武装冲突期间保护平民免受数字威胁

向各国、交战方、科技公司及人道组织提供的建议

红十字国际委员会武装冲突期间数字威胁全球顾问委员会的最终报告

报告

ICRC

武装冲突期间保护平民免受数字威胁

向各国、交战方、科技公司及人道组织提供的建议

红十字国际委员会武装冲突期间数字威胁全球顾问委员会的最终报告

内容

摘要

2021至2023年，红十字国际委员会召集了汇集法律、军事、政策、技术和安全领域高级别领袖和专家的全球顾问委员会，就数字威胁问题为该组织提供意见，并就保护平民免受此类威胁制定具体建议。本报告为交战方、各国、科技公司和人道组织预防或减轻平民居民面临的数字威胁提供了一系列具体的建议。

全球顾问委员会的建议背后的四项指导原则

I. **数字空间并非法外之地，武装冲突期间亦如此**。各国、交战各方以及所有开展和武装冲突相关的数字行动的人员，均须尊重国际法律限制，特别是国际人道法。在我们日益数字化的社会中，对这些存在已久的规则进行的解释和适用，需要确保对平民、民用基础设施、数据和其他受保护物体提供充分的保护。旨在澄清如何在数字环境中解释国际人道法的共识或指南，可有助于减少法律解释中的模糊地带并预防损害的发生。

II. **保护平民免受数字威胁要求我们在法律、政策和程序方面进行投入**。国家和社会应采取此类行动来增强抵御数字威胁的复原力，这些威胁来自包括构建和影响数字环境的国家及企业，以及开展数字行动的主体。我们不能允许武装冲突的数字化危及对平民的保护。虽然从事实上来说，通过和实施此类立法、政策和程序可能在政治、商业或技术上充满复杂性，但这不能成为不予以实施的借口。

III. **政治和军事领袖应当重点关注对平民的保护**。他们应该意识到参加与武装冲突相关的数字行动的平民越多，就越难以区分平民和战斗员。在实践中，这意味着平民和民用基础设施在武装冲突中被攻击的风险日益增加。

IV. **各国、科技公司、人道组织、民间社会和其他利益相关方应携手努力，使用数字技术来加强对平民的保护**。我们应共同发挥数字技术的潜力，保护平民免受伤害，赋能平民应对冲突中的自身需求，并助力更加有效和高效的人道服务。

全球顾问委员会对交战方的建议

建议1：交战方如果开展网络和其他数字行动，则必须遵守国际法律的限制，并评估、预防或减轻其行动在武装冲突期间可能对平民、民用基础设施以及其他受保护人员和物体造成的伤害。

建议2：交战方如果开展网络行动，则必须制定程序并采取技术措施，以防止或减轻其行动对平民居民和社会产生的影响。

建议3：交战方如果开展信息行动，则必须遵守其国际法律义务，并应评估、预防或减轻其行动在武装冲突期间可能对平民和其他受保护人员造成的伤害。

建议4：交战方应避免关闭平民居民访问互联网的渠道，因为这可能会对平民造成重大影响，并会加剧而非遏制虚假信息问题。如果出于迫切的军事必要需要中断或限制互联网访问渠道，则应采取缓解措施，确保平民不会受到过度影响，且平民的生活尽可能受到维护。

建议5：交战方不应鼓励平民通过数字行动直接参加敌对行动。交战方必须考虑到，如果它们鼓励平民参加与武装冲突有关的数字行动，平民就面临失去法律保护以及成为攻击目标的风险。

建议6：所有交战方均须尊重并保护为武装冲突受难者提供基本服务的人员的活动，特别是医务人员和医疗设施以及人道组织。各国应在线上和线下重申这一长期共识。

全球顾问委员会对各国的建议

建议7：国家和社会应通过加强民用基础设施、服务和数据的网络安全，以及制定应急预案，来构建抵御数字破坏的复原力。

建议8：国家和社会应构建抵御有害信息的复原力，维护表达自由的权利，并保护记者。

建议9：各国必须提高对在武装冲突期间适用的保护平民的法律规则的认识，特别是私人行为体对此的认识，并确保这些规则得到尊重。

建议10：如果要制定新的法律规则和规范，需要基于并加强——而非削弱——现有的国际法律规则对平民及其他受保护人员和物体的保护。

建议11：各国应在最大可行范围内，将军用和民用数据及通讯基础设施分割开来。

建议12：为防止对平民造成伤害，各国需要对日益增长的以开发和销售旨在伤害平民的能力和服务的科技公司市场进行规制。

建议13：如果国家或国际组织通过制裁或其他限制性措施对受武装冲突或其他人道危机影响的国家的信通技术的出口或进口进行限制，则有必要对信通技术设备和服务给予特定的人道豁免，以确保医疗服务的正常工作、运转、维护和安全，并且确保能够及时开展为满足平民居民的基本需求所需的人道活动或其他服务。

建议14：各国和其他行为体应支持和促进为人道组织制定适当的网络安全和数据保护措施和政策，并提供支持以加强这些组织应对有害信息的能力（另见下文建议19）。

全球顾问委员会对科技公司的建议

建议15：数字平台在助长传播有害信息方面能够产生很大影响，运营这些平台的科技公司可以采取更多措施来解决这一问题。它们应采取更多措施来检测信号，分析其平台上可能存在的有害信息的来源、传播方式和类型，尤其是与武装冲突局势有关的有害信息。它们的政策、程序和实践，包括内容审核，均应与国际人道法和人权标准保持一致。

建议16：在武装冲突局势中开展业务的科技公司应了解并持续关注其提供的服务是否可能使其员工构成直接参加敌对行动，以及使公司成为军事目标；除直接参加敌对行动外，其卷入武装冲突局势是否可能使其员工面临风险，如有必要，应相应调整其活动。

建议17：科技公司应在最大可行范围内，将其为军事目的和民用目的提供的数据和通信基础设施分割开来。

建议18：科技公司应确保其出于商业或其他原因自愿采取的措施——即其法律义务（如制裁和其他限制性措施）之外的措施——不会妨碍医疗服务、人道活动或其他对满足平民居民的基本需求至关重要的服务的运作、维护和安全。

全球顾问委员会对人道组织的建议

建议19：人道组织应采取强有力措施保护其收集和处理的数据，并应加强其IT系统及人道行动抵御数字威胁的复原力。

建议20：人道组织应做好准备，它们有可能成为有害信息的目标，这些有害信息可能对其人道行动和声誉产生影响；人道组织还应做好对此在线上和线下做出适当回应的准备。

建议21：人道组织应在其行动中就针对平民的有害信息制定应对措施。

建议22：具有相关专业知识和能力的人道组织应加强努力，提高各界（包括开展数字行动的私人行为体）对武装冲突期间关于保护平民所适用的法律规则的认识。

全球顾问委员会关于共同努力的建议

建议23：需要多方利益相关方开展对话，汇集各国、科技公司、人道组织、国际组织、学术界、民间社会和其他利益相关方的专业知识，发展专门针对冲突的理解、原则和/或指南，以保护平民免受数字威胁。

建议24：科技公司和人道组织应合作应对武装冲突期间的数字威胁。

建议25：人道组织应借鉴其他领域的经验，与公共和私营机构合作，开发创新解决方案，保护平民居民和人道行动免受数字威胁。

引言

在武装冲突局势中，使用数字技术可以拯救生命。例如，数字技术能够使民众获取关于寻求安全的信息，找到失联的家庭成员并与之重建联系；让医疗机构能够正常运作；也被人道组织和各国政府用于尽可能有效地援助民众。

武装冲突的数字化也给平民带来新的威胁。虽然在乌克兰的武装冲突让世界重点关注到这一问题，但我们在其他冲突和人道危机中也早已观察到数字威胁。我们今日所见可能预示着未来的走向：数字威胁将成为平民日益关切的问题。过去数十年间，国家和非国家行为体已经将数字技术用于在军事上战胜敌方，以支持和配合动能行动。此外，数字技术也被用于破坏关键民用基础设施和服务，煽动针对平民居民的暴力，破坏人道救济工作。恶意使用数字技术和传播有害信息的行为，正日益破坏社会稳定，导致平民处于更加脆弱的境地。当数字环境和物理环境日益相互依存，平民和民用基础设施不仅可能成为敌对行动的目标，还越来越多地被用于支持军事行动。随着数字技术逐渐渗透到我们的生活和社会中，网络和信息行动不再是抽象概念或“只在网上出现”，而是会对民众造成实际伤害。

在武装冲突期间，交战各方使用数字手段伤害敌方的权利并非毫无限制。国际人道法对敌对行动规定了基本限制，以保护平民、基础设施和不再参加敌对行动的士兵。红十字国际委员会武装冲突期间数字威胁全球顾问委员会所开展的工作基于这一国际共识，即国际人道法的既定原则和规则适用于所有作战形式和所有武器类型，不论新式、旧式，数字形式还是实体形式，均适用。

应对数字威胁变得日益复杂。新问题和新困境不断涌现。社会如何保护自身避免网络行动扰乱基本民用服务和基础设施的正常运作？如何保护个人和人道数据免遭损坏、破坏、盗用和未经同意的公开？对于信息行动存在何种限制，或者应施加何种限制？科技公司在保护平民居民方面发挥着以及应发挥何种作用？如果平民和科技公司越来越多地通过数字手段卷入武装冲突，如果民用数字基础设施被用于军事行动，会产生哪些风险？我们如何在数字时代维护长期以来达成的共识，即必须保护致力于救助武装冲突受难者的人员免受伤害？

为了防止或减轻对平民的伤害，必须即刻采取行动。红十字国际委员会为践行保护武装冲突受难者的生命和尊严的人道使命，召集了汇聚法律、军事、政策、技术和安全领域高级别领袖和专家的全球顾问委员会。2021年至2023年，全球顾问委员会就数字威胁问题以及在这方面如何定位为红十字国际委员会提供意见，并就保护平民免受数字威胁提出具体建议。全球顾问委员会希望凭借其在武装冲突方面的专业知识和关注，为关于在新技术中保持以人为本的方法以及在新背景下推进国际法的重要讨论做出贡献。

本报告向交战方、各国、科技公司和人道组织提出了四项指导原则和一系列具体建议，旨在防止或减轻平民居民面临的数字威胁。本报告反映了全球顾问委员会成员之间的共识，但并不一定反映成员所属组织、机构或公司的观点。

平民面临威胁：互联互通、不断演变的数字环境在武装冲突期间引发的四个令人担忧的趋势

从人工智能日益用于网络和数字行动以提升行动速度、扩大影响范围，到监控活动日渐深入人们的生活，数字创新在武装冲突中用途众多。每爆发一场新冲突，交战各方和平民使用数字技术的方式也会翻新。在迅猛发展的数字环境中，平民居民面临的威胁也与日俱增、界限在不断变化、各种行动也逐渐相互关联。例如，开展网络行动支持信息和动能行动，可用于防止攻击目标使用通讯渠道对抗敌对行动或增强信息和动能行动的影响。同样，信息行动的实施也可以巩固和增强网络行动的破坏影响为目的。人工智能被用于进攻性和防御性网络行动，并创造内容供信息行动使用。

鉴于军事创新的快速发展以及将数字技术用于战胜敌方的现象，我们担心战争数字化会给民众带来更多伤害。

1. 武装冲突期间的网络行动可能会破坏对人的安全和尊严以及社会运作至关重要的基础设施、服务和数据，从而对平民造成伤害。

民众日常生活依赖数字基础设施、服务及数据的程度越高，武装冲突期间的网络行动对平民居民造成伤害的风险就越大。网络行动可能使工业设施、通讯网络以及其他关键基础设施瘫痪或对其造成物理损害，从而直接或间接地造成平民伤亡，包括因阻碍基本服务的正常运行和人道救济物资的供应而造成平民伤亡。旨在操纵信息以实现认知和心理效果的网络行动也可能产生类似后果，包括通过窃取、泄露、操纵或删除数据等方式。由于网络空间具有互联互通的特性，网络行动——若经过相应设计或未经妥善测试或控制——确实存在风险，可能会不加区分地影响广泛使用的计算机系统以及与其相连的民用基础设施，影响范围将远远超出冲突地区，直接或间接造成平民受损害或伤亡，致使冲突进一步升级。

2. 使用网络和数字工具对于平民在武装冲突期间获取挽救生命的信息至关重要，但它们也可能放大有害信息。

信息行动早已成为武装冲突的一部分。在某些情况下，这些行动是法律允许的，例如向平民发出军事攻击的预警或在遵守国际法的前提下欺骗敌方。如今，数字化使此类行动的规模和范围得到扩大，速度得到提升。与虚假信息（通常理解为旨在造成伤害的错误或经篡改的信息）相重叠以及有时由虚假信息组成的信息行动，其影响可波及多个平台，歪曲事实，影响人们的信仰和行为，加剧紧张局势，通过在线上线下助长不信任情绪及传播仇恨言论导致平民受到伤害的风险增加。这尤其会影响处于弱势地位的妇女、儿童和少数群体。此外，有害信息还会对关键信息的可获取性、完整性和可靠性产生负面影响，而平民在冲突时期需要这些信息来确保生存和自身安全。与传统媒体相比，有害信息往往更容易在数字平台上传播，而且没有足够的编辑监督。平民可能会在不知情的情况下扩大有害内容的影响。

3. 在数字环境中，对平民与军事人员、对民用物体与军事目标的区分可能变得模糊——平民和民用基础设施可能成为被攻击的目标。

长久以来一直存在平民行为体（个人和公司）在武装冲突期间履行军事职能、协助战争活动的现象。随着社会的数字化，我们注意到他们开展的行动类型发生了根本变化，参与武装冲突的平民行为体的数量也在增加。有时，平民行为体出于自身动机或基于要求他们提供网络安全的合同而参与冲突；有时，他们的参与行为是受到国家授权、鼓励或协助的。这种发展对平民造成的风险经常被忽视：数字技术让平民越接近敌对行动，平民受到伤害的风险就越大。平民和军方共享的数字基础设施或服务越多，民用基础设施受到攻击的风险也就越大。国际人道法建立在区分平民和战斗员、区分民用物体和军事目标这一基本原则之上，但越来越多的平民通过数字手段参与军事行动，以及将民用数字基础设施用于军事目的，有可能会模糊两者之间的界限，从而破坏这一基本前提。

4. 网络行动、数据泄露和虚假信息削弱了人们对人道组织的信任以及人道组织向民众提供挽救生命的服务的能力。

最近针对人道组织实施的网络行动和虚假信息活动——例如在2022年针对红十字国际委员会的活动——应该给我们敲响警钟：在全球需求巨大、人道应对能力不足的背景下，数字威胁可以削弱人道行动和机构。数字威胁的形式多种多样，从破坏或摧毁人道组织数字基础设施和通讯的网络行动，到入侵其系统以窃取数据的行动，再到旨在损害人道组织声誉并削弱其行动能力的虚假信息行动。此类威胁一旦发生，可以造成重大伤害：人道数据可能会被滥用于针对或迫害接受人道服务的平民，而这些平民往往面临特别的风险。破坏人道救济行动，例如其后勤工作，很可能会加剧受冲突及其他人道危机影响的民众的需求。此外，虚假信息和数据泄露可能会削弱平民和武装冲突各方对人道组织的信任，继而影响这些组织获得救助民众的准入，而且可能危及其工作人员的安全。

呼吁全球行动：全球顾问委员会的建议

保护平民免受数字威胁，以及促进对国际人道法的尊重，必须成为战略优先事项。这需要多方行为体齐心协力、共同努力。根据我们不同的专业背景和经验，我们呼吁各国以及其他交战方重申对与武装冲突有关的数字行动加以限制的现有国际法律规则。各国应与民间社会和企业一道，就与武装冲突有关的数字行动的现有限制和未来可能的限制达成共识。

为了防止或减轻伤害，我们为交战方（国家或私人行为体）、各国、科技公司和人道组织提出了四项指导原则和一系列具体建议，以期防止或减轻武装冲突期间平民面临的数字威胁。

全球顾问委员会所提供建议背后的四项指导原则

I. **数字空间并非法外之地，武装冲突期间亦如此。**各国、交战各方以及所有开展和武装冲突相关的数字行动的人员，均须尊重国际法律限制，特别是国际人道法。在我们日益数字化的社会中，对这些存在已久的规则进行的解释和适用，需要确保对平民、民用基础设施、数据和其他受保护物体提供充分的保护。旨在澄清如何在数字环境中解释国际人道法的共识或指南，可有助于减少法律解释中的模糊地带并预防损害的发生。

II. **保护平民免受数字威胁要求我们在法律、政策和程序方面进行投入。**国家和社会应采取此类行动来增强抵御数字威胁的复原力，这些威胁来自包括构建和影响数字环境的国家及企业，以及开展数字行动的主体。我们不能允许武装冲突的数字化危及对平民的保护。虽然从事实上来说，通过和实施此类立法、政策和程序可能在政治、商业或技术上充满复杂性，但这不能成为不予以实施的借口。

III. **政治和军事领袖应当重点关注对平民的保护。**他们应该意识到参加与武装冲突相关的数字行动的平民越多，就越难以区分平民和战斗员。在实践中，这意味着平民和民用基础设施在武装冲突中被攻击的风险日益增加。

IV. **各国、科技公司、人道组织、民间社会和其他利益相关方应携手努力，使用数字技术来加强对平民的保护。**我们应共同发挥数字技术的潜力，保护平民免受伤害，赋能平民应对冲突中的自身需求，并助力更加有效和高效的人道服务。

对交战方的建议

建议 1

交战方如果开展网络和其他数字行动，则必须遵守国际法律的限制，并评估、预防或减轻其行动在武装冲突期间可能对平民、民用基础设施以及其他受保护人员和物体造成的伤害。

在武装冲突时期，交战方在网络空间的负责任行为必须至少从遵守国际法的角度来界定。国际人道法规定了保护平民免受军事行动所产生的危险的长期规则：这些规则必须有效适用于与武装冲突有关的网络和其他数字行动，并得到执行。交战各方尤其不得针对平民或民用物体实施网络行动。交战各方必须避免不分皂白或不成比例的网络行动，经常注意不损害平民和民用物体，尊重并保护医疗设施、医务人员、其他关键基础设施以及人道组织，包括它们所依赖的数据。

建议 2

交战方如果开展网络行动，则必须制定程序并采取技术措施，以防止或减轻其行动对平民居民和社会产生的影响。

为确保网络操作人员防止或减少其行动对平民、民用基础设施、医疗设施以及其他受保护人员和物体的影响，武装冲突各方必须制定明确的内部规则，并采用反映其国际法律义务的严格的目标选择程序。交战各方至少应在以下方面采用程序：核实将予攻击的目标在国际人道法上构成军事目标，并评估平民伤害的风险；为行动选择适当且可靠的手段或方法；在使用前对该手段或方法进行测试；采用适当精准的地理、时间和系统“防护工具”、“终止开关”和其他适当的技术和程序，以尽量减少附带平民伤害的风险；持续监控、控制和指挥行动，以防止意外后果；停止任何预期不符合这些原则的行动。交战各方还应采取一切可行措施，防止或限制其所使用的工具转作他用。

建议 3

交战方如果开展信息行动，则必须遵守其国际法律义务，并应评估、预防或减轻其行动在武装冲突期间可能对平民和其他受保护人员造成的伤害。

在武装冲突期间，国际法的多个领域对信息行动施加限制，特别是国际人道法和人权法。交战方不得开展旨在利用平民居民或伤害受国际人道法保护的人员、实体、活动和行动的信息行动。例如，这意味着交战方不得鼓励违反国际人道法的行为或任何鼓吹仇恨，致使煽动对平民的歧视、敌意和暴力的行为。交战方应评估、预防或减轻信息行动可能直接或间接、有意或无意对平民居民造成的伤害。与此同时，交战方还必须尊重和保护表达自由和媒体自由，确保记者的安全，以促进在冲突时期能够获取对平民安全和尊严至关重要的可靠信息。

建议 4

交战方应避免关闭平民居民访问互联网的渠道，因为这可能会对平民造成重大影响，并会加剧而非遏制虚假信息问题。如果出于迫切的军事必要需要中断或限制互联网访问渠道，则应采取缓解措施，确保平民不会受到过度影响，且平民的生活尽可能受到维护。

在武装冲突期间，数字信息和通信对平民至关重要，有时甚至能挽救生命。民众，尤其是那些处于弱势的人们，依靠数字通信与家人保持联系，或获取关于寻求安全或获得重要服务的信息。因此，关闭互联网可能会对平民居民产生重大影响，应予以避免，尤其是在可以采取影响较小的措施来实现军事目的的情况下。如果出于迫切的军事必要需要中断并限制互联网访问渠道，则应采取缓解措施，以确保基本服务的提供，并尽可能维护平民的生命和尊严。

建议 5

交战方不应鼓励平民通过数字行动直接参加敌对行动。交战方必须考虑到，如果它们鼓励平民参加与武装冲突有关的数字行动，平民就面临失去法律保护以及成为攻击目标的风险。

参加与武装冲突相关的数字行动的平民人数越多，就越难以在平民和战斗员之间加以区分。这使平民面临被攻击的风险，而且当他们实际位于敌对行动附近时，这种风险尤其高。因此，交战方应扭转鼓励平民参加与武装冲突相关的数字行动的趋势，并且避免向他们提供参加此种行动的手段。如果平民开展与武装冲突有关的数字行动，交战方必须采取措施，确保这些平民了解并遵守国际人道法，并知晓直接参加敌对行动的后果。交战方应发出明确的警告，包括在数字工具中发出警告，告知平民可能会失去免受攻击的保护，并就平民可采取的实际保护措施提供建议。根据国际人道法，如果平民出于直接参加敌对行动以外的任何原因（例如以个人身份、作为记者或为记录罪行）而使用数字手段，则不会失去免受攻击的保护。

建议 6

所有交战方均须尊重并保护为武装冲突受难者提供基本服务的人员的活动，特别是医务人员和医疗设施以及人道组织。各国应在线上和线下重申这一长期共识。

国家和其他交战各方应通过单边、双边和多边方式明确重申其承诺，即在线上和线下同等尊重和保护医疗服务和公正的人道活动、数据和人员，并为其在数字环境中的行动提供便利。重要的是，上述保护应体现在各国的国内法和政策中，并得到有效实施。

对各国的建议

建议 7

国家和社会应通过加强民用基础设施、服务和数据的网络安全，以及制定应急预案，来构建抵御数字破坏的复原力。

各国必须采取一切可行的预防措施，在不减损其人权义务的情况下，保护平民居民免受数字行动带来的危险。从世界范围来看，尽管多年来一直鼓励采取网络安全措施，但目前即使对基本网络安全措施的实施，仍然关注不足。各国政府、企业和非政府组织应携手勤勉努力，至少将保护设备、网络和数据免受大部分网络威胁的基本网络安全措施付诸实施（有时称为“网络卫生”），包括提高其员工和普通民众的网络安全意识和数字素养。为保护平民居民免受网络行动的影响，科技公司开发的产品应具有“设计安全性”。科技公司对冲突地区的民众负有特殊责任，在开发软件、发展基础设施和服务时应对此予以注意。

但即便做出了上述努力，各国也应预料到某些网络行动——尤其是最复杂的网络行动——仍将产生不利影响。因此，各国应构建对民众至关重要的基础数字服务的运营工作的复原力。例如， 各国应采取措施确保冗余度，备份数据（最好能存储于不同的地理和数字位置，如云空间），并针对失去互联网连接或数据被删除等情况制定应急预案，以维持基本服务和数据。

建议 8

国家和社会应构建抵御有害信息的复原力，维护表达自由的权利，并保护记者。

为构建社会抵御有害信息的复原力，包括在武装冲突期间，需要采取全社会的方法，以确保有可靠的信息来源且该来源为人所知，确保记者和媒体受到保护，并确保平民居民了解他们在紧

急情况下可以依赖哪些信息来源。构建这种复原力是一项长期工作，需要在冲突爆发之前就开始进行。为此，还要求各国（单独或集体）制定适当的法律和政策框架，以确保科技公司的服务不被滥用于违反国际法或以其他方式伤害平民。

各国必须维护表达自由的权利。在武装冲突期间，对这一权利的克减和限制必须进行狭义解释，并严格遵守合法、必要和比例原则，以保护国际人权法中规定的合法目标。由于人们往往无法就何为真假达成共识，仅仅是被指称为虚假信息或操纵信息在国际法上并不足以够成限制表达自由的充分理由。

建议 9

各国必须提高对在武装冲突期间适用的保护平民的法律规则的认识，特别是私人行为体对此的认识，并确保这些规则得到尊重。

在最近的一些冲突中，范围广泛的私人行为体（包括黑客和黑客团体以及科技公司）已经开展了与武装冲突有关的网络和其他数字行动，有时是在第三国领土上远程开展此类行动。这些行动可能具有防御和/或进攻的性质。如果无视国际人道法，这些行为体可能会导致冲突和紧张局势进一步升级。

在开展此类行动时，私人行为体不得攻击平民和民用基础设施，而且可能会因某些违反国际人道法的行为而承担国际刑事责任。各国对确保尊重国际人道法负有首要责任，尤其是确保在其指示、指挥或控制下或者从其领土上开展行动的主体尊重国际人道法，并且必须追究所有违反国际人道法的主体的责任。各国还应使私人行为体认识到参加敌对行动所带来的法律和实际风险。此外，各国必须保护其管辖范围内所有人的人权，包括免受私人行为体的数字威胁。

建议 10

如果要制定新的法律规则和规范，需要基于并加强——而非削弱——现有的国际法律规则对平民及其他受保护人员和物体的保护。

各国在制定国际人道法时，主要考虑的是传统的作战手段和方法。但是，有关保护平民居民和民用物体的既定国际法律规则和原则适用于“所有作战形式和武器类型”，包括“未来的作战形式和武器类型”。[1] 这就包括了与武装冲突相关的网络及其他数字行动。

我们呼吁各国就国际人道法如何适用于数字行动形成共识，以确保平民、民用基础设施（包括信通技术系统）以及数据在我们日益数字化的社会中得到充分保护。将国际人道法适用于武装冲突期间数字技术的使用，可能由于技术新颖性及其影响而遇到一些挑战，但这不能成为削弱对平民的保护的漏洞。我们尤其敦促各国向民用数据提供与民用物体同等的保护；将数字化的民用信息和其它内容排除在现有法律保护之外，是不合情理的。

我们认为并非每次作战技术革新都需要制定新规则。然而，如果发现既有国际法无法通过解释——或在实践中不被适用于——确保保护平民和民用基础设施及数据免受数字行动的影响，那么就可能需要额外制定规则。制定新规则时，必须以武装冲突期间对平民的现有保护为基础，并加强（而非削弱）这种保护。

我们重申，联合国进程中商定的任何自愿、不具约束力的网络空间负责任行为规范均可并行不悖。这些规范并不试图限制或禁止符合国际法的行动，且不削弱现有的法律框架。

1. International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996 (Nuclear Weapons Advisory Opinion), para. 86.

建议 11

各国应在最大可行范围内，将军用和民用数据及通讯基础设施分割开来。

各国应认识到如果其军事规划人员和操作人员在武装冲突期间使用民用数字基础设施——例如通讯系统或云存储空间——此类民用基础设施可能会成为军事目标。我们注意到，如果军方开展数字行动，大多数情况下，它们将使用互联网中普遍使用的某些民用基础设施、网络和平台。然而，为了保护民用基础设施和数据免受攻击，各国的默认立场应该是，只要可行，即应力求将军用数字基础设施（或其部分）与民用数字基础设施（或其部分）分割开来，即在物理上或技术上加以分割。例如，在决定是否在非分段式商业云、商业云的一部分或专用军事基础设施上存储军事数据时，军事规划人员和操作人员不应使用非分段式商业云。使用非分段式商业云的国家可被视为故意使用民用基础设施来掩护己方军事资产。我们重申，民用基础设施和服务不得受到攻击。

建议 12

为防止对平民造成伤害，各国需要对日益增长的以开发和销售旨在伤害平民的能力和服务的科技公司市场进行规制。

不同的科技公司向公共和私人客户提供一系列服务，其中涵盖的能力和服务可被用于和武装冲突相关的数字行动，并可能会——有意或无意地——对平民造成伤害。各国必须实施法规，确保科技公司不开发本质上不合法的工具，不提供导致违反国际法的服务。此外，各国还应利用出口管制等现有框架，禁止公司将数字行动能力和服务出售给可能将其用于实施违反国际法的行为的主体。

建议 13

如果国家或国际组织通过制裁或其他限制性措施对受武装冲突或其他人道危机影响的国家的信通技术的出口或进口进行限制，则有必要对信通技术设备和服务给予特定的人道豁免，以确保医疗服务的正常工作、运转、维护和安全，并且确保能够及时开展为满足平民居民的基本需求所需的人道活动或其他服务。

各国应以联合国安理会第2664号决议为基础，该决议明确将“提供必要货物和服务以确保及时运送人道援助或支持为帮助满足人们基本需求而开展其他活动”排除在联合国制裁范围之外，无论供应方是公共部门还是私营部门均如此。信通技术服务、硬件和软件对于向受武装冲突或其他人道危机影响的民众提供医疗和人道服务而言，往往至关重要。限制其进口、出口或交付均有可能影响医疗服务部门和人道组织的行动能力，并削弱其网络安全。例如，如果医疗机构无法更新其IT系统，其网络安全就会受到削弱。此外，如果人道组织不得不遵守与冲突方有关联或支持冲突方的实体所采取的制裁和限制措施，可能会损害人们对该组织的公正性、中立性和独立性的看法，并最终威胁人道组织的准入和安全。

实施限制性措施的当局应与所有相关行为体，特别是属于限制性措施范围内的科技公司，进行协商和协调，并提供充分的指导，以确保上述豁免在实践中得到有效执行。

建议 14

各国和其他行为体应支持和促进为人道组织制定适当的网络安全和数据保护措施和政策，并提供支持以加强这些组织应对有害信息的能力（另见下文建议19）。

人道组织必须建设人力和技术能力，在其现有手段范围内有效保护人道行动以及民众对人道组织的信任免受数字威胁。需要各国、公司和其他行为体共同努力，加强人道组织抵御数字威胁

的复原力——无论是通过提高认识，提供资金、服务，还是通过研发兼容人道组织工作程序（特别是公正、中立和独立原则）的技术解决方案。

对科技公司的建议

建议 15

数字平台在助长传播有害信息方面能够产生很大影响，运营这些平台的科技公司可以采取更多措施来解决这一问题。它们应采取更多措施来检测信号，分析其平台上可能存在的有害信息的来源、传播方式和类型，尤其是与武装冲突局势有关的有害信息。它们的政策、程序和实践，包括内容审核，均应与国际人道法和人权标准保持一致。

为了应对有害信息在受武装冲突及其他人道危机影响的国家传播的突出风险，运营数字平台的科技公司应在加强尽职调查及强化风险管理战略方面实施明确的政策。在这方面，《联合国工商企业与人权指导原则》和其他标准能够提供有益的指导。科技公司应评估并减轻其活动可能对民众的安全和尊严造成的任何负面影响。科技公司应充分投入并采取有效措施，限制有害信息的出现和传播。此外，运营数字平台的科技公司应对其业务实践进行审查，确保其运营、数据收集和数据处理实践不会鼓励或助长有害信息，并与国际人道法和人权标准保持一致。

运营数字平台的科技公司应使其政策、程序和实践与国际人道法和人权标准保持一致。此类公司尤其应采取措施，防止并处理煽动违反国际人道法的行为及传播构成针对平民的歧视、敌意和暴力或国际罪行的仇恨言论的行为。虽然使用人工智能可以有助于识别和分析有害信息，但科技公司应确保自动化程序包括强有力的人工审查，并采取措施减少偏见。科技公司应在专业知识方面进行投入，包括通过与事实核查组织和民间社会合作，以获得相关语言和当地环境方面足够的专业知识。

建议 16

在武装冲突局势中开展业务的科技公司应了解并持续关注其提供的服务是否可能使其员工构成直接参加敌对行动，以及使公司成为军事目标；除直接参加敌对行动外，其卷入武装冲突局势是否可能使其员工面临风险，如有必要，应相应调整其活动。

科技公司提供一系列产品和服务，例如通信基础设施、云存储和网络安全服务，以保护政府和私人用户。在武装冲突期间，科技公司应告知员工这些产品和服务的提供可能带来的风险和法律后果。在可行的范围内，科技公司还应密切关注交战各方是否将其民用服务用于军事用途，并于可行时防止或尽量减少此类使用行为。科技公司应尽一切可能将武装冲突情况下公司和平民客户面临的风险降至最低。

建议 17

科技公司应在最大可行范围内，将其为军事目的和民用目的提供的数据和通信基础设施分割开来。

科技公司应认识到，数字基础设施与服务（如通信系统或云空间）如果用于军事目的，在武装冲突期间可能会成为军事目标。因此，如果提供基础设施供军方使用，科技公司应尽可能提供与民用数字基础设施分割开来（即物理或技术上分离）的数字基础设施（或其部分），作为保护民用基础设施和数据免受攻击和附带伤害的一种手段。

建议 18

科技公司应确保其出于商业或其他原因自愿采取的措施——即其法律义务（如制裁和其他限制性措施）之外的措施——不会妨碍医疗服务、人道活动或其他对满足平民居民的基本需求至关重要的服务的运作、维护和安全。

科技公司必须履行法律义务，如制裁和其他限制性措施所规定的义务。它们也应在最大可行范围内，确保其自愿采取的法律义务之外的措施不会妨碍为受武装冲突或其他人道危机影响的民众提供医疗和人道服务的信通技术服务、硬件和软件。

对人道组织的建议

建议 19

人道组织应采取强有力措施保护其收集和处理的数据，并应加强其IT系统及人道行动抵御数字威胁的复原力。

人道组织往往拥有开展行动所必需的高度敏感的个人信息，这些信息的泄露可能给人们带来真正的伤害。因此，由于人道组织遭受有害数字行动的风险很高，此类组织应在其行动规划和实践中纳入充分的数据保护和网络安全措施。构建此方面的复原力要求人道组织将网络安全和数据保护作为一项机构优先要务，制定内部程序和架构来防范有害的数字行动，并在此类事件发生时尽量减轻其产生的影响。人道组织还应在适合其行动环境及组织职责的网络安全技术措施方面进行投入；以透明、负责任、完全尊重数据主体的权利和尊严且符合国际标准的方式处理数据；并持续培训员工。人道组织还应采取举措并倡导始终提供强有力、清晰明确的保护，包括保护其收集的数据仅能纯粹出于人道目的进行获取和使用。这关乎人道组织所服务的民众的安全、尊严和复原力。

建议 20

人道组织应做好准备，它们有可能成为有害信息的目标，这些有害信息可能对其人道行动和声誉产生影响；人道组织还应做好对此在线上和线下做出适当回应的准备。

为了预测并减轻有害信息对人道组织的威胁，这些组织应加强从经核实的线上和线下来源收集并传播准确信息的能力。这就要求确保人道组织在其应急准备和应急规划中虑及其受有害信息影响的风险，充分保护通信渠道并备有后备通信渠道。虽然有害信息可能会在网上传播，但将线上和线下措施结合起来的应对措施可能最为有效，特别是通过与冲突各方及受影响的社区和民众直接接触的方式。

建议 21

人道组织应在其行动中就针对平民的有害信息制定应对措施。

人道组织应努力在其开展行动的环境中识别针对平民传播有害信息的迹象。它们应认识到此类信息可能对受冲突影响的民众造成的风险和后果，提供易于获取的可靠信息，为获得人道援助和保护提供便利，并助力冲突环境中的受影响民众进行自我保护和复原力建设。在适当的情况下，它们应进行投入，提高信息行动实施主体对平民居民保护方面可适用的国际规则的认识并开展相关对话。同时，针对有害信息的人道应对措施不得扩大此类信息的影响或造成意外伤害。此外，人道组织应谨慎行事，以确保其保护平民免受有害信息影响的工作不会影响交战各方对其公正、中立和独立的人道工作的看法。

建议 22

具有相关专业知识和能力的人道组织应加强努力，提高各界（包括开展数字行动的私人行为体）对武装冲突期间关于保护平民所适用的法律规则的认识。

范围广泛的国家和私人行为体（包括私人黑客和团体以及公司）开展过似乎是为了支持武装冲突方的网络和其他数字行动。人道组织应基于其与武装冲突所有当事方接触的经验，加大力度传播国际人道法对数字行动所规定的限制。除了与各国就其确保私人行为体遵守国际人道法的义务进行接触（见建议9）外，人道组织还应提高私人行为体对国际人道法的认识，例如通过公共宣传、遵守国际人道法的示范行为准则、向此类行为体普及可适用规则的视频或应用程序，并与具有足够组织程度的黑客团体进行接触，促进其遵守国际人道法规则。此外，人道组织应与各国和科技公司协作，寻求与工程学院建立伙伴关系，使未来的操作人员了解在武装冲突期间开展数字行动时所适用的具体规则以及相关风险。

共同努力

建议 23

需要多方利益相关方开展对话，汇集各国、科技公司、人道组织、国际组织、学术界、民间社会和其他利益相关方的专业知识，发展专门针对冲突的理解、原则和/或指南，以保护平民免受数字威胁。

只有采取多维度、多利益相关方的应对措施，才能在武装冲突期间有效保护平民免受数字威胁，同时在数字空间保障和促进国际人道法和人权法。我们建议多利益相关方开展对话，为各国和科技公司打击包括有害信息在内的数字威胁发展专门针对冲突并基于国际法的原则或指南。应继续开展并支持专项研究，以更好地记录问题的规模及其造成的伤害，更好地找到符合并加强国际人道法和人权法的解决方案。

我们鼓励红十字国际委员会提供一个中立的空间，促进各国与其他行为体就武装冲突期间保护平民免受数字威胁的问题进行保密对话，以促进意见交流，力求在各种视角间寻求一致，并就法律限制和实际保护措施寻求共识。

建议 24

科技公司和人道组织应合作应对武装冲突期间的数字威胁。

科技公司和人道组织应共同努力，制定具体的危机处理流程，确保及时应对针对平民、人道组织和其他受保护行为体的数字威胁。我们还呼吁科技公司协助人道组织，分享它们对其开发的系统和平台上的数字威胁的独特见解，并在网络安全、数据保护和创新等领域提供支持。必要时，运营数字平台的公司应促进为有需要的民众提供公正、准确的人道信息。这种合作应虑及人道组织的工作程序，特别是公正、中立和独立原则。

科技公司和人道组织应根据需要向各国提供信息并征求意见，以保护平民。

建议 25

人道组织应借鉴其他领域的经验，与公共和私营机构合作，开发创新解决方案，保护平民居民和人道行动免受数字威胁。

人道组织应与公共和私营机构（学术、研究和专家机构以及公司）合作，调整现有产品和服务，或开发新的产品和服务，以保护平民免受数字威胁，并应对危机背景下公正的人道工作面临的具体挑战。我们乐见并赞扬红十字国际委员会在某些议题的研究和发展方面所做的工作，例如提议创设“数字标志”，以及通过设计保护数据等。

未来之路

数字技术在武装冲突中的应用只会有增无减。平民在日常生活中依赖这些技术；各国将其治理系统数字化；科技公司继续创造新产品和服务；人道组织需要数字技术来确保为有需要的民众开展有效且高效的服务。与此同时，交战方会继续将数字技术用于军事目的。确保以负责任且遵守国际法的方式使用数字技术是我们的共同责任。在各国、私营部门和民间社会讨论我们在数字时代的共同未来之际，必须要考虑受武装冲突及其他人道危机影响的民众的特殊需求及其面临的风险，并将其作为优先要务，加以有效解决。

我们呼吁国际社会携手努力，以开放包容的方式开展工作，在武装冲突期间保护平民免受数字威胁。每个领域都能发挥重要的作用。我们希望我们的联合工作和建议——其中汇集了政策、法律和技术方面的专业知识——将成为实现这一目标的行动号召。

红十字国际委员会
武装冲突期间数字威胁全球顾问委员会成员

达普·阿坎德（Dapo Akande），牛津大学国际公法教授，牛津大学布拉瓦尼克政府学院伦理、法律和武装冲突研究所联合所长

汤姆·伯特（Tom Burt），微软公司客户安全与信任企业副总裁

A.J. 库切（A.J. Coetzee）准将（已退役），南非国防部队

阿诺·库斯蒂利埃（Arnaud Coustillière）中将（已退役），Str@t–Algo公司网络与数字高级顾问，曾任法国国防部网络防御指挥部指挥官

卡米耶·弗朗索瓦（Camille François），Niantic公司信任与安全高级总监

玛丽娜·卡尔尤兰德（Marina Kaljurand），欧洲议会爱沙尼亚议员，曾任爱沙尼亚外交部长

艾琳·汗（Irene Khan），联合国促进和保护意见和表达自由权特别报告员

李晓东，伏羲智库创始人、主任，清华大学互联网治理研究中心主任，中国互联网络信息中心原主任

多丽丝·洛伊特哈德（Doris Leuthard），曾任瑞士联邦主席和联邦委员

帕特里夏·刘易斯（Patricia Lewis），查塔姆研究所冲突、科学与转型研究主任，国际安全项目主管

埃利娜·努尔（Elina Noor），卡内基国际和平研究院亚洲项目高级研究员

朱勒尚·拉伊（Gulshan Rai），印度政府总理办公室前国家网络安全协调员

玛丽安娜·萨拉萨尔·阿尔沃诺斯（Mariana Salazar Albornoz），墨西哥城伊比利亚美洲大学，美洲国家组织美洲法律委员会前成员，数据保护和适用于网络空间的国际法问题特别报告员

德米特里·萨马尔采夫（Dmitry Samartsev），BI.ZONE公司首席执行官

玛里切·沙克（Marietje Schaake），斯坦福大学网络政策中心国际政策主任，斯坦福大学以人为本人工智能研究所国际政策研究员

米里亚娜·斯波利亚里茨（Mirjana Spoljaric），红十字国际委员会主席（全球顾问委员会主席）

约翰娜·韦弗（Johanna Weaver），澳大利亚国立大学科技政策设计中心主任，曾任澳大利亚在联合国的独立专家和首席网络谈判官

马库斯·威利特（Marcus Willett），国际战略研究所高级网络顾问，曾任英国政府通讯总部网络主管和副部长

定义与概念

武装冲突——全球顾问委员会特别关注武装冲突期间的数字威胁问题。全球顾问委员会以国际人道法对“武装冲突”这一概念的理解为指导，即国家之间的武装冲突（“国际性武装冲突”）和国家与非国家武装团体之间或此类团体之间的武装冲突（“非国际性武装冲突”）。不过，就若干议题而言，全球顾问委员会提出的建议在和平时期就应予以实施，原因包括这些建议在武装冲突之外也同样重要；数字威胁何时与武装冲突有关或何时与引发冲突的因素有关并非总是清晰明确；或者这些建议旨在构建应对数字威胁的总体复原力。

平民——全球顾问委员会重点关注保护平民居民、民用物体和民用数据免受数字威胁。与国际人道法相一致，全球顾问委员会将“平民”理解为不属于军队的所有人员，将“民用物体”理解为不构成军事目标的基础设施、数据及其他物体。在主要关注平民保护的同时，部分建议也涉及武装冲突期间对其他人员和物体的保护，如被拘留或受伤士兵以及军事医疗设施。

网络行动——全球顾问委员会将“网络行动”一词理解为通过数字手段针对计算机、计算机系统或网络、或者其他相连设备开展的行动。全球顾问委员会主要对武装冲突期间作为作战手段或方法开展的网络行动进行考量。

数字威胁——全球顾问委员会重点关注“数字威胁”。数字威胁主要包括（往往重叠出现、彼此加剧的）“网络行动”和“信息行动”产生的威胁。此外，这一概念还涵盖平民使用数字手段参与武装冲突给平民和民用基础设施带来伤害的风险。全球顾问委员会在提及“数字威胁”时明确指出，此类威胁也可能在“线下世界”产生后果。

与武装冲突有关的数字行动——全球顾问委员会使用“与武装冲突有关的数字行动”一词来指称在武装冲突背景下实施且与武装冲突有关联的一系列和**数字威胁**相关的数字行动。

有害信息——全球顾问委员会认为“有害信息”涵盖在武装冲突期间违反国际人道法或人权法、可能对民众造成身体或心理伤害的信息，以及可能以其他方式对平民造成有害影响的信息。全球顾问委员会并不侧重于有害信息的描述（即错误信息、鼓吹宣传、虚假信息或仇恨言论）。在评估伤害时，全球顾问委员会强调需要考虑性别、年龄、文化程度、残疾状况等因素。

信息行动——全球顾问委员会将“信息行动”一词理解为使用信息和通讯技术或其他数字手段来影响敌方或平民居民的看法、动机、态度或行为，以实现政治和军事目的。网络行动，按照上文的定义，可能会助力信息行动。全球顾问委员会主要对使用数字技术并在武装冲突背景下作为作战手段或方法实施的信息行动进行考量。

科技公司——全球顾问委员会将提供数字平台、服务或基础设施（包括网络安全服务）的公司以及互联网服务提供商统称为科技公司。

使　命

红十字国际委员会（ICRC）是一个公正、中立和独立的组织，其特有的人道使命是保护武装冲突和其他暴力局势受难者的生命与尊严，并向他们提供援助。红十字国际委员会还通过推广和加强人道法与普遍人道原则，尽力防止苦难发生。

红十字国际委员会创建于1863年，它是《日内瓦公约》和国际红十字与红新月运动的发起者。该组织负责指导和协调国际红十字与红新月运动在武装冲突和其他暴力局势中开展的国际行动。

PROTECTING CIVILIANS AGAINST DIGITAL THREATS DURING ARMED CONFLICT
FINAL REPORT OF THE ICRC GLOBAL ADVISORY BOARD ON DIGITAL THREATS DURING ARMED CONFLICTS

ICRC
微信

ICRC
微博

红十字国际委员会东亚地区代表处
中国北京市建国门外大街9号
齐家园外交公寓3–2
邮编：100600
电话：+86 10 8532 8500
传真：+86 10 6532 0633
邮箱：bej_beijing@icrc.org　www.icrc.org

ICRC

4735/006　07.2024　封面图片：A. Saboh/ICRC