天地一体化信息网络安全动态赋能架构

张玲翠[1,2]，许瑶冰[1,2]，李凤华[1,2]，房梁[1]，郭云川[1]，李子孚[1]
（1．中国科学院信息工程研究所，北京 100195；2. 中国科学院大学网络空间安全学院，北京 100049）

摘 要：天地一体化信息网络的安全需求动态变化、威胁动态变化、防护技术动态变化等特征导致已有的安全防护技术不再适用于天地网络。针对上述需求，提出了融合安全服务能力编排、安全态势分析、安全威胁处置指挥等于一体的天地一体化信息网络安全动态赋能架构，并形式化定义了该架构；然后提出了一种对威胁处置效果的双重判定方法，并基于信念熵证明了双重判定的可信性。

关键词：天地一体化信息网络；安全动态赋能；安全服务能力编排；安全威胁处置指挥；双重判定；安全态势分析
中图分类号：TN 929
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021180

Dynamic security-empowering architecture for space-ground integration information network

ZHANG Lingcui[1,2], XU Yaobing[1,2], LI Fenghua[1,2], FANG Liang[1], GUO Yunchuan[1], LI Zifu[1]
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: To satisfy the above requirements that due to the dynamic characteristics (e.g., the dynamic variability of threats, and the dynamic changes of protection technology) of space-ground integration information network (SGIIN), the existing security technologies were no longer applicable. Firstly, a security-empowering architecture for SGIIN was designed and formalized, which integrated capability orchestration unit of security service, analysis unit of security situation and the response unit of security threat measure. Then, a double judgment method for the effectiveness of threat measure was proposed. Finally the method is theoretically proved to be credible by using belief mini-entropy.

Keywords: space-ground integration information network, dynamic security empowering, security service orchestration, security threat measure, double judgement, security situation analysis

1 引言

天地一体化信息网络由天基骨干网、天基接入网、地基节点网、地面网络组成，是由多种网络互联和融合形成的异构网络[1]，其结构如图 1 所示。其中，天基骨干网由地球静止轨道（GEO, geostationary earth orbit）上的骨干卫星节点互联组成，并与天基接入网实现高低轨组网；天基接入网由若干低轨卫星组成，实现星间组网、高低轨组网；地基节点网利用星间链路实现数据的回传落地。天基网络能够很好地弥补地面网络覆盖性的不足，为陆、海、空、天等场景提供通信和网络服务，因此，许多国家和相关商业公司都在积极地探索天基网络和地面网络的融合建设方式。

2015 年，美国太空探索技术公司提出了星链互联网卫星项目，计划通过部署 1.2 万颗卫星来提供覆

收稿日期：2021–01–18；**修回日期**：2021–03–09
基金项目：国家重点研发计划基金资助项目（No. 2016YFB0801001）；国家自然科学基金资助项目（No.U1836203）；山东省重点研发计划（重大科技创新工程）项目（No.2019JZZY020127）
Foundation Items: The National Key Research and Development Program of China(No.2016YFB0801001), The National Natural Science Foundation of China (No.U1836203),Shandong Provincial Key Research and Development Program (No.2019JZZY020127)

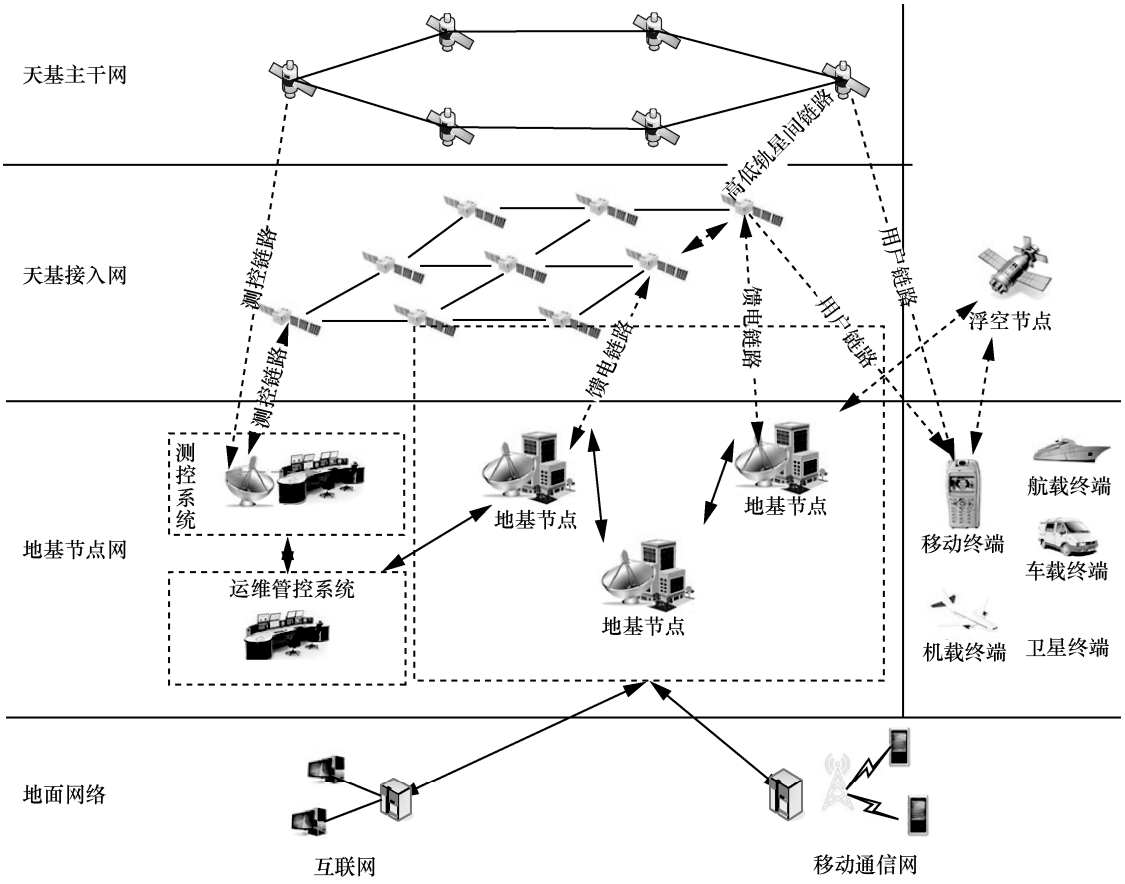

图 1　天地一体化信息网络结构

盖全美和全球的网络服务，截止到 2020 年 9 月 4 日，入轨卫星总数为 715 颗。当前 OneWeb 公司的在轨卫星已有 74 颗。我国在科技创新 2030—重大项目也启动了天地一体化信息网络的建设，该网络将为陆、海、空、天等商业大众应用提供通信和互联网服务。天地一体化信息网络具有如下特征。

1) 安全需求动态变化。天地一体化信息网络中存在大量不同类型用户，不同用户（甚至同一用户）在不同时刻不同位置的安全防护需求具有差异性和动态性[2]。例如，用户在高风险级的区域/时刻需开启重量级保护，在低风险级的区域/时刻则只需开启轻量级保护。此外，随着天地一体化信息网络的逐步建设，其安全需求也不断变化。

2) 威胁动态变化性。天基网络中卫星节点位置的实时改变导致网络拓扑高度动态变化，具有不同防护能力的安全设备在安全域中相对位置的改变及其频繁的接入接出，使整个网络的安全态势呈现动态性。

3) 防护技术动态变化。安全防护技术属于伴生技术，安全防护能力随信息技术的发展而发展。在天地一体化信息网络演进过程中，其防护技术也必将动态变化。

上述特征导致静态化的安全防护技术不再适用于天地网络，必须从宏观全局上洞悉网络的整体安全风险，分析全局安全威胁和局部安全威胁，动态调配差异化的安全防护资源处置威胁，从而避免威胁“跃出局部，延至全网”，甚至导致网络瘫痪的后果。

针对上述需求，业界分别提出了安全态势分析、安全服务能力编排、威胁处置指挥等技术，其中，安全态势分析技术从宏观上评估并预测网络安全风险，安全服务能力编排技术对安全服务保障能力进行调配，威胁处置指挥技术对威胁进行响应。但当前的安全态势分析技术、安全服务能力编排技术、威胁处置指挥技术相互独立、缺乏协同，未能形成闭环，不能成为有机整体，不能按需动态赋能天地一体化信息网络安全。

综上，现有防护手段未做到防护资源按需配置，这将浪费有限的防护资源、降低安全防护效果。针对上述问题，本文提出了天地一体化信息网络安全动态赋能架构，其主要贡献如下。

1) 提出了融合安全服务能力编排、安全态势分

析、安全威胁处置指挥等于一体的天地一体化信息网络安全动态赋能架构。通过结合包括安全需求、态势信息在内的多种安全要素进行编排，以协调不同的安全防护资源，并利用反馈信息实现闭环自适应的天地一体化信息网络安全动态协同赋能，为威胁安全防护提供统一框架。

2) 安全服务能力编排单元对安全态势分析单元、安全管理与处置指挥单元生成的综合分析结果、威胁处置结果和处置研判结果执行双重判定。利用信息论从理论上分析双重判定优于单重判定的先决条件；在实践中很容易满足该先决条件，因此，双重判定的可信度高于单重判定。

2　相关工作

本节从威胁处置指挥、安全态势感知和安全服务能力编排分析国内外研究现状。

2.1　威胁处置指挥

威胁处置方面，如何快速发现和响应各类威胁是一个难点[3-4]。文献[5]针对嵌入式设备中的恶意软件，提出了一个运行时基于硬件的恶意行为检测方法，该方法通过提取系统调用并分析恶意行为，基于恶意行为的高级语义构造恶意软件特征，最后构造多层感知器，在运行时对软件的恶意行为进行检测。文献[6]针对网络流量中难以准确发现威胁的问题，提出了基于互信息的网络流量特征选择算法，通过有监督的信息过滤算法对线性和非线性相关的数据特征进行去冗处理，最终实现了基于最小二乘支持向量机的威胁检测系统。文献[7]针对现有的静态威胁处置策略具有部署成本高、影响服务质量等局限性，提出了动态最优策略动态选择与部署框架，框架通过对服务间的依赖关系进行建模，度量安全防护成本与攻击损失成本，采用多目标优化的方法实现了对威胁的动态处置。威胁检测与处置技术能够有效检测系统的内部攻击和外部威胁，并响应这些攻击和威胁[8]，但其是在攻击发生之后才进行响应，存在一定的滞后性，这影响了系统的资产安全。由于上述 2 种技术存在局限，网络态势感知技术被提出，并被广泛研究。

2.2　安全态势感知

安全态势感知[9]在大规模网络环境中对能够引起网络态势发生变化的安全要素进行获取、理解、显示，以及最近发展趋势的顺延性预测，进而进行决策与行动[10]。文献[6]针对大多数现有的系统风险评估框架都需要大量与威胁相关的数据和知识，而这些信息往往存在难以获得或不适用的问题，因此提出了轻量级的框架（LiSRA, lightweight security risk assessment）来支持中小型企业的安全决策。该框架接收用户已有的安全数据或安全活动信息，并将其作为输入，评估网络的安全风险，同时通过对防护有效性和防护成本进行权衡，实现在对网络的风险和态势评估的同时选取最优的防护建议。针对基于风险因子分析的方法在实际场景中准确度低的问题，文献[12]将贝叶斯网络引入风险分析和计算方法中，得到了更高的风险评估效率和准确度。文献[13]通过对工业系统中的系统日志进行关联分析，筛选出可疑事件并跟进，对网络态势评估提供更准确的安全事件源。研究主要采用了大量非结构化的日志，采用熵加权的方法对事件进行打分和筛选，减少了对日志格式的依赖。

2.3　安全服务能力编排

静态网络的安全防护技术实现了对威胁的主动检测、分析、预警与响应[14]，但随着云计算、软件定义网络（SDN, software defined network）/网络功能虚拟化（NFV, network function virtualization）等服务与功能动态变化的虚拟化网络架构的出现，上述防护技术独立应用于这类架构中时并不能对威胁进行有效的处置与响应，即上述技术难以对动态变化的防护服务与资源进行部署与调配[15]。因此，面向虚拟化网络架构，基于编排技术的安全动态赋能技术被提出并得到广泛研究。

面向动态的虚拟化网络，其网络安全防护技术的研究主要着眼于安全动态赋能技术[9,11]。安全动态赋能技术以服务功能编排为核心，根据其网络架构和应用场景，可将现有研究分为面向云计算的安全功能编排和基于 SDN/NFV 的安全服务功能链编排[12-13]。具体来说，面向云计算的服务编排技术主要研究云环境下的设备、资源和服务的按需配置与部署。文献[9]针对现有云服务提供商的编排框架大多与平台绑定、可拓展性差、不直观等问题，提出了云资源描述模型（cRDM, cloud resource description model），该模型采用状态机的方法，独立于服务提供商和编排工具之外，降低了编排系统的复杂性，可应用于分布在多个云服务提供商之间的不同云资源，并使用不同的编排工具进行管理。文献[11]针对云环境下的多种无服务器计算需求，提出了编排框架 GlobalFlow，该框架采用基于副本或基于连接

器的策略，自动触发工作流中每个计算服务的执行，并根据它们的依赖关系同步其行为和状态，实现各类逻辑相关的无服务器计算的协调工作。

基于 SDN/NFV 的安全赋能技术主要研究软件定义网络/虚拟网络架构下，对虚拟网络中的安全资源进行调度的问题。文献[12]针对 SDN 架构中 OpenFlow 协议存在的可拓展性低、时延高的问题，提出了动态赋能框架 AG（avant-guard），该框架引入了驱动触发器，当针对网络的威胁出现时，触发器会为网络插入相应的流规则来应对威胁。AG 提高了 OpenFlow 标准网络的可拓展性和网络弹性，降低了网络时延，在支持增量部署的同时保证了对运行在终端主机上的软件的透明。文献[13]实现了 SDN 环境下可组合的安全服务原型系统。该研究基于 OpenFlow 标准，构建了信息流编排系统 FRESCO，该系统强调可组合安全性，包含多种安全功能，如地址过滤、网络流重定向等。若 FRESCO 的检测到模块报告的威胁，则生成流规则，并将其转换为安全指令，同时 FRESCO 还会检测规则更新产生的规则间的冲突和规则与安全策略间的冲突。

动态赋能技术实现了虚拟化网络中安全设备、资源与服务的按需调度与部署。但由于天地一体化信息网络具有威胁复杂多样、安全需求不断演进、网络环境多域异构的特点，需要将动态赋能技术与网络态势感知技术、安全威胁处置指挥技术协同联动，共同组成面向天地一体化信息网络的安全动态赋能架构，即以网络安全防护为目的，对安全编排、网络安全态势分析、威胁处置功能协同联动，通过对安全防护资源进行按需调配，确保安全防护功能的自适应能力，实现对网络威胁的及时发现与处置[16]。

3 问题陈述与安全防护需求

1) 防护资源针对性弱，缺乏多要素协同自适应编排。当前安全服务编排系统的安全需求仅来自人为输入，忽略了威胁处置结果；更重要的是，安全服务编排主体仅知道其辖域内安全威胁，不能有效准确获取全网范围内的安全态势和威胁趋势；同时，安全服务编排主体不能从安全态势分析系统和威胁处置指挥系统获取对威胁处置效果，从而不能对安全编排策略进行自适应矫正。上述 3 种原因导致安全服务编排策略只能做到局部优化，不能从根本上实现防护资源全局按需优化配置。

2) 威胁处置独立运行，与态势有限联动，与编排没有关联。由于威胁处置指挥系统和安全态势分析系统间相互独立，威胁处置指挥系统不能直接获取安全态势分析系统的安全态势结果，只有人工发现威胁后，才能启动对威胁进行处置；由于人工分析难以获得全局信息，导致不能准确获取威胁发生的根源，从而不能针对威胁根源执行恰当的处置，而且人工发现威胁时延长。上述 2 种原因导致威胁处置时效性低、效果差。

3) 威胁处置效果判定方式单一。当前主要由威胁响应系统或威胁处置指挥系统对威胁处置效果进行单源判定，其判定主体和判定方式单一，缺乏双系统双重判定机制，不能保障效果判定的准确性和客观性，从而不能从根源上确保威胁处置措施的准确性。

4 安全动态赋能框架

4.1 框架概述

针对安全需求变化、设备防护能力差异、威胁动态变化等特征与需求，本文提出融安全服务能力编排、安全管理与处置指挥、安全态势分析等于一体的天地网络安全动态赋能架构，如图 2 所示。其中，安全服务能力编排单元基于安全防护需求、融合分析结果、安全服务编排预案等生成安全编排结果；安全管理与处置指挥单元将安全编排结果细化为安全编排指令，并分析编排指令的执行结果；安全态势分析单元在主动或被动采集到安全数据或威胁处置结果后，分析威胁处置前后的安全状态变化，生成安全态势等信息。其交互过程主要包含 4 类信息流：安全编排信息流、威胁处置与研判信息流、安全服务能力编排指令执行信息流、威胁与安全态势分析信息流。

1) 安全编排信息流。安全服务能力动态编排单元接收到安全防护需求和来自安全态势分析单元的安全态势信息后生成安全服务能力编排结果，并将其发送给安全管理与处置指挥单元。

2) 威胁处置与研判信息流。安全管理与处置指挥单元接收到来自安全服务能力编排单元的编排结果后，生成安全服务能力编排指令，并将其下发至网络安全对象；在接收到网络安全对象的执行指令和来自安全态势分析单元的威胁处置结果、威胁报警/预警信息和态势综合分析结果后，向安全管理与处置指挥单元反馈执行结果；安全管理与处置指挥单元接收到该结果后向安全服务能力动态编排反馈编排执行结果和融合分析结果。

3) 安全服务能力编排指令执行信息流。网络安全对象接收并执行来自安全管理与处置指挥单元的安全服务能力编排指令后，向安全管理与处置指挥单元反馈指令执行结果，并将指令执行后产生的安全数据和威胁处置结果发送给安全态势分析单元。

4) 威胁与安全态势分析信息流。安全态势分析单元主动采集网络安全对象的安全数据（如运行状态、运行日志、关键流量等）和威胁处置结果，对各类安全数据进行安全融合分析，得到威胁报警/预警、态势综合分析结果、安全态势信息，并将安全态势信息发送至安全服务能力动态编排单元，将威胁处置结果、威胁报警/预警信息和态势综合分析结果发送或转发至安全管理与处置指挥单元。

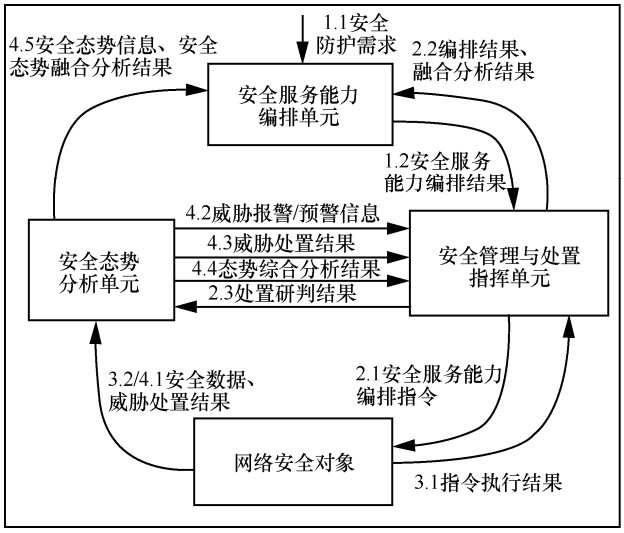

图 2　安全动态赋能架构

4.2　框架形式定义

定义 1　安全防护对象（SPO, security protection object）。安全防护对象集 SPO={spo_1, spo_2,⋯,spo_n}是一系列需实施安全保护的设备与系统集，其中，spo_i 表示第 i（$1 \leqslant i \leqslant n$）个需实施安全保护的设备与系统，如星载设备、地基节点网中的数据库系统、移动用户。

定义 2　安全防护目标（SPG, security protection goal）。安全防护目标集 SPG={spg_1, spg_2,⋯,spg_m}是用户为安全保护对象所指定的需要达到的安全目标，其中，spg_i 表示第 i（$1 \leqslant i \leqslant m$）个安全防护目标。安全防护目标可由安全保障属性（如机密性、完整性、可控性和可用性）、安全保障层次（如物理层、运行层、数据层和应用层）和阻止攻击（如阻止 DDoS 攻击、阻止洪泛攻击、阻止特洛伊木马）等描述。

定义 3　安全执行主体（SES, security execution subject）。安全执行主体是指执行安全操作的主体，包括安全保护代理、安全保护设备和安全保护系统，如防火墙设备、安全网关. 安全执行主体集合 SES={ses_1, ses_2,⋯,ses_m}；安全执行主体 ses 可以是单个不可分割的原子主体 a_ses（如 ID 为 001 的防火墙），也可以是可分解的抽象主体 c_ses（如 A 区域内的所有防火墙）。

定义 4　安全资源约束（SRC, security resource constrain）。安全资源约束是指可用来实施安全防护的资源，可用向量 $\boldsymbol{z}$ 表示，其中每个分量表示可用的计算资源、存储资源和传输资源等。

定义 5　服务需求（SeR, service requirement）。服务需求用于描述应给安全服务所支撑的业务系统提供的功能与性能需求，包括网络服务需求、并发服务需求和业务需求等。服务需求集 SeR={$\mathbf{ser}_1$, $\mathbf{ser}_2$, ⋯, $\mathbf{ser}_k$}，每个服务需求 **ser** 可用多维向量<netReq, currentReq,⋯>表示，其中 netReq 为网络服务需求，包括传输带宽需求、传输时延需求、串行化时延需求、处理时延需求和队列时延需求等；currentReq 为并发服务需求，包括在线服务并发数和并发切换性能等。

定义 6　安全报警/预警（SAW, security alarm/warning）。安全报警/预警集 SAW={$\mathbf{saw}_1$, $\mathbf{saw}_2$, ⋯, $\mathbf{saw}_n$}是指可危害网络安全的报警或预警的集合，其中，安全报警/预警 **saw** 可用向量<securityEvent, occTime, riskDegree, ConfDegree,⋯>表示，其分量分别为安全事件、发生时间、安全事件的风险度和安全报警/预警的置信度等，表示在报警或预警中安全事件发生时间、风险度，安全报警/预警的置信度。

定义 7　安全反措施（SC, security countermeasure）。安全反措施集 SC={$\mathbf{sc}_1$, $\mathbf{sc}_2$, ⋯, $\mathbf{sc}_n$}是指对安全事件采取的反制手段的集合，其中，安全反措施 **sc** 可用向量<es, op, para>描述，向量中的分量分别为执行主体、所执行的操作、操作参数，表示执行该反措施的安全执行主体以给定操作参数执行操作，操作参数 para 包括操作执行时间、执行次序、执行频率等。安全反措施包括更新防火墙配置、数据迁移、数据恢复和病毒查杀等。

定义 8　安全服务编排预案（OPSS, orchestra-

tion plan of security service）。安全服务编排预案是一组安全防护规则的集合，用于描述对于给定安全防护对象和安全防护目标，当触发安全报警/预警时，在安全资源约束下，防护主体为确保安全防护对象满足安全防护目标在给定时间内采取的措施以及措施执行顺序，可表示为

$$OPSS \subseteq SPO \times SPG \times SRC \times SeR \times SAW \times \prod SC$$

定义 9 安全编排（SO, security orchestration）。安全编排描述给定安全服务编排预案、安全防护对象、安全防护目标和安全资源约束，当触发安全报警/预警时，从安全服务编排预案中确定防护主体在给定时间内采取的措施以及措施执行顺序，可用描述为

$$so：SPO \times SPG \times SRC \times SeR \times SAW \rightarrow \prod SC$$

其中，so(spo,spg,**src**,ser,**saw**)={**sc**|< spo, spg, src, **ser**, **saw**, scet, **sc**>∈OPSS}。

定义 10 安全编排指令（SOI, security orchestration instruction）。安全编排指令集是指可在原子执行主体上可直接执行的指令的集合，可用 SOI={$\mathbf{soi}_1$, $\mathbf{soi}_2$,…, $\mathbf{soi}_n$}表示，其中指令 **soi** 可用向量<*a*_ses, *a*_op, para>表示，表示原子执行主体 *a*_ses 以参数 para 执行原子操作 *a*_op。

定义 11 安全编排指令生成（SOIG, SOI generation）。安全编排指令生成是由安全管理与处置指挥单元将安全编排结果细化为安全编排指令的过程，定义为

$$soig：\prod SC \rightarrow \prod SOI$$

定义 12 编排执行的分析（OEA, orchestration execution analyses）。安全管理与处置指挥单元依据威胁处置结果、安全态势综合分析结果，对编排指令的执行结果进行分析，获得处置研判结果和安全管理融合分析结果。威胁处置结果（TRR, threat response result）描述安全执行主体是否正确执行威胁处置指令以及执行参数，可用向量 **trr**=<ses, **soi**, true or false, parameters>表示；态势综合分析结果用于描述在威胁处置前或后安全保障对象在各安全指标上的指标值，可用向量 **scar**=<spo, <$secMetric_1$, $secValue_1$>, …, <$secMetric_n$, $secValue_n$>>表示，$secValue_i$ 表示安全指标 $secMetric_i$ 对应的指标值；融合分析结果用于描述对安全防护对象 spo 执行安全指令 **soi** 后的威胁处置执行效果，可用向量 **car**=<spo, **soi**, tre>表示，tre 表示威胁处置执行效果；处置研判结果用于描述对安全防护对象 spo 执行安全指令 **soi** 后威胁处置效果的结论，可用向量 **rjr**=<spo, **soi**, trrc>表示， trrc 表示威胁处置效果的结论，如优、良、中、差。

从定义 12 中可以看出，处置研判结果依赖于融合分析结果，融合分析结果依赖于态势综合分析结果。

定义 13 编排指令执行（OIE, orchestration instruction execution）。安全编排指令执行是部署在网络安全对象上的，安全执行主体接收到安全管理与处置指挥单元发送的编排指令后，执行该指令，并生成安全数据和威胁处置结果，可用函数描述为

$$oie：SES \times SOI \rightarrow SECDATA \times TRR$$

其中，SECDATA 表示所有安全数据集合，TRR 表示威胁处置结果集合。

定义 14 态势分析（SA, situation analysis）。安全态势分析单元在主动或被动采集到安全数据或威胁处置结果后，通过分析威胁处置前后的安全状态变化，生成安全态势信息、威胁报警信息、威胁预警信息、态势综合分析结果、态势研判结果和融合分析结果。

安全态势信息是指过去或现在某区域的安全状态和未来安全趋势，可用安全防护对象、时间区间、安全态势指标、安全态势指数等描述，表示在时间区间内安全防护对象在安全态势指标上的安全态势指数。安全态势指标包括漏洞统计、漏洞分布、高危漏洞统计、高危漏洞分布、脆弱性、事件趋势、告警统计、最新告警、热点事件等。当前一个或多个安全态势指数全部满足安全条件时，可触发安全威胁报警；所预测的一个或多个安全态势指数全部满足或部分满足安全条件时，或者当前的一个或多个安全态势指数部分满足安全条件时，可触发安全威胁预警。态势研判结果描述安全态势改变情况和威胁是否解决的结论。态势综合分析结果用于描述安全保障对象在各安全态势指标上的当前指标值，是安全态势信息的子集。

定义 15 双重判定（DJ, double judgment）。安全服务编排单元接收到来自安全态势分析单元的安全态势融合分析结果和安全管理与处置指挥单元的安全管理融合分析结果后，判定这 2 个独立单元根据各自的信息对同一事件的判断的一致

性，包括安全指标值的一致性、融合分析结论的一致性。

安全服务编排单元不会无条件地全盘接收安全态势分析单元的安全态势融合分析结果和来自安全管理与处置指挥单元的安全管理融合分析结果；它会利用安全态势融合分析结果和安全管理融合分析结果对威胁处置效果执行双重判定，来提升威胁处置结果的可信性，以协助生成下一次的编排结果。

5　基于信念熵的双重判定可信性分析

安全服务编排单元在接收到安全态势融合分析结果和安全管理融合分析结果信息之一后，依据从接收到的信息中获得的信念更新威胁处置效果；然后，在接收到其他信息后，进一步依据从接收到的信息中获得的新信念更新威胁处置效果。为了分析双重判定的可信性，本文采用信念熵度量单重判定和双重判定后关于威胁处置效果的不确定性，并基于信念熵分析双重判定的可信性。

定义 16　安全服务编排单元处置信念(belief)。信念是安全服务编排单元依据来自安全态势分析单元的安全态势融合分析结果或安全管理与处置指挥单元的安全管理融合分析结果，对威胁处置的效果的进行判断，用关于安全威胁特征信标的条件概率分布 p_β 表示。

安全服务编排单元关于威胁处置效果单重判定信念的示例如表 1 所示。表 1 中 $p_\beta(\text{trrc}=\text{优}\,|\,a_n=1)=0.60$, $p_\beta(\text{trrc}=\text{良}\,|\,a_n=1)=0.3$, $p_\beta(\text{trrc}=\text{中}\,|\,a_n=1)=0.05$，其中，变量 a_n 表示在给定时间段内观测到的攻击次数，a_n=1 表示安全威胁特征信标集合中的一个元素。$p_\beta(\text{trrc}=\text{优}\,|\,a_n\leqslant 1)=0.60$ 表示安全服务编排单元在观测到攻击次数等于 1 时，认为当前威胁处置效果为优的概率为 0.60。在实践中，这些条件概率的值源自统计分析。

表 1　威胁处置效果单重判定信念的示例

p_β	a_n=1	2≤a_n≤3	4≤a_n≤6	7≤a_n
优	0.60	0.40	0.10	0.05
良	0.30	0.50	0.30	0.05
中	0.05	0.05	0.50	0.10
差	0.05	0.05	0.10	0.80

单重判定威胁处置效果依赖于威胁处置后的网络状态（如日志中记录的攻击数量），是随概率分布的客观事实。为了便于描述，用 p_σ 表示威胁处置效果的实际概率分布。威胁处置效果示例如表 2 所示。

表 2　威胁处置效果示例

p_σ	a_n=1	2≤a_n≤3	4≤a_n≤6	7≤a_n
优	0.50	0.47	0.05	0.05
良	0.40	0.43	0.25	0.05
中	0.10	0.05	0.40	0.20
差	0.00	0.05	0.30	0.70

定义 17　信念最小熵（BME, belief mini-entropy）。给定 $p(\text{trrc})$ 为变量威胁处置效果 TRRC 的概率分布，安全服务编排单元关于 TRRC 的额外认知 B（为安全威胁特征信标集合）和信念 p_β，安全服务编排单元关于 p_β 的信念最小熵定义为

$$H_\infty(\text{TRRC}:B,p_\beta)=-\log\left(\sum_{b\in B}\left(\frac{1}{|\Gamma_b|}p_\sigma(b)\sum_{\text{trrc}\in\Gamma_b}p_\sigma(\text{trrc}\,|\,b)\right)\right)$$

其中，$\Gamma_b=\arg\max\limits_{\text{trrc}\in\text{TRRC}}p_\beta(\text{trrc}|b)$ 表示安全服务编排单元在给定额外认知 b 的情况下，依据其自身信念 p_β，确定的最佳威胁处置效果。

若令表 1 中特征信标 a_n=1、2≤a_n≤3、4≤a_n≤6、7≤a_n 发生的概率相同，即均为 0.25，则由信念熵定义和表 2 可知，表 1 中单重判定的信念熵为 −log(0.5×1/4+0.43×1/4+0.40×1/4+0.7×1/4) = −log 0.507 5=0.295。为了证明双重判定的可信性，下面给出信念支配概念。

定义 18　信念支配（BD, belief domination）。给定真实分布 p_σ 和关于额外认知 B 的信念分布 p_{β_1} 和 p_{β_2}，p_{β_1} 关于 p_σ 支配 p_{β_2} 当且仅当对于任意的 $b\in B$，$\dfrac{1}{|\Gamma_b|}\sum\limits_{\text{trrc}\in\Gamma_b}p_\sigma(\text{trrc}\,|\,b)\leqslant\max\limits_{\text{trrc}\in\text{TRRC}}p_\sigma(\text{trrc}|b)$ 成立。

命题 1　令 p'_β 和 p''_β 分别表示安全服务编排单元接收到来自安全态势分析单元的安全态势信息和安全管理与处置指挥单元的融合分析结果之一和之二后的关于威胁处置效果的信念，若 p''_β 支配

p'_β，则安全服务编排单元关于 p'_β 的信念最小熵大于 p''_β 的信念最小熵，即

$$H_\infty(\mathrm{TRRC}:B, p'_\beta) > H_\infty(\mathrm{TRRC}:B, p''_\beta)$$

成立。

证明 命题 1 可由信念支配的定义直接获得。

由命题 1 可知，若双重判定的信念支配单重判定的信念，则双重判定后的信念最小熵低于单重判定的信念最小熵。由于最小熵是最混乱的信息程度的度量，其值越低意味着信息的混乱程度越低；而在实践中双重判定的信念总是支配单重判定的信念。因此，一般情况下双重判定的可信度高于单重判定。下面给出一个例子。

若令特征信标 $a_n = 1$、$2 \leqslant a_n \leqslant 3$、$4 \leqslant a_n \leqslant 6$、$7 \leqslant a_n$ 发生的概率相同，即均为 1/4，则由信念熵定义可知，表 2 的信念熵为 $-\log(0.5 \times 1/4 + 0.43 \times 1/4 + 0.40 \times 1/4 + 0.7 \times 1/4) = -\log 0.507\,5 = 0.295$；若双重判定后信念等于真实分布，则由表 2 可知，其信念熵为 $-\log(0.5\times1/4+0.47\times1/4+0.40\times1/4+0.7\times1/4) = -\log 0.517\,5 = 0.286$，该信念熵小于单重判定的信念熵，由此可知双重判定的可信度高于单重判定。

基于上述分析，容易得出威胁处置效果的双重判定可信性度量如下：1) 利用历史数据等评估特征信标发生的概率；2) 采用专家系统或用户评分等方式，评估在不同特征信标下的威胁处置效果的概率分布；3) 基于特征信标发生概率、不同特征信标下的威胁处置效果的概率分布，利用信念最小熵计算，计算双重判定可信性度量。需要说明的是，信念最小熵越小，双重判定可信性越高。

6 结束语

天地一体化信息网络是由天基主干网、天基接入网、地基节点网、移动互联网等融合构成的异构网络，该网络具备全球持续高可靠安全通信等能力，为陆、海、空、天等场景的用户提供区域大容量通信、高机动全程信息传输。天地一体化信息网络的安全需求动态变化、威胁动态变化性、防护技术动态变化等特征，导致静态化的安全防护技术不再适用于天地网络，必须从宏观全局上洞悉网络的整体安全风险，动态调配差异化的安全防护资源，以高效地处置威胁。针对上述需求，本文提出了融合安全服务能力编排、安全态势分析、安全威胁处置指挥等于一体的天地一体化信息网络安全动态赋能架构，从理论上证明了双重判定的可信性。

参考文献：

[1] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.
LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.

[2] LIU J J, SHI Y P, FADLULLAH Z M, et al. Space-air-ground integrated network: a survey[J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 2714-2741.

[3] DAS S, LIU Y, ZHANG W, et al. Semantics-based online malware detection: towards efficient real-time protection against malware[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(2): 289-302.

[4] AMBUSAIDI M A, HE X J, NANDA P, et al. Building an intrusion detection system using a filter-based feature selection algorithm[J]. IEEE Transactions on Computers, 2016, 65(10): 2986-2998.

[5] SHAMELI-SENDI A, LOUAFI H, HE W B, et al. Dynamic optimal countermeasure selection for intrusion response system[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 755-770.

[6] SCHMITZ C, PAPE S. LiSRA: lightweight security risk assessment for decision support in information security[J]. Computers & Security, 2020, 90: 101656.

[7] CINQUE M, DELLA C R, PECCHIA A. Contextual filtering and prioritization of computer application logs for security situational awareness[J]. Future Generation Computer Systems, 2020, 111: 668-680.

[8] KHRAISAT A, GONDAL I, VAMPLEW P, et al. Survey of intrusion detection systems: techniques, datasets and challenges[J]. Cybersecurity, 2019, 2(1): 20.

[9] BRABRA H, MTIBAA A, GAALOUL W, et al. Toward higher-level abstractions based on state machine for cloud resources elasticity[J]. Information Systems, 2020, 90: 101450.

[10] YAO J Y, FAN X N, CAO N. Survey of network security situational awareness[M]. Berlin: Springer, 2019.

[11] ZHENG G, PENG Y. GlobalFlow: a cross-region orchestration service for serverless computing services[C]//Proceedings of 2019 IEEE 12th International Conference on Cloud Computing. Piscataway: IEEE Press, 2019: 508-510.

[12] SHIN S, YEGNESWARAN V, PORRAS P, et al. AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks[C]//Proceedings of the 2013 ACM SIGSAC Conference on

Computer & Communications Security. New York: ACM Press, 2013: 413-424.

[13] SHIN S, PORRAS P, YEGNESWARAN V, et al. FRESCO: modular composable security services for software-defined networks[C]// Proceedings of the Symposium on Network and Distributed System Security. Piscataway: IEEE Press, 2013: 1-16.

[14] XU S P, ZHANG Y H, ZHOU Y, et al. Design and application of a network security model[C]//Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation. Paris: Atlantis Press, 2013: 2773-2776.

[15] DEMIRCI M, AMMAR M. Design and analysis of techniques for mapping virtual networks to software-defined network substrates[J]. Computer Communications, 2014, 45: 1-10.

[作者简介]

张玲翠（1986− ），女，河北故城人，中国科学院信息工程研究所博士生、高级工程师，主要研究方向为网络与系统安全。

许瑶冰（1996− ），女，湖北武汉人，中国科学院信息工程研究所博士生，主要研究方向为网络安全。

李凤华（1966− ），男，湖北浠水人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。

房梁（1989− ），男，山西太原人，博士，中国科学院信息工程研究所副研究员，主要研究方向为网络安全、访问控制。

郭云川（1977− ），男，四川营山人，博士，中国科学院信息工程研究所正高级工程师、博士生导师，主要研究方向为访问控制、网络安全。

李子孚（1992− ），女，内蒙古赤峰人，博士，中国科学院信息工程研究所工程师，主要研究方向为网络与系统安全、访问控制。