本预印本已投稿至 *Journal of Cybersecurity*，2022年，1–15 doi:
DOI HERE 提前在线发表日期：日 月 年 论文

arXiv:2304.01142v1 [cs.CR] 3 Apr 2023

通过互动式网络防御游戏，从人类防御者身上了解模拟对手

Baptiste Prebot,[1] Yinuo Du[1] 和 Cleotilde Gonzalez [1],*

[1]卡内基梅隆大学社会与决策科学系，美国宾夕法尼亚州匹兹堡，15213 A

*通讯作者。coty@cmu.edu

仅供出版方使用 收稿日期：日期 月份 年份；修订日期：日期 月份 年份；录用日期：日期 月份 年份

摘要

随着网络犯罪的增加，网络安全分析师（即防御者）的需求量很大。防御者必须监控组织网络，以评估威胁以及网络可能遭受的安全漏洞。对手模拟通常用于测试防御者应对组织已知威胁的表现。然而，这种训练过程在帮助防御者胜任这项要求极高的工作方面究竟有多有效，目前尚不清楚。本文展示了如何利用对抗算法和交互式网络防御游戏，研究防御者对防御策略的学习情况。我们的交互式防御游戏（IDG）模拟了一个网络防御场景，要求持续监控传入的网络警报，并允许防御者根据网络中观察到的事件分析、移除和恢复服务。在我们的研究中，参与者面对两种模拟对手之一。Beeline 对手是一种快速、目标明确且掌握情报的攻击者；Meander 对手则行动缓慢，会在网络中游荡，直到找到合适的攻击目标。结果表明，尽管人类防御者起初更难阻止 Beeline 对手，但他们能够通过利用其攻击策略，逐渐学会阻止该对手。与 Beeline 对手交锋的参与者学会了预测对手的行动，并采取更多主动行动，同时减少被动响应行动。这些发现有助于理解如何帮助网络安全分析师加快训练进程。

关键词： 网络防御、人类行为、网络对手、交互式游戏

引言

攻击能力迅速演进，能够以空前的速度和规模发起日益复杂的网络攻击，因此需要训练有素的网络安全专家（即防御者、分析师）来应对不断演变的复杂攻击策略 [1, 2]。网络分析师负责保护组织的计算机网络和数字资产。防御者的工作包含各种各样依赖网络的任务，包括检查大量警报以识别入侵活动并判断网络是否遭到攻击、检测组织安全方面的缺陷、制定适当的防护措施，当然还包括缓解威胁。这些活动通常需要做出时效性决策，而为保护信息，可能需要中断组织的工作。

为调查这些网络情境、评估防御算法和策略，并训练防御者应对新威胁，网络兵棋推演和对手模拟是常见做法 3, 4。兵棋推演练习利用威胁情报来界定对手可能采取的行动和行为，从而模拟对组织构成的潜在威胁。兵棋推演模拟器构建场景，以呈现战术、技术和程序的某些方面，从而帮助测试防御的有效性并识别网络漏洞 [5]。通常会招募人类防御者与模拟对手场景进行交互，帮助他们从这种交互作用中学习 [6, 7]。

尽管近年来人们对网络防御行为的兴趣日益浓厚 [8–12], , 但我们对网络分析师所面临的认知需求仍知之甚少 [13]。对抗行为中的许多因素都可能影响防御策略。例如，众所周知，攻击者人格特质会影响其网络攻击行为 [14, 15]：长期模仿欺骗和马基雅维利主义被发现是隐蔽攻击的预测因素，而自恋和精神病态则与持续时间较短、攻击性更强的攻击（即“暴力破解”）相关。

开展人在回路中的网络防御实验室研究，对于研究防御性和进攻性网络作战，以及制定针对不同类型攻击策略的训练方案 [16]，都是必需的。然而，要通过模拟

© 作者 2 022。由牛津大学出版社出版。保留所有权利。如需授权，请发送电子邮件至：journals.permissions@oup.c om

对手来研究防御者行为，开展有意义的实验室研究颇具挑战。具备测试高度技术化任务和复杂对手所需技能与知识的参与者很难找到，而且他们通常工作繁忙，难以抽出时间测试模拟对手 [9, 17]。要设计在技术手段方面具有高保真度的模拟对手，还需要通过长期跟踪和聚类入侵活动来收集大量威胁情报 [18]。鉴于网络环境和潜在对手持续演变，要在具体技术的粒度上制定面向未来的防御策略同样不切实际。

为帮助缓解这一挑战，研究人员一直在使用仿真工具和简化的游戏 [19] 研究网络欺骗中的进攻与防御两方 [11, 20], 了解公众如何对网络钓鱼邮件进行分类 [15, 21], 探究攻击者的网络安全知识如何影响攻击的识别 [22], 并研究攻击者在对其策略存在不同程度不确定性时的行为 [23]。在本研究中，我们采用 *Intrusion kill chain* 模型 [24] ，将复杂的网络攻击简化为三个战术阶段 *Establish initial foothold, Propagate through network*和 *Act on objectives* [25]。因此，我们采用诸如 *Monitor, Analyze, Remove, Restore* 等对策来扰乱攻击生命周期的各个阶段。通过让防御者应对基于上述战术构建的各种对抗策略，我们可以了解人类防御者的行为，以及他们应对不同类型攻击者并适应动态网络环境的过程。

然而，关于不同对抗策略对防御行为及防御策略形成的影响，相关研究仍然不足。大多数对抗性网络安全游戏依赖博弈论方法来确定最佳防御策略。这些方法通常只考虑某个特定对手，并假定对手会“理性”行事（即表现出优化行为）。这些技术假定对手掌握相关信息，而非面对现实生活中更常见的不确定性，并向参与者提供精确的收益矩阵 [26, 27]。这导致对高度动态的网络环境作出失真的描述；在这种环境中，分析人员必须依靠不完整且有缺陷的信息开展工作。博弈论方法虽有助于针对已知攻击确定最优防御策略，却无法真实呈现攻击者的意图 [28–30]；因此，由此构建的防御方案在动态网络防御环境中面对陌生对手时，最终可能表现不佳 [30–32]。

目标与研究方法

本研究探讨人类防御者如何应对不同的攻击策略，以及这会如何影响防御策略的形成。我们在一个特定但通用的网络环境设定中定义了两种对抗策略。一种对抗策略（即 Meander）行事隐蔽，另一种则直接且迅速（即 Beeline），分别体现了两种攻击者的个性或目标。

在最近的一项实验中， [33] 使用基于实例的学习模型——一种旨在模拟人类决策的认知模型—— [34], 与这两种对抗策略进行对抗。该模拟实验揭示了攻击策略之间的差异及其对防御者表现的影响。总体而言，与 Meander策略相比，Beeline策略导致模型表现更差。然而，当时没有人类数据可用于验证这些观察结果。

我们在一个网络安全场景中设计了交互式防御游戏（IDG），并开展了一项实验室研究，以测试人类针对这两种对抗策略的防御行为。与 [33], 类似，我们预计，面对 Beeline策略的参与者，比面对 Meander策略的参与者更难以防御网络免遭入侵。

交互式防御游戏

交互式防御游戏（IDG）是一款基于网页的交互式网络防御游戏，旨在研究人类防御者在网络安全情境下如何做出决策。IDG 无需安装，可通过网页浏览器远程游玩。 [1] 它为人类参与者提供图形界面，用于观察网络事件并分析计算机网络相关信息，其方式与入侵检测系统（IDS）向人类防御者呈现网络事件的方式类似。IDS 是常见的工具，用于监控网络活动，并帮助检测可能的入侵或攻击 [13]。

IDG 中网络防御者的任务

在 IDG 中，参与者扮演受一家虚构制造公司聘用的网络安全分析师，负责保护公司的计算机网络免受外部恶意活动的侵害。我们使用的网络是常见企业网络拓扑的简化版本，由分组在各个子网中的主机、员工计算机和服务器组成。攻击者试图获取运营服务器（Op Server0）的访问权限，以窃取信息并扰乱生产。对他们来说，最容易的做法是从第一个子网中的一台员工计算机进入网络，然后逐步向上渗透，沿途获取每台主机的管理员访问权限，最终抵达关键的 Op Server0。

攻击者每在一台主机上获得管理员级别的访问权限，防御者就会损失一定的分数。防御者的目标是尽量减少失分。

为执行此任务，防御者使用图1所示的IDG界面。他们必须主动监控网络活动，尝试识别恶意活动，并采取行动阻止攻击者的推进。网络中的主机由其所属的子网、IP地址和主机名来标识。此外，系统还向防御者提供有关每台主机的两项动态信息：受损级别和活动。当攻击者将某台主机作为目标时，首先会尝试获得该机器的用户级访问权限，然后尝试通过权限提升获得管理员级访问权限，并继续攻击网络中的下一个目标。*Compromise level* 表示主机的感染状态。第二项动态信息提供有关系统检测到的最近一次信息

[1] 游戏演示： `http://janus.hss.cmu.edu:8084/`

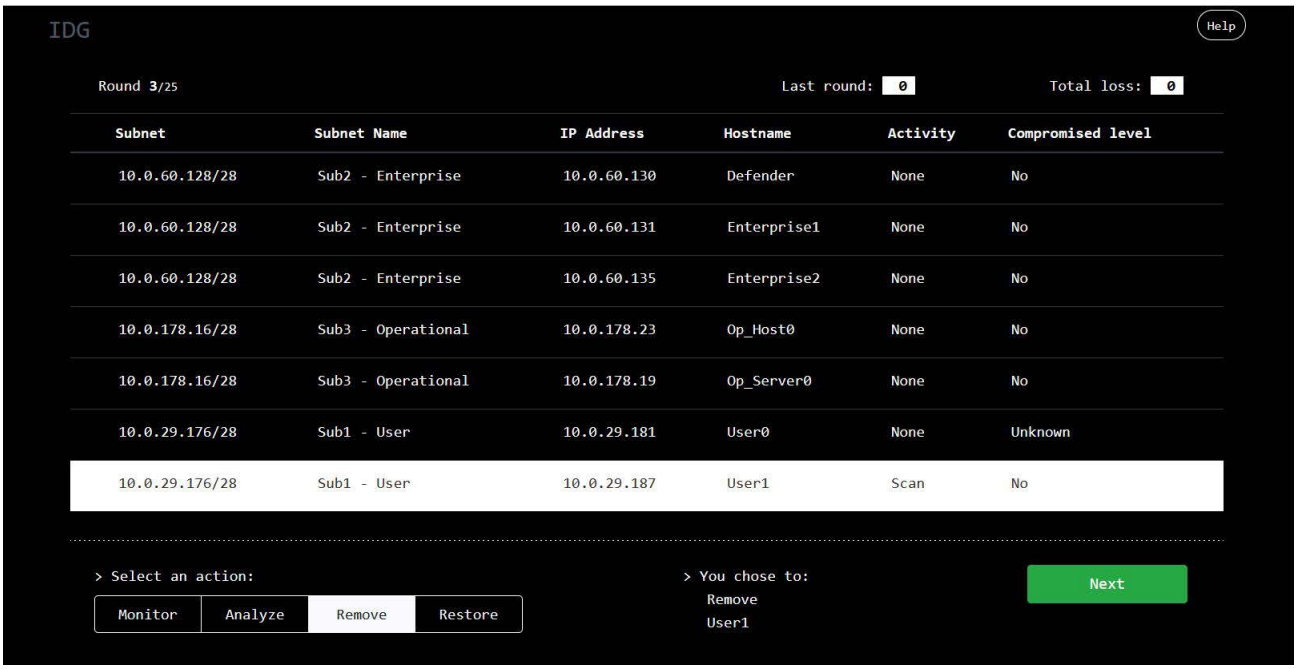

图 1：交互式防御游戏用户界面示意图。

，例如攻击者在该主机上执行的扫描或利用尝试。然而，并非攻击者的所有活动都能被系统检测到。例如，更高级的操作（如权限提升尝试及其后果）会被自动检测。因此，防御者必须理解可观察活动和受损级别，以预测攻击者未来的行动。

防御者可基于这些可观测元素，从屏幕右下角按钮所代表的一组操作中进行选择：监控、分析、移除和恢复。人类防御者可以通过点击表格中主机所在的行来选择一台主机，然后选择四种操作中的一种，在该特定主机上执行。只有监控操作不需要选择目标，它适用于整个网络。

随后，点击“下一步”按钮后，所选操作即会生效，防御者可在“上一轮”数值中查看执行该操作的结果（即损失的点数）。系统将向人类防御者呈现一个全新且更新后的环境，展示网络元素的新状态（活动和受损级别）。“上一轮”的结果会就过去操作的有效性提供即时反馈，而“总损失”则向人类防御者呈现游戏期间损失的累计情况。每场游戏持续固定数量的 $steps$，每个步骤代表一个操作。

防御场景和攻击策略

IDG 中的人类防御者需要保护计算机网络，抵御红队智能体的攻击。本场景中使用的具体网络如图 2 所示。

该网络由分布在 3 个子网中的 7 台主机（4 台计算机主机和 3 台服务器）组成。子网 1 包含非关键的用户主机，子网 2 包含为支持子网 1 上的用户活动而设置的企业服务器，子网 3 则包含关键业务服务器和一台业务主机。

实现了两种攻击策略。它们基于对攻击者先验知识的不同假设，并展示了攻击者人格特质差异可能导致的攻击行为 [14, 15]。在 $Beeline$ 策略中，攻击者会经由子网节点直接前往运营服务器。 $Meander$ 策略则假设攻击者对网络没有任何先验知识。采用这种策略的攻击者会在网络中四处游走，尝试获得子网内每台主机的特权访问权限，然后再继续深入网络。因此，与采用 Meander策略的攻击者相比，Beeline策略是一种直接、迅速且目标明确的策略，能够更快到达运营服务器。对于防御者而言，这意味着面对 Beeline策略时的理论最高损失（-160）高于面对 Meander策略时的理论最高损失（-100）。这些结果是在防御者完全被动的情况下得出的。如果防御者更难检测到此类中断，Beeline策略还可能造成更多中断，也可能导致更长的恢复时间。

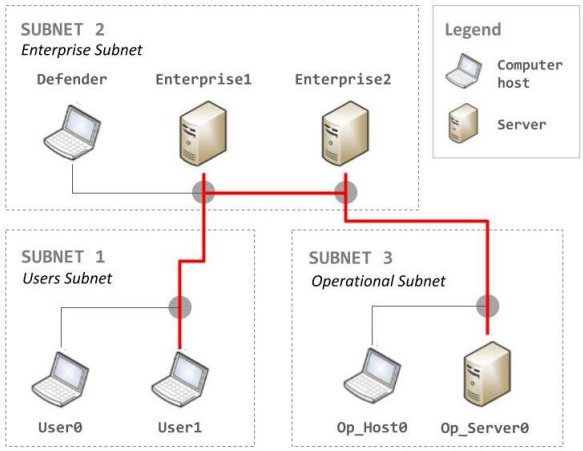

图 2：IDG场景中受到防御的网络拓扑。红线表示任何攻击者访问运营服务器都必须经过的路径。

方法

实验设计

本实验旨在比较人类防御者面对上述两种攻击策略（*Beeline* 和 *Meander*）时的行为。

鉴于Beeline策略相较于Meander策略速度更快、对防御者造成的损害更大，我们预期防御者最初应对Beeline时的表现会差于应对Meander时的表现。该假设已在开放科学框架上预注册 [2]。

参与者

参与者通过亚马逊土耳其机器人招募，参加一项网络安全研究。研究广告称参与时长为 35 至 45 分钟。所有参与者的平均用时为 $M = 47.02 \pm 13.16$ 分钟。参与者获得 4.5 美元的基本报酬，并可根据最终得分获得最高 5.6 美元的奖金（$M = 3.96 \pm 1.39$）。

共有 120 名参与者（89 名男性、30 名女性、1 名未注明）完成了研究，年龄为 21 至 65 岁（$M = 36.77 \pm 11.00$）。其中，12 名参与者（10%）在网络运维与安全领域拥有超过 5 年的经验，并至少拥有相关领域的硕士学位。每位参与者都被随机分配去应对两种对抗策略中的一种。

程序

参与者在提供知情同意并完成人口统计问卷后，会收到任务说明，随后参加简短测验，以确认其对任务说明的基本理解。参与者必须正确回答所有问题，才能进入实验的下一步骤。参与者会收到答题准确性的反馈；如果回答错误，可以修改答案。参与者答对问题的尝试次数不受限制。不过，我们记录了他们首次尝试的得分以及尝试答题的次数。

接下来，参与者观看了一段 介绍 IDG 的视频，内容讲解了界面、游戏控制以及 n ep回合的动态。

随后，参与者完成了由两个阶段组成的任务：(1) 练习环节和 (2) 正式任务。练习环节包括两个简短的回合（即游戏），每个回合有 10 个步骤。练习回合旨在帮助参与者熟悉界面和游戏控制。每个练习回合都对应一种攻击者策略；然而，由于两种攻击策略在前 10 个步骤中的差异并不显著，参与者在练习环节中没有足够的信息来区分这两种对抗策略。

练习环节结束后，参与者完成了正式任务，其中包括 7 个回合，每个回合 25 个步骤。任务没有时间限制。所有回合的实验条件始终保持不变，这意味着每位参与者都使用相同的对抗策略进行了 7 个回合。所有参与者的网络初始状态以及每个回合的网络初始状态都相同。

[2] `https://osf.io/u3nfh`[3] 由于本实验使用的得分为负值（损失），奖金按照与最大可能损失的差额计算，每分计 0.005 美元：奖金=(*total loss*+1120)*0.005。

表1. 每回合平均损失、中断次数、恢复时间和成功率的描述性统计（均值 ± 标准差）。作为背景参考，对抗 Beeline 时每回合的最大损失为 -160，对抗 Meander 时为 -100。

	Beeline	Meander
Loss	-56.12 ± 50.73	-34.76 ± 30.40
中断	0.94 ± 0.81	0.49 ± 0.52
恢复时间（步骤）	2.75 ± 3.55	1.31 ± 1.69

随后，参与者完成了实验后调查问卷，问卷分为两部分：（1）对自身表现和所感知策略的反馈；（2）他们在计算机科学和网络防御方面的经历。最后，参与者收到了最终得分并离场。实验说明、测验和调查问卷，以及数据和分析脚本，可通过 `https://osf.io/u3nfh` 获取。

结果与过程指标

我们使用三个指标衡量了 IDG 中的防御表现结果：

- **损失**：防御者在场景中损失的总分数。作为参考，由 Beeline 行动导致的每回合最大损失为 -160，而对 Meander 的最大损失为 -100。
- **中断**：每回合内发生的服务器中断次数。一次中断是指从对运行中的服务器发起影响攻击并成功，到防御者成功恢复之间连续步骤的集合。
- **恢复时间**：每回合中，服务器发生中断后，防御者将攻击者从运营服务器移除所用的平均步骤数。

除了防御者决策（即每个步骤选择的操作）之外，我们还衡量了防御过程行为。我们也记录了每个步骤中的攻击者行动，并用其分析人类行为和防御策略：

- **防御行动的比例**：每位参与者在每个回合中使用四种防御行动（ $Analyze$、 $Monitor$、 $Remove$、 $Restore$）中每一种的次数，除以回合长度（25 步）。
- **攻击者目标的比例**：攻击者在每个回合中以各主机或子网为目标的次数，除以回合长度（25 步）。这反映了攻击者在网络中的路径。
- **防御策略的比例**：每个回合中采用三种编码防御策略（$Reactive$、$Proactive$、 $Passive$）的频率。关于这些策略的计算详情见下文第 4.2.2 节。

结果

结果指标

表1列出了与 Beeline 攻击策略交手的参与者和面对 Meander 攻击策略的参与者的平均损失、中断次数及恢复时间。

这些观察结果证实了预期中的一些差异：在三项结果表现指标上，两种攻击策略各有不同。总体而言，参与者面对 Beeline策略时失分多于面对 Meander策略时。在一个回合中，面对 Beeline策略时，运营服务器遭受中断的平均次数高于面对 Meander策略时。此外，受到 Beeline 对手攻击而导致运营服务器中断时，将攻击者从运营服务器移除所需的步骤也多于受到 Meander 对手攻击时。

我们分析了各回合的结果指标，以确定防御者在针对两种对手进行练习后是否有所进步。图3展示了每回合三项结果指标的平均值。总体而言，与面对 Beeline 对手相比，参与者面对 Meander 对手时的结果在各回合间更加稳定。换言之，参与者面对 Beeline 对手时起初较差的表现会随着针对该对手练习次数的增加而有所改善，而参与者面对 Meander 对手时的表现则不会随着回合推进而有太大改善。

面对 Meander 对手时，参与者的 **损失** 较低且相对稳定；然而，面对 Beeline 对手时，参与者的损失较大，并且随着针对该对手的练习增加而减少。此外，与面对 Meander 对手的参与者相比，面对 Beeline 对手的参与者最初平均每台服务器的**中断**次数更高。然而，随着面对 Beeline 对手的回合数增加，中断次数会减少。每回合的**平均恢复时间** 也呈现出类似结果：与面对 Meander 对手的参与者相比，面对 Beeline 对手的参与者所需时间更长，但随着回合数增加而缩短。

这些观察结果通过混合效应方差分析（方差分析）进行了检验，其中对手为被试间因素，回合为被试内因素，并纳入两者的交互作用。表2报告了三项结果指标各自的结果。

统计结果表明，防御者面对 Beeline 或 Meander 对手时，其损失、中断和恢复时间存在显著差异。除**平均恢复时间**外，我们还发现，回合对损失和中断有持续且显著的影响，并且对手与回合之间存在交互作用。

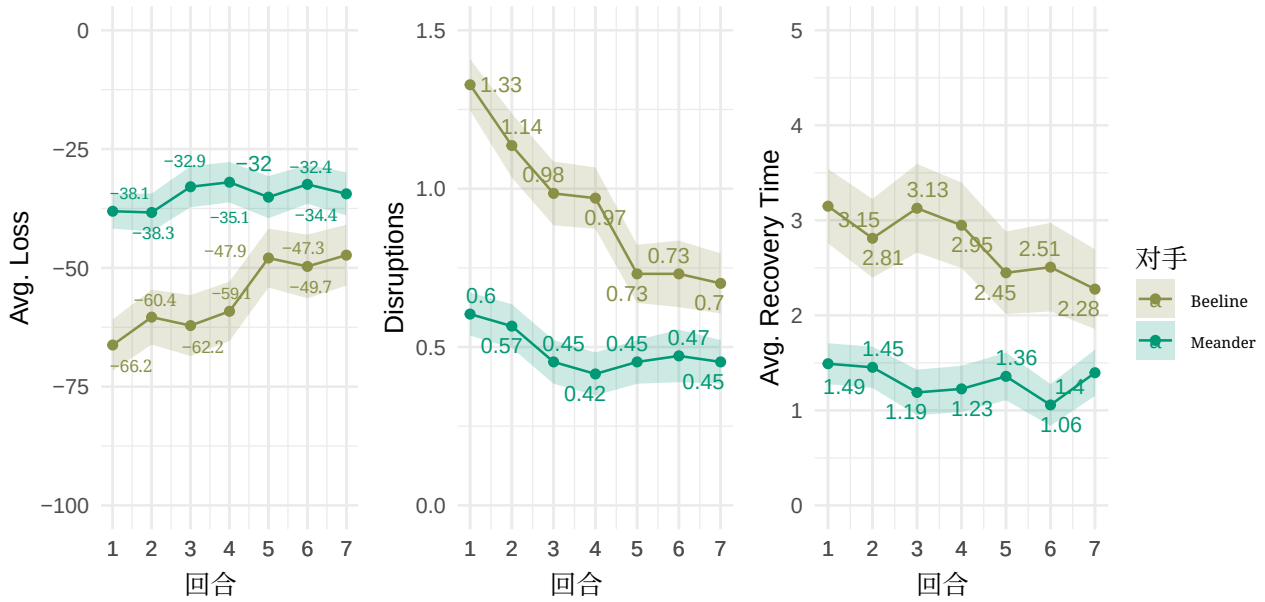

图3：结果指标　　随时间变化的指标及其均值标准误。从左至右：损失；中断；恢复时间。

表2。 关于对手类型和回合对结果指标影响的混合方差分析结果　　cs

指标		分子自由度	分母自由度	F值	p	p值显著性	η^2
Loss							
	对手	1.00	117.00	8.44	.004	**	.06
	回合	4.45	520.94	5.99	< .001	***	.01
	对手：回合	4.45	520.94	3.54	.005	**	.01
中断							
	对手	1.0	117.00	24.24	< .001	***	.10
	回合	5.1	596.38	10.08	< .001	***	.04
	对手：回合	5.10	596.38	4.34	< .001	***	.02
恢复时间							
	对手	1.0	117.00	8.87	.004	**	.06
	回合	4.78	559.48	2.09	.068		.00
	对手：回合	4.78	559.48	1.62	.157		.00

* p < 0.05, ** p < 0.01, *** p < 0.001。

针对各项指标进行的事后单因素方差分析证实了图中所示的结果：在参与者面对 Beeline 对手时，损失和中断会随着回合推进而改善 *only*；但与 Meander 对手交锋时则不会。只有在 Beeline 对手条件下，损失才会随着回合增加而降低（$F(4.29, 278.7) = 7.69, p < .001$, $\eta^2 = .02$），而在 Meander 条件下则不会（$F(4.12, 214.1) = 1.256, p = .29, \eta^2 = .01$）；中断次数也仅在 Beeline 对手条件下减少（$F(4.93, 320.45) = 10.70, p < .001, \eta^2 = .08$），而在 Meander 条件下则没有减少（$F(6, 312) = 1.95, p = .07, \eta^2 = .02$）。

上述分析表明，防御者面对 Beeline 或 Meander 对手时，防御结果存在显著差异。结果显示，起初，Beeline 对手采用的攻击策略比 Meander 策略造成的损害显著更大。根据该策略的定义，这一点并不意外：Beeline 对手会直接穿过各个子网，向运行服务器推进。然而，重要的是，参与者能够逐渐了解 Beeline 对手的行为，并改进防御；随着任务中回合数增加，损失和中断情况均有所改善。参与者应对 Meander 策略时更为成功；然而，随着回合数增加，他们的表现并未显著改善。

接下来，我们将进一步分析参与者在各回合中的行为过程。我们将分析参与者各类行动的比例、防御动作随时间的变化，并描述他们的防御策略。我们还将探讨这些行为的个体差异。

表 3. 各攻击者类型命令使用平均比例的描述性统计（均值 ± 标准差）。

	Beeline	Meander
分析	.20 ±.14	.19 ± .11
监控	.36 ± .20	.30 ± .19
移除	.32 ± .19	.39 ± .22
恢复	.19 ±.09	.19 ± .09

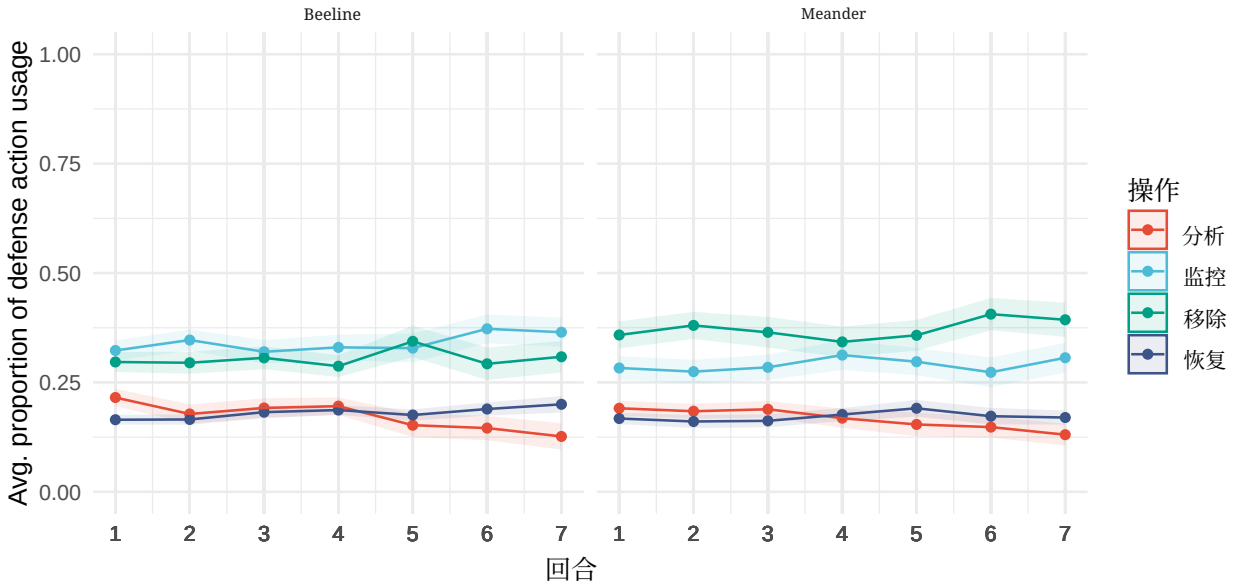

图4：各回合中防御行动平均使用比例及其均值标准误。

过程指标

防御动作

我们分析了防御行动 t 参与者执行任务时采取的行动。表 3 展示了总体平均比例
四种防御行动各自的使用情况 ons，*Analyze*，*Monitor*，*Remove*，*Restore*- 在两种对手策略中的每一种下。

总体而言，无论策略如何，防御者似乎更倾向于使用监控和移除操作，而非分析和恢复操作。针对每个对手组进行的方差分析显示，面对 Beeline 时（$F(3,\ 264) = 17.91,\ p < .001,\ \eta^2 = .17$）以及面对 Meander 时（$F(3,\ 208) = 18.80,\ p < .001,\ \eta^2 = .21$），这些操作的使用比例存在显著差异。采用 Tukey HSD检验进行的事后比较证实，无论对手类型如何，监控与分析、监控与恢复、移除与分析，以及移除与恢复的使用比例在 $p < 0.001$ 上均存在显著差异。

总体而言，两种条件下的参与者都 使用监控和移除操作的频率显著高于分析和恢复操作 [4]。

为了观察这些防御行动在各回合中的使用动态，我们从两个层面分析了行动比例：(1) 跨回合分析，以观察潜在的学习过程以及防御策略的逐步形成；(2) 回合内分析，汇总所有回合，并分析每个回合的 25 个步骤。

图4展示了七个回合中各项行动的平均占比。防御者在面对两种对手策略时，各回合中的行为似乎非常相似。观察到的主要差异是，监控和移除操作比分析和恢复操作更常见。此外，防御者面对 Meander 时，移除操作比面对 Beeline 对手时更常见。

然而，对各类操作所占比例进行的混合效应方差分析仅发现，在分别与 Beeline 和 Meander 对手对战时，回合对 Analyze 操作所占比例有显著影响（$F(4.33, 506.54) = 8.318,\ p < .001,\ \eta^2 = .02$）。对于任何行动，均未发现对手类型的影响。

[4] 我们注意到，参与者使用分析命令的比例与其网络安全背景之间存在微弱但显著的正相关（斯皮尔曼秩相关：$r_s = .23,\ p = 0.011$）。这一相关性或许可以解释参与者的背景与 *Loss* 之间发现的另一种微弱但显著的负相关（斯皮尔曼秩相关：$r_s = -.27,\ p = .0024$）。“专家”受试者似乎过于专注于分析操作。不过，讨论这一结果超出了本文的范围

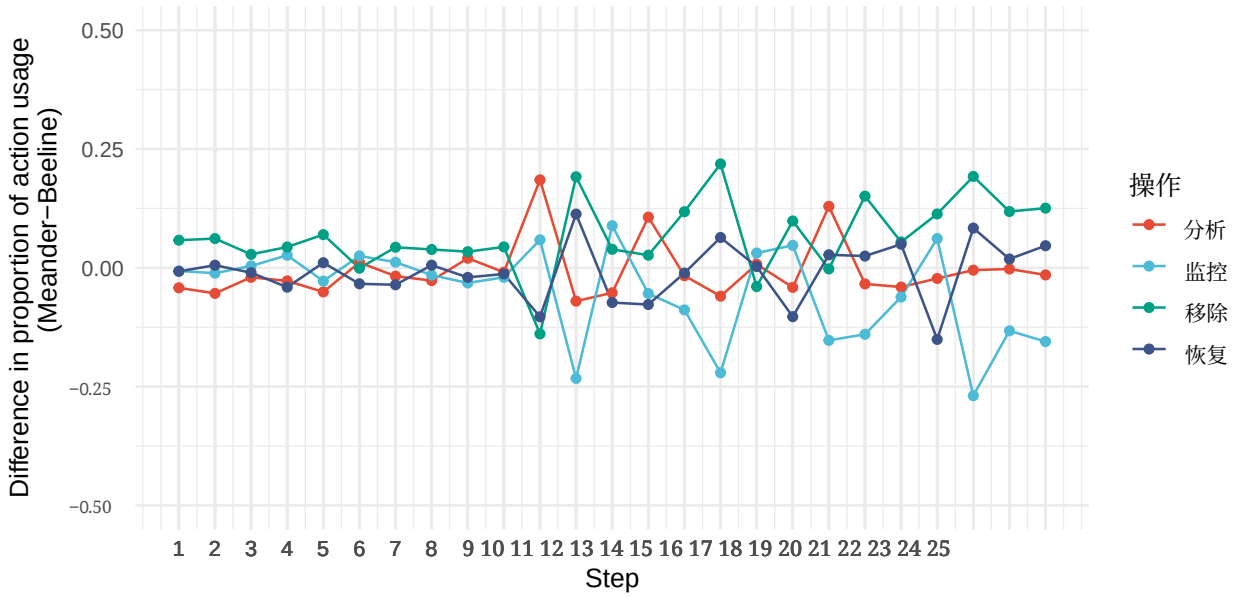

图5：Meander 与 Beeline 条件下操作使用平均比例的差异。正值表示该命令在 Meander 条件下的比例较高，负值表示在 Beeline 条件下的比例较高。

表4. 步骤1–10组和11月25日组中对手类型效应的方差分析结果

	命令	分子自由度	分母自由度	F值	p	p值显著性	η^2
1-10							
	分析	1.00	686.40	3.53	.06		.08
	监控	1.00	670.47	0.08	.784		.03
	移除	1.00	610.51	2.61	.107		.07
	恢复	1.00	685.28	0.27	.601		.04
11月25日							
	分析	1.00	1014.13	0.08	.78		.03
	监控	1.00	1016.06	38.80	< .001	***	.23
	移除	1.00	992.60	24.47	< .001	***	.20
	恢复	1.00	1025.17	1.72	.191		.05

*** p < 0.001。

我们还分析了所有回合中每个步骤所执行行动的比例。为突出两种对手之间的差异，我们计算了面对 Meander 对手的参与者所采取行动的比例与面对 Beeline 对手的参与者所采取行动的比例之差。图 5 展示了这一差异。

我们观察到，最初 Meander 中的移除行动数量多于 Beeline，而在前10个步骤中，Beeline 中的分析行动数量多于 Meander。前10个步骤中，行动比例的差异相对一致且稳定。然而，第10步之后，这种行动比例差异出现了显著波动；与 Meander 对手交战的参与者相比，与 Beeline 对手交战的参与者会采取更多监控操作。

我们分别检验了第1至10步骤以及第11至25步骤中，针对Beeline策略和Meander策略的各类操作所占比例。表4显示，唯一显著差异出现在第11至25步骤中监控和移除操作所占的比例。面对Beeline策略的参与者，其监控操作所占比例高于面对Meander策略的参与者。此外，面对Meander策略的参与者，其移除操作所占比例高于面对Beeline策略的参与者。

为了解释各回合中的这些防御行为，我们分析了汇总所有回合后，对手策略在每个步骤中攻击的目标类型。图6展示了每个对手在各步骤中攻击的目标所占比例。

我们观察到，两名对手都首先攻击子网 1，随后转向用户 1，再转向企业 1，最后到达子网 2。在游戏开始的前 8 个步骤中，可以看到这种对抗性行动具有相似之处。此后，Meander 开始将不同的主机作为目标，例如“防御者”，而 Beeline 则继续转向企业 2，随后直接前往运营服务器。这一示意图解释了

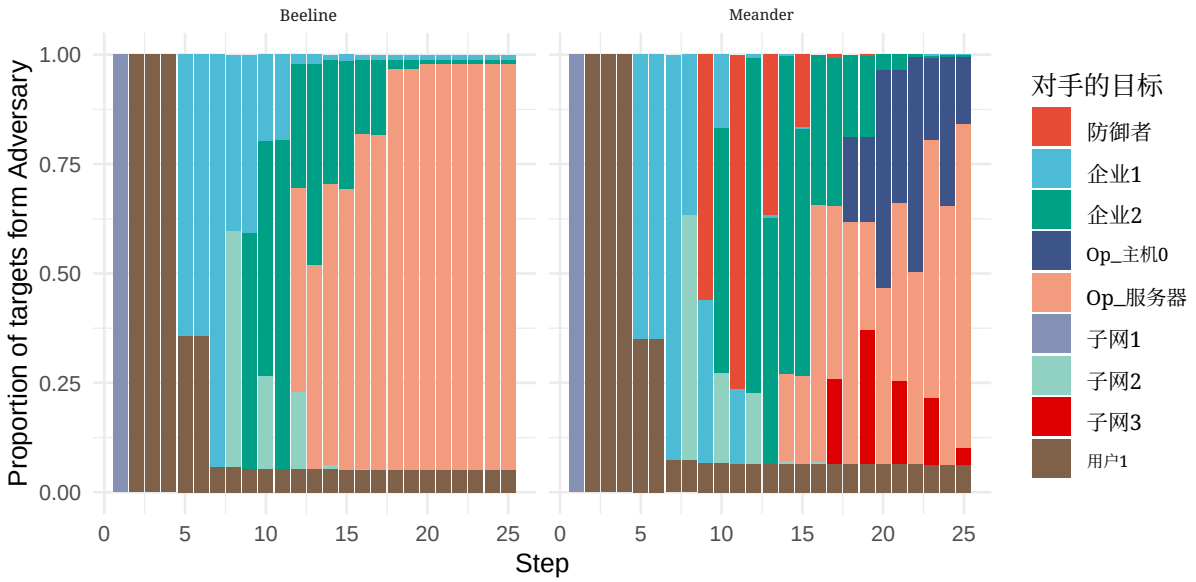

图6：按目标划分的攻击比例随步骤的变化。

表5.启发式策略。

行为	策略
在用户级别或管理员级别恢复受感染主机	反应式
在运营服务器受到影响后将其恢复	反应式
阻止初始影响尝试	主动
防止主机遭到入侵	主动
重复成功的操作	主动
监控或分析	被动

两种攻击策略之间的差异，并解释了为什么人类防御者的行动在第10步之后会有所不同，以及为何在第11步至11月25日的监控和移除行动中存在差异。

防御策略

为了在更具策略性的层面上理解防御者采取的行动，我们将防御动作分为三类策略：*Reactive*、 *Proactive* 和 *Passive* 策略。在网络安全文献中，*proactive* 和 *reactive* 策略通常指机构应对网络安全问题的总体方法，即预测未来威胁，还是修补可能使其暴露于已知威胁之下的安全漏洞 [35–38]。在这里，由于我们关注的是操作层面，而非组织层面，因此根据以下定义对每项具体决策和行动进行分类：

- *reactive* 策略是指能够改善网络状态的行动，例如恢复受感染主机。这些行动是防御者在主机已遭对手攻击且防御点已损失后采取的。
- *proactive* 策略以预防性行动为特征。这些行动体现了对对手下一步行动的预判，或对其意图的预测，从而使防御者能够阻止攻击的推进。
- 该 *passive* 策略表示那些不会直接影响网络状态，也不会减缓或阻止对手在网络中的行动进程的防御动作。

表5列出了用于将防御动作归入三种策略之一的高层启发式策略。我们根据防御者的操作、网络状态（例如，防御者是否将某台主机作为目标，而该主机当前或此前是否遭受过攻击）以及防御行动的效果，对这些启发式策略逐一进行了编码。采用这一编码方案后，91%的防御者行动得以归类。

表6展示了防御者面对 Beeline 和 Meander 对手时，其行动中被编码为反应式、主动和被动策略的总体比例。表中显示，被动策略比主动策略更常见。图7展示了这些策略在各回合中的比例。该图表明，无论对手类型如何，被动策略都最为常见。随着回合推进，反应式策略的比例逐渐下降，而主动策略的比例

表6。 各攻击者类型对应防御策略平均占比的描述性统计（均值 ± 标准差）。

	Beeline	Meander
反应式	.27 ±.15	.26 ± .16
主动	.19 ±.19	.15 ± .20
被动	.48 ± .22	.45 ± .24

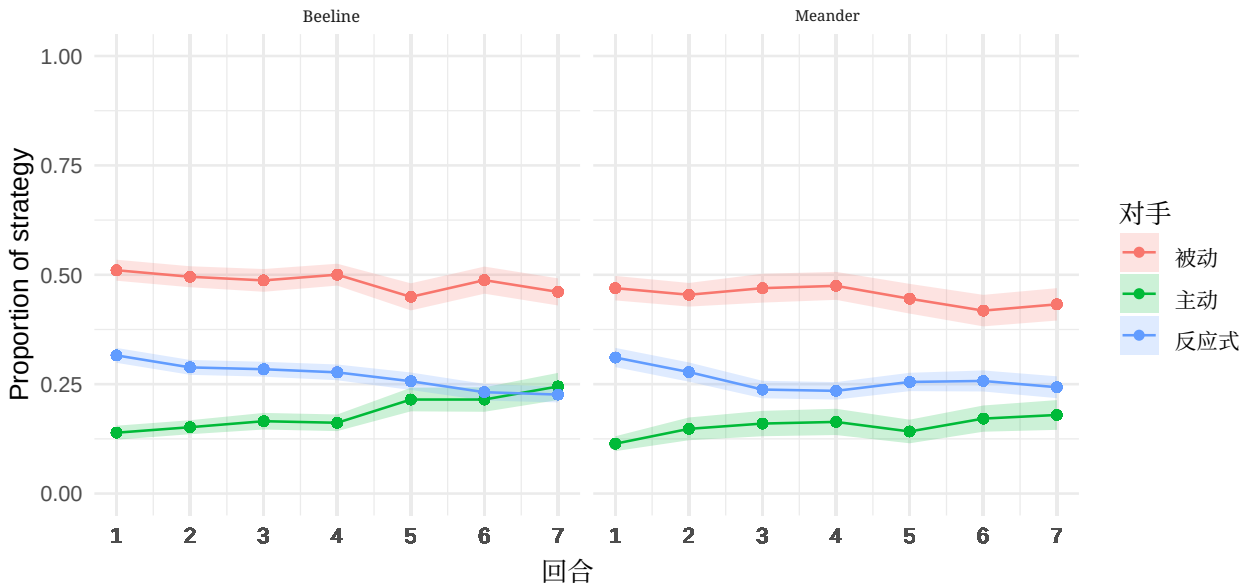

图7：每回合各策略的平均比例。

表7. 对手类型和回合对防御策略比例影响的混合方差分析结果

策略		分子自由度	分母自由度	F值	p	p值显著性	η^2
反应式							
	对手	1	117.00	0.18	.675		.00
	回合	4.15	485.82	8.83	< .001	***	.03
	对手：回合	4.15	485.82	2.30	.550		.01
主动							
	对手	1	117.00	1.09	.299		.01
	回合	3.03	354.99	9.23	< .001	***	.02
	对手：回合	3.03	354.99	2.70	.045	*	.01
被动							
	对手	1	117.00	0.66	.417		.00
	回合	3.73	436.85	3.51	.009	**	.01
	对手：回合	3.73	436.85	1.11	.352		.00

* p < 0.05, ** p < 0.01, *** p < 0.001。

逐渐上升。这种模式在两种对手面前似乎都非常相似，不过，与 Meander 对手相比，面对 Beeline 对手时，主动策略的比例似乎上升得更快。

表7所示的混合方差分析结果表明，在两类对手中，回合对各策略所占比例均有显著影响。此外，回合与对手类型之间对 *proactive*策略所占比例存在显著交互作用。

事后单因素方差分析，并考虑 Bonferroni校正后的p值（p.adj），可以看出，回合对主动式策略比例的简单主效应相对于 Beeline 显著（$F(2.46, 159.66) = 9.152, p.adj < .001, \eta^2 = .04$），但相对于 Meander 不显著（$F(3.11, 161.83) = 2.930, p.adj = .068, \eta^2 = .01$）。

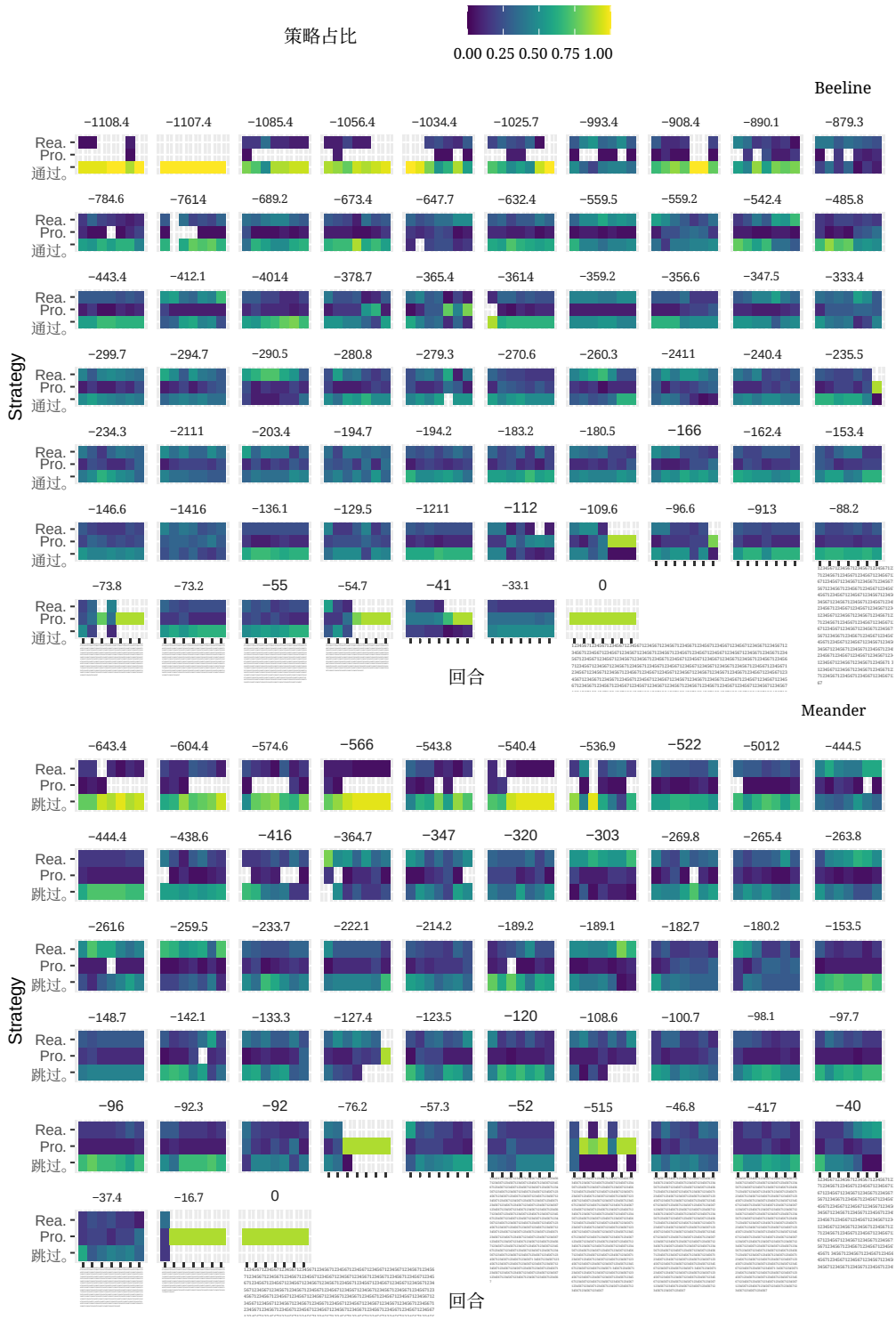

图8：每位受试者在每个回合中采用各策略的比例。受试者按损失从高到低排列。表现最差（损失最高）的受试者位于左上角。每张图上方均显示损失值。

个体差异

图8分别展示了每位参与者在每个回合中各策略拟合比例。此外，这些面板按照每位参与者的总体损失排列，其中左上方面板对应损失最大的参与者，右下方面板对应损失最小的参与者。

该图立即揭示了个体行为的差异，以及每位参与者所采用的策略与其个体损失之间的联系。许多表现不佳的防御者更常采用被动策略，而表现更好的防御者则更为主动。

策略与损失的相关性

对策略与总损失之间的关联图 9 展示了这种关系

也通过相关性进行了分析，这里的总损失涵盖双方对手。散点图每位防御者的总损失得分与各策略占比之间。

n

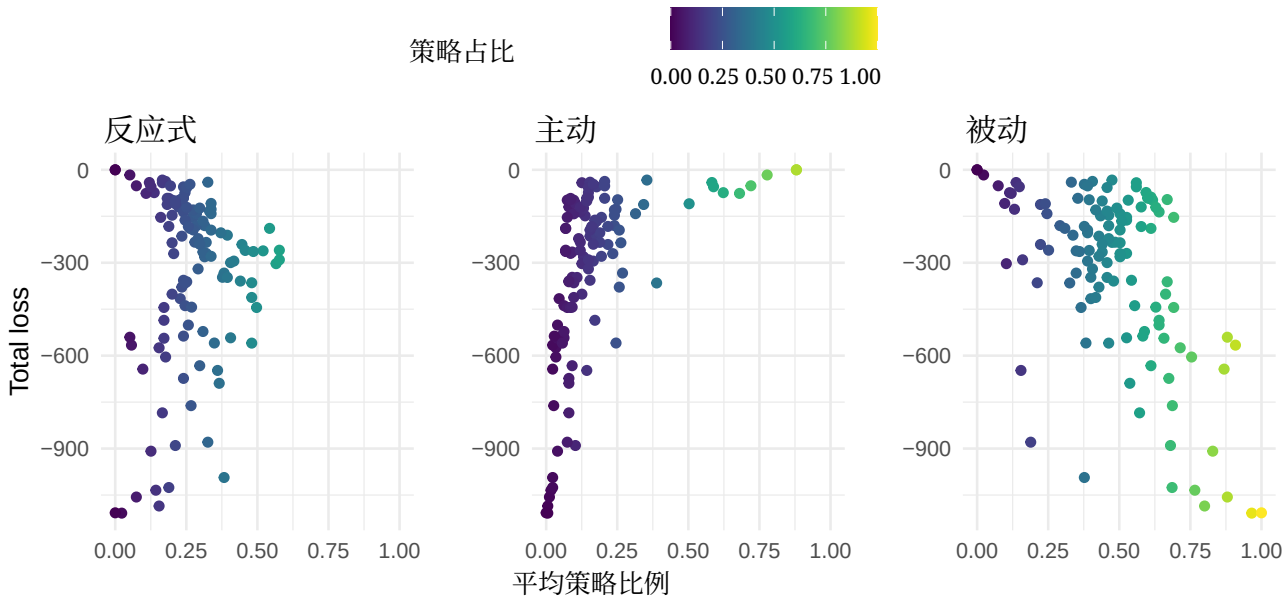

图 9：受试者总损失与策略占比的散点图。

斯皮尔曼相关性检验表明，参与者的损失与主动式策略占比之间存在显著的强正相关（斯皮尔曼秩相关：$r_s = 0.66$，$p < .001$）。也就是说，通常主动行为占比较高的防御者更有可能损失较少的分数，即更好地保护网络。采取主动行动，例如执行移除操作以防止主机遭到利用，是减少损失并更有效地保护网络的一种方式。

同样，斯皮尔曼相关性检验表明，防御者的损失与其被动式策略占比之间存在显著的中等负相关（斯皮尔曼秩相关：$r_s = -0.45$，$p < .001$）。被动操作次数较多的防御者更有可能损失更多分数，因为他们没有采取任何主动防御行动，也就是说，他们没有保护网络。

最后，防御者的损失与反应式策略所占比例之间的相关性并不显著。

讨论

我们设计了一款简单的网络防御游戏，并将其开发为 Web 应用程序，以研究人类防御者应对模拟对手时的防御决策。在本实验中，我们测量了两种不同确定性攻击策略对防御者行为的影响。为此，我们分析了他们的表现、防御选择与行为，以及策略。

正如预期，防御者的表现反映了攻击策略在损失、恢复时间和中断次数方面的“激进程度”差异。事实上，与采用 Meander策略的攻击者相比，采用 Beeline策略的攻击者更快到达运营服务器，因此给人类防御者造成了显著更大的损失、更多的中断以及更长的恢复时间。不过，我们观察到，随着回合推进，无论处于哪种实验条件，参与者都能逐步提升表现并减少损失。整体表现提升可能有两种解释：（1）随着受试者逐渐学会更有效地阻止攻击者到达运营服务器，中断次数有所减少；和/或（2）恢复时间有所改善，即受试者能够更快地使运营服务器从中断中恢复。

结果表明，随着时间推移，记录到的中断次数显著减少，而恢复时间方面则未见明显改善。这可以解读为：防御者逐渐学会更高效地阻止攻击者在网络中的推进，使其无法抵达运营服务器。

总体而言，面对 Beeline攻击者的参与者学会了制定高效的主动防御策略，以改善自身表现，无论是从损失、中断次数还是恢复时间来看都是如此。我们的解读是，尽管两种攻击策略都是确定性的，但与 Meander 相比，Beeline 的路线更加直接、连贯，且经过的主机数量更少。这

使防御者更容易构建 Beeline策略的心理表征，并随着防御经验的增加，更准确地预测对抗性行动。攻击策略的可预测性对人类学习有效防御策略产生了显著影响。

尽管面对 Beeline 对手的参与者似乎随着时间推移显著提升了表现，但他们最终也只是达到了与面对 Meander 对手的参与者相近的水平。从某种意义上说，Beeline 对手留下了更大的提升空间，这也可能是观察到学习速度差异的一个因素。以往针对同一任务进行认知模型实验的结果表明， [33], 防御智能体在面对 Beeline 攻击者时呈现出明显的学习曲线，但经过大量回合后，最终表现相近。若能了解人类如何改进策略，以及其表现如何随着回合增加而变化，将会很有意思。此外，在未来的工作中，延长回合时长（即超过 25 个步骤）或许能让我们使用模式识别方法并对行动序列展开更深入的分析，从而完善防御策略的分类，并可能识别出更复杂的启发式方法。

总的来说，本研究说明，人类防御者所面对的模拟对手类型可能会影响其学习速度以及制定恰当防御策略的过程。研究发现，与隐蔽且较难预测的攻击者相比，更具攻击性但也更容易预测的攻击者更容易被人类防御者学习和利用。

网络分析师必须在高度动态且信息有误、不完整的环境中工作。对抗性网络防御游戏和 IDG 等仿真工具有助于模拟此类决策情境，并更好地理解人类网络防御者所面临的认知需求。我们的工作揭示了为人类防御者的开发与训练提供动态且复杂的攻击者的重要性。这些结果支持了近期建模实验的发现：动态攻击策略是认知模型和人工智能防御的弱点 [33, 39]。为推动未来网络防御领域的人类与人工智能协作，我们可以研究动态攻击者对人类制定防御策略的影响，并探讨人类如何在人工智能代理团队中工作并与其协作。

利益冲突

未声明任何利益冲突。

作者贡献声明

B.P.：本研究的概念构思、方法设计、软件开发、数据分析、写作；Y.D.：本研究的概念构思、软件开发、写作；C.G.：本研究的概念构思、方法设计、写作——原稿撰写。

致谢

作者感谢匿名审稿人提出的宝贵建议。我们感谢动态决策实验室的 Jeffrey Flagg 协助审阅并开展本研究。本研究由陆军研究办公室通过澳大利亚—美国多学科大学研究计划资助（编号：W911NF-20-S-000）提供资助，并由陆军研究实验室依据合作协议（编号：W911NF-13-2-0045，ARL网络安全合作研究协议）完成。

参考文献

[1]Yuchong Li 和 Qinghui Liu。《网络攻击与网络安全综述：新兴趋势与最新进展》。 *Energy Reports*，7:8176–8186，2021年。[2] Cong Truong Thanh 和 Ivan Zelinka。《恶意软件中人工智能作为下一代威胁的调查》。载于 *Mendel*，第25卷，页27–34，2019年。[3] Edward JM Colbert、Alexander Kott 和 Lawrence P Knachel。《网络兵棋推演的博弈论模型与实验研究》。 *The Journal of Defense Modeling and Simulation*，17(1):21–38，2020年。[4]Kimberly Ferguson-Walter、Temmie Shade、Andrew Rogers、Michael Christopher Stefan Trumbo、Kevin S Nauer、Kristin Marie Divis、Aaron Jones、Angela Combs 和 Robert G Abbott。《图拉罗萨研究：量化网络欺骗有效性的实验设计与实施》。技术报告，桑迪亚国家实验室（SNL-NM），美国新墨西哥州阿尔伯克基，2018年。[5]Andy Applebaum、Doug Miller、Blake Strom、Chris Korban 和 Ross Wolf。《智能化自动红队模拟》。载于 *Proceedings of the 32nd Annual Conference on Computer Security Applications*，页363–373，2016年。[6]Hamdi Kavak、Jose J Padilla、Daniele Vernon-Bido、Saikou Y Diallo、Ross Gore 和 Sachin Shetty。《网络安全仿真：现状与未来方向》。 *Journal of Cybersecurity*，7(1):tyab005，2021年。[7]Maneesh Varshney、Kent Pickett 和 Rajive Bagrodia。《用于网络作战测试、评估和训练的实况—虚拟—构造（LVC）框架》。载于 *2011-MILCOM 2011 Military Communications Conference*，页1387–1392。IEEE，2011年。[8] Robert S Gutzwiller、Sarah M Hunt 和 Douglas S Lange。《面向刻画网络防御分析师网络认知态势感知（CCSA）的任务分析》。载于 *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*，页14–20。IEEE，2016年。[9] Vladislav D Veksler、Norbou Buchler、Claire G LaFleur、Michael S Yu、Christian Lebiere 和 Cleotilde Gonzalez。《网络安全中的认知模型：向专家分析师学习并预测攻击者行为》。 *Frontiers in Psychology*，11:1049，2020年。

[10]Vladislav D Veksler、Norbou Buchler、Blaine E Hoffman、Daniel N Cassenti、Char Sample 和 Shridat Sugrim。《网络安全仿真：网络攻击者、防御者和用户认知建模综述》。 *Frontiers in psychology*，9:691，2018年。[11] Edward A Cranford、Cleotilde Gonzalez、Palvi Aggarwal、Milind Tambe、Sarah Cooney 和 Christian Lebiere。《迈向网络欺骗认知理论》。 *Cognitive Science*，45(7):e13013，2021年。[12]Chelsea K Johnson、Robert S Gutzwiller、Joseph Gervais 和 Kimberly J Ferguson-Walter。《决策偏差与网络攻击者》。载于 *2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*，页140–144。IEEE，2021年。[13]Cleotilde Gonzalez、Noam Ben-Asher、Alessandro Oltramari 和 Christian Lebiere。《认知与技术》。载于 *Cyber defense and situational awareness*，页93–117。施普林格，2014年。[14]Daniel N. Jones、Edgar Padilla、Shelby R. Curtis 和 Christopher Kiekintveld。《网络发现、扫描策略与黑暗三联征》。 *Computers in Human Behavior*，122:106799，2021年。[15]Shelby R. Curtis、Prashanth Rajivan、Daniel N. Jones 和 Cleotilde Gonzalez。《黑暗三联征个体的网络钓鱼尝试：攻击模式与漏洞》。 *Computers in Human Behavior*，87:174–182，2018年。[16]Robert S Gutzwiller、Sunny Fugate、Benjamin D Sawyer 和 PA Hancock。《网络防御中的人为因素》。载于*Proceedings of the human factors and ergonomics society annual meeting*，第59卷，页322–326。SAGE出版社（加利福尼亚州洛杉矶），2015年。[17]Norbou Buchler、Prashanth Rajivan、Laura R. Marusich、Lewis Lightner 和 Cleotilde Gonzalez。《网络安全防御竞赛中的团队协作与领导力：社会计量学和观察评估》。 *Computers & Security*，73:114–136，2018年。[18]Blake E Strom、Andy Applebaum、Doug P Miller、Kathryn C Nickels、Adam G Pennington 和 Cody B Thomas。《MITRE ATT&CK：设计与理念》。载于 *Technical report*。MITRE公司，2018年。[19] Cleotilde Gonzalez、Polina Vanyukov 和 Michael K Martin。《利用微观世界研究动态决策》。 *Computersin human behavior*，21(2):273–286，2005年。[20] Palvi Aggarwal、Cleotilde Gonzalez 和 Varun Dutt。《Hackit：用于在实验室研究现实世界网络攻击的实时仿真工具》。载于 *Handbook of Computer Networks and Cyber Security*，页949–959。施普林格，2020年。[21]Kuldeep Singh、Palvi Aggarwal、Prashanth Rajivan 和 Cleotilde Gonzalez。《网络钓鱼邮件检测训练：经历过的网络钓鱼邮件频率的影响》。载于 *Proceedings of the human factors and ergonomics society annual meeting*，第63卷，页453–457。SAGE出版社（加利福尼亚州洛杉矶），2019年。[22] Noam Ben-Asher 和 Cleotilde Gonzalez。《网络安全知识对攻击检测的影响》。 *Computers in Human Behavior*，48:51–61，2015年。[23]Fr´ed´eric Moisan 和 Cleotilde Gonzalez。《不确定性下的安全：与随机攻击者相比，自适应攻击者对人类防御者更具挑战性》。 *Frontiers in psychology*，8:982，2017年。[24]Eric M Hutchins、Michael J Cloppert、Rohan M Amin 等。《情报驱动的计算机网络防御：基于对手行动和入侵杀伤链分析》。 *Leading Issues in Information Warfare & Security Research*，1(1):80，2011年。[25] Li Zhang 和 Vrizlynn LL Thing。《主动网络防御中三十年的欺骗技术：回顾与展望》。 *Computers& Security*，106:102288，2021年。[26] Milind Tambe。《 *Security and game theory: algorithms*、 *deployed systems*、 *lessons learned*》。剑桥大学出版社，2011年。[27] Yasaman Abbasi、Debarun Kar、Nicole D Sintov、Milind Tambe、Noam Ben-Asher、Don Morrison 和 Cleotilde Gonzalez。《了解你的对手：构建更完善的对抗行为模型的启示》。载于 *CogSci*，2016年。[28]Palvi Aggarwal、Zahid Maqbool、Antra Grover、VS Chandrasekhar Pammi、Saumya Singh 和 Varun Dutt。《网络安全：网站篡改博弈中防御者与攻击者策略的博弈论分析》。载于 *2015 International Conference on CyberSituational Awareness*、 *Data Analytics and Assessment (CyberSA)*，页1–8。IEEE，2015年。[29] Alan Nochenson 和 CF Heimann。《攻击者—防御者博弈的仿真与博弈论分析》。载于 *International Conference on Decision and Game Theory for Security*，页138–151。施普林格，2012年。[30] Cuong T Do、Nguyen H Tran、Choongseon Hong、Charles A Kamhoua、Kevin A Kwiat、Erik Blasch、Shaolei Ren、Niki Pissinou 和 Sundaraja Sitharama Iyengar。《网络安全与隐私中的博弈论》。 *ACM Computing Surveys (CSUR)*，50(2):1–37，2017年。[31]Afraa Attiah、Mainak Chatterjee 和 Cliff C Zou。《用于建模网络攻击与防御策略的博弈论方法》。载于*2018 IEEE International Conference on Communications (ICC)*，页1–7。IEEE，2018年。[32]Yuan Wang、Yongjun Wang、Jing Liu、Zhijian Huang 和 Peidai Xie。《网络安全博弈论方法综述》。载于 *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*，页631–636。IEEE，2016年。[33]Yinuo Du、Baptiste Pr´ebot、Xiaoli Xi 和 Cleotilde Gonzalez。《迈向自主网络防御：认知模型的预测》。 *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*，2022年。[34]Cleotilde Gonzalez、Francis J. Lerch 和 Christian Lebiere。《动态决策中的基于实例的学习》。 *Cogn. Sci.*，27:591–635，2003年。[35] John Grisham、Sagar Samtani、Mark Patton 和 Hsinchun Chen。《在在线黑客论坛中识别移动恶意软件和关键威胁行为者，以开展主动网络威胁情报工作》。载于 *2017 IEEE International Conference on Intelligence and Security Informatics(ISI)*，页13–18，2017年。[36]Soumitra Sudip Bhuyan、Umar Y Kabir、Jessica M Escareno、Kenya Ector、Sandeep Palakodeti、David Wyant、Sajeesh Kumar、Marian Levy、Satish Kedia、Dipankar Dasgupta 等。《推动医疗保健网络安全从反应式转向主动：当前状况与未来建议》。 *Journal of medical systems*，44(5):1–9，2020年。[37]Sagar Samtani、Maggie Abate、Victor Benjamin 和 Weifeng Li。《作为产业的网络安全：网络威胁情报视角》。 *The Palgrave Handbook of International Cybercrime and Cyberdeviance*

，第 135–154 页，2020。

[38]Alireza Zarreh、Can Saygin、HungDa Wan、Yooneun Lee 和 Alejandro Bracho。《基于博弈论的先进制造系统网络安全评估模型》。*Procedia Manufacturing*，26：1255–1264，2018。第46届SME北美制造研究会议（NAMRC 46），得克萨斯州，美国。[39]Yinuo Du、Baptiste Pr´ebot 和 Cleotilde Gonzalez。《机器人之间的网络战：对于防御者而言，类人攻击者比确定性攻击者更具挑战性。》*Accepted to the 56th Hawaii International Conference on System Sciences HICSS 2023*，2023。

作者姓名。 这是示例作者简介文本。这是示例作者简介文本。这是示例作者简介文本。这是示例作者简介文本。这是示例作者简介文本。这是示例作者简介文本。这是示例作者简介文本。这是示例作者简介文本。