联合国 A/76/151

大 会

Distr.: General
15 July 2021
Chinese
Original: English

第七十六届会议

临时议程* 项目 74

人民自决权利

以雇佣军为手段侵犯人权并阻挠行使人民自决权

秘书长的说明

秘书长谨根据大会第 75/171 号决议和人权理事会第 42/9 号决议，向大会转递以雇佣军为手段侵犯人权并阻挠行使民族自决权问题工作组的报告。

* A/76/150。

21-09837 (C) 300721 160821

以雇佣军为手段侵犯人权并阻挠行使民族自决权问题工作组的报告

雇佣军、雇佣军相关行为体以及私营军事和安保公司从事网络活动对人权的影响

摘要

在本报告中，以雇佣军为手段侵犯人权并阻挠行使民族自决权问题工作组审查雇佣军、雇佣军相关行为体以及私营军事和安保公司在网络空间提供军事和安保产品及服务的情况及其对人权的影响。

有关各方在网络空间提供广泛的军事和安保服务，包括数据收集、情报和间谍活动。国家和非国家行为体可通过各种代理关系雇用私人行为体，开展进攻或防御行动，保护己方网络和基础设施，实施网络作战，削弱敌方武装部队的军事能力和实力，或破坏他国领土完整。实施网络攻击的个人可跨越不同辖区，造成远程损害。因此，可被视为从事雇佣军相关活动，如符合所有资格标准，甚至可被视为雇佣军活动。

本专题研究旨在探讨上述行为体的表现和活动，这些行为体开发、维护和运营可被用于在冲突和非冲突环境中开展敌对行动的网络能力，并从中获利。本研究评估这可能对人权、包括人民自决权产生的影响，并探讨网络空间军事和安保产品及服务的规范问题。

本报告编写期间，工作组由耶莱娜·阿帕拉茨(Jelena Aparac)(主席)、莉莲·博贝亚(Lilian Bobea)、拉文德兰·丹尼尔(Ravindran Daniel)、克里斯·夸贾(Chris Kwaja)和索查·麦克劳德(Sorcha MacLeod)组成。

目录

一. 导言与背景

1. 本报告由以雇佣军为手段侵犯人权并阻挠行使民族自决权问题工作组依据大会第 75/171 号决议和人权理事会第 42/9 号决议提交大会。

2. 根据以上授权，工作组负责监测世界各地一切形式和表现的雇佣军与雇佣军相关活动以及私营军事和安保公司。此外，工作组还研究其活动及对人权、特别是自决权可能产生的影响。

3. 本报告基于广泛的案头研究和相关利益攸关方应工作组 2021 年 1 月呼吁而提供的资料。[1] 2020 年 12 月 7 日，工作组就网络安全和新技术背景下的雇佣军和相关行为体问题举行了一次专家在线磋商，磋商结果纳入本报告。工作组感谢所有提交资料、参加专家磋商、为编写报告献计献策的人员。

4. 多年来，关于雇佣军活动的讨论焦点是雇佣军代表国家或其他客户参与的传统战争模式。最近，雇佣军、雇佣军相关行为体以及私营军事和安保公司在网络空间变得活跃。工作组在关于雇佣军和雇佣军相关活动不断演变的形式、趋势和表现的报告(见 A/75/259)中提到，所谓的“网络雇佣军”构成了一类可产生雇佣军相关活动的行为体。此外，工作组年度报告经常就各种专题提出技术使用和知识转让问题。[2] 本报告审查雇佣军、雇佣军相关行为体以及私营军事和安保公司在网络空间提供军事和安保产品和服务的情况及其对人权的影响。

5. 工作组在之前分析中即指出，一系列雇佣军和雇佣军相关行为体继续通过网络活动等手段，影响当代武装冲突进程，侵犯人权，破坏自决权。如今，网络空间成为国家和非国家行为体的主要地缘战略舞台之一，各种私人实体调动和利用防御性和进攻性网络能力，追求代理目的或利益，对人权享受和人民自决权利造成破坏性后果。

6. 工作组以前曾特别指出，现代武装冲突的不对称性日益增强，私人行为体的参与日益增多(A/75/259)。虽然传统运动战继续在当代冲突中扮演重要角色，但随着新技术的发展和不断演变，网络攻击等活动正变得日益普遍，甚至在传统武装冲突范围之外。这些发展的必然结果是，当代雇佣军和其他行为体已适应并活跃于网络空间，甚至在某些情况下，已是网络作战的必要成员。

二. 定义方面的考虑

7. 《1949 年日内瓦四公约第一附加议定书》第 47 条、《反对招募、使用、资助和训练雇佣军国际公约》和《非洲统一组织消除非洲雇佣军制度公约》对“雇佣军”一词作了定义。然而，国际法中“雇佣军”的定义一直受到诸多分析和反思，关注焦点是其限定过多的性质。工作组认识到，该定义范围存在问题，标准难以

[1] 见 www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx。

[2] 见 A/75/259，第 50 段；A/HRC/45/9，第 39 段起；A/HRC/42/42。

达到，特别是对于当代形式的雇佣军相关活动，包括非国家行为体在网络空间开展的此类活动。

8. 此外，在缺乏国际商定法律定义的情况下，工作组曾将“私营军事和安保公司”一词定义为由自然人和(或)法人有偿提供军事和(或)安保服务的公司实体。[3] 此类实体可在冲突与和平时期运作，是网络领域军事和安保产品与服务的重要提供方。

9. 虽然上述定义均未明确提及网络活动或网络行为体，但显然，网络领域的一些行动可上升至雇佣军水平，或可被视为雇佣军相关活动，也可影响武装冲突与和平时期的人权。此类行动可包括网络中介机构进行的恶意网络作战，不论其国籍或作战地点，也不论其是离线或在线操作，或直接或间接造成损害。[4] 恶意网络作战被理解为采取蓄意行动和操作，改变、扰乱、欺骗、降级或破坏计算机系统或网络，或以其他方式破坏个人和社区的计算机系统或网络的保密性、完整性和可用性。[5] 不包括计算机网络之外产生动能影响的新兴技术，例如无人机技术。

10. 然而，工作组希望强调，不应将网络空间的军事和安保服务视为泛指雇佣军相关行为体的行动，而应根据具体背景和情况评估上述类别中的每一种可能情况(见 A/75/259，第 54 段)。

11. 2020 年，工作组确认网络战为战争方法之一，不仅可渗透、破坏、损害甚至摧毁军事或民用物体，还可造成严重人员伤害。红十字国际委员会认为，网络战与常规战争类似，必须遵守国际人道主义法律。[6] 随着战略能力日益依赖于基础设施和技术，这一点愈加重要(见 A/75/259，第 42 段)。

12. 除其他外，促使工作组关注这一现象的原因包括：当代冲突的转变和新战争形式的迅速演变，以及缺乏监管、监测和监督，以及调查跨辖区犯罪的困难。某些发达国家和富裕行为体在获得技术和相关知识方面的不平等，也令工作组感到关切。

13. 工作组注意到，雇佣军活动环境对妇女、儿童和其他群体产生了不成比例的不同影响(见 A/75/259，第 5 段)。工作组注意到，由于在国际人道主义法范围内，对什么构成网络攻击或网络敌对行动缺乏国际商定的定义，目前在概念上很难将网络敌对行动纳入国际人道主义法框架并查明不遵守和违反情况。

14. 在目前关于何时、何地以及如何监管此类网络活动的辩论中，关键辩论要素之一是非国家行为体(特别是雇佣军、雇佣军相关行为体、私营军事和安保公司以

[3] 完整定义见 A/HRC/15/25，附件，第 2 条。

[4] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 31。

[5] Herbert S. Lin, “Offensive cyber operations and the use of force”, *Journal of National Security Law and Policy*, vol. 4, No. 1 (13 August 2010), pp. 4-63; and ISO/IEC 27000:2009。

[6] 红十字国际委员会，“武装冲突期间的国际人道主义法和网络行动”，红十字国际委员会立场文件，2019 年 11 月。

及其他私营和商业实体)在网络活动和网络战争中的作用。因此，在本报告中，工作组旨在审查网络空间提供的一系列可导致雇佣军相关活动的军事和安保服务，以促进讨论如何更好地界定和处理此类活动(见 A/75/259，第 52 段)。应对之策是，除监管外，相关行为体须在国家和国际层面建立有效合作。

三. 网络空间的军事和安保服务：活动、行为体类别以及国家和非国家行为体之间的关系

15. 军事和安保服务包括数据收集和间谍活动等一系列服务。国家和非国家行为体可通过各种代理关系聘用私人行为体，开展进攻或防御行动，保护己方网络和基础设施，或开展网络作战，削弱敌方武装部队的军事能力和实力，或破坏他国领土完整。上述行为体利用进攻性或防御性网络火力，企图或努力识别、入侵、破坏关键军事或民用设施，旨在摧毁这些设施。

16. 如上所述，必须指出，上述行为体在武装冲突之外向国家提供网络服务，所涉目的不仅包括收集和监视情报，还包括促进国内执法和维护安全。[7] 此外，网络服务既包括向国家提供与现有网络能力有关的支持服务，也包括提供可供各国使用的网络产品。必须指出，大量产品和服务正被提供，并可在公开市场上购买。在审查网络服务监管过程中，须考虑这一点。

17. 目前正在发生的多种类型的网络活动和网络作战方法包括，除其他外，通过恶意软件和勒索软件开展破坏活动、间谍活动和涉及提供错误信息和虚假信息的颠覆活动。实际中，此类活动的表现形式可能是关闭或破坏关键基础设施，包括水电供应、医院、监控服务和通信设施，或可配合攻击军事防御等系统，使之丧失功能。

18. 网络安保公司在面向私营公司和国家的服务中，提供针对网络攻击和网络战争的防御措施。此类纯属防御性的操作包括防火墙、补丁和杀毒软件，更主动但仍属防御性的步骤包括创建蜜罐和焦油坑以及发出信号警告和诱捕攻击者。[8] 此类防御操作无论是被动还是主动，都符合现有的网络安全操作法律准则。

19. 然而，私营和政府网络安保公司以及流氓运营商还具备进攻能力，工作组特别关注这一领域。网络安保公司的进攻能力可被用于对付发达国家，例如，攻击选举基础设施，此类攻击据信由国家支持的行为体或为国家效劳的代理人实施。恶意网络活动还包括攻击虚拟资产和虚拟资产服务提供商，攻击国防公司，非法获取军事技术等(见 S/2021/211，附件，第 125-126 段)。购买此类技术的国家和非国家行为体并无明显、清晰的统一模式。从外部供应商处获取进攻性技术的包括民主国家和非民主国家，拥有内部网络能力的国家和缺乏此类资源的国家亦是如此。

[7] 见信息通信技术和平基金会(ICT for Peace)提交的资料。

[8] 密封提交的资料。

20. 进攻性网络能力市场正迅猛增长，几乎不受监管，提供了利润丰厚的商机。因此，许多传统私营军事和安保公司正在发展网络安全部门。[9] 网络安全供应商无论出处如何，如同更传统的私营军事和安保公司，与国家政府携手合作，成为国家权力的延伸，因此可被视为类似雇佣军代理人。

21. 进攻性和防御性服务之间的区别，以及法律地位上的透明度和模糊性之间的区别，适用于网络空间的军事和安全服务。国家和非国家行为体聘用私人行为体，不仅可保护己方网络和基础设施，还可开展网络作战，削弱敌方武装部队的军事能力和实力，或破坏他国领土完整。雇佣军在网络空间的存在以及对生产和销售进攻性网络武器的参与，突显了其适应能力。[10] 个人实施网络攻击可被视为从事雇佣军相关活动，如符合所有限定标准，甚至可被视为雇佣军活动(见 A/75/259，第 71 段)。

A. 相关网络行为体的类别

纳入正式武装力量的网络部队或网络司令部

22. 近年来，网络影响力战略刺激了对网络专长的竞争，显示了对现代地缘政治关系的破坏性影响。[11] 一些国家正在参与所谓的“网络空间信息战”，[12] 并将军事影响战略行动纳入自身军事能力。数字技术的快速发展深刻改变了战争，促使有关方面投资发展网络部队或网络司令部并将其纳入正规武装力量。此外，两支武装力量之间的经典战争形式现在也伴有网络战争，网络部队在区分防御和进攻行动的微弱界限附近作战。[13] 网络作战可单独进行，也可与传统军事行动相结合。然而，最令人关切的情况仍是与“混合行动”有关的情况，在这种情况下，国家以网络军事行动作出反应，但根据国际人道主义法规则，此类网络军事行动不被视为达到武装冲突的门槛。当正规武装力量将部分网络活动外包给第三方时，网络空间信息战变得更加复杂。

正式武装力量之外的行为体

23. 未纳入武装力量的非国家实体在面向国家或代表国家提供网络服务方面，发挥着非常重要且日益强大的作用。通过所谓“网络雇佣军”的新一代私营公司进

[9] W.J. Hennigan, “Defense contractors see opportunity in cybersecurity sector”, *Los Angeles Times*, 21 January.可查阅 www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html。

[10] Tom Burt, “Cyber mercenaries don’t deserve immunity”, Microsoft website, 21 December 2020.可查阅 https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/。

[11] 见 https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf, pp. 9-10。

[12] 见 https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf, pp. 7-8。

[13] Neri Zilber, “The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?”, *Foreign Policy* (FP), 31 August 2018.可查阅 https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/。

行的网络安全攻击私有化的威胁不断演变，[14] 私营领域和国家领域之间的界限日益模糊。[15]

商业实体

24. 传统私营军事和安保公司通常将曾经由国家垄断的职能和能力私有化，与此不同的是，网络安全供应商首先在私营部门出现并蓬勃发展。虽然全球最先进的军队已发展出内部的网络安全专长和能力，但即使是这些复杂的军事行动也严重依赖私营部门的网络安全专长。[16] 私营网络安保公司包括历史悠久的营利性公司和灵活的初创公司，初创公司在快速扩张的市场中赢得了市场份额。

25. 分析范围内的私营软件和技术公司可分为两类。一类由大型技术平台组成，这些平台与政府实体相通，以使政府能够获取信息和实施监控方案。[17] 另一类由规模和收入水平小得多、但具有制造可用于实施恶意活动的产品的特定能力的公司组成。私营网络安保公司领域正在迅速增长和发展。此外，一些私营军事和安保公司已进入网络安全领域，通常是通过收购精品技术公司并将其并入。

26. 传统上从事国防领域的武器和军事设备生产商已将业务扩至数字领域。此类承包商在很大程度上开发了内部网络安全解决方案和服务，尽管一些承包商也聘请了商业网络安全公司作为子公司，以增强自身能力。关于国防承包商的公开信息有意模糊了旨在纯粹捍卫网络空间弹性的行动和服务与允许客户开展进攻性行动和潜在恶意活动的破坏性技术之间的界限。

高级持续性威胁团体

27. 高级持续性威胁团体的成员是参与持续渗透国家和公共及私人行为体的网络安全系统的流氓/犯罪行为体。它们精通技术，掌握重要财务和技术资源，具备长期战略目标，并经常得到各国政府某种方式的支持。[18] 它们能内部开发进攻能力，实施大规模网络作战。国家军队的网络部门也可发动高级持续性威胁。“雇佣黑客”也可持续测试私营公司和政府的网络防御。就性质而言，高级持续性威胁团体具有长期目标，而非通过使用勒索软件实现快速盈利。

网络民兵

28. 另一类是所谓的网络民兵，其中包括由志愿者维持的各种组织。因此，此类民兵可能超出雇佣军或雇佣军相关行为体的范畴。它们与高级持续性威胁团体不同，既无周密组织和充足资金，也无长期战略目标。基于志愿者的进攻性网络民兵的理论模型区分了论坛、分队和等级。论坛是临时性的网络民兵结构，以一个

[14] 见立即普及组织提交的资料，第 1 页。

[15] 见 Ori Swed 和 Daniel Burland 提交的资料，第 15 页。

[16] 见 www.cmi.no/publications/file/6637-russian-use-of-private-military-and-security.pdf。

[17] 见 https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/。

[18] 见 https://targetedthreats.net/media/1-ExecutiveSummary.pdf。

中央交流平台组织为核心，成员在此分享对所选择目标进行网络攻击所需的信息和工具。分队模式在黑客分队中得到了体现，这些分队在很长一段时间内从事具有政治动机的黑客活动。此种等级反映了传统的等级模式，这种模式可能体现在政府支持的志愿者组织，以及有凝聚力的自我组织的非国家行为体。网络民兵类别还包括攻击自愿击退网络攻击有组织的网络专业人士团体。[19]

个人

29. 拥有信息技术专长的网络专家常在组织结构之外工作，开展旨在检测软件漏洞或错误的独立研究。[20] 此类人员被称为安全研究人员，他们可将与这些漏洞相关的信息出售给对手。[21] 根据不同情况，他们经常通过所谓的“漏洞赏金”来获得工作酬劳。他们通过在线门户联系潜在客户。

网络犯罪分子

30. 犯罪敲诈团伙是流氓犯罪分子，其目标不一定是扰乱经济或进行政治破坏，而是利用持有公司数据作为敲诈机制。他们是为自身利益而行动的个人或团体，目标是由公共和私营部门提供的、整个社区和人口都依赖的服务、产品和基础设施。他们勒索赎金，而目标受害者对索要赎金的反应所产生的经济和政治影响超出了个人行为本身，涉及到此类攻击可能扩大和延续。例如，干扰会持续到直至赎金支付。

B. 国家和非国家行为体之间的关系

31. 国家与这些网络行为体的接触可采取不同形式。在授权模式下，国家通过筛选和选择行为体、惩罚性制裁和对潜在影响的明确评估，对代理方的行为进行明确监督。[22] 在这种情况下，通过市政法律和政策的渠道向代理方分配明确责任，例如，对感知到的关键基础设施的网络威胁[23] 进行先发制人的打击。[24] 在策划模式下，国家向代理方提供被动支持，但不对其行动建立明确监督机制。[25] 通

[19] 见 Rain Ottis, “Proactive defence tactics against on-line cyber militia”, *in Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01-02 July* (Reading, United Kingdom, Academic Publishing, 2010), pp. 233-237。

[20] Steve Ranger, “Meet the hackers who earn millions for saving the web, one bug at a time”, ZD Net, 16 November 2020.可查阅 www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecu。

[21] 见国际妇女争取和平与自由联盟提交的资料。

[22] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 29。

[23] Amanda N. Craig, Scott J. Shackelford and Janine S. Hiller, “Proactive cybersecurity: a comparative industry and regulatory analysis”, *American Business Law Journal*, vol. 52, no. 4 (winter 2015)。

[24] Ellyne Phneah, “S’pore beefs up cybersecurity law to allow preemptive measures”, ZDNet, 14 January 2013), 可查阅 www.zdnet.com/sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/。

[25] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018)。

常是通过松散定义(或不存在)的策略框架以及通过“网络关系”进行临时协作实现。[26] 在默许模式下，国家不承认在其境内活动的私人行为体所采取的行动。[27]

32. 国家通过将一些信息行动和军事影响战略私有化的进程，把不再能够或愿意提供的任务外包给私人行为体。多个供应商执行以前可能由公共安全部队执行的任务，以及从未属于国家安全部队领域的其他任务(见 A/74/244)。

33. 国家将网络服务外包给非国家行为体出于若干原因。与国家往往缺乏传统战争模式的必要能力一样，某些国家可能不具备足够的网络能力，特别是在相关技术不断发展且成本巨大的情况下。同样，国家可能无法维持这种网络能力，因此倾向于临时外包。对网络能力的需求正在蓬勃发展。[28] 同时，各国内部存在广泛的能力和潜能短缺，致使对网络能力的需求增加。[29] 在一些国家，招募私人行为体或外包的做法可能与国防预算的减少以及让私营部门参与提供公共服务(包括军事行动和安保服务)的更普遍趋势相关。[30] 此外，这种外包可使国家与网络活动撇清关系，避免受到审查和承担后果。[31]

34. 工作组注意到，很难有把握地确定国家利用雇佣军和雇佣军相关行为体并将网络服务外包给非国家行为体的具体实例。鉴于此类行动的高度敏感性以及网络行业的隐蔽性和不透明性，也很难确定提供这些服务的确切范围和性质。需进行更多研究，确定哪些行为体正在提供哪些类型的服务。[32] 目前关于国家和非国家行为体如何签订网络能力合同以及购买何种服务的研究既不完善也不全面。信息残缺源于若干因素，因素之一是从事这一领域的大多数公司都是私营(非上市)公司。[33]

35. 然而，所获资料强烈表明，这种承包和外包正在进行，并将持续至未来。网络服务行业发展迅猛，早在网络活动作用扩大之前，各国既已将传统的安全职能和军事职能外包给非国家行为体，因此，也可有把握地推断这种承包和外包正在发生。政府通常跟不上私营部门开发新技术的步伐。[34] 在技术快速发展以及数字

[26] Arindrajit Basu and Elonnai Hickok, ”Conceptualizing an international framework for active private cyber defense”.可查阅 https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049_e1a28ac2850d49fbb6f52eeb9fc79ae7.pdf。

[27] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018)。

[28] 见 Krieg 提交的资料，第 1 页。

[29] 同上。

[30] 密封提交的资料。

[31] 见 Krieg 提交的资料，第 1 页。

[32] 见信息通信技术和平基金会(ICT for Peace)提交的资料，第 2 页。

[33] 见公民实验室(The Citizen Lab)提交的资料，第 1 页。

[34] 见信息通信技术和平基金会(ICT for Peace)提交的资料，第 2 页。

技术和人工智能获得投资的情况下，工作组坚信，网络服务和网络产品将继续外包给非国家行为体。

36. 网络攻击涉及多阶段、多步骤，因此极难将责任归因于实施者及其客户。例如，在僵尸网络攻击中，僵尸管理员渗透到由易受感染的计算机组成的大型网络中，指挥被感染计算机组成的网络攻击目标网络。追查遥控攻击的僵尸主，需跨越数个国家和数个辖区。[35] 网络作战可能严重损害人权，引发严重关切。网络代理可能跨越国界，逃避监管控制和问责机制，这一严重问题令人担忧。[36]

37. 各国以及各非国家行为体已开始利用私人行为体投射网络力量，因为与常规战争相比，此类行动的成本相对较低，而且可隐藏在身份很难被揭露的行为体背后。代理的使用在行为人及其目标之间造成了一定程度的分离，网上的高度匿名性和难以及时确定网络行动责任归属的问题，更加剧了这一点。[37] 利用这类行为体的好处在于，与受国际人权和人道主义法律议定书约束的国家不同，私人行为体在此类议定书的权限之外运作，从而难以归咎、逮捕和起诉。[38] 这反过来又使主使国家能与网络战撇清关系，从而避免审查以及责任和义务归属。[39]

四. 规范雇佣军、雇佣军相关行为体以及私营军事和安保公司在提供网络服务方面的作用和参与

38. 在国际一级规范雇佣军、雇佣军相关行为体以及私营军事和安保公司在提供网络服务(包括网络攻击和网络战)方面的作用和参与，面临诸多挑战和困难。具体而言，这些挑战和困难涉及：(a) 对包括网络战争和网络攻击在内的网络活动的构成要素进行概念化；(b) 查明网络攻击和其他网络活动的来源；(c) 将此类攻击或活动归因于特定个人或实体；(d) 查明开展此类活动的非国家行为体与其所代表的国家(如存在)之间的关系，以及特定网络活动是否构成参与或直接或间接参加持续敌对行动。很多讨论和辩论焦点都集中在目前对网络活动的监管程度和国际一级应在多大程度上对其进行监管。

39. 上述挑战源于网络活动的不透明性、来源、活动实施实体以及国家和其他非国家行为体之间的关系。这种撇清关系的做法在传统的动能武装冲突中并不容易实现，撇清关系有利于国家和非国家行为体，因为可使他们免于为自身行动承担责任；然而，这导致更难以监管这些活动。网络行动的归因问题，以及故意使此

[35] David D. Clark and Susan Landau, “Untangling attribution”, *Harvard National Security Journal*, vol. 2, No. 2 (2011)。

[36] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018)。

[37] 见国际妇女争取和平与自由联盟提交的资料，第 4 页。

[38] Ataa Dabour, “The rise of cyber-mercenaries”, 2021.可查阅 www.hscentre.org/technology/the-rise-of-cyber-mercenaries/。

[39] 见信息通信技术和平基金会(ICT for Peace)提交的资料，第 2 页。

种行动与国家武装部队撇清关系、以便可以“貌似可信的否认”的问题，显然是阻碍推行监管的严重障碍。

40. 现有相关国际监管框架包括《联合国宪章》、国际人道主义法、《适用于网络战的国际法塔林手册》、国际刑法、国际人权法、软法和国内法。

A. 《联合国宪章》

41. 《联合国宪章》，特别是禁止对任何国家的领土完整或政治独立进行武力威胁或使用武力的第二条第四款，将在管制和制裁包括雇佣军活动在内的网络活动方面发挥作用。这是基于这样一个事实，即网络活动的规模和效果可能构成“使用武力”，因此可能为《联合国宪章》所禁止。同样，此类活动可能达到“武装攻击”的门槛，触发国家根据《联合国宪章》第五十一条的规定，采取行动，行使自卫权。此类网络活动是否达到相关门槛，特别是在必要性和相称性原则方面，是一个事实和程度问题，[40] 但毫无疑问，鉴于现代网络活动的性质和影响，它们在特定情况下可达到这些门槛。

42. 不过，需考虑的更困难问题之一是，非国家行为体进行的网络攻击或其他活动是否涉及《联合国宪章》有关规定。鉴于《联合国宪章》只适用于主权国家之间的局势，答案将取决于根据《国家对国际不法行为的责任条款草案》，这些个人或实体的行动能否归因于某个国家。

43. 鉴于提供网络活动服务的实体往往是在与国家保持相当距离的情况下运作，而且网络攻击来源可能难以甚至无法追踪，因为它们是远程启动，可包括不同地点和行为体的各种投入，因此归因问题可能在证据方面面临巨大挑战。当然，另一原因是存在当事方故意使用机制规避对攻击的侦查和归因的情况。

B. 国际人权和人道主义法

44. 各国在和平时期和武装冲突期间均须尊重国际人权规则，但有相关的具体例外和减损。各国还须通过国内法律和执法，保证其境内的私人行为体遵守国际人权规则。全面而发达的国际人权保护框架及其各种条约、监督机构和执行机制，是网络空间监管的现成手段。

45. 红十字国际委员会在从国际安全角度看信息和电信领域的发展不限成员名额工作组的发言中申明，国际人道主义法的规则适用于包括网络战在内的新形式武装冲突。[41] 这一结论依据的是国际法院在核武器的合法性或使用一案中的咨询意见，该法院在该意见中得出结论认为，国际人道主义法适用于当前及未来的武

[40] 见 https://international-review.icrc.org/articles/can-jus-ad-bellum-override-jus-bello-reaffirming-separation-two-bodies-law。

[41] 红十字国际委员会高级军备控制顾问维罗尼克·克里斯托尔(Véronique Christory)在从国际安全角度看信息和电信领域的发展不限成员名额工作组的发言，2019 年 9 月 10 日，纽约。

器和战争类型。[42] 虽然关于国际人道主义法的相关原则适用于武装冲突背景下的网络行动的具体解释还在辩论中，但似乎这些规则在原则上确实适用。这一方法在关于网络战适用法律的《塔林手册》中得到确认。该手册明确指出，“武装冲突法适用于网络作战，如同适用于武装冲突中的其他行动”。

46. 然而，同样，此种做法也绝非容易，特别是考虑到提供这种网络服务的非国家行为体的角色。对于在国际人道主义法中，什么构成网络攻击或网络敌对行动，国际上尚未达成一致定义。然而，“攻击”概念本身很重要，主要涉及区分原则以及军事和民用目标的构成。目标的军事或民用性质可能有不同解读，但这种解读并不取决于攻击期间使用的战争方法。无论攻击是通过动能战争工具还是通过使用网络技术实施，目标的民用性质都应得到尊重。

47. 另一令人关切的问题是武装冲突期间网络作战的地位，具体而言，需确定网络作战是否构成直接参与敌对行动(这与满足《1949 年日内瓦四公约第一附加议定书》第 47 条规定的雇佣军分类标准有关)，或是否与具体武装冲突有足够联系。在某些情况下，旨在摧毁国家能力和国家基础设施的网络攻击相当于非国家行为体在武装冲突背景下直接参与敌对行动。[43] 任何特定网络行为是否可能影响冲突一方的军事能力，是否可能对冲突一方造成伤害，以及该行为与武装冲突之间是否有足够联系，是一个关于事实和程度的问题。除了法律方面，这一问题还有更实际的一个层面，因为可能并非总能识别网络攻击或更微妙网络活动的发生。对所有概念的解释很可能取决于国家实践。

48. 具体到雇佣军，符合雇佣军定义的人无权享有战斗人员地位及其固有保护。更重要的是，目前，雇佣军可因参与敌对行动这一事实而受到起诉，无论是国家还是非国家行为体雇用其参与(网络)敌对行动。雇佣军还可因参与雇佣军活动而受到起诉，前提是相关国内制度规定了此类法律条款。此外，根据 1949 年日内瓦四公约的共同第 1 条，各国有义务确保尊重该公约，这包括确保代表本国行事的实体(可包括代表国家行事的非国家行为体)的行为符合国际人道主义法。

49. 因此，有人提出，雇佣军的传统定义可能不适合以网络战或其他网络活动为特征或至少涉及使用网络战或其他网络活动的战争手段和当代冲突的演变，因此有必要针对网络领域内雇佣军的构成，重新定义概念。[44]

50. 在国际人道主义法适用于网络空间方面，出现并需考虑的另一问题涉及适用于非国际和国际武装冲突的不同法律制度，以及是否需要对网络服务采取同样做法。另一问题是，随着网络战争和网络作战的演变，这种传统区别能否保持。

---

[42] 《以核武器进行威胁或使用核武器的合法性，咨询意见，1996 年国际法院案例汇编》，1996 年 7 月 8 日发布；红十字国际委员会，关于武装冲突期间国际人道主义法和网络作战的立场文件，2019 年 11 月，第 4 页。

[43] Nils Melzer, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Geneva, ICRC, May 2009). 可查阅 www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf。

[44] 见 Van der Waag-Cowling、Van Niekerk 和 Ramluckan 博士提交的资料，第 4 页。

51. 此外，还有一个根本问题源于以下事实：虽然国际人道主义法提供了完善、全面的监管框架，可适用于网络活动，但显然只适用于武装冲突时期。现在的情况是，许多网络活动(或许是大多数网络活动)都是在武装冲突之外发生，因此，国际人道主义法的监管制度将不适用。

C. 国际刑法

52. 国际刑法适用于任何犯下国际罪行的自然人，国际刑事法院对战争罪、危害人类罪、种族灭绝和侵略战争有管辖权。因此，如自然人提供的网络服务满足一项或多项犯罪的一个或多个要素，并符合其他相关标准，国际刑事法院就可能对网络领域的雇佣军和雇佣军相关行为体犯下的犯罪行为拥有管辖权。国际刑法的另一用处在于，其指挥责任原则可帮助克服有关查明和定位实际犯罪人的一些障碍。这类个人的上级如与犯罪行为有牵连，例如下令实施毁灭性网络攻击，或未能阻止此类恶意网络攻击，则不应逃避责任。[45] 除上述挑战外，国际刑法还要求在国际诉讼程序中证明罪行，排除合理怀疑，达到最高的证据标准。此外，鉴于网络作战可涉及数个国家，可能出现管辖权和互补性方面的问题，给调查和起诉带来更多挑战。

53. 《反对招募、使用、资助和训练雇佣军国际公约》和《非洲统一组织消除非洲雇佣军制度公约》均将雇佣军活动定为犯罪，为起诉和惩罚雇佣军相关活动提供了另一法律依据。批准这些公约的国家应将有关规定转用于国内法律制度，使国内法院能够起诉雇佣军活动。

D. 软法和正在进行的倡议

54. 除了具有约束力的国际法框架外，过去十年中还出现了一些针对各种行为体的多利益攸关方和多边倡议，力求在使用信息和通信技术过程中促进负责任的行为。其中包括针对私人行为体的非约束性规范框架，如西门子制定的《网络安全技术协议》和《信任宪章》。全球网络空间稳定委员会和起草《塔林手册》的独立专家组等详细阐述了关于规范和适用国际法的建议。其他多利益攸关方倡议，如“网络空间信任与安全巴黎呼吁”，均针对私营部门、民间社会和政府。

55. 在人权理事会一级，一个不限成员名额的政府间工作组在拟订一项关于监管、监测和监督私营军事和安保公司活动的国际监管框架内容方面发挥了重要作用。由于操作环境和所提供服务瞬息万变，通过这一进程制定的任何监管机制都应采用术语“服务”或“活动”，而非“私营军事和安保公司”，以更有效地捕捉侵犯人权或国际人道主义法行为。[46]

56. 大会为讨论信息和通信技术领域更广泛的安全问题而设立的以下两个小组可就此提供指导：从国际安全角度看信息和电信领域的发展不限成员名额工作组(见大会第 73/27 号决议)；从国际安全角度促进网络空间负责任国家行为政府专

[45] 见立即普及组织提交的资料，第 10 页。

[46] 见雇佣军问题工作组主席耶莱娜·阿帕拉茨(Jelena Aparac)的发言。可查阅 www.ohchr.org/EN/HRBodies/HRC/IGWG_PMSCs/Pages/Session2.aspx。

家组(见大会第 73/266 号决议)。这两项进程均审议了六个主要领域，包括现有和潜在的威胁；负责任国家行为的规则、规范和原则；国际法；建立信任措施；能力建设；定期机构对话。

57. 2021 年 3 月，从国际安全角度看信息和电信领域的发展不限成员名额工作组通过了一份共识报告，其中概述了对所有成员国的一些不具约束力的建议。虽然这些建议均未涉及雇佣军或雇佣军相关行为体问题，但报告多次提及人权问题，而且报告指出，一些非国家行为体展示了以前只有国家才具备的信息和通信技术能力。报告指出，涉及国家和非国家行为体恶意使用信息和通信技术(信通技术)的事件持续增多，这一趋势令人不安(见 A/AC.290/2021/CRP.2，第 16 段)。大会在 2020 年 12 月 31 日第 75/240 号决议中决定，召集一个新的不限成员名额工作组，任期直至 2025 年。以雇佣军为手段侵犯人权并阻挠行使民族自决权问题工作组认为，这为讨论在网络领域活动的雇佣军和雇佣军相关行为体问题提供了重要契机。

58. 从国际安全角度促进网络空间负责任国家行为政府专家组在 2021 年共识报告中重申，“各国不得利用代理人利用信通技术实施国际不法行为，并应努力确保非国家行为体不利用其领土实施此类行为”。[47] 虽然这并未为国家制定法律标准，但确实谴责了国家策划和支持代理人的行为。政府专家组指出，各国为促进尊重和遵守人权以及确保负责任和安全地使用信息和通信技术(信通技术)所做的努力应相辅相成、相互依存，同时承认大规模监控可能对包括隐私权在内的人权产生负面影响。[48]

59. 据述，新制定的标准制定举措将构成网络安全“制度综合”，涉及各种努力安排，而非具有约束力的等级文书。

五. 对人权的影响

60. 不可否认，网络活动涉及人权规范和规则，并有能力在武装冲突和和平时期造成侵犯，因此牵涉各种权利。工作组回顾其调查结果，即私营军事和安保公司开展的活动所产生的性别风险和影响有许多共同点，无论其规模和提供的服务如何(见 A/74/244，第 6 段)。此外，工作组还确定了特别受国家雇用的雇佣军和雇佣军相关行为体影响的群体，如人权维护者、移民、反对派领导人和记者，以及性别暴力背景下的男女同性恋、双性恋、跨性别者、间性者和非常规性别者。

61. 新的和正在出现的战争形式可对军事目标和平民人口产生重大影响，并可导致在武装冲突和其他情况下违反国际人道主义法以及个人权利和自由。工作组先前指出，网络战已被确认为一种战争方法，不仅可以渗透、破坏、损害甚至摧毁

[47] 见 https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf，第 71(g)段。

[48] 同上，第 39 和 37 段。

军事和民用目标，还可造成严重的人员伤害。[49] 网络破坏可对关键基础设施的运作产生巨大次生影响，可能破坏公共卫生、安全和安保。在此情况下，生命权、不遭受酷刑和其他不人道或有辱人格待遇的权利是可能被网络作战侵犯的主要权利。

隐私权和表达自由权

62. 任何情况下，隐私权和表达自由权都有受到侵犯的风险。当雇佣军和雇佣军相关行为体被部署以攻击国家时，他们无一例外地成为破坏这些国家主权和领土完整的关键工具，这也阻碍了隐私权的行使。

63. 隐私权也可能因监控和情报收集而受到损害。令人深感关切的是，存在针对民间社会、特别是人权维护者和记者的网络作战，其目的是扰乱他们的活动，以期压制异见并加强国家对其人口的控制。尽管各国政府长期以来一直使用不同方法监控和跟踪本国公民、持不同政见者、政治对手和人权维护者，但现在可用的技术工具，如恶意软件和间谍软件，使政府能够以更低成本这样做，并扩大监控地理范围，扩大覆盖和规模，从而使政府能够比以往任何时候都更彻底地实施数字镇压。[50] 某些形式的间谍软件是可对目标进行远程监控的工具的典型例子。[51]

64. 此外，有人认为，一些国家管制互联网内容或散布虚假信息和错误信息，可能侵犯表达自由权。政府客户开展或雇用的颠覆性网络作战可破坏网络空间完整性、言论自由和其他公民自由，不仅影响个人，而且影响某些群体甚至整个社会。[52] 定向监视还导致被监视对象的自我审查，直接损害记者和人权维护者进行调查并与信息来源建立和保持关系的能力。[53]

65. 私营公司开发、维护并有时操作的监视技术的另一重要影响是，导致移民路线从可探测区域转至监控设备范围之外区域。因此，移民在水路或陆路移民途中，被迫选择更危险的绕道路线，行动难度和相关生理和精神损失、痛苦和折磨加剧，常常导致中暑、严重脱水和其他痛苦的死亡。[54]

66. 网络能力的作用可转化为对机构和个人的实质性有害影响，损害了政府提供保护和确保大部分人口福祉的能力，并阻碍了人权的享受。例如，对选举制度的攻击直接影响到被剥夺投票权的公民的基本民主代表权。还有报告称，一些国家

[49] 红十字委员会，“武装冲突期间的国际人道主义法和网络行动”，立场文件，2019 年 11 月。

[50] 见公民实验室提交的资料，第 8 页。

[51] A/HRC/41/35，第 9 段；Bill Marczak and others, *Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries*, Citizen Lab, 18 September 2018。

[52] S/2021/569，第 103 段。

[53] 见 A/HRC/38/35/Add.2，第 53 段；A/HRC/41/35，第 26 段。

[54] A/HRC/45/9，第 44-45 段。

经常对平民区发动网络攻击，使用黑客攻击私营公司，或破坏外国军队，利用在线工具操纵信息或数字宣传，左右他人观点，并为此招募数字雇佣军。[55]

67. 有报告称，网络攻击造成了广泛的物理破坏，包括对电网、金融机构和政府部委的破坏。[56] 破坏包含平民信息的数据库可迅速使政府服务和私营企业完全停顿，因此对平民造成的伤害比破坏实物更大。[57]

自决

68. 关于自决权，通过在网络空间使用军事以及安保产品和服务，网络安全公司可严重阻碍人民行使自决权。上述行为体可能以最终可能损害自决权的方式影响国内叛乱(见 A/71/318，第 20 段)。

六. 结论和建议

69. 技术发展和数字化直接影响民众生活各领域。军事领域也日益依赖数字技术。日益增长的数字化趋势反映在信息空间和网络空间日益融合，可在和平时期和武装冲突期间对民众产生负面影响。

70. 工作组考虑了雇佣军、雇佣军相关行为体和私营军事安保公司在网络空间提供军事和安保产品和服务的演变以及对人权享受造成的相应影响。工作组注意到仅侧重于符合适用国际法律框架下“雇佣军”定义的活动所面临的挑战，采取更广泛做法，审查了符合更具适应性的雇佣军相关活动概念的各种行为体和表现形式。

71. 工作组关切地注意到，一些国家通过作为或不作为，掩盖自身对恶意网络作战的参与，试图逃避国际法规定的责任(包括对为此招募的非国家行为体所犯违法和侵权行为的责任)，借以获得战略军事影响力。然而，招募私人行为体在网络空间提供军事和安保服务并不能免除国家在国际法下的义务。

72. 因此，鉴于雇佣军相关行为体的新的和不断演变的表现形式，各国和其他相关利益攸关方应予以紧急关注。本报告阐述了在更有效制定对网络空间行为体的监管时应考虑的因素，以支持各国和其他行为体，确保尊重、保护和实现人民的自决权，在武装冲突情况下保护平民，并维护不干涉和领土完整原则。任何关于监管的讨论应以有关雇佣军的国际法律框架为基础，尽管该框架存在缺陷，并以更广泛的国际人道主义和人权法律框架为基础。

---

[55] Paul D. Shinkman, “America Is losing the cyber war”, U.S. News and World Report website, 29 September 2016.可查阅 www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries。

[56] Neri Zilber, “The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?”, *Foreign Policy* (FP), 31 August 2018.可查阅 https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/。

[57] 红十字委员会，“武装冲突期间的国际人道主义法和网络行动”，立场文件，2019 年 11 月。

建议

73. 为防止和减轻雇佣军和雇佣军相关行为体以及私营军事和安保公司在网络空间产生的负面人权影响，各国应避免招募、使用、资助和训练雇佣军，并应在国内法中禁止此类行为，有效监管私营军事和安保公司。

74. 各国应致力于实现军事支助服务(包括网络作战)合同方面的透明度，并将其付诸实施，以足够详细和及时的方式公布关于服务性质、采购程序、合同条款和服务提供商名称的信息。各国不应援引国家安全关切作为限制获取此类信息的一般理由；相反，根据表达自由权，对获取信息的限制必须符合合法性、必要性和相称性标准。

75. 各国须调查、起诉和制裁雇佣军、雇佣军相关行为体以及私营军事和安保公司涉嫌违反国际人道主义法和侵犯人权的行为，并向受害者提供有效补救。调查、起诉和审判必须尊重和保障获得公正审判和正当法律程序的权利。

76. 在国际一级，各国应启动对话，讨论如下方面：新的和不断演变的雇佣军形式，特别是网络领域各种形式的雇佣军；雇佣军对国际人道主义和人权法构成的风险；更有效地处理和打击雇佣军的方法。任何此类对话都应包括国际和区域组织、民间社会和专家，并考虑现有工具和举措。

77. 各国应重振与不限成员名额政府间工作组的讨论，以拟定关于监管、监测和监督私营军事和安保公司活动的国际监管框架的内容，[58] 包括有关私营军事和安保公司何时提供网络服务和在网络战背景下开展业务的内容。有必要制定一份关于管理网络空间的具有法律约束力的文书。国际法律框架将通过明确的法律义务，提供确定性和可预测性，这些义务可通过专门的争端解决论坛予以执行。治理制度碎片化则会加剧监管混乱，往往对发展中国家和民间社会行为体不利。

78. 从国际安全角度看信息和电信领域的发展不限成员名额工作组以及从国际安全角度促进网络空间负责任国家行为政府专家组应进一步处理因雇佣军和相关行为体参与网络作战而引起的人权问题。

79. 关于与非国家武装行为体有关的雇佣军、雇佣军相关及私营军事和安保公司的活动，各国应商定并支持国际进程，以确定、评估和进一步发展机制，更明确和正式地承认非国家武装行为体的国际人权义务，包括确定后者履行人权义务的能力的标准。

[58] 见人权理事会第 36/11 号决议。