章 1

利用博弈论进行安全风险评估

利萨·拉吉班达里和艾纳尔·阿瑟斯奈克内斯

1.1 引言

组织受到许多因素的影响，这些因素可能阻碍其商业目标的实现，并造成声誉、金钱、牙科数据等的损失。物联网等，信息安全的重要性甚至更高。为了应对越来越多的威胁，组织需要向前迈出一步。在安全风险评估中，组织可以获得其信息系统风险的可靠画面，并决定分配其资源来保护其系统免受严重风险。因此，安全风险评估对于那些想要承受当前威胁环境的组织来说是非常有价值的方法。如果我们能够正确地识别、评估和评估风险，我们可以更好地减轻或对待它们。

在大多数风险评估方法中(例如，ISO/IEC 27005:2011[2])，风险是作为事件的后果和可能性的组合来测量的。似然和结果的值以定性或定量的形式表示。例如，在确定似然或后果时，使用 1-5 的缓慢、中等、高或序数刻度等定性方法。ALDATA 正截面统计数据是不充分或不相关的，似然值收集使用专家启发。此外，对手的适应性可能会导致这些评估是基于主观判断。考克斯还指出了风险。

基于“频率”和“严重性”的矩阵具有以下局限性：分辨率差、误差、次优资源分配和输入输出模糊。此外，考克斯解释了“风险=威胁×脆弱性×后果”组合在分析恐怖袭击中的局限性。传统风险评估方法的另一个局限是对机会风险的考虑。机会主义风险在于“担心某些可取的事情可能不会发生，因为其他玩家可能没有动机采取某种策略，因为他必须承担损失或者他的收益可能是微不足道的”。

利用博弈论，我们可以考虑具有共同兴趣的玩家如何在相互依赖的情况下进行交互，他们选择的策略，以及他们如何通过选择这些策略来评估结果的价值。利用博弈论，我们可以利用现有的鲁棒性数学非合作博弈模型进行风险评估，而不依赖于主观概率。然而，这很少在组织中使用。在确定似然度时依赖于主观判断是传统风险评估方法的主要局限之一。因此，研究博弈论如何与传统的风险评估方法相结合显得尤为重要。此外，偶尔在组织中使用博弈论进行风险评估背后的原因可能是难以适应不同的方法，以及缺乏实施该方法所需的技能，尤其是我们在第 1.5 节中讨论的。

本章展示了三种现有的风险评估/管理方法，ISO/IEC 27005:2011，NIST 特别出版物 800-30 修订版 1（NIST 80030r1）[3]和科拉斯[5]，如何映射到一般的风险评估过程和术语。这说明了大多数传统风险评估方法有一些共同的步骤。博弈论的安全性在许多著作中都被强调为[6, 17]。然而，据我们所知，除了[25]之外，还没有发表任何著作来展示如何利用现有的风险评估方法来映射博弈理论步骤。在[25]中，ISO/IEC 27005:2008 用于通过将每个博弈理论步骤与 ISO/IEC 27005:2008 的步骤进行映射，并确定在哪里丢失了通信，来展示博弈理论方法如何可用于风险评估。本章的目的是将博弈论方法与一般风险评估方法相结合，介绍如何将博弈论用于风险评估，并强调其中的一些要点。

攻击者和防御者之间的游戏主要在安全性方面进行研究，如[26, 17]所示。合作博弈理论模型可以用来捕捉组织所面临的机会风险。然而，在解决安全游戏时，很少考虑合作博弈模型。例如，由于首席信息安全官（CISO）希望提高安全意识，所以组织存在机会风险，但是员工进行安全培训的动机较小，因为他需要花时间浏览在线材料和通过测试。CISO 和工作人员之间的这种设置可以建模为合作博弈，以确定 CISO 需要采取什么策略来解决此安全问题。

本章其余部分的结构如下。在第 1.2 节中，我们提供了风险评估过程和阶段的简要概述，以及常见风险评估步骤和三种选定方法之间的映射。第 1.3 节用一个例子概括了风险评估的博弈论步骤，并显示了博弈论步骤与一般风险评估步骤（如第 1.2 节所推导的）之间的映射。在第 1.4 节中解释了解决机会风险的合作博弈模型。我们讨论了将博弈论用于风险评估的一些挑战，并在第 1.5 节中结束了本章。

1.2 风险评估

即使与某些坏事的可能性相联系，它也可能包括正反两方面。这种风险观点在经济学界或项目管理学界都已存在[12]。在风险管理领域中使用的术语有不同的定义。我们认为风险评估是一个系统过程，包括三个步骤——风险识别、风险分析和风险评估——如 ISO/IEC 27005:2011 标准[2]中所考虑的。此外，风险管理程序包括初始准备（上下文建立）、风险评估、风险处理、风险监测和审查、以及风险沟通和咨询。在下面的小节中，我们首先描述了一般风险评估的阶段。然后，我们展示了如何在公共框架中查看三种选定的风险评估方法——ISO/IEC 27005:2011、NIST 800-30r1 和 CORAS。这些措施决定了信息安全风险管理过程。除了所选择的方法，还有许多风险评估/管理标准，比如 ISO31000:2009 标准[1]，它为进行

风险管理和以 ITriskscenarios 为中心的风险 IT[14]框架提供了共同的指导方针。通用框架可以扩展到 ISO31000：2009 年，并风险 IT 框架。

1.2.1 一般风险评估阶段

如上所述，有许多方法来进行风险评估，每个方法都有后续步骤。即使评估可以在不同的序列中完成，但是它们都有一些共同的步骤。从现有方法的文献综述中，一般风险评估过程的更宽广的视角可由以下阶段来表示：初始准备、风险情景的识别（识别威胁、脆弱性、后果）、风险的估计（评估可能性，assESS 后果，并确定风险）和风险评估。这四个阶段是为了简化评估过程，创造了上述不同方法的统一框架。

1. 初步准备：此阶段包括确定组织的范围、风险偏好和目标、识别资产及其所有者、以及收集风险评估范围内的系统或应用程序或项目的文档。这一步骤的关键挑战之一是范围渐变，这可能导致不必要的资源利用和增加的工作量，从而破坏风险评估过程的成功完成。主要利益相关者（除了资产所有者之外）及其责任也被确定为在整个风险评估过程中建立沟通与合作。
2. 识别风险场景：这个阶段包括三个子阶段：识别威胁、识别漏洞和识别后果。识别前一步骤中确定的对资产的威胁，然后识别可能被利用的资产中的漏洞（考虑现有控制）。然后，如果威胁源（例如攻击者）成功地利用了漏洞，那么后果也被识别。这提供了要分析的风险场景的清晰画面。
3. 估计风险：这个阶段包括三个阶段：评估后果，评估可能性，并确定风险。使用定性量表或定量值评估识别风险情景发生的后果和可能性。考虑威胁、脆弱性、后果和当前实施的控制（如果有的话），评估风险的可能性。其后果可能涉及财务、信誉受损和客户损失，或者涉及机密性、完整性或可用性（CIA）的损失。最后，风险等级通常被确定为下面给出的可能性和后果的组合。

风险=可能性·后果

4. 评估风险：在这一阶段，对所有风险的总风险进行审查和优先考虑。X 轴表示风险的可能性矩阵，Y 轴表示红色、橙色和绿色的后果和颜色方案，代表高风险、中等风险和低风险，可以用于容易的可视化和通信。

风险评估之后是风险处理阶段（超出本章范围）。在这一阶段，对识别风险进行分类。分

类文件根据成本效益标准和组织的风险偏好，是否应该接受、减轻、避免或转移风险[2]。接受选项与保持风险原样有关，减轻选项与通过应用安全控制措施来降低风险有关，避免选项与排除导致风险的任务有关，而转移选项涉及与另一方分担风险，例如。买保险。然后，开发了风险控制方案。风险防范应该定期监控，并在范围内进行变更。此外，整个过程应定期进行有效的风险管理。此外，如 ISO/IEC 27005:2011 所述，风险沟通和咨询应该贯穿整个风险管理程序[2]。

1.2.2 一般风险评估与三种选择方法之间的映射

我们将以下三个风险评估/管理标准或方法的过程和术语与上面提到的一般风险评估步骤进行映射：ISO/IEC 27005:2011、NIST 800-30r1 和 CORAS。该映射基于作者对三种方法的理解，并且限于覆盖评估步骤，而排除了风险处理、风险通信和风险监视/维护阶段。

ISO/IEC27005:2011 是国际标准化组织/国际电工委员会制定的国际化风险管理标准。风险管理过程包括以下几个阶段：环境建立、风险评估、风险处理、风险接受、风险沟通、以及风险监测和审查。

美国国家标准与技术研究所开发的 NIST 800-30r1 为进行风险评估提供了指导和支持 NIST 800-39 标准。维护评估。

CORAS 是一种基于模型的安全风险分析方法。它使用 Uni edModelingLanguage(UML)建模语言对风险进行建模，包括七个步骤：引入、高水平分析、批准、风险识别、风险激励、风险评估和风险处理。

表 1.1 所示的映射表明，ISO/IEC 27005:2011 标准、NIST 800-30r1 和 CORAS 的所有风险评估步骤都可以与一般风险评估步骤进行映射。如上所述，[28]也支持这一点，它为不同的风险评估方法提供了统一的框架。当在一般风险评估步骤中识别漏洞时，隐含地包括对现有控制的识别，因此不作为单独的步骤提及。除了 ISO/IEC 2500 5:2011 之外，其他方法也没有明确地提到这一步骤。此外，这些方法都不考虑机会的识别。

表 1.1：评估过程与术语之间的映射

一般风险评估步骤	ISO/IEC27005:2011	NIST800-30r1	CORAS
组织准备 风险评估和组织目标 确认资产和资产所有者	信息安全风险管理的标准、标准与边界、组织	准备评估（识别目的、范围、假设和约束、信息源、风险模型和分析方法）	介绍会议（标识范围，目标和资产保护），高级别分析，批准
识别风险情景识别威胁源和事件 识别威胁场景 漏洞识别	识别脆弱性和易感条件 识别漏洞 结果的标识	包含在确定可能性和可能性时包含威胁图的建模评价结果的评价	碰撞判定 估计序列 事件似然估计的评价方法 决定性事件的发生估计值 确定风险等级
估计值 评估结果 评估可能性 决定性事件	后果评估 事故评估 似然性 水平危险度测定	碰撞判定 发生决定性事件	估计序列 估计值 计算机价值
评价材料 优先识别 IDERISK 方案	ListFox 优先排序	监听风险 风险的识别水平	评估矩阵和风险图

1.3 安全风险评估的博弈论

一个博弈论模型包括玩家，他们可以采取的策略，以及他们通过移动获得的收益。在某些情况下，在进行风险评估时，缺乏历史数据，或者现有数据可能缺乏科学依据。然而，我们可能已经看到，不同的利益相关者重视他们可能采取的不同行动的结果。在利益相关者是理性的假设下，博弈论提供了一种将这些收益值转换为概率的方法。因此，博弈论可以提供可用信息（偏好强度）与典型风险评估方法（概率）所要求的之间的联系。

在下面的小节中，我们提供了风险评估的博弈理论步骤，并以管理员和攻击者之间的简

单两人博弈为例，详细阐述了这些步骤。然后，对博弈的理论步骤和一般风险评估步骤进行了映射。

1.3.1 博弈理论步骤

下面给出了风险评估的博弈理论步骤（改编自[25]）。这些步骤应该系统地进行，并且可以重复该过程。对于每个步骤，我们提供一个简短的描述，并通过解释如何收集数据（在可行的情况下）来阐述：

1. 调查场景：在调查场景时，需要与其所有者一起保护的范围和资产是相同的。此外，确定了用替代策略或回报进行重复分析的标准。
2. 确定参与者：其行为相互影响的决策者是相同的。这些决策者包括获得利益或必须承担损失的玩家（风险所有者（RO））和具有对 RO（战略所有者（SO））的欺骗性激励的玩家。我们假设球员是理性的。
3. 对于每个玩家，收集以下数据。为了全面了解玩家，需要考虑他们的动机、能力（例如，实施或防御攻击的资源）和经验：
    a) 确定所获得的信息：玩家决定收集的信息。与决策时的信息相关，可以将博弈划分为完全或不完全和完全或不完全信息博弈。在完美信息游戏中，每个玩家都知道所有其他玩家以前的动作（不完美信息游戏也是如此）。在完全信息游戏中，每个玩家都知道所有玩家的策略和报酬，但是可能知道也可能不知道以前的动作（副业已完全信息游戏）。
    b) 确定策略：确定与玩家（即 ROandSO）的行动相关的策略。这些策略包括面对威胁、制造威胁或获得机会。这些行为可以基于一个独立的群体。此外，这些选项可以协商。
    c) 身份参照：玩家看重结果的多重性（例如，金钱、声誉、隐私、信任等）或机密性、完整性、可用性（CIA）。这些也被称为效用因素。这些可以通过询问他们如何评价研讨会的结果、通过调查或调查心理学的研究来获得。
    d) 用收益/效用来表示：比较结果的尺度、测量方法和权重。然后，根据获得的等级和效用来表示优先顺序。通常，玩家会剃掉激励，以使他们的收益/效用最大化。效用可以利用多属性效用理论（MAUT）的加性效用函数来估计[7]。对玩家的加性效用函数是如下给出的其个体效用因子的加权平均值。

$$U(a)= m \sum k=1 wk \cdot ak .$$

其中 M 是玩家的效用因子的数量，WK 是效用因子 AK 的赋权，并且 Sigm M k = 1WK = 1。

4. 公式化游戏：假设 RO 和 SO 在做出自己的选择时不知道其他玩家的选择，那么就以图 1.1 所示的标准形式制定场景。
5. 找出最优策略/均衡：对每一个参与者的最优策略进行识别。使用博弈论的要点是提出策略或激励其他玩家，从而达到最佳均衡。玩家选择的最佳或最佳策略的组合是纯策略纳什均衡。均衡是运动员比赛的结果。然而，纯策略纳什均衡可能不存在，另一种计算平衡解的方法是混合策略纳什均衡，它总是存在的。利用它，我们可以得到的概率，预期的结果，玩家得到的每一个策略，以及预期的游戏结果 [29]。

这些步骤可以迭代，直到结果令人满意（即使这超出了本章的范围，我们也包括它以提供如何评估风险评估的博弈理论步骤的结果的想法）。一个令人满意的结果可能是 RO 的游戏价值（或者在平衡中的 RO 回报）是在标准设定的限度之内，或者“不做任何事”可能是 RO 的最佳策略。

如果结果不可接受，则可添加替代控制，并重复该过程。然而，请注意，整个过程假设两个参与者都具有与另一个参与者所设想的策略相关的共同知识。例如，计算涉及另一玩家不知道的策略的平衡打破了分析的有效性。因此，建议进行灵敏度分析，以确定在何种程度上球员知识的小变化可能影响均衡计算的结果。

1.3.2 阐述博弈理论步骤的一个例子

我们以一个双玩家游戏为例详细阐述了上面的游戏理论步骤。

1. 调查场景：我们的示例基于一个场景，在该场景中，组织正在对其中一个系统（资产）进行风险评估，该系统（资产）在过去几年中遭到攻击。管理员（资产所有者）负责系统的保护。
2. 识别玩家：在我们的例子中，玩家是管理员（RO）和攻击者（SO）。我们假设球员是理性的。
3. 前述玩家（这里是管理者和攻击者），下面的数据收集如下：

a) 确定获得的信息：我们假设管理员和攻击者之间的给定场景是一个完全但不完全的信息游戏。

b) 确定策略：管理员可以限制其操作以使用现有控件（即，“什么都不做”）或执行新的控制措施来减轻风险。实现的控件被分类为“无所事事”（这里，NotDefend）选项。攻击者的策略基于他可以在系统中利用的漏洞和他可能对组织造成的威胁。因此，管理员的策略空间是{防御，NoTe}}，而攻击者是{攻击，NoTask}。

c) 身份参照/效用因素：对于这种情况，我们认为管理员关心组织的经济损失和声誉，而攻击者关心他的经济收益。

4. 按收益/效用表示：对于这个场景，我们假设 w1 和 w2 分别是管理员为组织的财务损失和声誉分配的权重，其中（w1>w2）。由于攻击者只关心他的收益，他的分配重量是 W1 = 1。市盈/亏损的比例是货币单位，信誉度是面试所得到的%，因为假设系统以前受到过攻击。因此，使用给定的尺度和测量方法（如果有的话），可以获得对管理员和攻击者的效用因子值。关于一些有用的测量方法和尺度，如声誉等因素，详见〔24〕。我们将等式 1.1 应用到每个策略所产生的属性向量，对于所有的玩家。如图 1.1 所示。让管理员和攻击者的策略数量为 R 和 S。管理员和攻击者的效用函数分别在 Fuffu1（Xi，j）和 Uu2（Yi，j）中表示，其中 i = 1…r，j = 1…s，Xi，j，Yi，j 是效用因子向量。

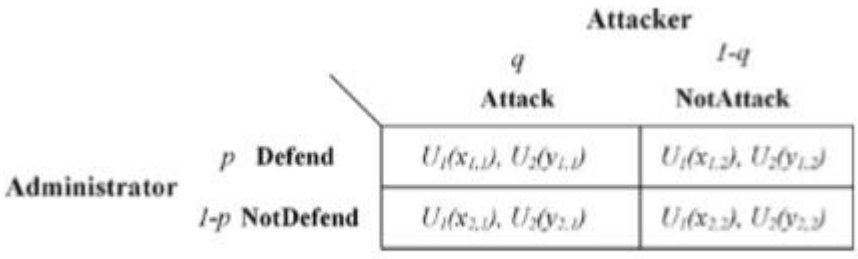

Fig. 1.1: Normal form representation of the scenario

5. 公式化游戏：我们假设 RO 和 SO 在执行自己的决定之前都不能观察其他玩家的决定；因此将设置设置为正常形式的游戏是合适的，如图 1.1 所示。由于这是不完美信息的游戏，玩家对其他玩家选择的策略形成信念。管理员认为攻击者分别以概率 q 和 1_q 在(0≤q≤1)处进行攻击和未攻击策略。同样地，攻击者认为管理员分别以概率 p 和 1_p 来

玩.d 和 Not.d 策略，其中(0≤p≤1)。管理员的策略被放置在列中的行和攻击者中。矩阵中每个单元格中的变量对分别表示管理员和攻击者的效用函数，如以上步骤中所获得的。

6. 找到优化的策略/均衡：假设一个纯策略的纳什均衡，策略 prole（防御，攻击）是游戏的结果。这表明存在系统被攻击的风险，但是通过采用防御策略，管理员可以减轻风险。

1.3.3 风险评估与博弈论方法的映射

一般来说，博弈论和经典的风险评估方法都包括三个阶段：数据收集、风险评估/博弈论模型和决策。我们对游戏理论步骤和一般风险评估步骤进行映射（如 1.2.1 节所述）。除了风险评估过程中威胁的识别外，我们还包括机会的标识。

如表 1.2 所示的映射表明，所有的风险评估步骤都涵盖在博弈论方法中。然而，传统的风险评估没有明确考虑战略所有者获取的信息等博弈论步骤及其信念和激励。根据所使用的游戏模型，可以考虑 SO 可能拥有关于 RO 的什么信息，这些信息包括他以前的行为、策略和收益，反之亦然。在安全风险评估中应该考虑参与者的这种战略思想，因为这将有助于获得正在分析的场景的完整画面。一般来说，这相当于在进行评估时没有明确考虑对手的行为和动机[22]。尽管有些方法在确定威胁的过程开始时考虑对手的动机，但这些人为因素没有明确考虑。D 在评估阶段。此外，经典的风险评估方法不包括玩家的策略优化。

此外，映射表明，使用博弈论过程计算概率。因此，它解决了传统风险管理方法的主要局限性之一。映射清楚地描述了博弈论可以用于安全风险评估。

1.4 合作博弈解决机会风险

球员的激励可能会根据他们所面对的情况而不同。同样地，在经济学中，参与者的激励在维护组织安全方面很重要。通常，玩家有获胜的动机或效用最大化。然而，除了个人激励之外，球员们也可以协商并提出团体奖励。合作博弈理论有助于将谈判结果模型化为联合行动〔29〕。它主要用于研究合同关系，例如，雇主与组织中的员工之间的工作合同可能有助于避免欺诈并协调激励。在非合作博弈中，玩家的行为被视为个体行为，而在合作博弈中，玩家可以而且将合作或交流以形成由裁判[19]或合同强制执行的联盟。

攻击者和防御者之间的游戏主要是在安全性研究[17, 26, 10]。然而，在解决安全博弈时，很少考虑合作博弈模型。如上所述，经典风险评估方法的局限之一是缺乏对机会风险的考虑。合作博弈理论模型可以用来捕捉组织所面临的机会风险。

表 1.2：风险评估与博弈论方法之间的映射（改编自[25]）

一般风险评估程序和术语		博弈论过程与术语
初步准备	组织范围、风险偏好、组织目标	对替代策略或回报的重复分析的情景、范围、判断标准的研究
	识别资产和资产所有者	确定谁拥有该资产，谁将获得 BNE/T/BED 损失（RO）识别球员 RO 等（即，与反竞争对手相反的激励）。
识别风险情景	识别威胁和机会	确定战略目标；确定 RO 战略（已经实施和实施的控制措施）
	识别漏洞	识别可被威胁利用的选项。包括在确定策略的同时
	识别后果	识别玩家对结果的多个正交方面，确定每个玩家的偏好或效用因素。
估计风险	评估后果	比较收益和效用表示的结果和排名偏好的德涅规模、度量方法和权重
	评估可能性	球员的每个策略的计算概率
	确定风险	计算的预期结果是对 RO 的风险的各种策略，反之亦然。
风险评估	区分身份风险情景的优先次序	优先考虑球员的预期结果
未显式包含		确定运动员获得的信息
没有明确包含的球员		确定球员的信念和激励
未包括		寻找优化策略

例如，由于 CISO 希望提高安全意识，所以组织存在机会风险，但是由于工作人员需要花时间浏览在线材料和通过测试，因此他们没有动力进行安全培训。这导致了相互依赖的情况，因为员工的行为可能会对组织产生负面影响。CISO 和工作人员之间的这种设置可以被建模为合作博弈，以确定组织需要采取什么策略来解决此安全问题。

组织可以通过根据获得的测验分数奖励一些完成培训的分数，而不是采取可能产生反作

用的其他方式，来帮助调整员工参加培训的动机。这种组织战略可能导致双赢局面。因此，通过使用使参与者双方受益并使其效用最大化的合作模型，可以获得获得组织获得机会的战略不确定性（提高工作人员的安全意识）。

1.5 讨论和结论

安全风险评估是一种识别和处理组织可能面临或面临的安全威胁的方法。分配预算以减轻或处理风险的决定往往是基于风险的严重性。因此，正确识别和评估风险情景是非常重要的。然而，传统的安全风险评估方法由于缺乏统计资料和适应性，可能导致对安全风险的评估建立在主观判断的基础上。此外，这些方法大多没有考虑机会风险。

组织安全风险的增加为指导其安全风险评估和投资的新方法开辟了一条道路。由于现有风险评估方法的局限性，基于数学模型的博弈理论模型的应用是有益的。

结果表明，不同的风险评价方法可以推广到一些常见的步骤。尽管在本章中映射了三种风险评估方法，但是映射可以扩展到包括其他方法，例如 ISO 31000:2009[1]和风险 IT 框架[14]。此外，在经济风险评估过程/术语和博弈论步骤之间的划分突出了某些博弈论步骤与其评估步骤缺乏对应性。映射清楚地描绘了博弈论可用于分析各种情景。然而，博弈论步骤的用途。理论没有挑战就不会到来。

许多组织都有自己的风险评估方法，因此采用完全不同的方法来适应另一种方法是一个挑战。此外，工作人员需要掌握使用该方法的技巧。在博弈论中，一个球员的策略是基于他认为另一个球员可能做的，反之亦然。因此，建模现实世界中的一个工具。即使一些工具，如 Gambit[18]或 GAMUT[30,20]可用，这些工具需要与风险评估结合起来以制定和分析风险情景。然而，博弈论的优点胜过上述缺点，而将博弈论应用于风险评估可以为安全风险提供独到的见解。

需要更多的研究来为组织利用博弈论进行风险评估。此外，需要研究解决机会风险的合作模式，这将使组织关注威胁和机会。

1.6 章节笔记与进一步阅读

博弈论在经济学、生物学、政治学、信息安全等多个学科中有着广泛的应用。已经进行了研究合并或使用博弈论与传统的风险评估〔11, 4, 13，10〕。博弈论一般也被用于信息安全，以捕获攻击者的动机[15]或量化安全风险[6]。此外，它已被广泛用于网络安全〔21, 31, 26，16,

17〕。

Hausken 认为，考虑到影响风险的个体-集体因素，博弈论可以与概率风险分析相结合[11]。班克斯等。强调传统的风险分析方法在大多数情况下是不可靠的，并建议使用与博弈论相结合的统计风险分析方法[4]。他们通过将天花攻击建模为具有随机收益的零和博弈来分析攻击策略，并利用极大极小法和贝叶斯法来解决它。因苏亚等人的研究。涉及博弈论的概念和统计风险分析来解决对抗风险分析（ARA）〔13〕。他们还提出了 ARA 的贝叶斯方法。在_10_中，Cox 指出，与使用经典的风险评分模型相比，使用博弈论模型，ARA 在分配有限资源方面可以得到改进。

刘等人利用基于激励的方法对攻击者的意图、目标和策略（AIOS）进行建模，并发展了一种干扰 AIOS 的博弈论方法[15]。QuERIES 方法是为了量化网络安全风险而开发的，以便组织能够提出适当的投资策略[6]。

应用博弈论模型对移动 Ad Hoc 网络中的入侵检测进行了补丁分析。利用不完全信息的多级动态非合作博弈〔21〕。Xiaolin 等人。提出了一种基于马尔可夫博弈论的网络信息系统风险评估模型〔31〕，同时对 Maelet 等人提出了一种风险评估模型。解释各种非合作博弈理论方面的安全游戏，以覆盖网络安全问题[16]。[2]中的两项调查显示了博弈论在网络安全中的广泛应用。在〔17〕中，曼沙伊等人。介绍攻击者和防御者之间的网络安全游戏。罗伊等人。〔26〕调查了在非合作博弈下应用于网络安全的现有博弈论解决方案。

游戏理论应用中存在的一些工具是 GAMBIT 和色域。Gambit 是一个包含一组博弈论工具的软件，通过这些工具，游戏可以以正常形式和扩展形式构造和分析[18]。在其他特征中，有计算纳什平衡和量子响应平衡的工具。色域包括用于生成游戏和测试博弈论算法的工具[30, 20]。

我们感谢匿名审稿人的宝贵意见和建议。免责声明这是第一作者的独立研究，因此本书章节中表达的观点与她所属的任何组织无关。

参考文献：

1. ISO 31000 Risk management – Principles and guidelines. 2009.

2. ISO/IEC 27005 Information technology -Security techniques - Information security risk management. ISO/IEC, 1st edition, 2011.

3. NIST Special Publication 800-30 Revision 1. Guide for conducting risk assessments.

Technical report, 2012.

4. David L. Banks and Steven Anderson. Combining Game Theory and Risk AnalysisinCounterterrorism:ASmallpoxExample.SpringerNewYork,2006.

5. F. Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen. Model-based security analysis in seven steps — a guided tour to the coras method. BT Technology Journal, 25(1):101–117, January 2007.

6. L. Carin, G. Cybenko, and J. Hughes. Cybersecurity strategies: The queries methodology. Computer, 41(8):20–26, Aug 2008.

7. Robert T. Clemen. Making Hard Decision: An Introduction to Decision Analysis. Duxbury, second edition, 1996.

8. Jr. Louis Anthony Cox. Some limitations of "Risk = Threat x Vulnerability x Consequence" for risk analysis of terrorist attacks. Risk Analysis, 28(6):1749– 61, 2008.

9. Jr. Louis Anthony (Tony) Cox. What's wrong with risk matrices? Risk Analysis, 28(2):497–512, 2008.

10. Jr. Louis Anthony (Tony) Cox. Game theory and risk analysis. Risk Analysis, 29(8):1062–1068, 2009.

11. Kjell Hausken. Probabilistic risk analysis and game theory. Society for Risk Analysis, 22, 2002.

12. David Hillson. Extending the risk process to manage opportunities. International Journal of Project Management, page 235–240, 2002.

13. David Rios Insua, Jesus Rios, and David Banks. Adversarial risk analysis. Journal of the American Statistical Association, 104(486):841–854, Jun 2009.

14. ISACA. The Risk IT Framework, 2009.

15. PengLiuandWanyuZang.Incentive-basedmodelingandinferenceofattacker intent, objectives, and strategies. In Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS '03, pages 179–189, New York, NY, USA, 2003. ACM.

16.PatrickMaill´e,PeterReichl,andBrunoTufn.OfThreatsandCosts:AGameTheoreticApproachto SecurityRiskManagement,pages33–53.SpringerNew York, New York, NY, 2011.

17. Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacs¸ar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. ACM Computing Surveys

(CSUR), 45(3):25, 2013.

18. Richard D. McKelvey, Andrew M. McLennan, and Theodore L. Turocy. Gambit:Softwaretoolsforgametheory,version16.0.1.http://www.gambit-project. org, 2016. [retrieved: 15-9-2017].

19. John Nash. Non-cooperative games. Annals of mathematics, pages 286–295, 1951.

20. Eugene Nudelman, Jennifer Wortman, Yoav Shoham, and Kevin LeytonBrown. Run the gamut: A comprehensive approach to evaluating gametheoretic algorithms. Autonomous Agents and Multiagent Systems, International Joint Conference on, 2:880–887, 2004.

21. Animesh Patcha and Jung-Min Park. A game theoretic formulation for intrusion detection in mobile ad hoc networks. International Journal of Network Security, 2:131–137, March 2006.

22. LisaRajbhandari.Riskanalysisusing“conflictingincentives”asanalternative notion of risk, 2013.

23. Lisa Rajbhandari and Einar Snekkenes. Risk acceptance and rejection for threat and opportunity risks in conflicting incentives risk analysis. In International Conference on Trust, Privacy and Security in Digital Business, pages 124–136. Springer, 2013.

24. Lisa Rajbhandari and Einar Snekkenes. Using the conflicting incentives risk analysis method. In IFIP International Information Security Conference, pages 315–329. Springer, 2013.

25. Lisa Rajbhandari and Einar Arthur Snekkenes. Mapping between Classical Risk Management and Game Theoretical Approaches, pages 147–154. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

26. Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya,andWuQishi.Asurveyofgametheoryasappliedtonetworksecurity. In System Sciences (HICSS), 2010 43rd Hawaii International Conference on, pages 1–10. IEEE, 2010.

27. Einar Snekkenes. Position paper: Privacy risk analysis is about understanding conflicting incentives. In IFIP Working Conference on Policies and Research in Identity Management, pages 100–103. Springer, 2013.

28. Gaute Wangen, Christoffer Hallstensen, and Einar Snekkenes. A framework for estimating information security risk assessment method completeness. International Journal

of Information Security, pages 1–19, 6 2017.

29. Joel Watson. Strategy : An Introduction to Game Theory. W. W. Norton & Company, 2nd edition, 2008.

30. Jenn Wortman, Eugene Nudelman, Mark Chen, and Yoav Shoham. Gamut: Game-theoretic algorithms evaluation suite. http://gamut.stanford.edu/. [retrieved: 15-9-2017].

31. Cui Xiaolin, Tan Xiaobin, Zhang Yong, and Xi Hongsheng. A Markov game theory-based risk assessment model for network information system. In CSSE '08: Proceedings of the 2008 International Conference on Computer Science and Software Engineering, pages 1057–1061, Washington, DC, USA, 2008. IEEE Computer Society