作为一座拥有 2500 万人口的超大型城市，安全是城市运行的绝对底板。大会特设的应急救援等高难度赛道，直面火场、废墟等极端场景，其根本目的就在于检验并催生能代替人类进入高危环境的“新力量”，致力于打造以具身智能为支撑的“全栈式”安全护城河。

与此同时，一群白帽黑客们也正在为快速迭代发展的具身智能机器人敲响了安全警钟。肖轩淦是全球非营利性的安全极客技术活动平台 GeekCon（中文名：新极棒）的高级研究员，他在接受《新民周刊》采访时指出，现在许多具身智能机器人或者说智能穿戴设备都存在着一定的安全隐患。“现在机器人是用遥控器控制的，一旦有黑客控制了遥控器，就有可能让机器人转而攻击人类。面对失控的‘钢铁侠’，人类是不可能直接冲上去拔掉电源的，所以厂商们必须设置紧急制动键，在关键时刻让机器人直接瘫痪倒地，‘就地伏法’。”

作为国内顶尖的网络与信息安全企业，安恒信息的核心工作就是利用技术手段，帮助政府和企业的数据和系统安全。安恒信息数据安全运营总监程文博告诉《新民周刊》：“我们既用 AI 来增强防御能力（让安全更智能），也研究如何防御针对 AI 大模型的攻击（让智能更安全）。说得通俗一点，就是用 AI 去对抗 AI。”在程文博看来，当 AI 从虚拟世界跨越到物理世界的时候，就触及到了这个领域的核心痛点：当机器人拥有了“身体”和“大脑”，如何防止它“生病”“失控”或被“教坏”？

目前，行业内外主要通过硬件防护、软件算法、数据通信以及法律法规这四道防线来构建机器人的安全底座。“虽然上述技术听起来很完善，但正如你在大赛中看到的，目前的具身智能安全仍处于“补短板”的阶段。”

> 上海不仅以开放的胸怀呼唤先锋，**更以系统的政策支撑、丰富的场景开放和完整的产业链条，**为他们实现软硬结合的梦想提供了一片不可多得的沃土。

政策大礼包呼唤先锋

除了推出全球首创的具身智能机器人技能大赛，本届大会以“开发者，找找找”为主题，云集全球顶尖开发者、科研团队与行业领袖，核心目标是推动人工智能从虚拟算法迈向实体落地应用，深度探索人机协同发展的未来路径。

在大会开幕式上，浦东新区支持人工智能创新创业发展若干措施的发布，以精准的政策工具包，为全球先锋开发者与创新企业提供了扎根上海的第一重保障，展现了制度创新的“上海速度”。其中明确提出，全面启动张江人工智能创新小镇建设。针对新注册 OPC 企业（一人创业公司），提供最高 30 万元的免费算力。政策还配套推出“十个一”创梦政策包，包括免费工位、人才公寓、创业资金、算力券、场景对接等全方位支持，通过打造“低创新成本、高智力密度”的创业土壤，助力浦东三年内新增千家企业、人工智能产业规模突破 2500 亿元，进一步夯实上海在全球 AI 赛道上的竞争力与吸引力。

同时发布的上海市具身智能应用十大场景，清晰规划了技术从实验室走向工业制造、社会服务等真实世界的“施工图”，为软硬结合提供了明确的价值锚点与广阔的需求土壤。

与此同时，上海市人形机器人中试联盟正式成立。这一联盟的成立，是打通从技术原型到成熟产品“最后一公里”的关键机制创新，标志着上海在构建协同创新生态、加速产业闭环形成上迈出了实质性步伐。上海不仅以开放的胸怀呼唤先锋，更以系统的政策支撑、丰富的场景开放和完整的产业链条，为他们实现软硬结合的梦想提供了一片不可多得的沃土。

下图：比赛中的具身智能机器人展现出强大的工作技能。