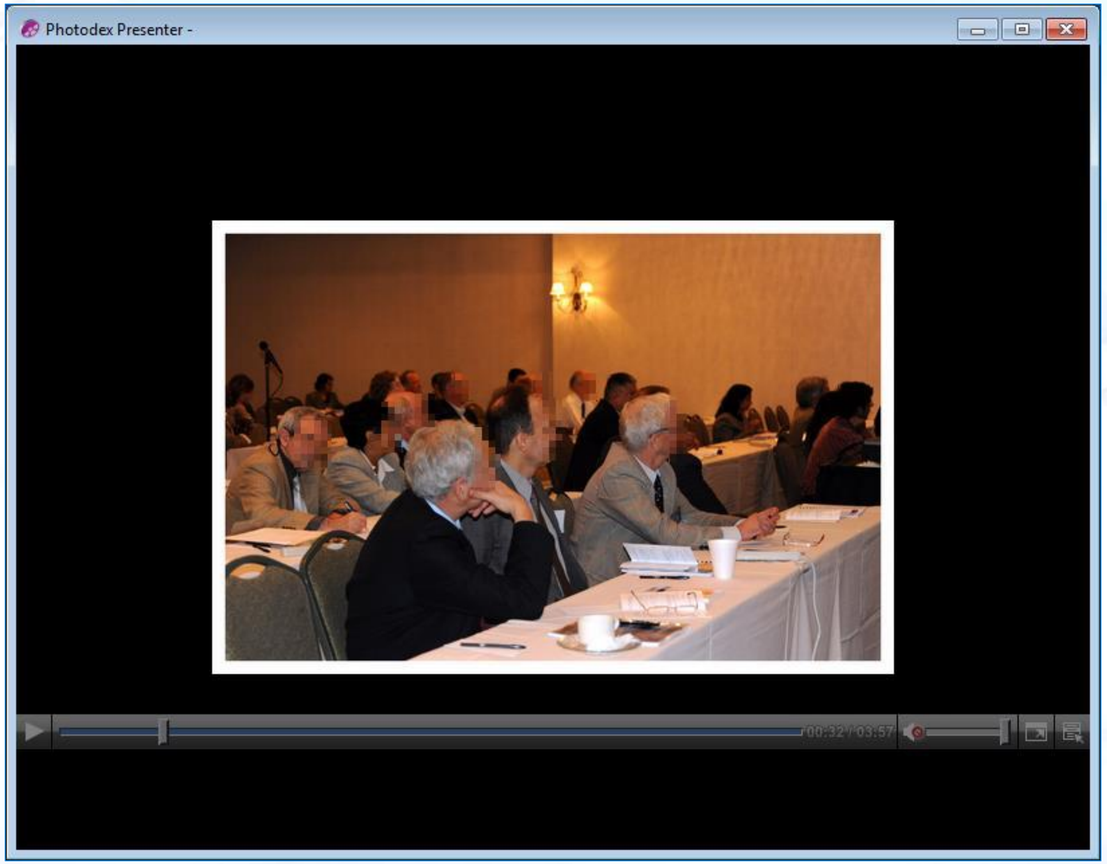


Booz | Allen | Hamilton
SDS
SIGINT | Development | Support

TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

4

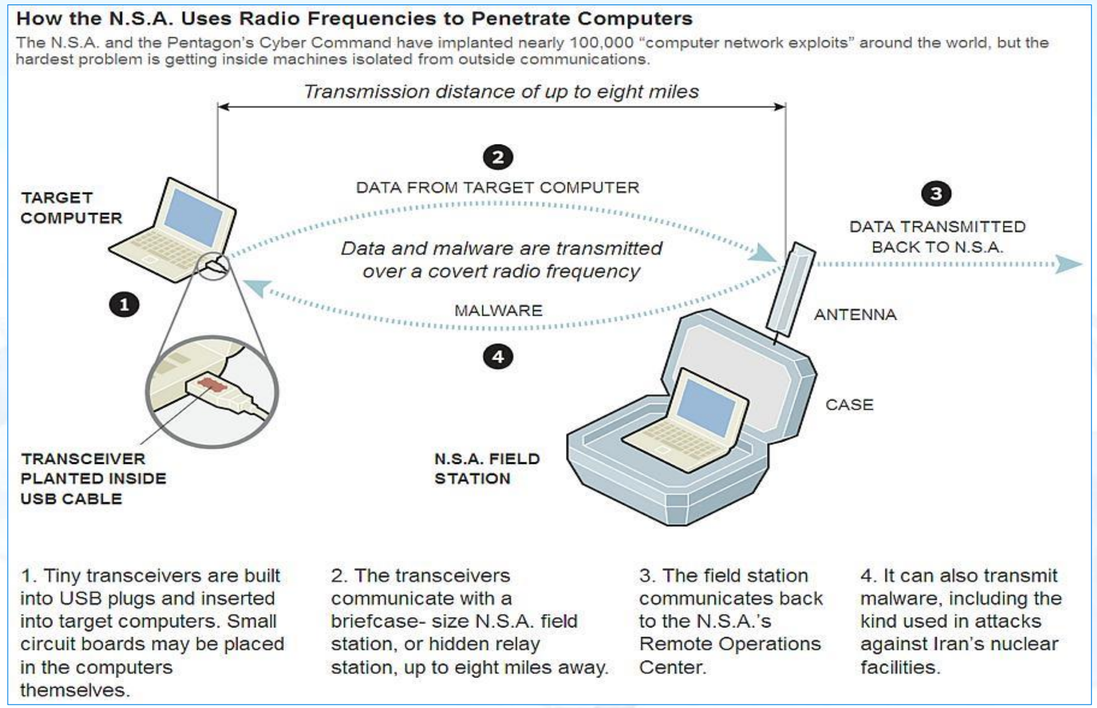
寻找突破点：社会工程结合技巧



- 2009年在美国休斯敦举行的专业学术会后，美情报部门向与会外国专家投递会议剪影光盘。
- 使用了不少于3个0day漏洞，对系统进行攻击。
- **MS09-025**
- **MS12-034**
- **MS13-081**

边界和隔离网突破能力

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

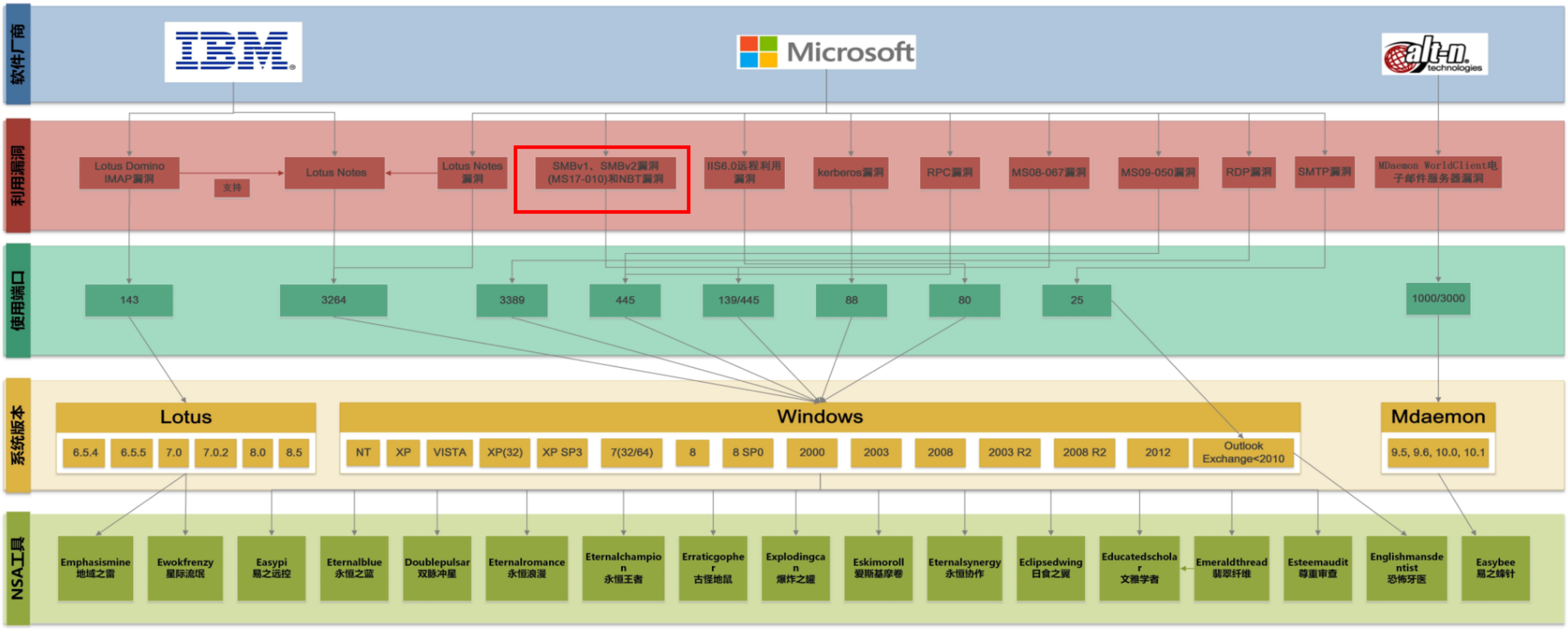


在物流链劫持、人员带入等方式实现把门踹倒的背景下，基于持久化节点的“横向移动”和在这个场景下，隔离的内网因为没有成为最不安全的环节，对手一经植入则横扫全网。单点孤岛节点更有可能成为“最最”不安全的节点，因为其根本不受到有效的安全感知和持续性的安全保障。

横向移动能力

2017年4月14日泄露的NSA网络军火装备的漏洞利用关系图

2017年5月21日 安天实验室绘制



安天认为：414所泄露军火，是美方面向内（隔离）网作业的打点和横向移动部分

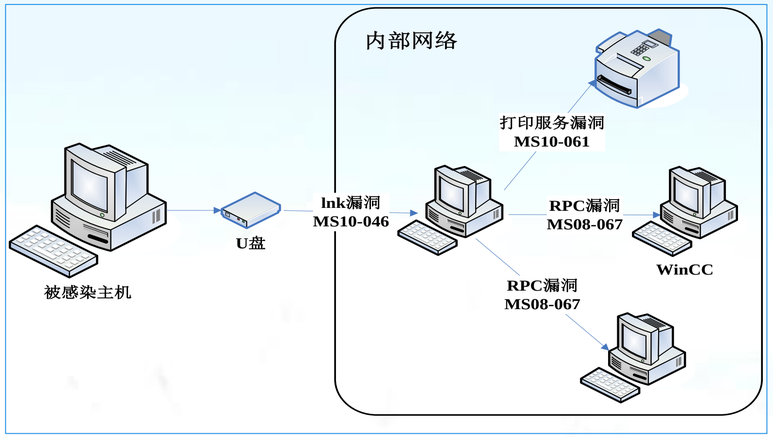
作业控制：依托精致、严密的指令体系

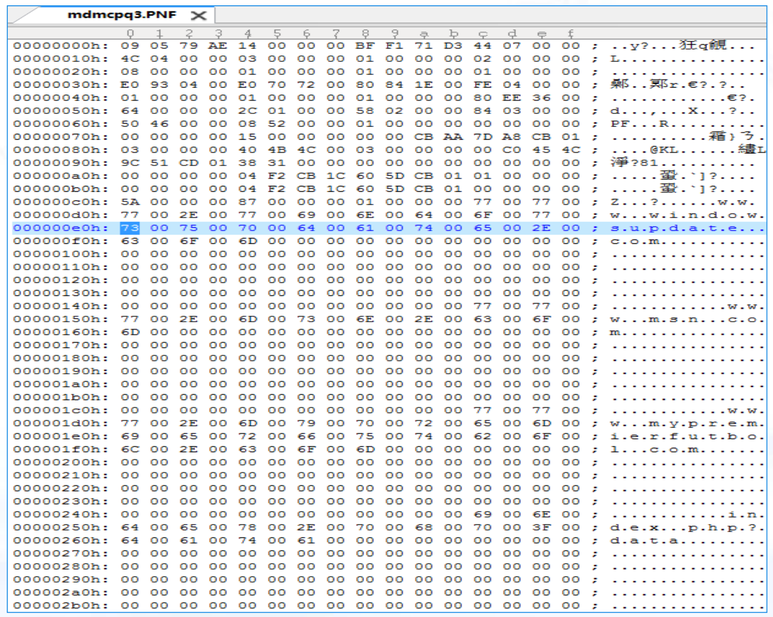
发包数据第一字节	功能
0x42（B）	清理感染痕迹，删除自身
0x4A（J） 0x92（不可显字符	创建文件
0x44（D）	写入文件
0x56（V） 0x95（不可显字符	执行文件
0x53（S）	读取文件回传
0x4B（K）	设置读取文件指针
0x60（’ ）	收集大量信息回传（具体格式见下表）
0x70（p）	更新样本配置信息
0x75（u）	更新样本sleep时间，并重新收集信息回传
0x76（v） 0xA2（不可显字符	更新远程C&C
0x80（不可显字符	删除指定文件

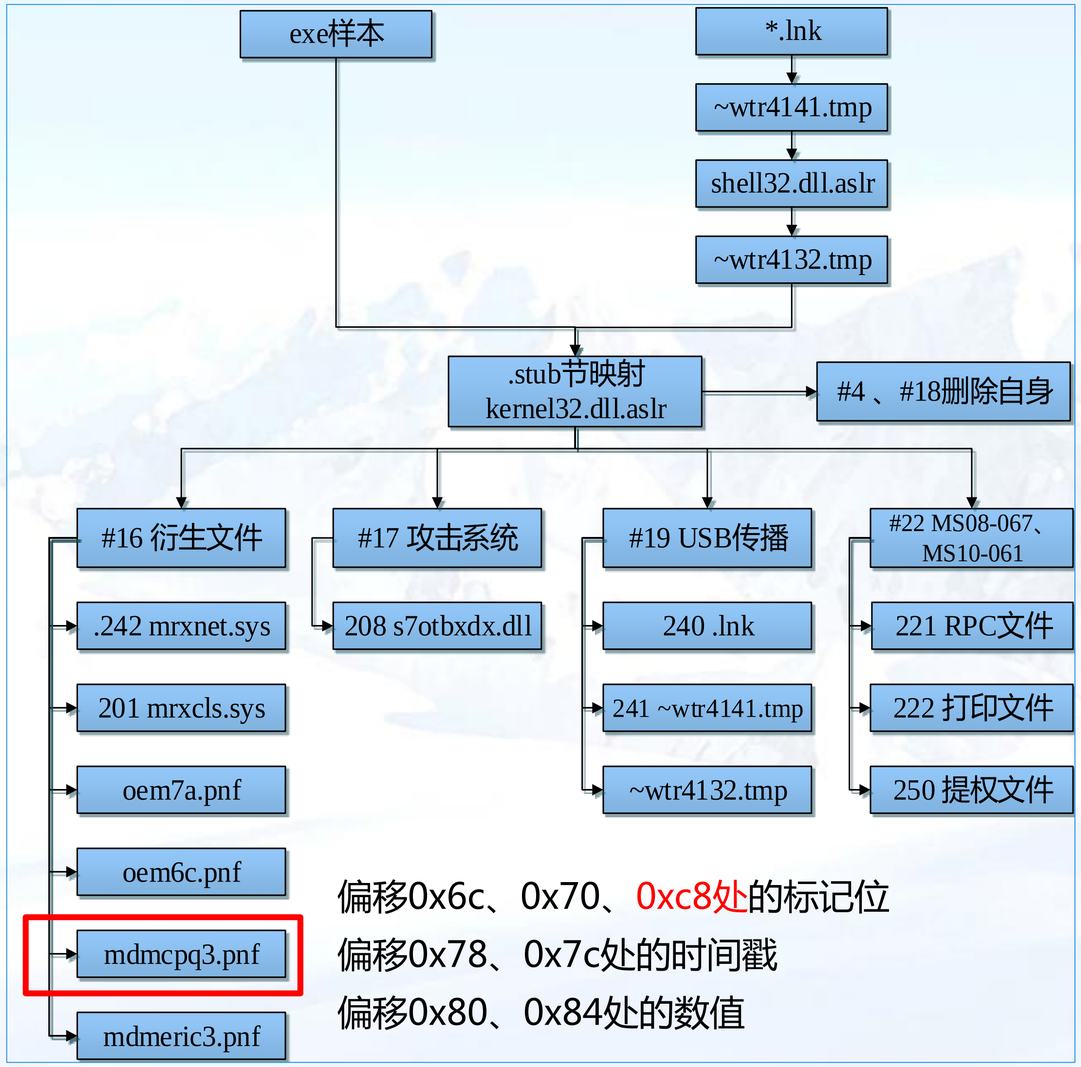
回包数据第一字节	解释
0x61(a)	收集系统详细信息，大概20类，在上文中对不同系统有过说明
0x42(B)	删除文件成功
0x43(C)	写文件成功
0x44(D)	读取文件
0x47(G)	创建文件成功
0x55(U)	读取完成
0x71(q)	指令执行失败（多个指令失败，都返回此代码）
0x73(s)	设置文件偏移成功
0x74(t)	执行文件失败
0xa1(不可显字符)	更新远程C&C

来源：《从方程式到“方程组”EQUATION攻击组织高级恶意代码的全平台能力解析》，2016年11月首发

作业控制：后端研判支撑下的复杂的条件逻辑

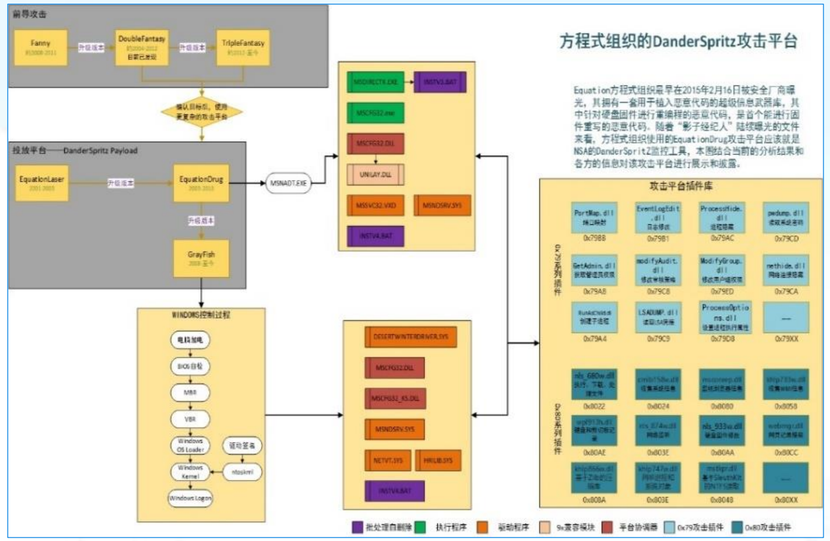


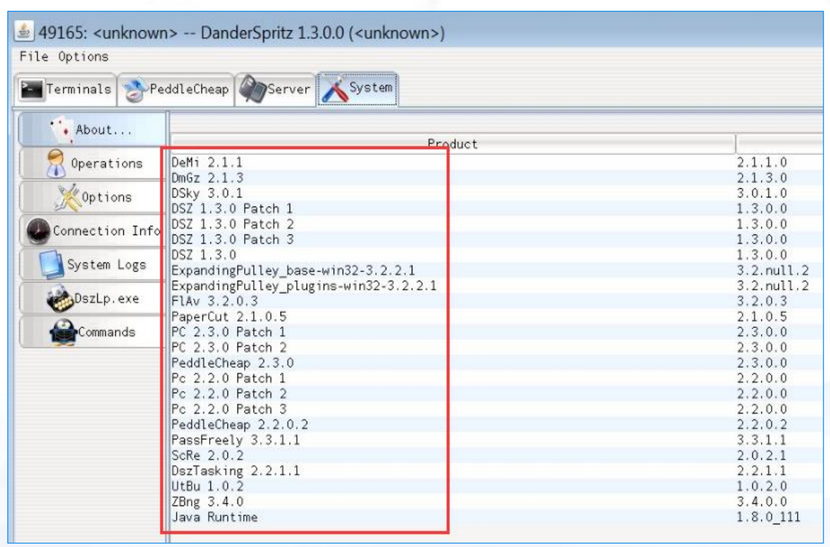


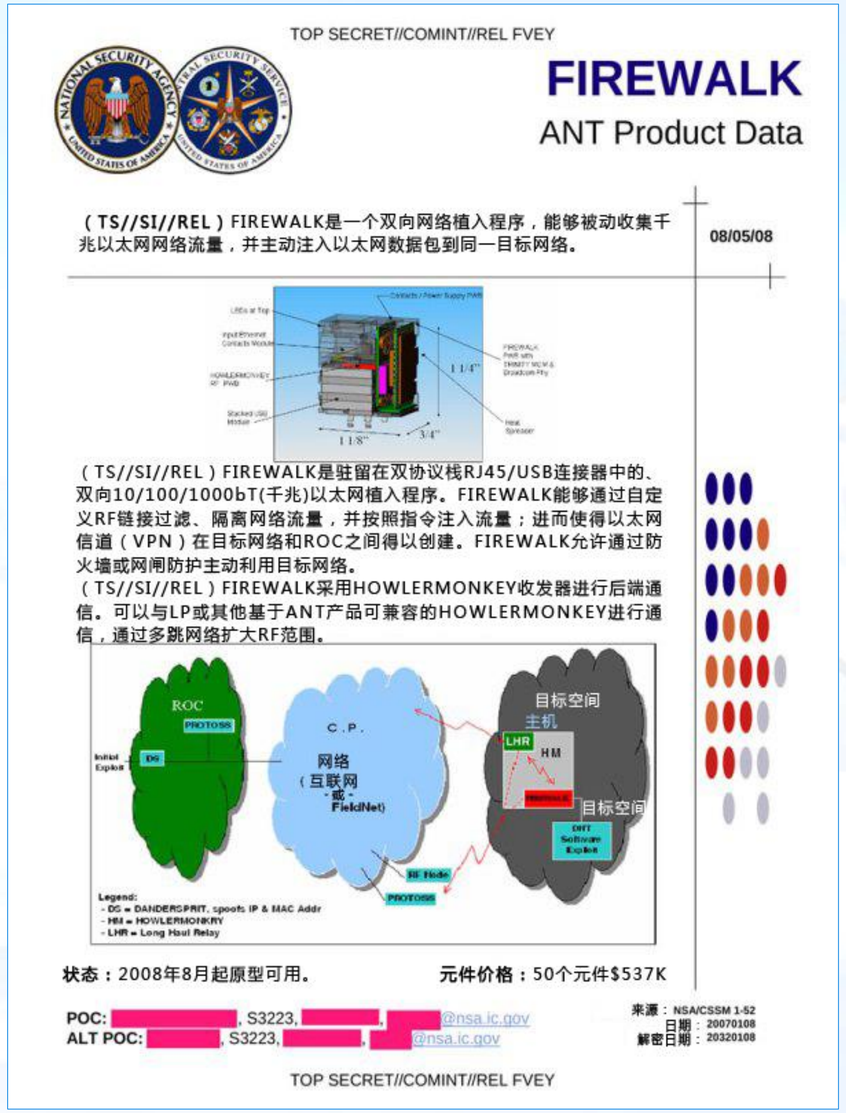


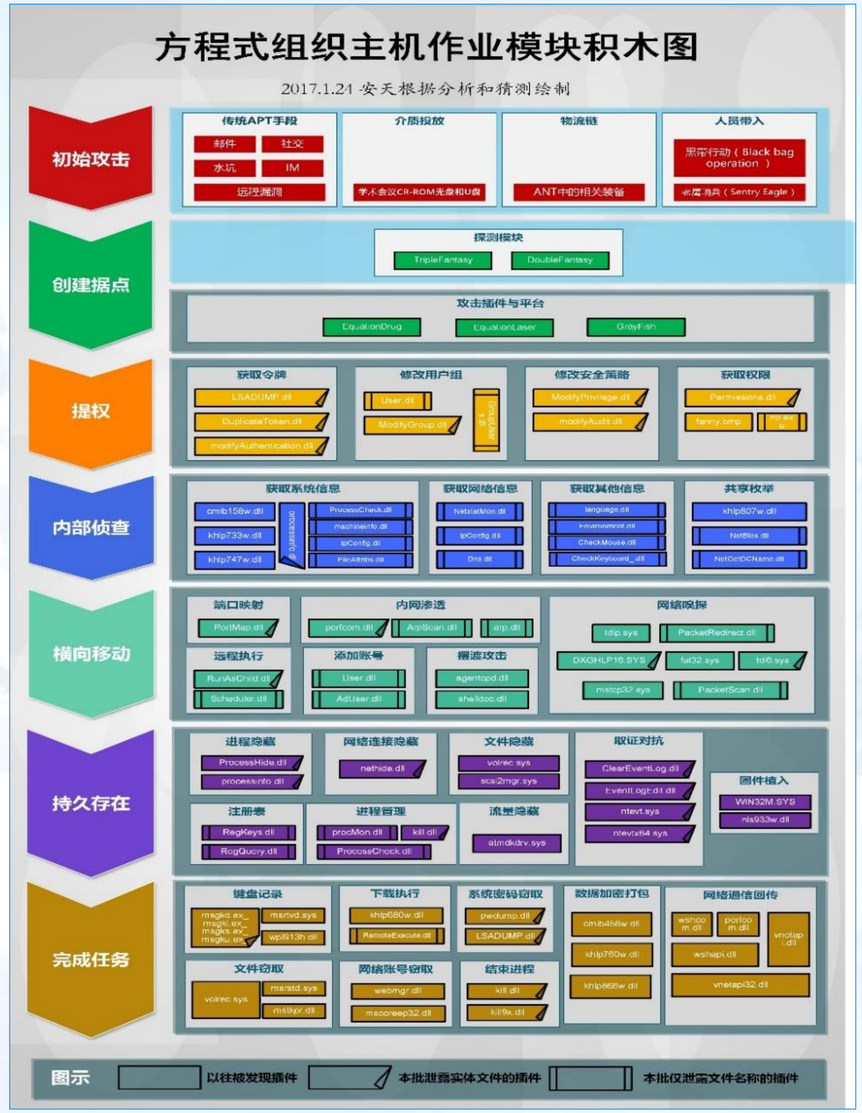
来源：安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》，2012年9月首发

对打击点的有效机理性穿透





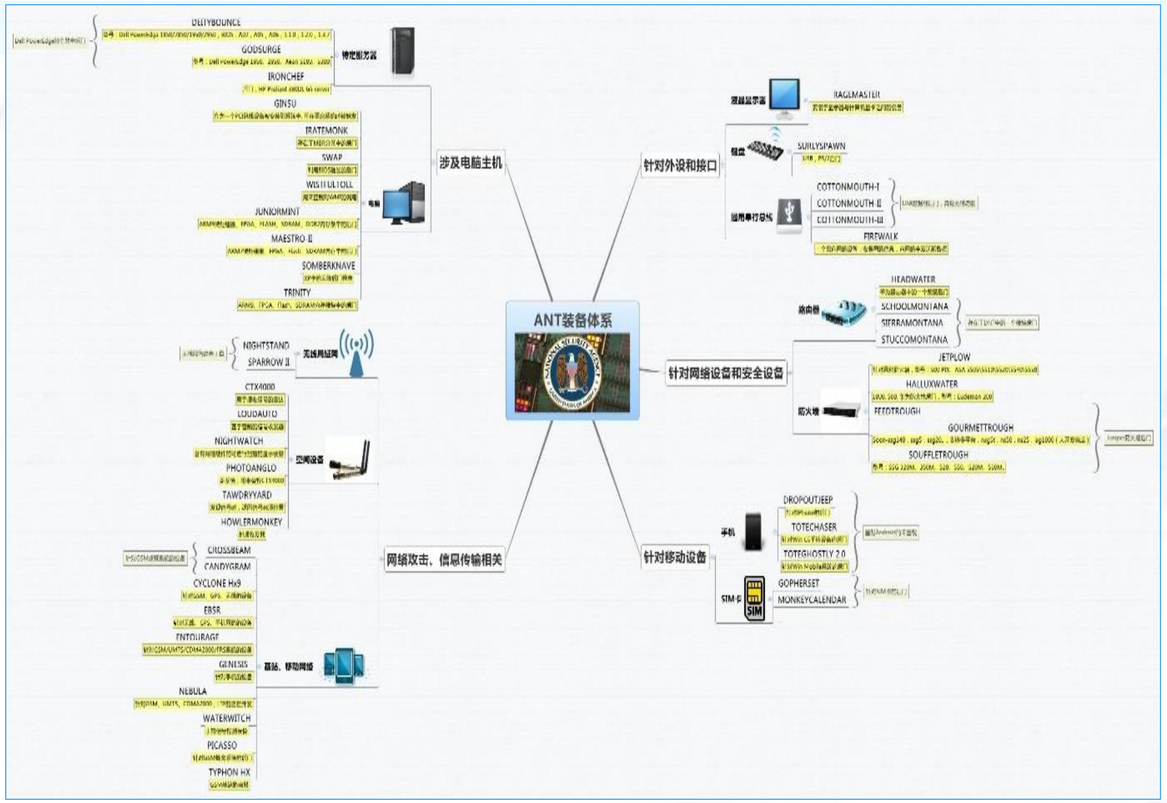




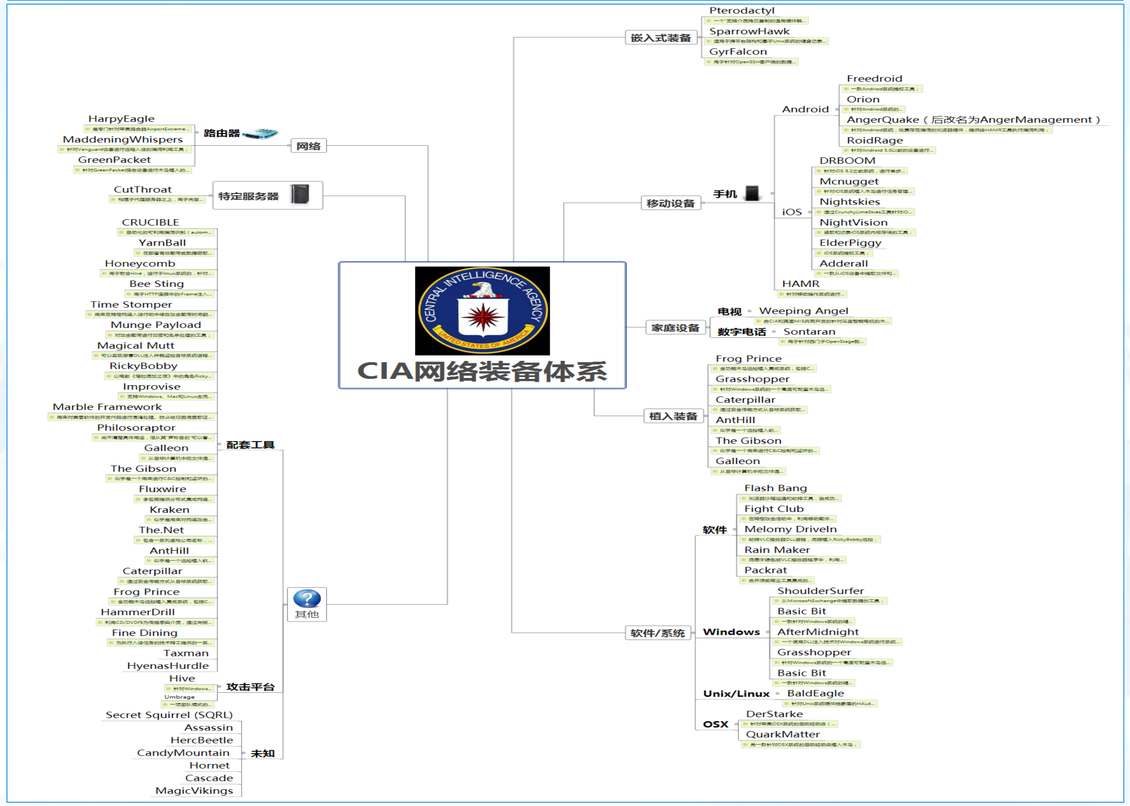
配图：引自安天针对方程式攻击组织的系列分析报告之《方程式组织EQUATION DRUG平台解析》

全场景覆盖作业

NSA的ANT平台



CIA的装备体系



CIA装备曝光引发的热度，其实是一个不正常的现象，**CIA并不处于美方能力的第一平台**，其相对今天的IT场景的覆盖深度**并没有NSA ANT对08年的IT场景覆盖力更强**，但其都展示了美方全场景覆盖的装备特点。

脑图来源：均引自安天内部分析报告

可以达成传统军事手段物理等效性的毁伤效果

	凋谢利刃与巴比伦行动（传统物理攻击伊拉克核反应堆）	奥林匹斯行动（网络空间攻击伊朗）
合作攻击方	以色列、美国、伊朗（两伊战争）	美国、以色列
被攻击方	伊拉克（没有成熟的自主国防体系，视图从法国“买来”核能力）	伊朗（有相对成熟的工业体系）
时间周期	1977-1981年	2006-2010年
人员投入	以色列空军、特工人员、伊朗空军、美国空军和情报机构	美、以情报和军情领域的软件和网络专家，还有工业控制和核武器的专家
作业准备	多轮前期侦察和空袭，核反应堆情报	战场预制、病毒的传播和、伊朗核设施情报
各方装备投入	伊朗：2架F-4鬼怪式以12枚MK82减速炸弹-轰炸核反应堆假设工地 10架F-4-袭击伊拉克H-3空军基地。 以色列：2架F-4E（S）-侦察任务；8架F-16A（美方提供）、4架F-15A、2架F-15B、16枚MK84炸弹-空袭反应堆 模拟搭建反应堆 特工人员暗杀伊拉克关键人员 美方：战略卫星和情报、空中加油机	美国： “震网”恶意代码 运维和控制体系 模拟搭建离心机和控制体系 以色列: “毒曲”恶意代码（环境采集准备）
效费比	打击快速，准备期长，耗资巨大、消耗大，行动复杂、风险高	周期长，耗资相对军事打击较低，但更加精准、隐蔽、不确定性后果更低
训练成本	18个月模拟空袭训练，2架F-4鬼怪攻击坠毁，3名飞行员阵亡。	跨越两位总统任期，经过了5年的持续开发和改进
消耗	人力、军力、财力、装备力、情报	人力、财力、情报
毁伤效果	反应堆被炸毁，吓阻了法国供应商，伊拉克核武器计划永久迟滞	导致1000台至2000台离心机瘫痪，铀无法满足武器要求，几乎永久性迟滞了伊朗核武器计划

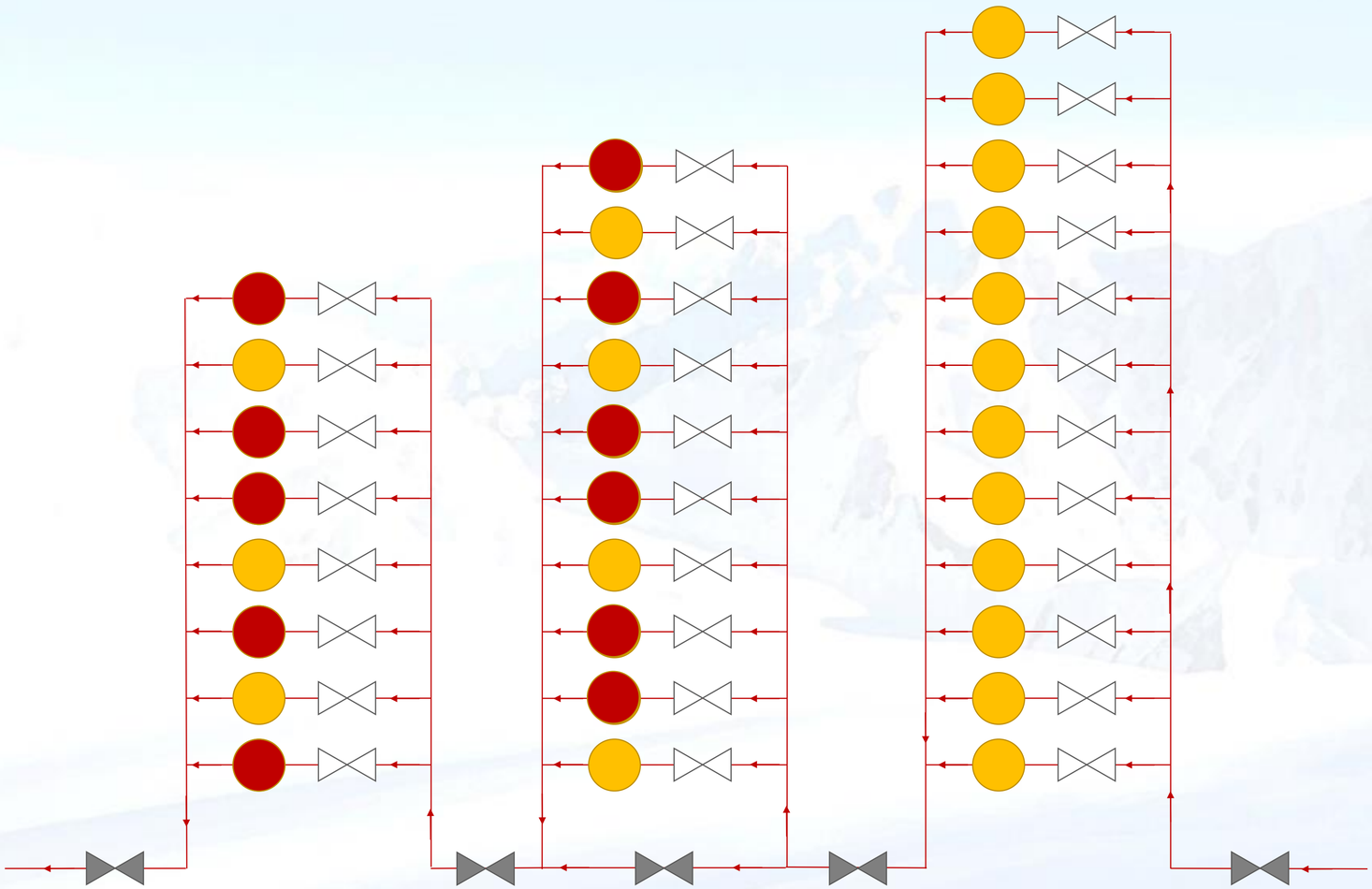
可以达成传统军事手段物理等效性的毁伤效果（续）

故障离心机

正常离心机

离心机阀门

辅助阀门



State7 完成	State6 等待攻击	State5 攻击辅助阀门	State4 等待二级压力	State3 读取二级压力	State2 攻击离心机阀门	State1 记录	State0 等待

超级大国对网络作战的需求理解

大规模与分散作战

确保能够随时投入**大规模**作战，和**多个、地理**上分散的作战，需要**各种军事能力的结合。**

建立能力，达成速度

建立需要战略深度，或**应对**可能出现在世界**任何地方**的挑战的能力；达成传统的军事平台可能无法满足的**速度。**

研发装备，应对挑战

研发针对**外交和军事**领域的更多的**网络攻击装备**，以应对削弱国家权威、政治权力分散、大规模杀伤性武器扩散等挑战。

超级大国对网络武器的理解

低成本（高效费比）

网络工具可以有许多适应环境的属性。从**生命周期成本**的角度来看，它们比其他武器系统更优越。这些系统都具有研究及开发成本，空间计划和传统平台也有很大的生产和部署成本，而网络武器的成本是最低的。从生命周期成本的角度来看，它们比其他武器系统更优越。这些系统都具有研究及开发成本，空间计划和传统平台也有很大的生产和部署成本，而网络武器的成本是最低的。

全空间和时域作战

它们可用于从参与到高端作战的所有军事行动。因为它们的影响是可逆的，所以非常适合于作战的所有阶段，包括**环境塑造**、**高烈度对抗**以及**重建**。它们可以在多个时间点发起攻击，包括针对**早期开发**（例如导致可靠性问题）、**使用决策**。

网络攻击的装备体系、支撑体系和作业方式的总结

端点目标

桌面计算机

- RAGEMASTER
- OCEAN
- SURLYSPAWN
- MOCCASIN
- COTTONMOUTH-I
- COTTONMOUTH-II
- COTTONMOUTH-III
- FIREWALK
- DEWSWEEPER
- COMMONDEER
- EGOTISTICALGIRAFFE
- MULLENIZE
- OLYMPUS
- QWERTY
- EQUATION
- Stuxnet
- TURBINE
- YELLOWPIN
- GINSU
- IRATEMONK
- SLICKERVICAR
- SWAP
- WISTFULTOLL
- SOMBERKNAVE
- ARKSTREAM
- BULLDOZER
- RADON
- UNITEDRAKE

移动终端

- TOTEGHOSTLY 2.0
- TOTECHASER
- DROPOUT.JEEP
- PICASSO
- MONKEYCALENDA
- GOPHERSET

服务器

- FLUXBABBIT
- IRONCHEF
- GODSURGE
- DEITYBOUNCE

微型计算机

- MAESTRO II
- TRINITY
- JUNIORMINT

网络场景

网络设备

- NIGHTSTAND
- SPARROW II
- HEADWATER
- SCHOOLMONTANA
- SIERRAMONTANA
- STUCCOMONTANA

网络安全设备

- SOUFFLETROUGH
- GOURMETTROUGH
- FEEDTROUGH
- HALLUXWATER
- JETPLOW

信号设备

- TAWDRYYARD
- PHOTOANGLO
- CTX4000
- NIGHTWATCH
- DRTBOX
- HOLLOWPOINT
- WATERWITCH
- TYPHON HX
- NEBULA
- ENTOURAGE
- EBSR
- BSR
- CYCLONE Hx9
- CANDYGRAM
- CROSSBEAM
- MAGNETIC
- ANGRYNEIGHBOR
- LOUDAUTO
- wx
- HOWLERMONKEY
- GENESIS

作业方式

- 人
- 供应链
- 物理劫持
- 仓储
- 摆渡

支撑体系

资源库

- COTS
- TURBINE
- FLYING PIG
- FOXSEARCH
- RONIN
- CADENCE

技术库

- QUANTOMINATION
- SHORTSHEET
- CONJECTURE
- SPECULATION
- FINKOTTERENT
- ZESTYLEAK
- FREEZERAMP
- THROWDUSINGFIRSTY
- EGOTISTICALGOAT
- DIETYBOUNCE
- EXPLOITS

攻击∞分析平台

- QUANTUM INSERT IOE
- QUANTUMBOT
- QUANTUMCOOKIE
- QUANTUMCOPPER
- QUANTUMDNS
- QUANTUMHAND
- QUANTUMPHANTOM
- QUANTUMSKY
- DanderSpritz
- FuzzBunch
- OLYMPUSFIRE
- BUZZDIRECTION
- BLASTSING
- BARGLEE
- BANANAGLEE

配套工具

- MAILORDER
- FERRETCANNON
- MUTANT BROTH
- MJOLNIR
- BLINDGATE
- TURBO
- TOOLS
- SCRIPTS
- OPS

其它

- Pinwale
- Overhead
- FORNSAT
- CHIMNEYPOOL

标签图示

logo	名称
目标	形态
恶意代码分类	涉及厂商

不同国家和政经集团背景攻击组织具有能力层次化特点

层次	组织	整体能力	我们能做到什么
高纬度（A^2PT）	方程式等	超级攻击组织，拥有最强的系统化和体系装备。 作业是谨慎和受控的，具有高度隐蔽性，难以分析追溯。	对获得的有限的其投放样本进行分析，根据泄露出的一些信息进行作业复现。
中高纬度（APT）	破烂熊、沙虫等	拥有高级能力的单兵精英团队， 拥有较高水平的恶意代码和漏洞利用程序。 作业是相对谨慎和受控的。作业相对隐蔽。 与民间能力有深度互动机制。	对其样本进行相对完整的分析，对其作业过程进行沙盘推演分析。
中纬度（APT）	白象2、绿斑点等	有一定能力的攻击组织。 使用水平不高的自研恶意代码和商业漏洞。 作业相对容易暴露。	可以根据事件线索快速提炼其整个攻击资源，对其攻击作业链进行相对完整的分析。
低纬度	白象1、海莲花等	一般化能力攻击组织 作业是普遍的和失控的。	可以不依赖外部线索捕获其攻击，可以深度分析其比较完整的作业链条，作业回路。基于开放式情报的追踪溯源画像攻击组织，部分可以关联到自然人。

2 新威胁、新装备、新手段

精确打击与低成本半定向打击

	震网事件	乌克兰变电站遭受攻击事件	伪装必加（PETYA）事件
主要攻击目标	伊朗核工业设施	乌克兰电力系统	系列关键信息基础设施
关联被攻击目标	Eoolad Technic Engineering Co（该公司为伊朗工业设施生产自动化系统） Behpajooh Co.Elec & Comp.Engineering（开发工业自动化系统） Neda Industrial Group（该公司为工控领域提供自动化服务） Control-Gostar Jahed Company（工业自动化公司） Kala Electric（该公司是铀浓缩离心机设备主要供应商）	乌克兰最大机场基辅鲍里斯波尔机场 乌克兰矿业公司 乌克兰铁路运营商 乌克兰国有电力公司UKrenergo 乌克兰TBS电视台	乌克兰（副总理Pavlo Rozenko、国家储蓄银行（Oschadbank）、Privatbank等银行、国家邮政（UkrPoshta）、国家电信、市政地铁、乌克兰首都基辅的鲍里斯波尔机场、电力公司KyivEnergo）
作用目标	上位机（Windows、WinCC）、PLC控制系统、PLC	办公机（Windows）、上位机（Windows）	办公机（Windows）、上位机（Windows）
造成后果	大大延迟了伊朗的核计划	乌克兰伊万诺-弗兰科夫斯克地区大面积停电	乌克兰多个关键信息基础设施瘫痪
核心攻击原理	修改离心机压力参数、修改离心机转子转速参数	通过控制SCADA系统直接下达断电指令	对文件进行加密并影响系统引导
使用漏洞	MS08-067（RPC远程执行漏洞） MS10-046（快捷方式文件解析漏洞） MS10-061（打印机后台程序服务漏洞） MS10-07（内核模式驱动程序漏洞） MS10-092（任务计划程序漏洞） WINCC口令硬编码	未发现	MS17-010（“旧”漏洞）
攻击入口	USB摆渡[24] 人员植入（猜测）	邮件发送带有恶意代码宏的文档	入侵软件升级
前置信息采集和环境预置	可能与DUQU、FLAME[19][20]相关	BlackEnergy采集打击一体	无
通讯与控制	高度严密的加密通讯、控制体系	相对比较简单	TOR（暗网）
恶意代码模块情况	庞大严密的模块体系，具有高度的复用性	模块体系，具有复用性	模块简单，具有复用性
抗分析能力	高强度的本地加密，复杂的调用机制	相对比较简单，易于分析	相对比较简单，易于分析
数字签名	盗用三个主流厂商数字签名	未使用数字签名	无效的微软数字签名
攻击成本	超高开发成本、超高维护成本	相对较低	成本极低

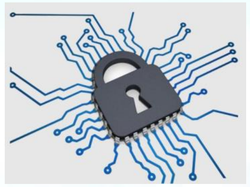
从“硬”目标到软目标（战争潜力网）“杀伤”

震网事件

攻击目标	伊朗铀离心设施
核心攻击原理	修改离心机压力参数、转子转速参数
攻击成本	超高开发、维护成本
威胁后果	延迟伊朗的核计划

V S

乌克兰电力事件



攻击目标	乌克兰电力系统
核心攻击原理	控制SCADA系统直接下达断电指令
攻击成本	相对较低
威胁后果	乌克兰伊万诺地区大面积停电

V S

伪装“必加Petya“事件

攻击目标	系列关键信息基础设施
核心攻击原理	对文件进行加密并影响系统引导
攻击成本	成本极低
威胁后果	乌克兰多个关键信息基础设施瘫痪

参考安天报告：

《安天针对攻击乌克兰等国的“必加”(PETYA)病毒分析与应对》

《乌克兰电力系统遭受攻击事件综合分析报告》

《对Stuxnet蠕虫攻击工业控制系统事件的 综合分析报告 》

复合民间行为体——“素人”式攻击

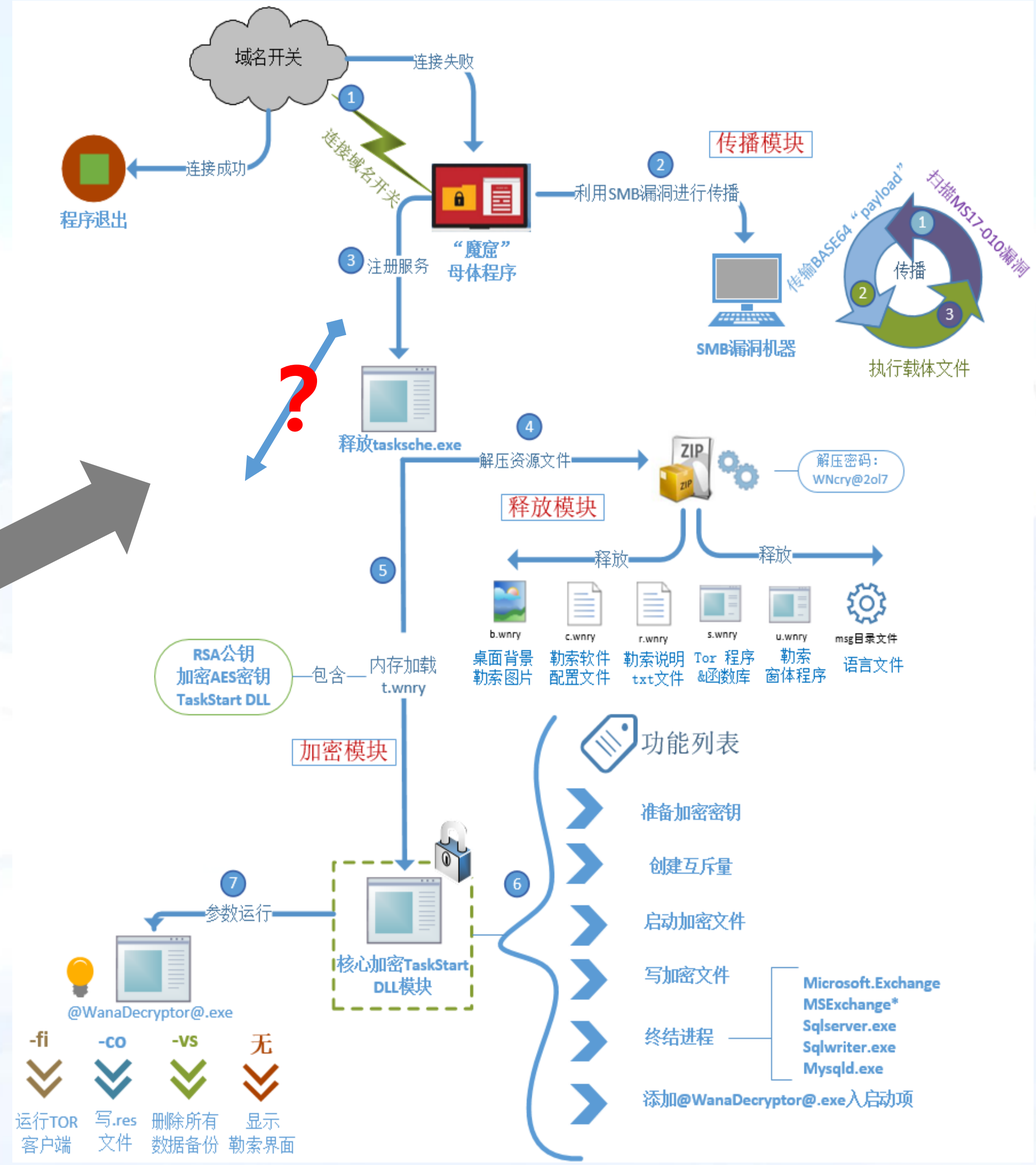
2016年12月30日，美国国土安全部和FBI公布13页俄利用黑客介入美国选举的报告，这是美国首次在官方报告中点名俄罗斯主使恶意黑客攻击。

《纽约时报》报道，普京称有“爱国心的”俄罗斯黑客可能以私人方式卷入干涉美国总统大选的网络袭击事件。普京称这些“爱国的黑客”可能了解了一些国际关系后，以“自认为正确的方式打击他们认为对俄罗斯不利的事”。

看似用粗糙的方法，打击到对手的关键部位，影响对手基础稳定性。
战略性的行动并不必然使用先进的武器

复合民间行为体成为了一种必须考虑的作业样式

- 主要已知证据均在于勒索模块和此前朝方样本相关的关联（代码和场景关联）。
- 最核心的证据断链在于其主体和勒索模块之间还没有强同源性证据关联
- 安天完成了这一闭环证明



信息军工复合体与新的装备供应商

传统军工复合体正在成长为军工信息复合体

Raytheon Buys Websense for $1.9B as Traditional Defense Shifts to Cyber

Kyle Alspach - National Tech Editor
4/20/15 @8:31am in Tech

243

On Monday, Waltham, Mass.-based defense giant **Raytheon** announced it is spending big in an area well outside the realm of missile defense and military electronics. In an acknowledgment of the rising importance of cyber defense, Raytheon (RTN) paid $1.9 billion to acquire cybersecurity firm **Websense**, as part of a deal that will combine the Austin, Texas-based firm with Raytheon's Cyber Products business unit.

Specifically, Raytheon is forming a new joint venture with private equity firm **Vista Equity Partners**, which had acquired Websense in mid-2013 for about $1 billion. That amounts to the valuation "basically doubling in almost two years despite very modest growth at the company," writes Daniel Ives of **FBR Capital Markets** in a research note.

雷神公司1.9亿收购Websense

Raytheon

大型国防承包商，爱国者导弹系统制造商，军工技术、政府与商业电 子技术、公务飞机和特殊任务飞机等行业的龙头老大。

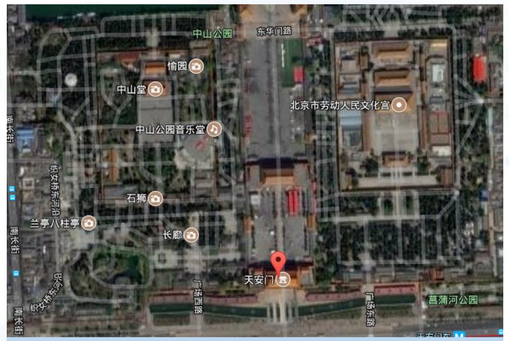
Websense

整合Web、信息和数据安全防护解决方案提供商。主营

Email Security、Web Security和Data Security.

信息复合体正在向信息军工复合体成长

谷歌大狗训练



谷歌街景地图

网络安全企业正在向网络装备供应商成长

2013年开始，通过美国国防预算法案932.b，美国五角大楼要求所有与美国五角大楼连接的基础供应商，开始叠加新的动态检测能力。

网络商业军火的“军火商”

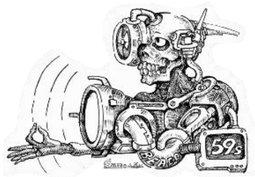
- **Cobalt Strike作者：Raphael Mudge（美国）**
  - LLC创始人（the creator of Armitage and founder of Strategic Cyber LLC, develops Cobalt Strike）；
  - 基于华盛顿的公司为RED TEAM开发软件，为Metaslpoit创造了Armitage、sleep程序语言和IRC客户端jIRCii；
  - 曾是美国空军的安全研究员，渗透实验的测试者；
  - 他设置发明了一个语法检测器卖给了Automattic；
  - 发表多篇文章，定期进行安全话题演讲，给许多网络防御竞赛提供RED TEAM，曾参加2012-2014年黑客大会；
- **教育背景：**Syracuse University 美国雪城大学，密歇根科技大学
- **目前就职：**Strategic Cyber LLC（战略网络有限责任公司），特拉华州空军国民警卫队

公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6
Automattic	代码Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息 军官	2004.3-2008-3

商用攻击平台+恶意代码为核心的军火扩散影响地区平衡

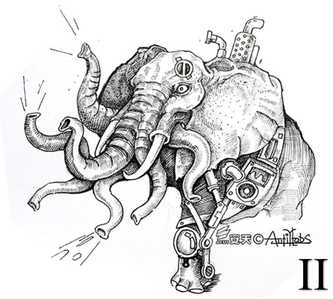
行动能力

商业军火支持的APT



2015.5
APT-TOCS

常规的APT



2015.12
II 白象II代

A²PT

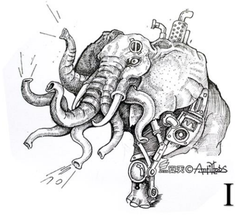
2015.2
Equation
方程式

2007或2008
Duqu
毒曲

2010.3
Flame
火焰

2009.6
Stuxnet
震网

初级的APT



2013.5
I 白象I代

成本投入

3 敌情想定的完善和具象化

指挥员对敌、我、民情及地形要熟悉……敌情、我情、地形是下决心的依据。

——彭德怀《关于陕北九个月作战的几点认识》

什么是无有效敌情想定的安全思维？

- 假想某一手段是不可逾越的屏障——如物理隔离。
- 假想内部人员都是可靠的——好人假定。
- 假想系统布防是从纯白环境开始的——从零开始。
- 假定安全规范是被100%落实——纸上谈兵
- 假定某种单点创新能解决所有问题——银弹
- 假定供应链、仓储、物流等环节是可靠的，或者没有关注这些环节。
- 假定对手是完全基于线上完成安全作业的。
- 假定云、通讯链路等基础环节是可靠的。

防御体系的建立需要以有效的敌情想定为前提

- 减少应激驱动，建立常态化防御能力改进。
- 物理隔离+好人假定+规定推演，构成了当前最大的自我安全麻痹。

“物理隔离”防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。

——引自习近平总书记《在网络安全和信息化工作座谈会上的讲话》

- **内网：已经被渗透**
- **供应链：被上游控制**
- **运营商网络：关键路由节点被控制**
- **物流仓储：被渗透劫持**
- **关键人员和周边人员：被从互联网进行定位摸底**
- **内部人员：有敌特的人员派驻或被发展**

（战时）高烈度对抗
（平时）持续性对抗
（平战）无底线对抗
（平战）高成本对抗

2016年6月2日，在有关部门组织的内部研讨会上，安天首次提出了“有效敌情想定”是网络安全工作的前提的观点。

以总体安全观视角完善网络空间的敌情分析

政治安全

国土安全

军事安全

经济安全

文化安全

网络空间

社会安全

科技安全

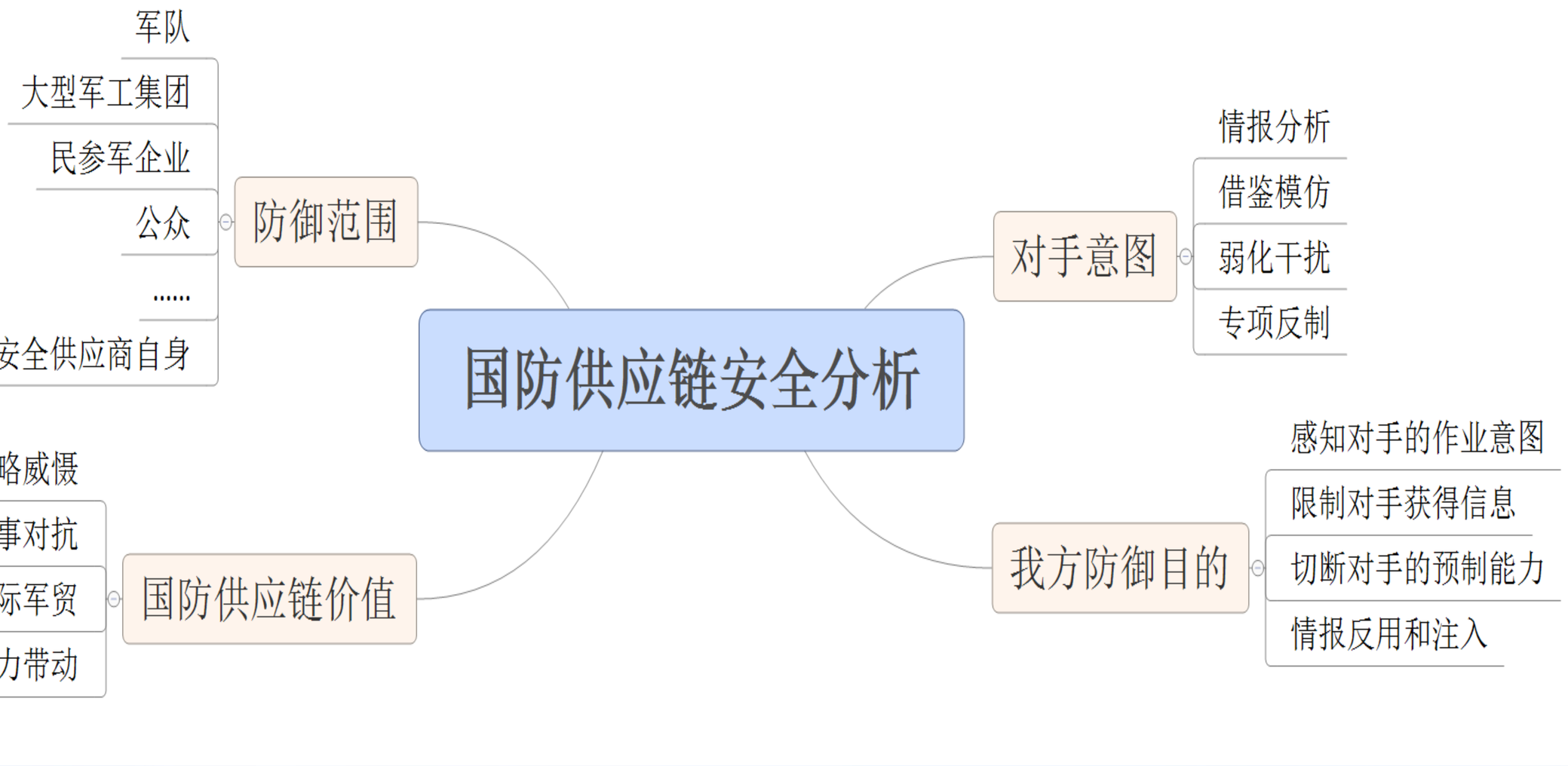
信息安全

生态安全

资源安全

核安全

准确分析对手意图建立合理防御指向和布防范围



传统安全问题的网络空间延展与总体安全视角

美方如何削弱越南对中国武器的信任

投放"陷阱弹“+ "邪恶心理战"

炸膛的56式自动步枪

破坏对手对军贸伙伴的信任。

在己方军贸产品中实现感知和情报能力延展。

上述行为在网络空间时代具有了更大的实施空间。

美方对以色列飞行员的“所见即所得”

战斗机出口+联合头盔提示系统

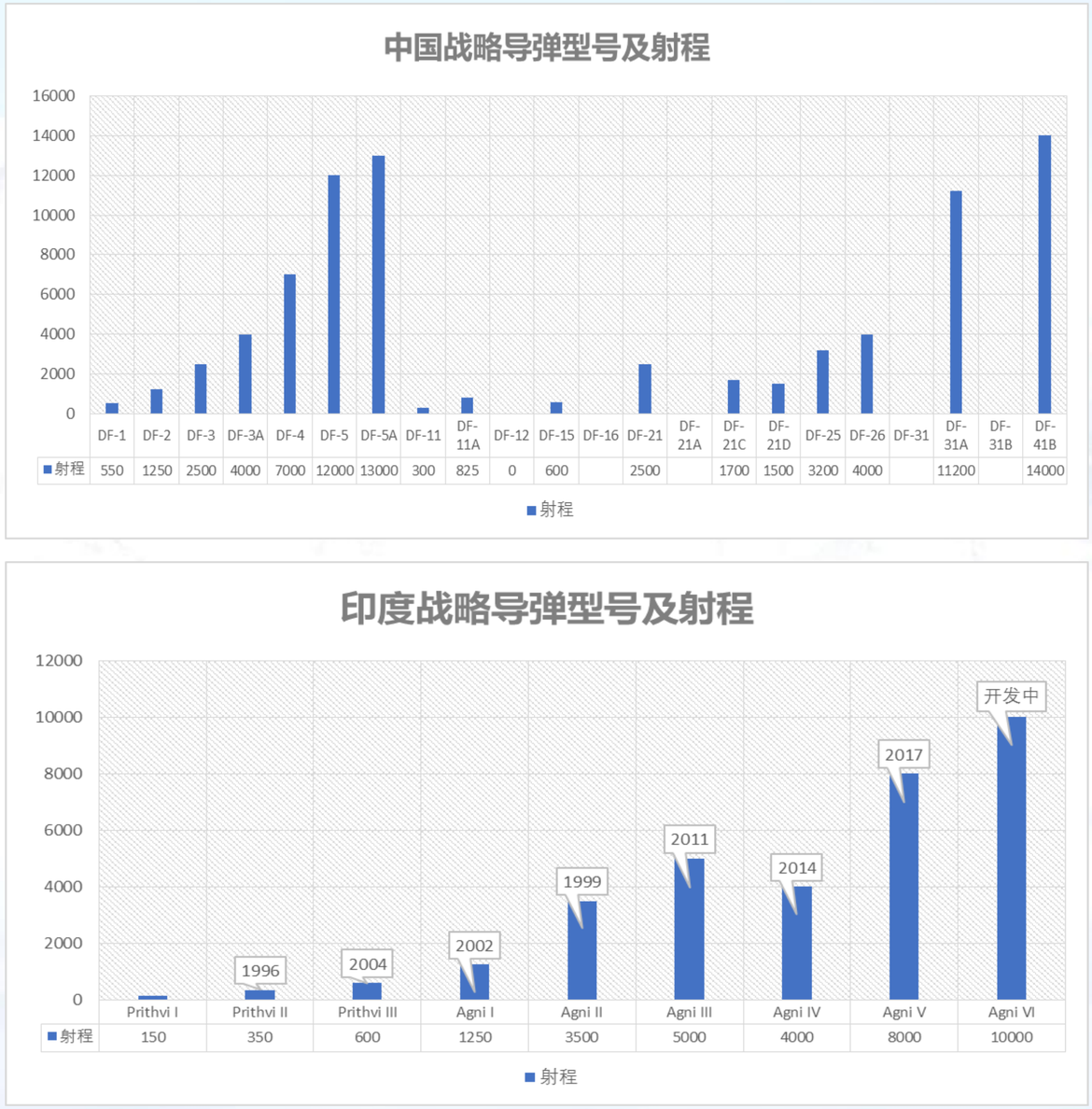
美方“长子行动”(ProjectELdestSon)：

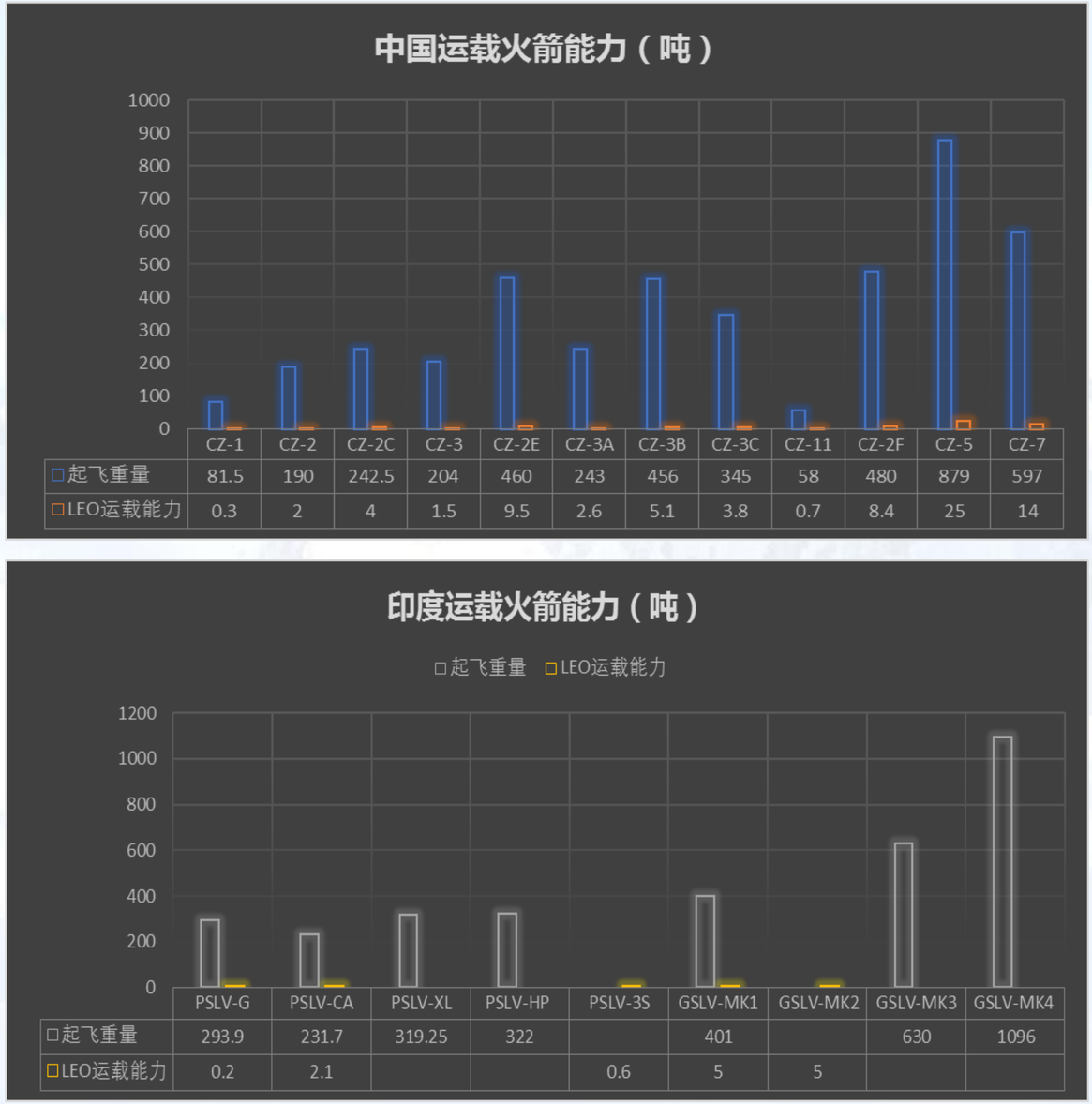
在侵略越南期间，美军特种作战团(SOG)开展了一项绝密计划，称为“长子行动”(ProjectELdestSon)，以期在北越方面制造全面混乱，并使北越战士和游击队员对中国援助的武器安全性产生怀疑。

联合头盔提示系统：

美军F-16战机配备的联合头盔指示系统，能显示武器瞄准标记和主飞行信息及累加合成图像。Tac-Eye显示系统是专为美军设计的，由美国空军实验室和美国特种部队司令部进行了部分投资,Icuiti公司用3年时间开发了这套系统。

国土安全、军事安全和科技安全的综合视角





敌情想定是针对性的、具象的

我方机构和行业领域	敌方攻击意图	攻击目标和入口	目前场景特点和缺陷
自主产品企业	植入漏洞弱化我产品安全性;获取我方代码和产品进行漏洞分析挖掘;窃取产品证书绕过白名单	环境入侵、跳板攻击、人员带入等	开发人员自身的安全能力和经验不足；缺少有效的安全开发方法引入；缺少场景安全保障
高科技企业	获取我方技术成果进行抄袭模仿；在商业竞争中获取谈判等优势；在产品进行预制弱化下游环节安全	互联网侧直接攻击、基于上游供应链入口的攻击等	人员高度依赖互联网，容易被从网上定位摸底，
军工企业、民参军企业	获取装备信息参数；借鉴模仿；弱化干扰我方武器能力，进行针对性对抗	针对关键人员摸底的间接攻击、人员带入等	较大比例是制造、电子、精密加工企业，网络安全意识和投入不足
高等院校、科研院所	窃取我方科技成果；获取我方重大工程项目进展；了解国防和其他关联领域情报	互联网入口；学术交流活动和等	缺少持续性的安全防御投入和能力；依赖阶段性的保密检查推动安全改进；人员流动性较大。
遥感测绘部门	获取我方基础数据、干扰篡改测绘数据	监听还原信息传输、入侵存储数据等	以发展和效率为主导的思路，缺少总体安全观的指导
智囊机构	获取我方决策支持思路、	社会工程；基于互联网以邮件等入口直接攻击等	个人单点目标价值大、人员安全意识差、

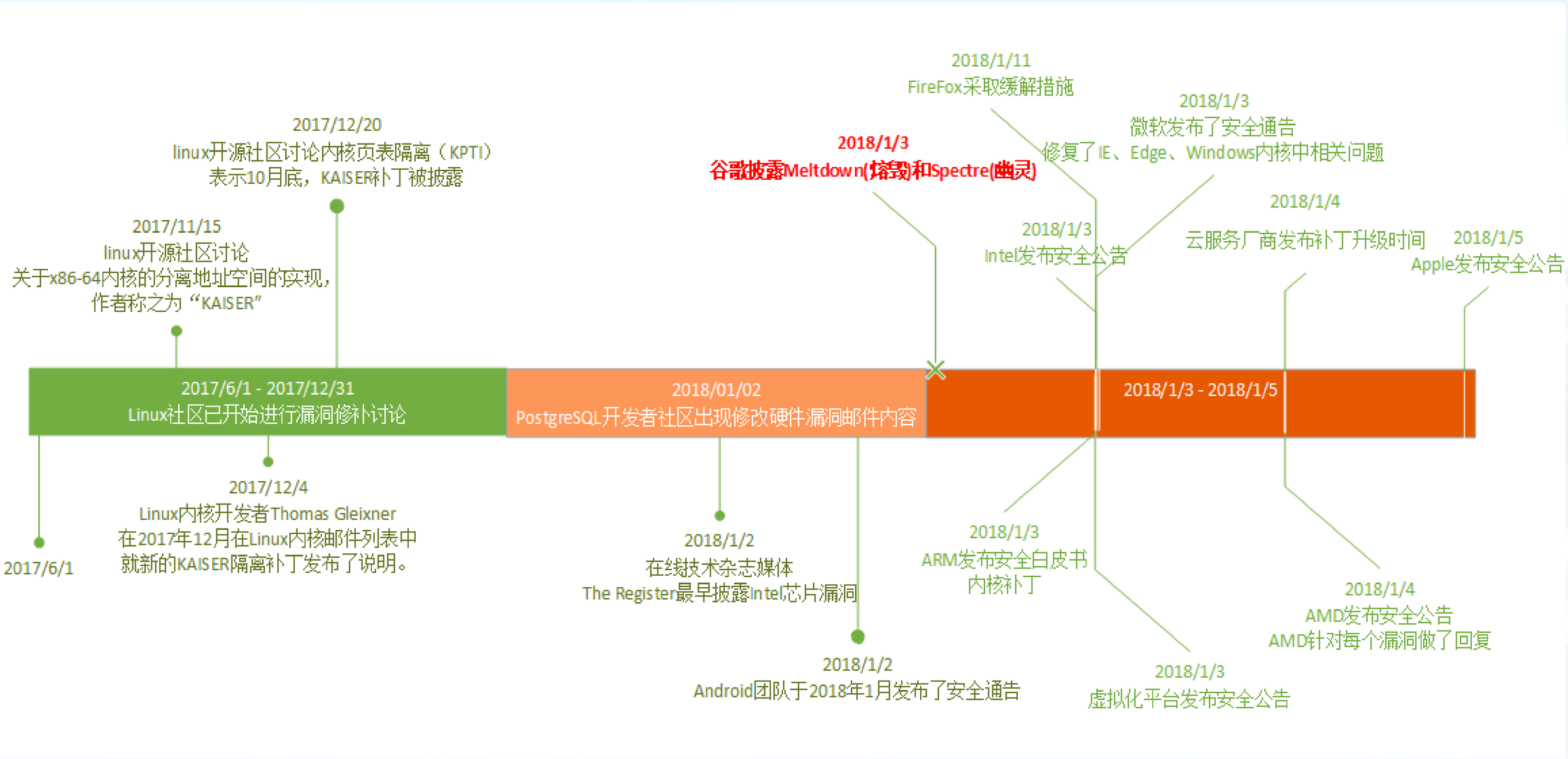
几个典型的需要梳理敌情想定的攻击场景

敌情想定是基于对手作业能力和机会窗口期的对位

	白象一代（2012）	白象二代（2015）
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标（如高等院校）	以中国的大面积目标为主，包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE双扩展名、打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114 CVE-2012-0158 CVE-2015-1761
二进制攻击载荷开发编译环境	VC、VB、DEV C++、AutoIT	Visual C#、AutoIT
二进制攻击载荷加壳情况	少数使用UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10~16人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

- 我们不只面临风险，而是面临后果。
- 对手作业窗口遭遇未修复漏洞，要以对手已经利用漏洞完成植入为想定，形成深入排查和重新布防，而非简单的漏洞修补。
- 恶意代码、僵尸网络感染未及时处理，不是简单的消杀，而是要基于已经被对手劫持控制利用来进行应对。

信息化现状的复杂性与攻击机会窗口叠加是一个复杂问题



A级漏洞Meltdown(熔毁)和Spectre(幽灵)的处置分析说明重大漏洞补丁处置极为复杂
而攻击时间窗口需要深入分析推演

以正确网络安全观为指导

网络安全观

- 本质
  - 对抗
- 支点
  - 防御能力
  - 威慑能力
- 核心特性
  - 整体：网络安全是整体的，不是割裂的
  - 动态：网络安全是动态的，不是静态的
  - 开放：网络安全是开放的，不是封闭的
  - 相对：网络安全是相对的，不是绝对的
  - 共有：网络安全是共有的，不是孤立的
- （对抗的）层次结构
  - 技术博弈：技术对技术，技术管技术
  - 理念博弈：四项原则，五点主张；网络主权；网络空间人类命运共同体
  - 话语权博弈
- 策略与成本
  - 关键基础设施设施：相关机构、人民军队死看死守
  - 基本设施：地方政府适度防护
  - 其他目标：完全交给市场
- 供应链、技术合作路径选择
  - 可控引进
  - 消化吸收再创新
  - 合作开发
  - 完全靠自己的力量

建立从无损到量损、止损的安全认知

从网络安全本质和有效敌情想定出发

充分认知网络安全的对抗本质，对斗争的烈度、持续性、复杂性和变化性建立充分的认识。展开更细粒度的敌情想定工作。

立足实际的基本条件

立足于整体、动态、开放、共有，作为网络领域斗争的基本条件，以相对性重新看待网络安全的策略设定和要求。

建立新的工作导向

追求无损是一种绝对安全思维，追求常态有效防护；
应急有效量损、快速止损、积极反制才是实事求是的选择。

习近平强调，**“备豫不虞，为国常道”**。当前，我国正处于一个大有可为的历史机遇期，发展形势总的是好的，但前进道路不可能一帆风顺，越是取得成绩的时候，越是要有**如履薄冰的谨慎**，越是要有**居安思危的忧患**，绝不能犯战略性、颠覆性错误。面对波谲云诡的国际形势、复杂敏感的周边环境、艰巨繁重的改革发展稳定任务，我们既要有**防范风险的先手**，也要有**应对和化解风险挑战的高招**；既要**打好防范和抵御风险的有准备之战**，也要**打好化险为夷、转危为机的战略主动战**。我们要继续进行具有许多新的历史特点的伟大斗争，准备战胜一切艰难险阻，朝着我们党确立的伟大目标奋勇前进。