靶场发展态势③美国防部赛博安全靶场（IAR/CSR）

原创

systemino 于 2019-11-17 19:52:30 发布 1323 收藏 7

美国国防部在2018年依据美国白宫公布的《国家网络战略》（National CyberStrategy），制定其《国防部网络战略》（Department ofDefense Cyber Strategy），阐明落实网络战略目标的五大路线：建立致命战力、网络空间竞争与吓阻、强化同盟并吸引新合作伙伴、部内组织改革、以及人才培育。依循此路线，美国国防部在其网络战略中，亦明确指出三个作战概念，遂行网络作战：收集情报、为危机或冲突时所需的军事网络作战能力进行准备、「前沿防御」（Defend forward）以从源头破坏或终止恶意网络行动（disrupt or haltmalicious cyber activity at its source）。新的作战概念「前沿防御」，意味着美国会采取更具攻击性的手段进行防御，此概念势必透过网络任务部队的编制、演训等来实施，为此美军已实施网络空间靶场综合体及网络作战平台“统一平台”等实施载体，CSR作为网络空间靶场综合体的一部分，本小节将介绍美国国防部赛博安全靶场。

2.4.1.CSR背景

CSR全称是DoD Cyber SecurityRange，中文简称赛博安全靶场，是美国国防部国防信息系统局组织建设的一个专门模拟仿真美军国防网络环境的测试与评估靶场，是美国国防部四大靶场之一。美军国防信息系统局赛博安全靶场（CSR）前身是2010年美军组建的信息保障/计算机网络防御靶场（DoD IA/CND Range，IAR），以下简称IAR靶场。后来根据使命任务及作战演训需要，以及2014年美军将“信息保障”重新定义为“赛博安全”，奇热将“全球信息栅格GIG”变更为“国防部信息网络”，该靶场的名称也随之变更为美国国防部赛博安全靶场（CSR）或美军国防信息系统局赛博安全靶场。同时，作为美国国家网络空间靶场综合体计划的一部分，美军国防信息系统局赛博安全靶场（CSR）同时也和国防部的其他三大靶场如JIOR、NCR以及C4AD靶场进行互联互通和资源共享。

全球信息栅格（GIG）的普遍互连性使其日益成为网络攻击新的源头，对攻击者的吸引力日益增加，美军为保障全球信息栅格（GIG）的信息安全，着手准备建立针对全球信息栅格（GIG）的模拟仿真靶场，以研究和测试全球信息栅格（GIG）信息保障和防御技术，并更好的保护全球信息栅格（GIG）。全球信息栅格GIG是美国在2014年之前主要运行的，通过光缆连通分布全球的美军基地国防信息基础设施全部节点，囊括各军种作战网络和军事卫星网、联合战术无线网络的全球军用作战网络。2014年升级为国防部信息网络（DoDIN）。

IAR靶场基于美国国家全面网络安全计划（CNCI）、国家安全总统令54、国土安全部总统令23进行构建，由国防部CIO、DISA和HQMC C4联合执行。计划支持信息保障（IA）、计算机网络防御（CND）和其他源自网络中心战略和国家综合网络安全计划（CNCI）的国防部（DoD）网络要求，以提高国网网络的安全性网络并培育网络安全教育。IAR靶场提供了操作上逼真和可控的网络仿真模拟环境，以支持演习、培训、测试和评估，而不会对运营网络造成任何风险。它还提供网络操作（NetOps）、CND、IA以及可利用和攻击的网络事件，并支持新功能的测试和评估，具有快速经验积累的沉浸式培训，战术技术和程序（TTP）的开发和验证，系统互操作性和集成测试，运营和开发测试以及认证和鉴定能力测试等。

该靶场主要由美泰科技（ManTech）进行构建，包括第一代的IAR靶场以及第二代的CSR靶场。美泰科技创立于1968年，总部位于美国弗吉尼亚州Fairfax，全职雇员7,000人，是一家国防信息安全技术服务供应商，为美国国防及政府设计、开发、采购和维护任务关键的企业信息技术。美泰科技为CSR提供的现实世界网络效果建模如下图所示：

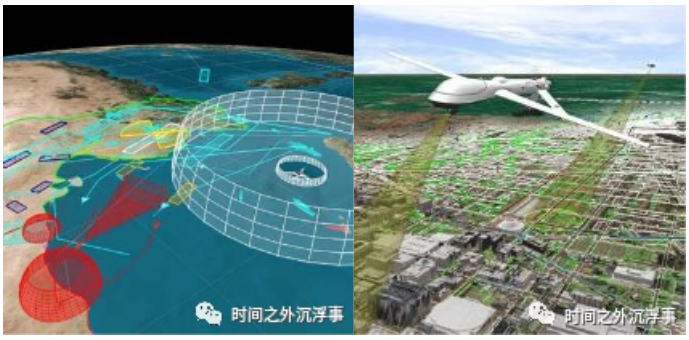

图27 CSR现实世界网络效果建模

和上述小节我们概述的JIOR和JCOR靶场的不同点在于，IAR靶场/CSR是模拟美军国防及涉及国防的企业网络环境，而JIOR是美军诸多兵军种网络测试环境的联合体，JCOR则是美军诸多兵军种各自的模拟器建模的专网环境的测试环境联合体。CSR最初是的使命也是为了基于仿真的国防网络环境测试和评估新功能以及培训国防网络维护者的计算机防御技能。

2.4.2.IAR架构

IAR靶场是一个基础架构平台，旨在将分布式和异构的信息保障（IA）体系结构系统和解决方案与国防部（DoD）计算机网络防御（CND）操作层次结构进行集成。IAR靶场为国防部利益相关者提供了增强GIG安全态势的途径。

IAR靶场为网络演习，CNDSP培训以及CND产品和操作策略、技术和程序（TTP）的测试和评估提供了一个联合服务环境，该环境反映了DoD NetOps 1-3层上的全球信息栅格（GIG）的信息保障/计算机网络防御（IA/CND）功能和网络服务。IAR靶场1-3层典型的层级结构如下图所示：

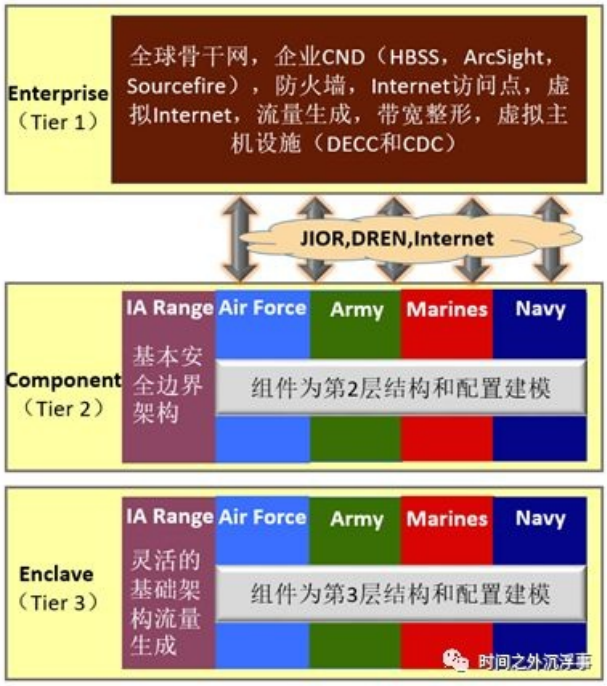

图28 DoD NetOps 1-3层级结构

如图所示，IAR靶场提供了通用的国防部（DoD）第1、第2和第3层功能。

第1层-企业层：提供模拟仿真的全球骨干网、企业CND工具（HBSS，ArcSight，Sourcefire）、企业服务（防火墙，网络流量生成，带宽整形，虚拟主机设施（DECC和CDC））、虚拟互联网（Internet访问点，虚拟Internet）等。该层通过上述服务模拟仿真GIG的全球网络，包括位于全球的美军基地的国防信息基础设施节，包括各军种作战网络和军事卫星网、联合战术无线网络等。

第2层–组件层：提供特定的安全服务，如边界访问控制、安全隔离、安全防御等；以及包括海军区域网络、空军机载网络、陆军战术互联网等战区网络远程连接（隧道）到IAR靶场的网络通道，接口；并在服务/组件级别对这些资源进行管理。

第3层-资源层：提供基础的网络架构，以及海量的主机设备等靶场资源。该层主要模拟的是GIG的战术网络，包括海军区域网子网、陆战队战术网、空军战术网、营区/哨所/兵站节点等大规模的节点。

IAR靶场可以在独立的模拟器模式下运行，也可以与作战司令部，服务和机构（CC/S/A）提供的其他靶场进行交互和互操作。IAR靶场的所有部分与作战司令部，服务和机构（CC/S/A）靶场之间的通信经过加密信道传输，保障在传输过程中的安全性。所有IAR靶场流量路由及与其他靶场互联路由均位于封闭的网络环境中，不会影响到真实环境中运行的网络。

在建设的第一期美军IAR靶场中，IAR靶场提供了一个多协议标签交换（MPLS）云，该云由代表DISA GIG的多个供应商边缘（PE）路由器组成。在PE路由器的下游是交互式基础设施，该基础设施由用于网络（核心层，分布层，访问层）的标准Cisco设计模型组成，具有8个不同的分布区域（用户区域），以模拟给定的基础设施，以及托管以下服务的服务器场：电子邮件（MS Exchange），Active Directory，域名系统（DNS），超文本传输协议（HTTP），文件共享和打印服务。一个基地内的每个用户区域可以支持10个虚拟局域网（VLAN），每个VLAN包含254个用户。从第六台PE路由器的下游有两个设施，用于托管专用应用程序，类似于国防信息系统局（DISA）国防企业计算中心（DECC）和社区数据中心（CDC）的功能。比如IAR靶场CDC托管的ArcSight和SourceFire。

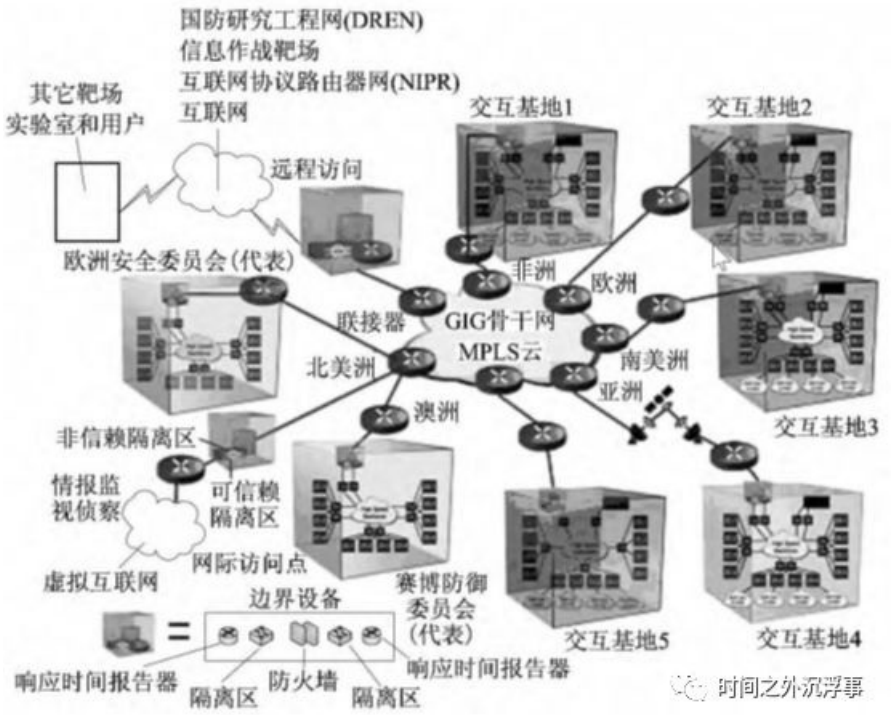

图29 GIG与其他靶场连接和互操作

如上图所示，处于图中央的核心部分是以骨干网级路由器构成的美军全球信息栅格（GIG）骨干网模拟区域，周围是依托美军全球信息栅格（GIG）骨干网而存续的美国防保障网络模拟区域及区域下属的模拟交互式基地；每个交互式基地都具有传统的边界体系结构，该体系结构由屏蔽路由器，防火墙和接入路由器组成。在此边界结构内，存在受信任区和不受信任区域的非军事区（DMZ），DMZ将作为隔离两区域而存在，并设置网络感测设备对流量进行感测分析。

此外，IAR靶场还提供了由恶意网站和正常网站组成的虚拟互联网功能，以及真正的DNS体系结构。还复制了互联网的接入点（IAP），允许GIG结构与虚拟互联网连接。IAP体系结构中提供了互联网屏蔽路由器，.mil代理（国防网络站点）和企业递归服务。真实再现美军国防网络互联环境及安全防护体系，结合美军全球信息栅格（GIG）骨干网模拟区域及交互式基地环境以及互联网模拟区域，美军将真实再现演练模拟攻击者通过互联网对美军全球信息栅格（GIG）骨干网实施网络攻击的情形，并测试和评估计算机网络防御策略。

IAR靶场基于灵活的开放式体系结构设计，并配置为支持每个攻防事件/练习的要求。包括培训和演习所需的网络流量生成，威胁注入，操作系统类型，补丁程序级别，计算机和网络服务等，这些所需资源均根据攻防事件/练习要求进行配置。该靶场的开放式体系结构允许在国防网络1，2和3层上集成作战司令部，服务和机构（CC/S/A）的特定设备，应用程序和配置。因此，该靶场允许测试、评估和确保企业信息保障（IA）设备和应用程序的互操作性。并可以根据特定的测试要求配置虚拟网络环境和区域资源。

2.4.3.IAR网络环境和流量生成

IAR靶场使用诸如Systems AdministratorSimulation Trainer（SAST）和Breaking Point之类的工具来创建和仿真模拟真实的国防网络环境。

SAST是由太平洋西北国家实验室创建的一套软件，旨在为培训人员进行练习及测试工具时为其提供一个逼真的网络靶场环境。是一个用于构建靶场网络环境功能的框架，该功能允许用户通过输入参数描述用户行为并生成相应的活动流量和行为特征，仿真和模拟真实环境下的网络活动。SAST中有一个网络流量合成器（ANTS）功能套件：

1、多用户流量工具（MUTT）：是一整套插件，可让ANTS用户人员通过定义描述并产生用户操作行为，即用户行为流量生成器。它主要是为产生正常的自然活动流量而设计。MUTT是一款合成使用邮件客户端，Web客户端，SSH客户端等工具的虚拟人代理插件集。当虚拟人代理插件集在靶场环境运行时，根据用户定义的描述参数或自定义默认参数，这些虚拟人代理插件集就会创建比如邮件发送、Web访问、SSH连接等用户操作行为的网络流量，为靶场人员测试安全设备和培训提供自然流量。

2、协同攻击工具（CAT）：是一整套插件，可让ANTS描述攻击者并生成其行为。CAT本身并不真正攻击网络，而是依赖于现成的攻击工具（如Metasploit）的攻击方案创建攻击行为。CAT是该靶场创建攻击流量所使用的工具，同时，靶场人员也可使用该协同工具实时网络攻击，或根据攻击方案编写自动化脚本实施自动化攻击。

3、虚拟互联网提供模块（VIPER）也是一套插件，使ANTS能够描述和提供在互联网或靶场本地局域网上可以找到的服务，比如Web服务，DNS解析服务，电子邮件服务等。此功能的目的是增加通常靶场的互联网仿真度，为该靶场的添加互联网模拟资源。

4、管理套件工具SEAL。用于管理IAR靶场广泛的资源以及参与者的本地和远程体验，并具有多对多视图。它具有以下概念：管理员可被授予管理靶场的权限，并对靶场的资源进行增删改查等操作，参与者将创建测试和评估任务，并基于靶场环境进行测试和攻防演训，管理员将监控参与者的靶场任务活动情况并可对参与者任务进行干预。

此外，IAR靶场还通过商业产品BreakingPoint来进行实际应用程序，实时安全攻击和数百万用户模拟来重新创建大规模互联网的仿真模拟。包括：

1、用户及网络流量：为交互式基地、虚拟互联网、美军全球信息栅格（GIG）骨干网和其他军兵种靶场创建大量逼真的用户及应用程序流量。

2、大规模网络仿真：创建可以与IAR靶场交互并使IAR靶场实现大规模网络环境仿真的模拟网络节点。

3、管理及网络服务流量：在IAR靶场内创建逼真的网络管理和服务流量，以模拟网络管理员和专门的网络服务。

4、其他通讯介质模拟：修改给定网段的特征，使其看起来像跨其他某种媒体类型（如卫星通信模拟、无线网络模拟）。

5、威胁流量：创建大量以交互式基地和其他靶场位置为目的地的逼真威胁流量。

6、用于设备测试的脚本测试数据流（可重复和比较测试）。

7、捕获遍历IAR靶场的流量并将其保存（以供后续处理和数据流量在IAR靶场内重放）。

8、支持和仿真MPLS和IPv6等高级网络协议。

9、创建将以上各项组合到单个测试方案中的方案管理和应用流程。

2.4.4.IAR物理组成

IAR靶场构造具有多个服务器场来管理网络服务，所有服务器场均从刀片服务器中央机架中提取其计算资源。在2010年建设的IAR靶场中，IAR靶场采用Dell Blade Center的刀片服务器，该刀片服务器具有16个（双CPU）服务器刀片，并安装运行虚拟阿虎程序为IAR靶场提供虚拟化计算资源，然后，虚拟机将运行为Iat靶场的服务器场运行所需的服务及应用程序。其中，每个模拟的DECC和CDC需运行10台虚拟服务器（每台），基础数据库运行需20台虚拟服务器，其他的各类应用程序及虚拟互联网等模块也将运行各自所需的虚拟机服务器数量。这些虚拟机运行的服务及应用程序所需数量及资源都是弹性伸缩的，会根据用户定义场景的大小进行缩减和扩容以满足要求。此外，模拟ArcSight和Sourcefire采用的是物理服务器。在存放IAR靶场的物理机架中，除了上述服务器提供的资源外，IAR在机架内还将提供安全设备、网络设备以及靶场使用的系列专用设备。

IAR靶场构造使用路由器和交换机来创建交互式环境，如DECC、CDC、虚拟互联网和GIG骨干网等。像真实世界一样，IAR靶场在不同的位置使用不同的技术来确保功能适当并且设计看起来尽可能的真实。为此IAR靶场构造设计使用3层设计模型：1）用户连接的访问层，2）远程办公室连接到网络其余部分的分发层，以及3）数据运行到达的核心层（或网络主干）外面的位置。每个交互式环境有4个Cisco路由器（每个交互式环境可以增加到10个），虚拟的GIG骨干网中有8个Cisco路由器，DECC和CDC中有1个Juniper路由器（每个）。

IAR靶场构造使用防火墙来模拟军事基地在边界获得外部连接的位置。在IAR靶场构造中，这些是必需的，以便为战斗人员提供他们在其基地看到的正常结构并应用该基地具有的常规安全惯例。在2010年建设部署的架构设计中，防火墙采用有Cisco ASA防火墙、Cisco PIX防火墙和Fortigate防火墙等主流常见防火墙产品。

此外，IAR靶场还基于McAfee ePO产品套件构建了基于主机的安全系统（HBSS）。

2.4.5.IAR任务支柱

IAR靶场在初始目标构建中，其主要核心目标是加强全球信息栅格（GIG）的安全防护，并基于构建的IAR靶场通过安全演习、安全测试与评估及人员训练来达成目标。

图30 IAR靶场任务支柱

演习以及训练都是基于IAR靶场构建的网络环境及工具进行的攻防活动，在美军十几年的重大靶场构建中，JIOR以及JCOR等均已经为其提供了足够强大且经验丰富的构建框架和运营方式。因此，美军针对IAR靶场构建的测试与评估（T&E）任务格外重视。为了支持其测试与评估任务，IAR靶场结合“深度防御”设计原则，为国防部组织提供了系统的、可重复的和可验证的网络测试与评估（T&E）框架（由基于绩效的指标支持），以衡量（即量化和鉴定））网络防御人员协同整合人员组织、运营和技术以保护、监视、检测、分析、诊断和响应（包含清除和恢复）网络安全攻击的能力。除了提供与运营环境隔离的真实测试与评估（T&E）环境（降低IA风险并将技术和运营影响最小化为零）之外，IAR靶场还为国防部组织提供了一个衡量安全人员运营绩效的网络环境，该环境将就网络安全服务的充分性（CND工具和机制）进行衡量，并验证已建立和强制执行的信息保障（IA）和计算机网络防御（CND）策略，技术和程序（TTP）。

IAR靶场测试与评估（T&E）框架将根据改进的要求和规范验证信息保障（IA）和计算机网络运营（CNO）技术和运营概念。具体来说，IAR靶场将寻求实现以下测试与评估（T&E）目标：

l 通过评估改善网络安全人员的运营绩效和能力；

l 验证计算机网络防御（CND）工具和机制提供的功能和服务；

l 验证和改进计算机网络防御（CND）的策略，技术和程序（TTP）；

l 验证计算机网络防御服务提供商（CNDSP）的可接受服务水平；

l 验证记录IA缓解策略。

（1）通过评估改善网络安全人员的运营绩效和能力

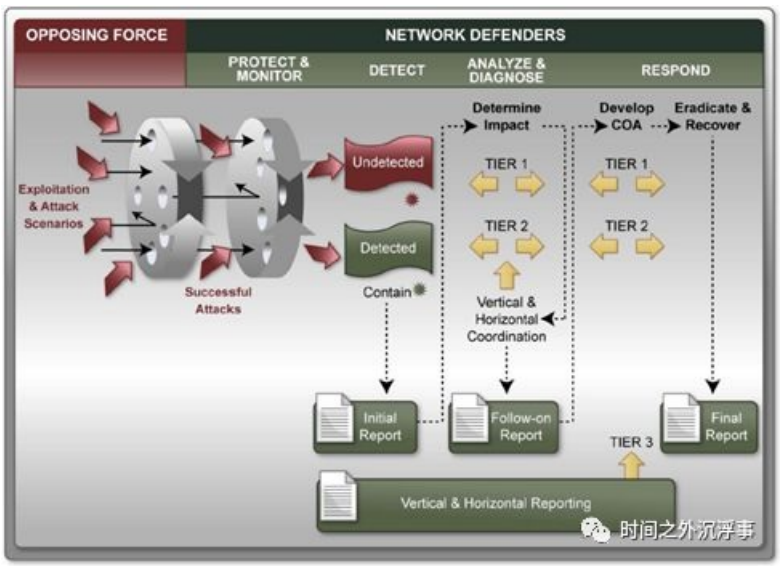

图31运营绩效指标

如图所示，IAR靶场通过性能指标来衡量模拟敌军的网络攻击活动以及保护、监视、检测、分析、诊断和响应网络攻击的计算机网络防御情况，从而提高了网络安全人员的运营绩效和能力。首先，IAR靶场为模拟敌军网络攻击配备了一支部队（OPFOR）来执行网络攻击方案，并根据黑客或网络攻击部队攻击可能执行的攻击步骤进行分解并建立攻击行为模型，类似于ATT&CK攻击生命周期的攻击行为模型。通过攻击行为模型，观察攻击者的TTP（技术、战术和过程），并将其应用于检测、防御和响应过程，并针对攻击行为、检测、防御和响应过程进行性能指标基线关联分析和评估，为提高网络安全人员的运营绩效和能力构造可行的评估模型。

（2）验证CND工具和机制提供的功能和服务

CND工具或机制是一种提供以下一项或多项功能和服务的设备：保护、监视、检测、分析和诊断/或对事件做出响应（包含清除和恢复）。为了支持计算机网络防御（CND）新兴技术，IAR靶场提供了一系列的工具和服务，可以更有效地提高计算机网络防御（CND）技术的设计，实施和验证。这包括验证这些设备提供的功能和服务，以及在整个全球信息栅格（GIG）中实施不同和替代安全技术策略的评估及权衡。

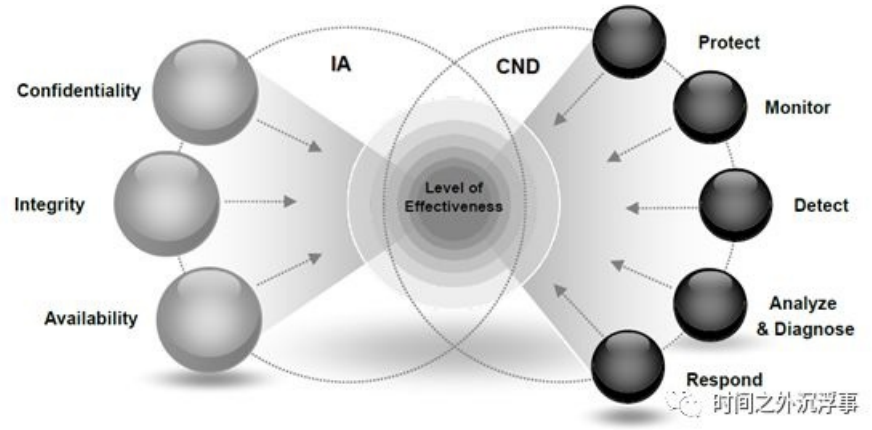

图32验证CND工具和机制提供的功能和服务

另外，由于构成全球信息栅格（GIG）的组件、系统、基础设施和操作环境的规模，复杂性和多样性在国防部中是空前的，因此在全球信息栅格（GIG）没有一种解决方案能适合所有情况。为此IAR靶场设计了一套标准规范，所有接入IAR靶场的解决方案都需要遵循共同指导原则、标准、接口和数据类型；并设计了一套支配系统设计和演进的功能和工具集，从而实现多个组件间集成的互操作性。基于此，IAR靶场将为全球信息栅格（GIG）的测试与评估提供全生命周期的保障支撑。既可以改善仍处于研发阶段的技术，也可以测试现有的部署机制，从而验证IT的大规模架构模型的系统和基础设施，从概念到深度防御功能的测试评估，并促进这些功能的成熟可用。

（3）验证和改进CND策略，技术和程序（TTP）

在实施一个计算机网络防御（CND）技术体系时，往往需要人员、运营和技术三个方面的配合协同工作要，而这三者在实施策略，技术和规程（TTP）中通常是主要验证和改进的对象。

图33人员、运营、技术三要素

IAR靶场将在整个靶场内验证和改进计算机网络防御（CND）和信息保障（IA）的TTP，并达到最佳的准备状态。

（4）验证CNDSP的可接受服务水平

CNDSP指的是为美国国防部（DoD）提供计算机网络防御（CND）和事件响应服务的供应商，这些供应商所提供的服务与计算机紧急响应小组（CERT）和计算机安全事件响应小组（CSIRT）所提供的服务相似。传统的这些服务小组可以计算给定系统的安全风险并证明该系统的安全控制措施可以充分缓解该风险，而CNDSP则可以评估IAR靶场内解决方案风险并保证最低接入服务标准。也就是说，IAR靶场开发了专门针对国防部采购解决方案的测试与评估标准，可使用IAR靶场来验证常规的服务及解决方案是否满足预定义的标准或GIG体系结构设计的要求。具体来说，其可通过利用度量标准来衡量CNDSP在以下四个主要类别中提供的服务的充分性来验证这些标准：

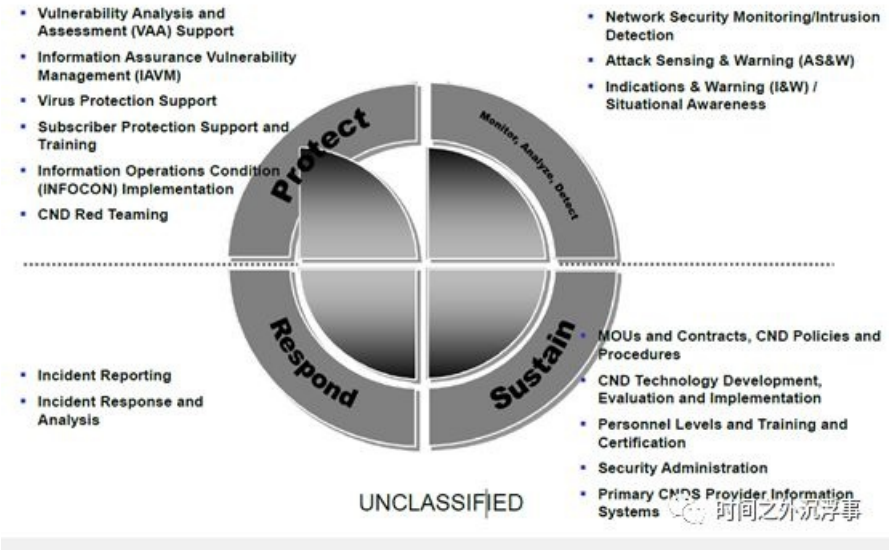

图34 CNDSP服务及解决方案测试验证标准

如图所示，具体的度量指标包括**保护、监视、检测、分析和诊断、响应**以及**事件恢复和持续运营能力**。

（5）验证记录IA风险缓解策略

IAR靶场还可以帮助验证反复出现的计算机网络防御（CND）和信息保障（IA）缓解策略，并改善用于测试和评估其缓解策略的功能和有效性。计算机网络防御（CND）和信息保障（IA）风险缓解包括通过风险评估的手段确定优先级，然后根据级别评估和实施适当的降低风险的控制措施。因为风险不可能完全消除，因此可以使用IAR靶场来测试和验证成本最低的方法和最适当的控制措施，以将任务风险降低到可接受的水平。

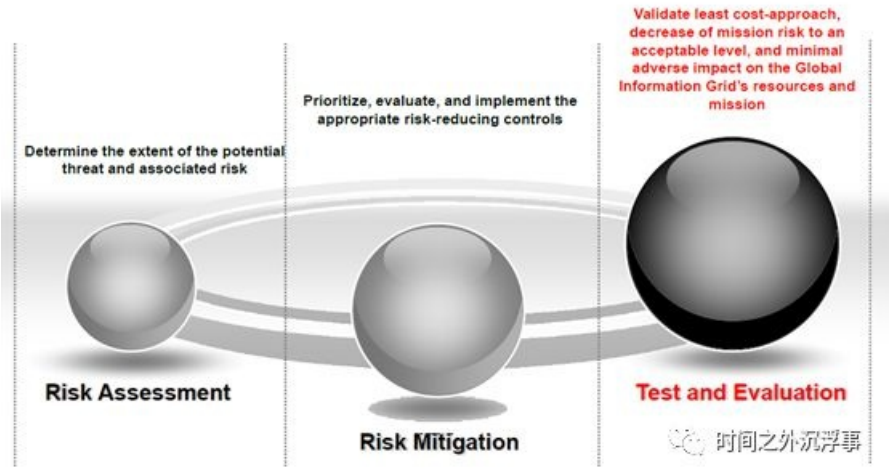

图35风险缓解策略实施流程

此外，IAR靶场的测试评估功能还用于验证信息保障（IA）控制继承的状态。信息保障（IA）控件继承是一种常见状态，其需要继承的信息包括控件的验证结果和合规性状态，这些信息保障（IA）控件状态可从原始信息系统（IS）传递或“继承”到接收IS。通过信息保障（IA）控制合规性状态共享，可以加速从业人员在多个IS之间共享安全机制的建模环境，加速他们的测试和评估进程。此外，也可保证每个控件被测试评估过后，其验证结果和合规性状态可以重复使用。

2.4.6.IAR靶场的使用情况

□IAR靶场的使用情况根据DISA的说法，截止于2013年，主要包括以下演训事件：

□DISA PEO-MA –DISA组织的小型网络CTF夺旗练习–以及TTP开发

□DISA FSO – HBSSCNDSP 501培训（国防部供应商的主机安全防护代理）

□USAF–美空军战术通信培训演习

□USSTRATCOM – JCCLOE网络警察培训

□USCYBERCOM –小型网络CTF夺旗练习

□NSA –非持久性桌面浏览器测试

□USA–“旅者级”网络战士培训

□USMC –指挥参谋学院网络选修课

□USN –用于SAGA战舰网络通讯器岸上命令测试培训

□DIA--反英特尔调查培训

□OSD –向服务学校提供攻防培训支持

□VPE--供应商产品评估

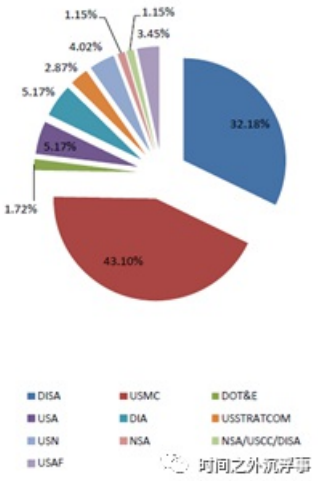

图36使用频率统计

2.4.7.CSR2.0情况

美国国防部DISA将IAR靶场的信息保障（IA）运行时期称为DoD Cyber Security RangeV1.0(DoD CSR1.0)版本，除了其支撑的信息作战概念是“赛博安全（Cyber Security）”之前的“信息保障（IA）”，DoD CSR1.0还体现在其主要由物理设备进行构建，包括定制化的物理机架和物理设备堆栈以及需要经过大量的手工繁琐的密集型配置；进化到DoD CyberSecurity Range V2.0(DoD CSR2.0)版本后。CSR2.0设计的主要目标是设计和实施所有分类级别的通用靶场自动化框架、自动化GIG环境控制和配置、集成商品硬件，虚拟化和专用硬件的自动化控制。CSR2.0大量使用虚拟化云计算、大数据、软件定义网络、网络虚拟化等技术，最大限度实现物理设备虚拟化，并基于靶场演训重用构建标准环境镜像组件，以进行大规模环境的复制生成和资源快速回收利用。赛博安全靶场2.0还提供所有密级的共用靶场自动化框架，自动化环境控制与供给，集成的、自动化的硬件，虚拟化与专用硬件控制等复杂资源异构管理。DoD CSR2.0最大限度地使用虚拟化的资源池和技术，大批量的将专用设备移植到虚拟化中，且将C/S架构更改为B/S架构，B/S架构通过浏览器技术管理虚拟基础架构及CSR靶场所有的资源，并基于网络拓扑及管控资源建立典型的模拟仿真场景网络环境，以便在培训和练习中重复使用。

通过CSR2.0的通用逻辑层虚拟化，将虚拟机、容器、专用硬件及商品硬件资源通过通用资源对象进行定义，逻辑抽象为CSR资源虚拟化或数字对象。基于逻辑抽象的虚拟化或数字对象实现自动化操作和配置，并保证后续攻击事件、流量事件等创作的一致性，提高后续安全事件的创作和编排效率以及配置、验证、监视、控制和评估功能。

定义了CSR2.0所有异构资源的通用逻辑抽象后，CSR2.0的架构设计将来自资源对象的持久库的图形化通过拖放拓扑的可视化界面操作与配置来进行资源对象的管理和编排。通过可视化的拓扑资源对象网络及位置关系的定义，可从所有CSR资源（虚拟，专业硬件和商品硬件）的统一视图中构建事件拓扑，快速实现自动安全事件拓扑定义，并可快速定位连接到事件拓扑，以进行事件特定的配置、验证、监视、控制和评估。

除了自动化安全事件编排和定义，基于可视化拓扑的CSR2.0资源对象还可针对构建的拓扑实现拓扑实例化（生成环境）编排。比如针对虚拟化的对象资源，根据拓扑定义的逻辑资源对象，可自动化生成虚拟化实例资源，并对其进行配置编辑和管理；此外，网络的实例化、专用硬件及服务器等的实例化编排，均通过不同程度的代理或插件技术等实现自动化的生成和配置管理。基于拓扑的实例化，CSR的承建单位美泰科技采购了美国初创公司Cypherpath.com的SDI软件定义基础设施软件来构建。Cypherpath SDI OS是一个单一的分布式软件操作系统，可将IT基础架构和应用程序抽象为便携式自包含软件定义的网络环境（SDI）。Cypherpath SDI OS最初上线时有社区版本以及相应的社区场景包，后来在2019年9月份关闭了社区版本的下载，在此之前，公共还可以申请下载社区版本进行测试和使用。

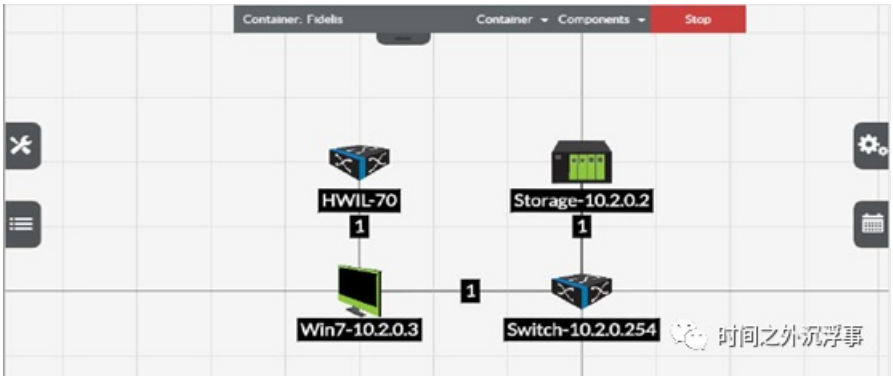

图37基于拓扑实例化构建的网络环境

2014年，全球信息栅格GIG升级为"国防部信息网络"（DoDIN），作为模拟全球信息栅格GIG的CSR2.0也相应的针对国防部信息网络（DoDIN）进行复制和建模。美泰科技在这其中，一直不断根据DoD的要求对CSR进行开发和技术架构升级。（美泰科技目前主要为美国国防部的靶场建设和维护三大合同项目：1、美国国防部赛博安全靶场（CSR）；2、美海军陆战队网络靶场（MCCR）；3、网络培训与评估平台（CTEP）CSR2.0提供了DoD信息网络（DoDIN）的持续不断的环境复制，而MCCR提供了美海军陆战队Tier2 / Tier3网络测试，培训和训练环境，以模拟/复制/仿真真实的实时网络情形和体验。CTEP提供了一个训练环境，可以模拟网络战场并模拟网络防守和攻击行动）。

CSR2.0最终的建设目标是为美军提供训练即实战的真实感。美军可以通过安全的虚拟专网采用边界组件远程访问赛博安全靶场（CSR）。赛博安全靶场（CSR2.0）目前真实地重建国防部信息网（DODIN）环境，提供对事件的直接指挥控制以及观察，支持赛博事件的重复、刷新以及回应，支持红队/蓝队，帮助用户快速熟悉靶场及作战环境，改进赛博战士工具，验证预先制定的计划并生成配置变更，评估并验证各种战术、技术与程序（TTP）以及赛博安全/计算机赛博防御工具，支持渗透测试以及突发事件响应能力等。

CSR2.0互联架构如下图所示：

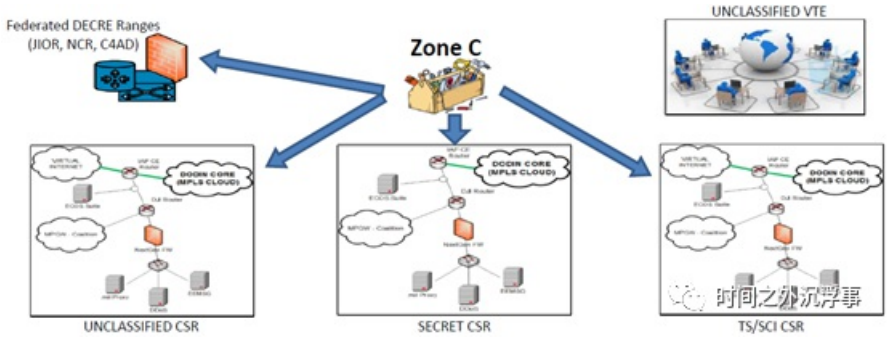

图38 CSR2.0互联架构

CSR1.0升级到2.0架构如下图所示：

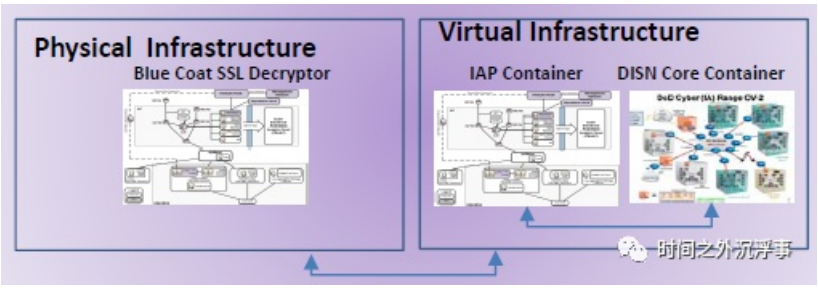

图39 CSR1.0升级到2.0架构

在CSR2.0中，在基础架构层提供DISN核心路由器与骨干、DODIN域名核心服务、MPLS路由、感知节点、因特网接入点以及联合区域安全栈（JRSS）。其中，非密靶场提供非密基础架构层，并协调DISA互联网接入点与JRSS。保密靶场将提供全混合基础架构层以及全虚拟基础设施互联网接入点与JRSS栈。

图40虚拟基础设施互联网接入点与JRSS栈

每个联合区域安全栈（JRSS）的架构如下图所示：

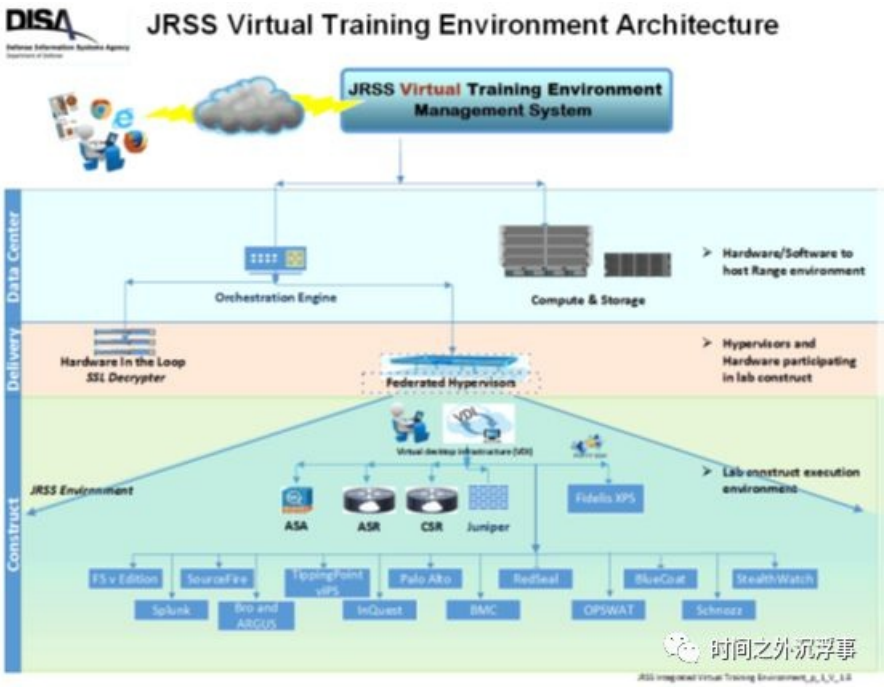

图41联合区域安全栈（JRSS）架构

JRSS由一系列相辅相成的安全站点、设备和机制构成的定制化机架式设备组合，主要执行防火墙功能、入侵检测和防御、企业管理、虚拟路由和转发（VRF）并提供大量网络安全功能。vJRSS是完全由虚拟技术构建的JRSS预生产堆栈的镜像，也就是JRSS的虚拟化版本，用于部署在CSR2.0中，所有B/P/C/S流量都经过vJRSS（例如VLAN间，基地间，机构间，互联网等），并通过vJRSS大数据分析处理和其它安全能力（如审计）等功能实现流量管控。在之前的CSR1.0或IAR中，这部分的功能是通过DMZ区域中的部署的安全设备如入侵检测等实现的。目前vJRSS主要用于CPT练习和CND情景训练。

vIAP和vJRSS类似，也是互联网接入点的虚拟化版本部署到CSR2.0中，主要为CSR2.0提供提供因特网和DoDIN之间的第一道防线和连接。提供以下功能的套件：

l Web内容过滤（WCF）：PaloAlto，Splunk，ArcSight

l 企业协同操作传感器（ECOS）：（SourceFire，SiLK，WireShark，Bivio）

l 分布式拒绝服务防护（DDoS-TR）：Arbor

此外，vIAP还需实现虚拟互联网与DoDIN第2层、DoDIN第3层之间的路由功能。

目前在CSR2.0中，虚拟化版本的vJRSS和vIAP在2018年DISA Defender中正式进行了测试和使用，后续将根据演习和训练使用进行迭代优化，不断改进虚拟化版本的vJRSS和vIAP功能，使其达到物理版本的功能与性能。

下图显示了CSR2.0的最终最核心的功能：

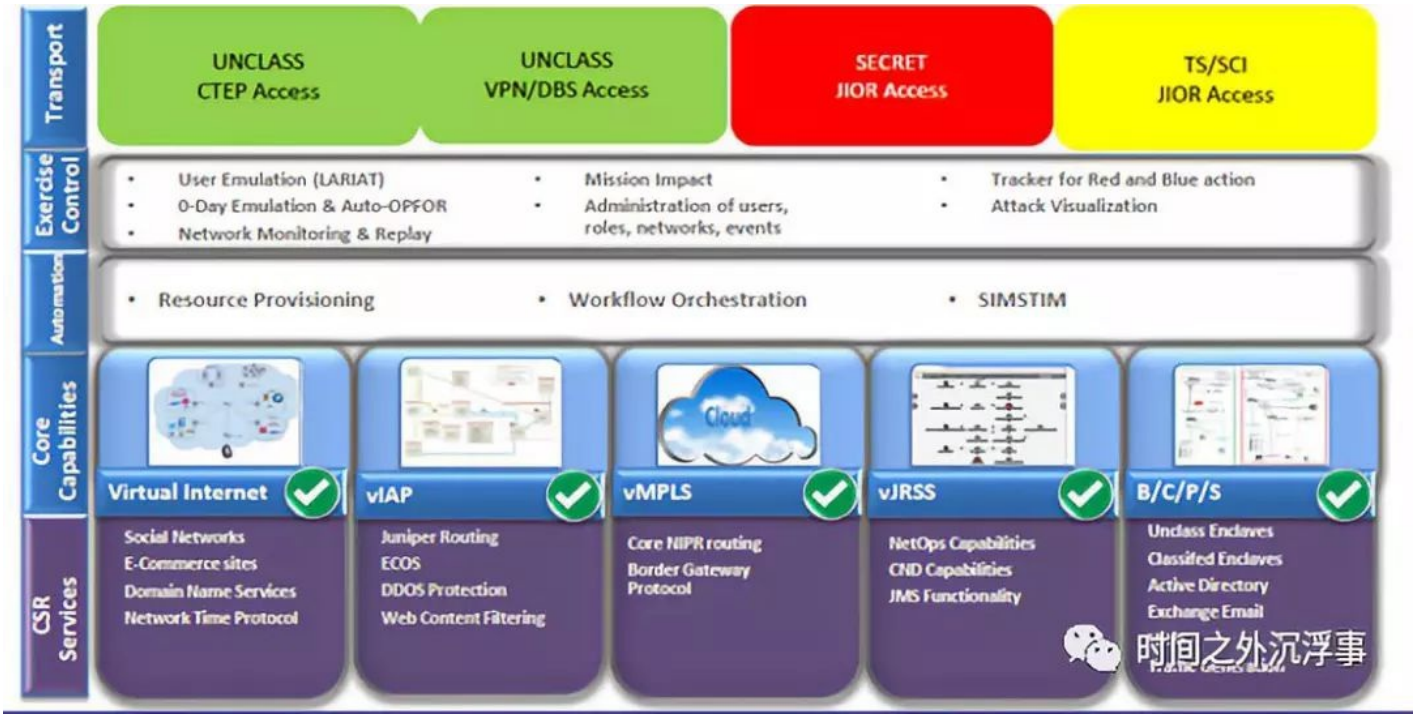

图42 CSR2.0的核心功能

如图所示，虚拟互联网、vIAP、vJRSS、vMPLS、B/P/C/S将作为CSR2.0的核心功能。其他DoDIN企业功能还包括：

l 企业电子邮件（EEMSG）

l PKI和证书管理

l SSL中断和检查

l 大数据分析和机器学习

其他社会责任能力集成包括：

l 改进的环境可访问性，用于远程配置管理

l PCTE支持和集成

2.4.8.美海军对CSR的管理和使用

美海军部在2012年由首席信息官签署《海军网络空间靶场政策指引》备忘录指出，美海军要以美国国防部赛博安全靶场（CSR）统一海军和海军陆战队的网络空间作战训练、演习、测试和评估活动。目前美海军和美海军陆战队已陆续将自个的网络靶场训练环境通过集成或互联的方式接入到了美国国防部赛博安全靶场（CSR），其中包括美海军陆战队网络空间靶场（MCCR），美海军网络空间作战靶场（NCOR）等海军单位的网络靶场环境。其构成的总体架构如下图所示。

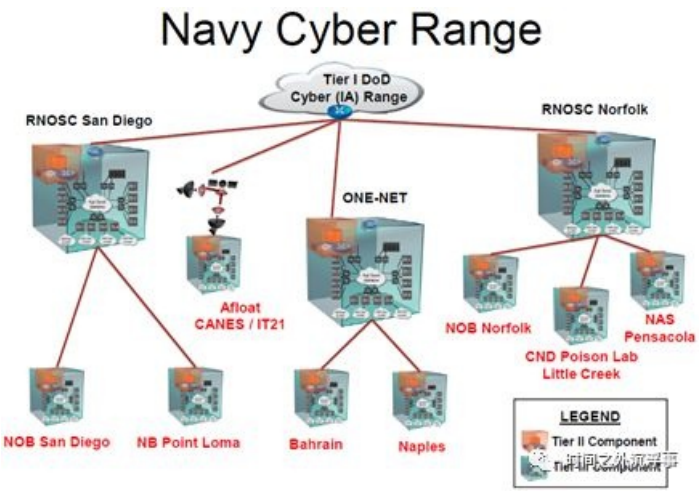

图43美海军CSR靶场体系

美海军首席信息官（DON CIO）的目的是巩固和开展DoD CSR靶场内的美海军和美海军陆战队网络培训、演习以及测试和评估活动。该备忘录将总部海军陆战队（HQMC）指挥、控制、通信和计算机（C4）确立为建立、运营和维护美海军和美海军陆战队网络靶场环境的管理和运营组织。

【1】https://defensesystems.com/articles/2010/12/01/dod-launches-cyber-test-range.aspx

【2】美军信息网络安全架构解析--贺小川

【3】Cyber Security Range (CSR)v2.0 Architecture and Capability --James Curry .2016

【4】Cyber Security Range 2019--James Curry

【5】DoD IA Range Overview--Mr.Ray A. Letteer

【6】Modeling & Simulation ofCyber Effects in a Degraded Environment ITEA 2012 Cyber Conference—ManTech 2012

【7】Department of Defense InformationAssurance Range:A Venue for Test and Evaluation In Cyberspace--Timothy"Kevin" Holmes 2011

【8】DEPARTMENT OF THE NAVY CYBERRANGE POLICY GUIDANCE --2012

【9】新领导新气象，紧抓网络攻防不放松-东方证券