HZ BOOKS 华章IT
Springer
安天 ANTIY

· 网络空间安全技术丛书 ·

网络空间安全防御与态势感知

[美] 亚历山大·科特 克利夫·王 罗伯特·F. 厄巴彻 编著
(Alexander Kott) (Cliff Wang) (Robert F. Erbacher)

黄晟 安天研究院 译　　黄晟 审校

- 系统介绍网络空间安全态势感知的基础理论
- 全面解析网络安全态势感知的内涵、实现框架和前沿问题
- 重量级序言深入解读领域研究成果和产业实践

机械工业出版社
China Machine Press

网络空间安全防御与态势感知

CYBER DEFENSE AND SITUATIONAL AWARENESS

[美] 亚历山大·科特 克利夫·王 罗伯特·F. 厄巴彻 编著
(Alexander Kott) (Cliff Wang) (Robert F. Erbacher)

黄晟 安天研究院 译 黄晟 审校

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络空间安全防御与态势感知 /（美）亚历山大·科特（Alexander Kott）等编著；黄晟，安天研究院译 . —北京：机械工业出版社，2018.10
（网络空间安全技术丛书）
书名原文：Cyber Defense and Situational Awareness

ISBN 978-7-111-61053-3

I. 网… II. ①亚… ②黄… ③安… III. 计算机网络－网络安全－研究 IV. TP393.08

中国版本图书馆 CIP 数据核字（2018）第 226240 号

本书版权登记号：图字 01-2017-4111

网络空间安全防御与态势感知

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：朱秀英
责任校对：殷 虹
印 刷：北京市荣盛彩色印刷有限公司
版 次：2019 年 1 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16
印 张：22.75
书 号：ISBN 978-7-111-61053-3
定 价：99.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426 88361066
购书热线：（010）68326294 88379649 68995259
投稿热线：（010）88379604
读者信箱：hzit@hzbook.com

华章IT

HZBOOKS | Information Technology

译 者 序

黄 晟

本书是一部关于网络空间安全防御与态势感知的专题学术文章合集，覆盖了网空态势感知研究方面的各个理论要点，并提供了大量面向实践的实验数据和经验教训资料，对从事网空态势感知研究与开发工作的读者具有非常重要的指导作用，而且对广大网络安全从业人员也有较大的参考价值。在本书的前言中，对所涉及各个理论方面的主要内容和贡献价值做了非常清晰的概括，建议读者在阅读正文之前先通过前言从整体上了解本书的内容结构和各章节间的相互关系。对于从事网空态势感知研究的读者，建议带着在工作中遇到的问题，全面阅读各个章节；对于从事网空安全防御工作并希望了解网空态势感知的读者，则建议至少深入阅读第 1 章以理解态势感知的基本概念，深入阅读第 2 章以军事进攻与防御视角了解网空态势感知，并且深入阅读第 3 章以了解围绕着网空安全防御过程有哪些主要角色职责、各自对应的态势感知需求及其所需要的支撑工具。

译者在十余年中致力于从事网络安全防御相关工作，并由于参与相关项目，从 2013 年开始重点关注网络空间态势感知这一热点领域。在参与本书翻译工作的过程中，深刻感受到与我国的网络空间态势感知研究与实践现状相比，国际上在这一相对“年轻”的学术应用领域的相关工作已达到较高水平；因此，也感受到迫切需要将国际上的网空态势感知研究成果和先进理念应用到我国的网络空间防御工作实践中，从而在日益严峻的网络空间威胁环境中为网络强国建设提供安全保障。因此，译者希望通过撰写本序言，以若干个在开展网络空间防御工作中遇到的与网空态势感知相关的问题或困惑为引子，结合我们的网络安全基础条件和实践工作现状，阐述对本书中的一些重要学术观点和研究成果的理解，从而在一定程度上帮助读者消化吸收书中的知识，并为推动实践应用提

供一些启发。

第一个问题：网络空间防御为什么需要态势感知？

这是一个需要以网络空间发展的视角，从信息网络技术应用发展、安全防护工作模式转变、网络安全防御理念演化、网络安全防御体系建设模式变革与网络安全防御机制创新等多个方面加以考虑才能回答的根本性基础问题。

在信息化发展初期，信息技术以“办公自动化辅助手工操作”的原始模式为主，当时信息安全被认为是与信息化建设运维相互独立甚至略有矛盾的“边缘化”工作，而且在工作模式上以小范围研究为主，甚至很多时候工作资源运用侧重于攻击利用研究而不是防御保障方向。在这种信息交流较贫乏的情况下，信息安全防御的理念主要围绕着如何对网络和信息系统进行隔离，试图通过避免接触来保持系统的安全运行，并相应地将当时尚具有可行性的物理隔离作为最值得信赖的防御措施。在此情况下，态势感知与早期信息安全防护工作几乎不存在交集。

随后出现了信息化与网络化大规模建设与发展的阶段，广大企业开始依托网络与系统开展管理经营等工作，互联网也开始进入社会生活。此时，信息安全工作逐步被作为信息化工作的有益补充，并出现了一系列的信息安全标准与法律法规，以强制合规的方式推动了基础的信息安全保障体系建设工作。为了支撑业务管理与经营，网络信息系统间出现了频繁的信息交互，导致物理隔离机制逐渐变得难以奏效，随之出现了在网络和信息系统数量依然较少时尚能有效得到落实配置与漏洞管理的“一刀切式”信息安全防护理念，用于应对尚属于探索性的少量业余爱好式攻击行为。之后，随着大量网络与信息系统投入运行，为了确保对有限安全防御资源的有效利用，发展出的信息安全风险管理模式则强调“突出重点”的防御理念，优先保护那些有直接业务价值的信息系统和数据资产，防止其被当时水平有所提升但依然以非定向模式为主的攻击行动影响。从当前网络安全认知的视角回顾来看，当时信息安全防护工作主要表现为“被动合规”模式，“平衡风险、适度安全”的信息安全防御理念也偏重于“主观判断”。相应地，当时出现了将态势感知运用在网络空间中的早期研究尝试，但是并未在信息安全保障体系中发挥出必不可少的作用。

随着互联网技术应用的飞速发展，信息化程度得到了巨大的提高，特别是在移动互联网、云计算与大数据等新技术得以普遍落实运用的驱动下，迅速进入了网络化信息技术全面渗透社会运行、业务运营和日常生活的各个方面且已经密不可分的网络空间时代，

并通过物联网建设和数字化转型发展实现了网络化信息技术与数字化生产制造技术的深度融合。由于日常工作与生活对网络化信息技术的依赖程度日益提升，网络与信息系统的地位也变得越来越重要，其中部分支撑社会运行的网络与信息系统已经被列为不容有失的关键信息基础设施。

因此，在高度依赖网络信息技术的网络空间时代，保障网络和信息系统可靠运行的安全防御工作已经变得不可或缺，甚至达到了与国家安全和国家利益密不可分的程度。网络空间的安全防护应当立足于更加积极的合规驱动工作模式，并进一步针对关键信息基础等重要领域实现主动有效的全方位体系化防护工作模式。

相应地，在网络空间时代，随着安全防护工作模式的转变，安全防御理念也出现了重大变化。正如本书第 1 章所述，网络空间时代的关键信息系统和重要数据资源，已经成为包括国家级行为体在内的各种网空威胁行为体所觊觎的目标。而且，网络空间中的网络威胁往往非常复杂，存在着从业余爱好者到高度组织化高水平实体的多层级网空威胁行为体。其中，那些具有中高能力水平且组织严密的网空威胁行为体，开始广泛利用网络空间开展意图明确的攻击性行动。因此，在安全防御方面不得不将网络空间与传统物理空间中的安全威胁综合起来统一考虑，从而进一步发展出以威胁对抗有效性为导向的网络空间安全防御理念，要求必须根据网络与信息系统的国家安全、社会安全和业务安全属性，客观判断必须有效对抗哪些层级的网络空间威胁，并据此驱动网络空间安全防御需求。

正如本书第 11 章所强调的，针对政企网络展开的网空攻击已经进入了新的时代，威胁行为体在网络空间展开了大量的侦察刺探、攻击利用和混淆隐匿行动，不仅以潜伏隐藏与数据窃取为目的的网空间谍行为达到了几乎无孔不入的程度，相应的网络战争的可能性也在日益增加。为了在网络空间时代对抗目标意志坚定的高水平网空威胁行为体，为了应对日益严峻的网络空间风险与威胁形势，为了切实保障好支撑网络空间良好运行的网络系统和信息资产，需要探索更加积极主动的网络空间安全防御模式，从而做到像本书所描述的那样，由安全分析与防御专业团队在网络空间中与各种威胁行为体展开积极的“隔空对决”。根据本书第 2 章所提出的观点，传统军事领域的很多实践对网络空间中的威胁对抗及安全防御具有重要借鉴作用。正如美国国防部 2001 年《四年防务评估报告》（U. S. Department of Defense 2001）中所提出的，随着冷战结束，国际形势日益复杂化，已经很难清晰地识别出所有的敌对威胁行为体，因此需要从基于威胁的规划模式转为基于能力的规划模式，更聚焦于敌对方可能采用的进攻方式，识别出为了达到威慑和

击败敌人所需要的军事能力，同时关注随着科技发展而出现的潜在能力领域，并据此通过分析过程形成指导性的军事需求。借鉴国防军事领域的实践经验，需要把尝试罗列各种可能的网空威胁并设计零散防御措施进行被动应对的传统式威胁导向建设模式，演化为全面建设必要的网络安全防御能力，并将其有机结合以形成网络空间安全综合防御体系的能力导向建设模式。

在美国网络安全研究机构 SANS 所提出的“滑动标尺”模型（Lee R. M.，2015）的基础上，国内多家能力型厂商在取得共识后进行了延伸拓展，进一步提出了叠加演进的网络空间安全能力模型。该模型将网空安全能力分五大类别，其中基础结构安全、纵深防御、积极防御、威胁情报四大类别的能力都是完善的网络安全防御体系所必需的，而反制能力则应当由国家级网空安全防御体系提供。其中基础结构安全类别的能力，来自于在信息化环境的基础设施结构组件以及上层应用系统中所实现的安全机制，兼具安全防护和系统保障的双重意义，主要作用是有效收缩信息化环境中基础设施所存在的攻击面。纵深防御类别的安全能力，来自于附加在网络、系统、桌面使用环境等信息技术基础设施结构之上综合的体系化安全机制，以“面向失效的设计”为基本原则构建防御纵深，通过逐层收缩攻击面以有效消耗进攻者资源，从而实现将中低水平的攻击者拒之门外的防御作用。积极防御类别的安全能力，则如本书第 1 章所述，通过动态的体系化安全机制，实现对网空威胁行为体的侦测识别，并对所发现的网空攻击做出动态的自发响应，通过重新配置、恢复和重建等弹性恢复保障措施使任务关键系统能够持续正常运作，并随着技术发展引入事中阻断、猎杀清除和操控反制等针对威胁展开对抗的积极防御响应措施，从而达到本书第 13 章所提出的目标：即使在支撑工作任务的网络系统遭受网空攻击并被攻击控制的情况下，依然能够保持工作任务持续进行，并及时恢复到可接受的工作任务保障水平。在这一系列类型的网络安全防御能力的支撑下，通过实战化的网络安全防御运行，能够达到本书第 3 章中对全面完善的网空安全防御过程所提出的要求。

从叠加演进的视角来看待网络安全防御能力体系，基础结构安全与纵深防御能力具有与网络信息基础设施“深度结合、全面覆盖”的综合防御特点，而积极防御与威胁情报能力则具有强调“掌握敌情、协同响应”的动态防御特点，并且这些能力之间存在辩证的相互依赖关系与促进作用。

一方面，正如本书第 1 章所指出的，需要充分理解网络空间运行的技术与管理复杂性，以及由于复杂性而产生的不可回避的管理脆弱点和技术漏洞，并客观认识到这些问题将给网空威胁行为体提供突破已有防御机制的入口。况且，本书第 2 章指出，由于行

动匿名性、攻击针对性、攻击自由度、人性弱点可利用性和取证困难等方面的特点，与网空防御者相比，网空威胁行为体具有较为明显的优势。事实上，正如为美国政府、军方和情报机关提供极高水平网络安全防御的美国国家安全局（NSA）下属信息保障局（IAD，以下简称 NSA IAD）在相关专题论文（Willard，2015）中所指出的，即使他们在网空防御方面做出了巨大的努力，但是依然认为在工作中必须假定“敌人终将成功入侵”，并据此确立“敌已在内”的基本敌情想定。也就是说，那些具有高技术能力的威胁行为体，客观上可能采用各种手段来利用所有能够找到的脆弱点和漏洞，从而突破由偏静态的综合防御能力所构成的防线，进入我方网络环境持久潜伏并伺机展开行动。需要注意到，“内网基本安全，只需查漏补缺”的传统安全假设与实际情况在客观上已存在较大偏差；并应当意识到，在此假设上形成的零散式“漏洞扫描＋修补整改”工作机制也已经难以应对眼前高度复杂的威胁环境。因此，有必要借鉴本书第 13 章所提出的理念，在敌情想定的基础上提升网络系统的可弹性恢复水平，特别是依靠具有动态特性的积极防御能力，在威胁情报能力的驱动下，通过全面持续监控发现威胁踪迹，并针对潜伏威胁展开“猎杀”（hunting）行动，从而做到对突防威胁的“找出来”和“赶出去”。

另一方面，也必须客观认识到叠加演进网络安全防御能力体系中各类能力之间存在着不可割裂的依赖关系。具有综合防御特性的能力虽然偏静态，但是在整个防御体系中起到了消耗进攻者资源的作用，不仅能够有效抵御大量中低能力水平威胁行为体的进攻行动，而且也能够对高能力水平威胁行为体的攻击行动起到压制作用，特别是可以收缩攻击面以降低攻击行动的自由度和隐匿性。因此，综合防御能力所构建的基础防线，能够为动态防御能力提供有利的威胁对抗环境，既能够有效防止由于低水平攻击行动泛滥的干扰而无从发现的潜伏的高能力水平威胁行为体，还能够有效利用实现综合防御能力的各种机制措施产生的大量安全信息，加强对高隐匿性攻击行动的发现能力。

综合来看，为了做好网络空间时代的安全防御工作，不仅需要通过完善并强化已有的静态防御机制实现兼顾结合面与覆盖面的综合防御能力体系，还必须加快建设动态防御能力体系，其中的关键正是针对网络空间时代的高水平复杂威胁行为体展开协同响应对抗的积极防御能力。要实现积极防御能力，不仅需要配备针对攻击行动进行响应对抗的装备系统和处置流程，更重要是必须为积极防御建立一套有效的动态指挥控制体系，从而保障响应行动的及时性、准确性、全面性和有效性。

正如本书第 1 章所总结，通过实现网空态势感知，能够高效地综合分析各种网空安全相关数据和威胁情报，对不断演化的网空威胁做出识别、理解和预见，在掌握整体安

全情况的同时定向发现潜伏的安全威胁，并提供清晰明确的响应决策信息支撑，从而有效指挥对威胁行为体开展协同响应对抗行动，做到及时抵御攻击、进行恢复甚至实施反制。第 1 章中引用了美国空军的调研结果，认为“网空态势感知正是实现网络空间保障的先决条件”，突出强调了网空态势感知的重要性。而且 NSA IAD 的相关论文（Herring 等人，2014），也明确指出了在高效快速对抗高水平威胁的网空积极防御体系（Active Cyber Defense，ACD）中，分布式共享态势感知具有决定性的重要作用。

因此，网络空间时代需要动态综合的网空安全防御能力体系，其中针对威胁行为体的攻击行动展开协同响应与处置的积极防御能力具有不可或缺的关键作用，而运用威胁情报驱动高效积极防御的动态指挥控制机制依赖于网空态势感知。

第二个问题：态势感知是什么?

按照本书第 1 章作者 Mica R. Endsley 于 1995 年（Endsley 1995）所提出的最为广泛使用的态势感知定义：态势感知是“在一定时间和空间内观察环境中的元素，理解这些元素的意义并预测这些元素在不久的将来的状态”。基于这一定义，态势感知由三个分层级的阶段所组成——观察、理解和预测，而且其输出将被直接馈送至决策和行动的周期中。在此基础定义的基础上，为了深入探讨如何在高度动态的系统环境中通过态势感知支持高效的决策制定与行动执行，Endsley 进一步明确了相关术语的定义，提出态势感知应当被作为一种“知识的状态”，而“实现、获取或维持态势感知状态的过程”则应被称为态势评估，并且强调应当对这两个概念加以区分。

尝试从网络空间安全防御工作视角加以理解，需要将积极防御中各种与指挥控制相关的工作结合至态势感知概念定义的三个层级阶段，按照本书第 1 章中描述的态势感知动态决策模型来实现网络空间态势评估过程，确定对各类型网络空间动态环境信息的输入需求，接收持续监测网络和系统所采集的网空数据和安全事件信息，结合关于工作任务目标、网络与系统架构、威胁情报乃至国际关系与地缘政治环境等的上下文信息，理解潜伏威胁的攻击行动、当前影响节点范围与可带来的网空效应，进而对下一步攻击行动、未来影响节点范围与可能造成后果等方面做出合理推测和预估，并通过对备选行动方案进行对比评价以确定行动计划，进而有效指挥针对威胁的积极防御响应处置行动。

值得注意的是，在对网络空间中态势感知概念的理解上，有时候存在一些不甚清晰的情况。其中，“态势”经常因为常用语境而被片面理解为“宏观态势”，但实际上还必须包含“中观情境”，才能够有效支撑决策制定和响应处置；另一方面，“感知”也经常

被理解成为“感官观察”，进而在网络空间领域被理解为数据采集和可视化呈现，但实际上正如本书第 8 章所引述的韦伯斯特词典定义，“感知是指人们在观察中的警惕性，以及对所经历事物展开推导所得到的机敏性”，其内涵超越了简单的观察，并且更强调通过运用知识而获得面向响应处置的机敏能力。

困惑 1：态势感知应当面向策略调整还是战术响应？

在实现网空态势感知的网络空间安全防御工作实践中，经常会将态势感知理解为对“宏观态势”的“把握掌控”。对应地，就出现了一个令人困惑的情况，因为如果网空态势侧重于对宏观态势的掌控，其输出的决策支持信息将主要被用于引导对安全策略的优化调整，虽然这种“宏观”模式与基于 PDCA（Plan-Do-Check-Adjust，计划 – 执行 – 检查 – 调整）循环的信息安全风险管理生命周期相比具有更高的主动性和动态性，但是在攻防对抗的时间周期上仍然无法适应高速多变的攻击行动，而且在调整范围上也只能局限于较粗的粒度。简而言之，正如本书第 4 章所提出的，这种面向策略调整的网空态势感知确实具有一定的网空防御作用，但是仅依靠这种宏观态势感知也确实难以支撑有效的积极防御体系。本书第 3 章中明确提出，必须围绕当前态势关于是否存在攻击行动、攻击行动的当前阶段和攻击者位置等方面回答一系列基础问题，这说明态势感知还应当面向在宏观层面之下但又高于微观细节的“中观层面”。

事实上，正如本书第 1 章所指出的，网空攻击行动可能在不到一秒的时间内发生。同时，如本书第 3 章所指出的，为了有效抵御快速发生的网空攻击行动，不仅需要阻止攻击者入侵导致的网络系统初始“沦陷”，还必须能够发现已被入侵控制的计算机，并采取响应措施预防或阻断攻击者的后续行动。因此，网络空间中的积极防御行动更应采用源自于美国空军飞行员作战训练的 OODA（Observe-Orient-Decide-Act，观察 – 调整 – 决策 – 行动）循环，快速针对网空安全事件展开事件检测、事件理解、决策制定和行动执行，从而实现抵御攻击、进行恢复甚至实施反制的积极防御目标。因此，正如 NSA IAD 在相关专题论文（Herring 等人，2014）中论述的网空积极防御体系，网空态势感知应当能够支撑战术响应，而且应当能够接受与处理所采集的微观层面数据，以及侧重于微观层面的入侵检测事件信息，进行观察并在中观层对所观察信息进行组织与理解，进而根据在中观层面的合理推测来制定决策，然后通过执行响应行动对网空环境中的节点实体产生微观层面的安全影响。

进一步从与高水平威胁的对抗角度来看，由于网空攻击发生速度极快，对高水平威

胁行为体长期潜伏后某一次快速发生的突然进攻做到事前或事中阻断可能非常困难。因此，需要结合在中长时间周期中对抗威胁进攻行动所积累的经验知识，根据所监测到的突发事件信息，采用网空态势感知发现潜伏的高级威胁并确定其影响节点范围，指挥对所暴露威胁展开猎杀清除等响应行动，并通过向积极防御体系中的具有实时监控响应能力的设备或系统下发威胁对抗策略，实现对越来越多的“已知”攻击行动展开实时阻断。

综合来看，网空态势感知需要兼顾宏观与中观两个层面，需要将实时的监测采集数据与中长期的情报、经验和知识积累结合在一起，支撑实现短期的响应行动与中长期的策略调整工作。

困惑 2：态势感知只是为了满足整体安全状态展示的需要吗?

近些年我国在网空态势感知方面取得了较多的成果，建成了许多与态势感知具有一定关系的网空防御平台。但是，一个实践中的困惑也随之而来：现在这种以整体安全状态展示为主的模式，代表了态势感知所必须满足的主要需求吗?

首先，我们必须客观地认识到，与忽视采集分析安全监测数据且不主动掌握安全状况的早期网络安全运行模式相比较，通过建设与态势感知相关的系统平台，加强对安全数据的统计汇总和对安全状况信息的主动展示，确实具有较大的积极意义，并且也确实能够揭示一些中长期存在的安全问题，并推动展开优化调整安全策略等解决措施。

然而，正如本书第 13 章所指出的，网空态势感知的最终目标是对情境态势进行有效管理，需要不断地针对攻击行动做出积极防御的响应对抗，及时调整网络及其所支撑的工作任务，实现以工作任务为中心的可弹性恢复网空防御能力，从而达成业务运营保障和业务风险控制的目标。又如前文所探讨的，网空态势感知作为网络安全积极防御体系所依赖的动态指挥控制机制，必须能够有效支撑中观层面的战术响应行动，因此就需要对经过聚合的系列安全事件进行中观层面的结构化呈现，需要向网空防御人员提供备选的积极防御响应行动方案，并基于比对和评价对抗措施以提出行动建议。正如本书中多个章节所强调的，网络空间安全防御不仅面临海量数据规模的严峻挑战，还必须能够及时处理以极高速度源源不断产生的各种安全相关事件信息，因而即使经过态势感知相关机制的聚合汇总后，依然会有大量疑似安全事件需要由网空安全防御人员进行甄别分析，从而制定准确的决策并展开有效的响应处理行动。因此，围绕着网空态势感知的积极防御工作，必须由参与网空防御的各个角色人员协同完成，通过“分片包干”以覆盖规模日益增长的信息化环境，通过“专业分工”以确保提供充足的经验与能力来对抗高水平威胁。类似地，本书第

3 章通过对网空防御过程的分析，提出了安全分析师等一系列必不可少的网空安全防御角色。况且，为了保证响应行动的有效性并降低潜在的负面影响，还应当得到信息化建设与运维人员的协同配合。如本书所强调的，必须在组织机构的网空安全防御总体使命与愿景的驱动下，对涉及积极防御的各个角色的当前工作职责做出适应调整，根据态势感知和协同响应的工作特点确定各个角色的高阶目标，并采用目标导向任务分析（GDTA）方法来列出各个角色所需要做出的主要决策，进而详细描述为了支持每个决策而在态势感知三个层级所应当满足的需求。针对网空防御行动中每个参与人员的独特岗位，根据上述态势感知需求，确定需要向其提供哪些基本数据，以及确定相关系统需要以何种方式对信息进行整合，进而定制面向不同角色的网络空间通用作战态势图。

综合来看，积极防御中的态势感知，不能止步于向网空安全防御人员展示整体安全状态信息，而是需要根据具体工作目标和工作任务确定多种角色的不同态势感知需求，并以交互方式向承担各个岗位的网空安全防御人员乃至信息化建设运维人员提供必要的信息支撑和分析能力。

困惑 3：“地图 + 炮”形式的态势感知为何效果不显著？

在最近几年的网络安全建设发展过程中，逐渐出现了一种趋同的实现模式，许多与网空态势感知相关的平台都将叠加在地图上的安全告警地理信息、安全告警分类聚合统计和最近发生安全告警清单作为主要的展示信息，而且越来越多的用户和厂商都开始将这种信息展示形式理解为“态势感知”。可能是为了加强安全告警的形象化展示效果，大多数厂商都采用了绚丽的“炮击”视觉效果，在地图上呈现安全告警所代表的疑似攻击行为的发生方向，因此被业界戏称为“地图 + 炮”形式的“态势感知”。

从运行效果来看，通过这种生动的安全告警可视化展现方式，确实能够向安全防御人员揭示当前网络安全状况的严峻程度，从而打破以往因为看不到而盲目自信的被动局面，进而促使各级企业机构启动对网络安全防御体系的完善工作。然而，随着这些平台上线运行时间周期的延伸，也有越来越多的网络安全从业人员对其效果提出了疑问。

实际上，目前的这种趋同模式，主要侧重于展现宏观的整体安全状态，并罗列部分微观的安全事件信息。根据本书第 3 章，这种模式只能回答关于当前态势的“有没有正在进行的攻击”这一问题，而无法提供关于攻击行动阶段和攻击者位置的信息，更难以回答关于影响、演化、行为、取证、预测和信息源评价的一系列问题。事实上，由于缺乏在中观层面对安全信息进行结构化组织与聚合呈现的能力，所以难以支持网空安全分

析人员对威胁行为体的攻击行动做出有效理解，实际上是“感而不知”；而且，由于缺乏网空分析人员对疑似安全事件进行甄别核实所需的交互分析能力，以及网空安全防御人员制定决策并开展响应行动所需的交互操作能力，所以难以有效满足各种网空安全防御角色的态势感知需求，更无法有效指挥积极防御工作，实际上是“感而不为”。

总体来看，确实迫切需要完善当前的网空态势感知实现模式，强化态势感知对各种网空防御人员角色的支撑能力。值得注意的是，本书的各章节中阐述的主要观点和研究成果，对开展网空安全防御体系中的态势感知发展创新工作，能够起到重要的参考借鉴作用。

第三个问题：如何实现态势感知？

那么，应当采用何种方式在网络空间安全防御工作中达到态势感知这种状态呢？根据书中的态势感知定义，最直接的回答可能是：“加强网络安全数据和日志信息采集以实现态势感知的观察层，通过可视化展现让安全分析师掌握网空态势以实现态势感知的理解层，并采用各种数学模型测算未来的发展状态以实现态势感知的预测层。”值得注意的是，我国网络安全行业在近些年还出现了一种很常见的提法，认为态势感知可以逐层分阶段实施，例如，可以优先做数据采集与可视化实现第一层“观察式的态势感知”，然后等待网空安全分析人员水平提高后再着手实施第二层“理解式的态势感知”，接着等待人工智能 / 深度学习等技术成熟后才尝试第三层“预测式的态势感知”。更有甚者，会因为“ perception”（观察）一词具有“感知”的中文译法，认为类似“地图 + 炮”形式的安全数据采集与可视化模式，就属于一套完整的“简单态势感知”，而“理解”与“预测”则属于所谓“高级态势感知”的范畴。

事实上，在本书第 1 章描述的态势感知模型中，实现态势感知的过程包含观察、理解和预测三个阶段，虽然从认知过程发展的角度来看也对应着三个层级，但并不意味着这三个层级可以割裂开来分别实现，更不能将其视为三套不同水平的“完整态势感知”体系。此外，必须清楚认识到，态势感知的目的是支持决策制定和行动执行，如果止步于观察或理解阶段的态势感知相关过程，则仅能达到“感而不为”或“知而不为”的残缺效果。正如本书第 5 章所明确指出的，态势感知本身并不是最终目的，而只是在快速演变复杂环境中用于支持明智决策的手段，因此也是通过做出准确的积极防御决策以有效对抗威胁的先决条件。

根据本书所描述的态势感知模型，在第一级态势感知（观察阶段）需要对其所关注网络和系统及其运行环境中的显著信息进行传感（ sensing，也经常因为被翻译为“感知”而

引起对态势感知的错误理解）检测，从而形成对各类系统节点、当前协议、已被攻击受控节点、活动历史记录和受影响系统 IP 地址等侧重于微观层面的环境元素状态的感知；在第二级态势感知（理解阶段），则应当结合网空防御目标来解释前述状态信息的含义或显著性，像“2+2=4”那样结构化地组织整合信息以形成中观层面的全貌图景，并聚焦于针对当前情境回答“那意味着什么”这个核心问题，从而对正在发生的网空安全事件形成理解，而且重点关注特定节点易于遭受攻击的程度（节点视角）、攻击行为的检测特征（检测特征 / 模式角度）、哪些攻击事件可能相互关联（事件间关联关系视角）、给定事件对当前任务运行的影响以及对竞争性事件的正确优先级排序；在第三级态势感知（预测阶段）需要对所理解的安全事件信息展开前向时间的推断，以确定其将如何对运行环境的未来状态产生影响，也就是根据所理解的威胁攻击轨迹等信息对攻击行动的发展方向做出合理推测，基于网空防御人员对当前情境态势的理解，结合对网络和系统的了解，预测下一步可能发生的情况，特别是受影响节点范围的扩展情况，以及威胁行为体攻击行动的延展情况。

根据 Endsley 在 1995 年（Endsley，1995）提出的动态系统中基于态势感知实现高效决策制定的研究成果，在态势感知模型中不仅仅存在观察、理解和预测三个层级阶段，还与一系列认知因素密切相关，其中注意力与工作记忆的局限性的影响非常明显，并有很高可能性将会导致出现低水平的态势感知。

如果简单地按照对态势感知三个层级阶段的理解直接设计相关系统平台，就像本书第 9 章中相关研究调研部分所提到那些回避恶意行为检测和上下文情景化的例子，将观察阶段实现为单纯的数据采集和处理，将理解阶段实现为可视化展示呈现和按需交互分析，并在预测阶段将问题丢给网空安全分析人员，让他们各自猜测可能的未来发展情况，并让网空安全防御人员自行琢磨应当采取哪些响应行动措施，就有可能导致低水平态势感知，而且在海量网络流量面前，这种完全依赖分析人员处理能力的模式不具有可持续性。其中，导致这种问题情况的决定性因素，正是来自于上述的两大制约因素：注意力与工作记忆。具体来看，一方面，如果在观察阶段缺少对明显线索的识别发现，则无法引导网空安全分析人员的关注方向，导致他们不得不耗费大量精力在海量的多样化数据信息中查找可能有意义的线索，而且数据过载问题会使情况变得更加难以控制；另一方面，如果在理解阶段只能提供某些固定的宏观整体情况信息可视化呈现，或者仅提供开放性的交互式数据查询与数据钻取功能，则需要分析人员耗费大量精力在脑海中尝试对多样化的信息做出组织与解释，而且在很多情况下无法保证分析人员能够正确理解哪些属于关键信息，也无法发现关键信息之间的关联关系；还有就是，如果在预测阶段无法

提供充足的信息来引导分析人员，则可能使原本应当依据攻击轨迹做出的合理推测，变成凭空进行的无依据猜想；最后，如果无法向网空防御人员提供响应行动的决策支持信息，那么他们可能绞尽脑汁也无法制定出可行的威胁对抗行动方案。其实，如果采用偏学术的语言来描述这些问题，观察阶段引导信息查找关注方向的问题涉及注意力，各个阶段所提到的“精力”问题则与工作记忆密切相关，而那种给工作记忆带来巨大压力的临时应激工作方式则属于“启发式的细致心智计算”。诚然，对于某些经验极为丰富的高水平网空安全分析人员来说，利用这些缺乏整合且分阶段割裂的“原生态”式基础功能，还是有可能达到态势感知效果的，但是在时效性和高水平对抗方面难免存在不足；然而，对于大部分缺乏经验的网空安全分析人员和网空安全防御人员来说，则几乎无法在略微复杂的网络空间环境中实现态势感知。正如本书第 2 章所指出的，在网络系统中能够获取海量的安全信息，如果仅片面地加大提供和共享信息的数量，而未能相应地通过快速处理提高数据的质量，会导致超越人类认知局限性的阈值，压倒相关人员及时进行分析处理的能力，从而给指挥控制人员带来挑战；而且，片面强调数据采集和可视化，还可能导致网空安全分析人员产生“我可以看到一切”式的虚假安全感，进一步因为缺少引导，导致放大“乐观偏差”、易得性偏差与确认偏差等认知偏差所带来的负面影响。

实际上，目前所建设的不少态势感知相关平台都存在着这种情况。随着网络流量飞速剧增，必须改变依赖网空安全分析人员直接查看监测系统与工具输出信息的低效模式，并促成网空安全分析人员的工作职责转向更抽象且更高阶的验证分析任务。因此，如何为网络空间安全防御实现高效的态势感知，已经成为一个难以回避的迫切问题。

第三个问题延伸出的增补问题：如何实现高效的态势感知？

本书在介绍态势感知模型时，重点提出了长时记忆机制对态势感知的影响作用，指出根据经验和知识在长时记忆中形成的认知结构——主要是图式与心智模型——有助于实现更高效的高水平态势感知，而在第 5 章中也结合 ACT-R 模型和基于实例的学习理论（IBLT）对相关的认知机制进行了分析。如 Endsley 在其经典文献（Endsley，1995）中所指出的，图式这种认知结构来自于人员曾经面对过的情境态势，在去除一些细节信息后成为可用于模式匹配的一致性结构化知识理解框架，涉及系统组件、系统状态和系统运作等方面的信息，并在认知机制中可用于对知识的长时存储与查找获取，而且能够关联绑定与对应情境态势的行动方案脚本（本质上也是一种包含动作序列的特殊图式）。心智模型作为一种与图式关联的认知结构，代表着人员对系统的目的和形态形成的描述、对

系统运作机制和所观察系统状态做出的解释以及对未来状态做出的预测，可以被描述为一种能够对系统行为进行建模的复杂图式，也可以被认为是某个特定系统的图式。

结合网空安全防御的上下文来看，图式和心智模型来自于对工作任务目标、网络与系统结构、网络与系统运作机制、威胁行为体情况和威胁情报等多种具象信息的理解与抽象。其中，图式主要包含检测发现威胁行为体攻击行动所需要的匹配模式；与图式关联的心智模型则是采用结构化形式整合组织相关信息以帮助网空安全分析人员进行理解的模型框架，而且也包含着所表征情境态势对应的可能发展轨迹及未来状态；与图式关联绑定的脚本，则包含着所表征态势情境对应的待选响应处置行为序列。正如本书第 8 章所描述的，如果结合 STIX 威胁情报框架来看，图式与 IOC（威胁指示器）密切相关，心智模型与 TTP（战术、技术和行为模式）/ 攻击模式密切相关，而脚本与行动方案密切相关。此外，在心智模型中还需要包含通过了解已有网络系统而形成的知识，特别是需要解决“与业务结合”这一长期困扰网络安全行业的问题，从而在模型中包含网络节点或系统组件等实体与业务运行的关联关系。而本书第 10 章和第 13 章中提出的工作任务建模方法，能够将工作任务分解后与网络空间中的相关实体进行依赖 / 支撑关系的对应映射，进而借鉴书中描述的攻击轨迹、攻击图与漏洞树等建模机制，将与实体关联的漏洞、进攻行动与技术影响等信息关联至工作任务，从而面向态势感知的理解阶段，实现可推理至业务影响层面的模型。

通过充分利用以图式和心智模型为代表的长时记忆机制，可以实现高效的网空态势感知，能够有效规避注意力和工作记忆局限性的制约影响。结合书中所介绍的态势感知模型，可以形象地理解为：采用长时记忆机制，能够把各个层级的态势感知阶段串接起来，并且在相邻两层级之间实现由长时记忆中认知结构引导的模式匹配或者关联推导，从而通过提高各阶段内认知任务的定向确定性，以降低对网空安全分析人员和网空安全防御人员经验知识的要求和对工作记忆的压力负荷。

具体来看，在观察阶段之前对所采集数据与事件信息等网空环境中的元素进行并行处理，对大量网络数据和安全事件信息进行缩减、过滤与预处理，并根据预先确定的经验知识完成数据丰富化、基础特征值抽取和基本标签标定等处理操作，从中识别出某些并不存在于原始数据信息中的涌现特征，从而引导观察阶段所需要聚焦的关注方向；在观察阶段，则需要超越基于线索的简单观察模式，而应当根据以图式等形式存在于长时记忆中的认知结构，借鉴第 10 章所描述的告警关联方法，采用信息融合机制（Steinberg & Bowman，2008）将所观察到的证据型环境元素聚合为攻击轨迹等安全信息（George P.