Humanity In War

Under the Global Initiative to Galvanize Political Commitment to International Humanitarian Law (Global IHL Initiative), **Ghana, Luxembourg, Mexico, Switzerland and the International Committee of the Red Cross (ICRC)** are pleased to present the:	在“激励对国际人道法做出政治承诺的全球倡议”（简称“国际人道法全球倡议”）下，加纳、卢森堡、墨西哥、瑞士和红十字国际委员会荣幸呈上：
WORKSTREAM 6	工作领域 6
SECOND STATE CONSULTATION ON UPHOLDING INTERNATIONAL HUMANITARIAN LAW IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES DURING ARMED CONFLICTS	**武装冲突期间使用信息和通信技术时维护国际人道法第二轮国家咨商**
For government officials specializing in IHL, cybersecurity, or military cyber operations in capitals, as well as representatives from permanent missions in Geneva	邀请来自各国首都、专门从事国际人道法、网络安全或军事网络行动工作的政府官员，以及各国常驻日内瓦代表团的代表参会

MONDAY, 24 NOVEMBER 2025	星期一，2025 年 11 月 24 日
9:00–18:00 (UTC+1)	9:00-18:00（UTC+1）
FORMAT: IN PERSON (ICRC HUMANITARIUM IN GENEVA) AND ONLINE (ZOOM)	会议形式：线下（红十字国际委员会日内瓦人道中心）和线上（ZOOM 网络会议）结合
# Background	# 背景
The growing use of information and communication technologies (ICTs) during armed conflicts raises significant humanitarian and legal questions. While it is generally accepted that international humanitarian law (IHL) imposes limits on the use of ICTs in armed conflict, the specific characteristics of the ICT environment give rise to complex questions regarding the implementation of IHL. States have recognized the need to continue discussing these questions.	信息和通信技术（以下简称“信通技术”）在武装冲突期间的使用日益增多，这带来了重大的人道和法律问题。虽然国际人道法对武装冲突中信通技术的使用施加限制已获得普遍接受，但信通技术环境的特性仍在国际人道法的实施层面引发了复杂问题。各国已经认识到，有必要就这些问题持续进行讨论。
The ICT workstream of the global IHL initiative builds on the global discussions on the use of ICTs and the progress achieved to date, particularly Resolution 2 of the 34th International Conference of the Red Cross and Red Crescent, titled “Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict". This workstream is part of an ongoing effort to develop a shared understanding of the limits that IHL imposes on ICT activities during armed conflict, with a view to safeguarding civilians from harm.	本工作领域的基础是有关使用信通技术的全球讨论以及目前已取得的进展，尤其是第 34 届红十字与红新月国际大会通过的第 2 号决议——标题为“在武装冲突期间保护平民和其他受保护人员及物体免受信息和通信技术活动的潜在人类代价之影响”。本工作领域属于一项持续性努力，旨在促进各方就国际人道法在武装冲突中对信通技术活动的限制达成共识，从而保护平民居民免受伤害。
The first consultation on this workstream was held on 15 May 2025. It focused on identifying legal and humanitarian issues and concerns arising from the unique characteristics of ICT activities in armed conflict, and on exploring how they should be addressed – with a view to upholding the protection that IHL affords to civilians and civilian objects, and other protected persons and objects, during armed conflict. This second consultation will advance that discussion. It will be held, in a hybrid format, on 24 November 2025 in Geneva.	本工作领域的第一轮国家咨商已于 2025 年 5 月 15 日召开。第一轮咨商的工作重点是明确武装冲突中信通技术活动的特性所带来的法律和人道问题以及关切，并探讨应对之道，从而维护国际人道法在武装冲突中为平民和民用物体以及其他受保护的人员与物体所提供的保护。第二轮咨商将继续推进这一讨论。会议将以线上线下相结合的方式，于 2025 年 11 月 24 日在日内瓦召开。
For further details on the issues addressed in this workstream, participants are invited to consult the **background paper** attached to this concept note.	关于本工作领域所讨论议题的更多详细信息，请参与方查阅本概念说明所附的**背景文件**。

Objectives	目标
The second consultation will build on the discussions that took place in the first consultation and on key takeaways from that consultation. It will focus on deepening the discussion of legal and humanitarian issues arising from the use of ICTs during armed conflict. The consultation will aim to advance shared understanding and identify potential legal and practical recommendations to ensure better protection for civilians and civilian objects in digitalized warfare.	第二轮咨商将以第一轮咨商进行的讨论及关键结论为基础展开，聚焦于深入讨论武装冲突期间使用信通技术所带来的法律和人道问题。本轮咨商力求增进共识，确定潜在可行的法律和实践建议，确保在数字化战争中强化对平民和民用物体的保护。
The consultation will pursue the following objectives:	本轮咨商的目标如下：
• **provide an update on the workstream and its progress**:	• **介绍本工作领域的最新情况及进展：**
○ brief participants on the findings of the first consultation reflected in the progress report and on insights gained from subsequent supporting events	○ 向参与方简述进展报告反映的第一轮咨商结论，以及后续支持活动所贡献的见解
○ outline the next steps towards identifying the workstream's final recommendations.	○ 概述后续工作步骤，推动本工作领域形成最终建议。
• **deepen discussion of identified legal and humanitarian issues to advance a shared understanding thereof:**	• **深入讨论已提出的法律和人道问题，推动在下列方面增进共识：**

○ facilitate in-depth exchanges on issues identified during the first consultation for further consideration, such as:	○ 推动就第一轮咨商期间提出的问题开展深入交流，以供进一步考量，例如：
▪ implications for IHL of ICT operations that result in non-physical effects, such as the loss of functionality of the targeted system	▪ 造成目标系统丧失功能等非物理性影响的信通技术活动，对国际人道法及其适用有何影响
▪ protection, under IHL, for civilian and other data from, for example, being tampered with, damaged or deleted, or extracted and published	▪ 依据国际人道法，保护民用数据和其他数据，免遭篡改、破坏或删除，或提取及发布等
▪ specific protection under IHL of persons, objects and activities from the effects of ICT activities during armed conflict, including their data and digital infrastructure	▪ 依据国际人道法，为特定人员、物体和活动（包括其数据和数字基础设施）提供特别保护，使其免受武装冲突期间信通技术活动的影响
▪ limits imposed by IHL on information spread through ICT activities	▪ 国际人道法对通过信通技术活动传播的信息所施加的限制
▪ implications for IHL of the military use of civilian ICT infrastructure and civilian involvement in ICT activities in the context of an armed conflict, and measures grounded in IHL to mitigate the associated risks of harm for civilians and essential civilian services	▪ 武装冲突中将民用信通技术基础设施用于军事用途和平民参与信通技术活动，对国际人道法及其适用有何影响，以及依据国际人道法可采取哪些措施来减轻对平民和基本民用服务的相关伤害风险
○ strengthen practical measures to ensure IHL compliance and mitigate civilian harm.	○ 强化实践措施，确保遵守国际人道法并减轻平民伤害。
# Next steps	# 后续工作步骤
A third state consultation is planned for early 2026 to further advance the discussions of the first and second consultations and shared understandings emerging therefrom. These consultations will lay the groundwork for the workstream's recommendations. Feedback for the workstream's recommendations will be sought from all interested states in the second quarter of 2026, and the recommendations will be further considered in future state consultations.	计划于 2026 年上半年举行第三轮国家咨商，以进一步推进前两轮咨商的讨论，并深化由此形成的共识。各轮咨商将为本工作领域所提建议奠定基础。2026 年第二季度将向所有感兴趣的国家征求有关本工作领域所提建议的反馈意见，相关建议将在后续举行的国家咨商作进一步考量。
State consultations will be complemented by regional discussions and other supporting events, which will be announced on the Humanity in War website.	国家咨商将由地区性讨论和其他支持活动予以补充，这些活动将通过“战火中的人道”网站发布。

Participants	参与方
• The consultation will be held primarily in person in Geneva. Online participation is also possible.	• 咨商主要在日内瓦线下举行，也开放线上参会渠道。
• The consultation is **open to all interested states**. There is a strong preference for capital-based government officials specializing in IHL, cybersecurity, or military cyber operations, as well as representatives from permanent missions in Geneva.	• 咨商**欢迎所有感兴趣的国家参会**，尤其欢迎来自各国首都、专门从事国际人道法、网络安全或军事网络行动工作的政府官员，以及各国常驻日内瓦代表团的代表参会。
• Other representatives with specific expertise in the subject matter (e.g. members of international organizations, civil society and academia) will also participate upon invitation.	• 就会议主题事项具备专业知识的其他代表（如国际组织、民间社会和学术界人员）也将应邀参会。
• Kindly register no later than 15 November 2025, using this link: https://forms.office.com/e/LuDKik93vY.	• 请至迟于 2025 年 11 月 15 日前完成注册，注册链接：https://forms.office.com/e/LuDKik93vY。
Procedure	**程序事项**
• The working languages will be **Arabic, Chinese, English, French, Russian and Spanish**, with simultaneous interpretation.	• 会议工作语言为**阿拉伯文、中文、英文、法文、俄文和西班牙文**，会议提供同声传译。
• We ask states to kindly limit their statements to **four minutes** to ensure sufficient time for all participants to take the floor. At the end of each session, and after all participating entities that wish to contribute have done so, states and other participants will be given an opportunity to discuss ideas proposed by others.	• 请各国将发言时间限制在**四分钟**内，确保所有参与方都有足够时间发言。在会议每个部分结束时，待有意发言的所有参与方发言完毕后，各国及其他参与方将有机会就他方提出的观点进行讨论。
• When preparing their statements, participants are kindly requested to consider the **guiding questions** provided in the agenda below. Some guiding questions are accompanied by **illustrative scenarios** that should be read together with the questions. An updated **background paper**, to help frame and facilitate the discussion, is attached to this concept note.	• 在准备发言内容时，请各参与方对以下会议议程所列的**引导性问题**进行考虑。部分引导性问题随附有**情景说明**，应与问题一并阅读。本概念说明附有一份更新后的**背景文件**，以帮助确定讨论框架并促进讨论。
• Given the technical challenges of hybrid meetings, we encourage delegations who are in the room to make their statements in person, and in all cases to give their full attention to delegations speaking online.	• 鉴于线上线下混合会议存在的技术限制，我们鼓励线下参会的代表团进行现场发言，并务必在一切情况下认真听取线上代表团的发言。
• The **inclusive, constructive, non-politicized and solution-oriented** nature of the discussions will be maintained throughout the consultation. While	• 咨商全程的讨论将始终保持**包容性、建设性、非政治化**，并**以解决方案为导向**。鼓励各参与方在咨商

participants are encouraged to refer to their state's domestic practice during the consultations, they are asked to kindly refrain from discussing specific contexts or the practice of other states.	会议中提及其本国国内实践，但请避免讨论具体国家和地区或其他国家的实践。
• To facilitate interpretation, we invite participants to share a copy of their statements by 21 November 2025, via email to ihlinitiative@icrc.org, with "ICT workstream second consultation" in the subject line. We also encourage participants to send their full written statements by email after the meeting. **Unless confidentiality is explicitly requested, these statements will be published on the ICRC website.**	• 为协助会议口译，请参会者于 2025 年 11 月 21 日前将发言稿通过邮件分享至 ihlinitiative@icrc.org，邮件标题栏请注明"信通技术工作领域第二轮咨商"。我们也鼓励各参与方会后通过电子邮件提交完整的书面发言稿。**除非明确提出保密请求，上述发言稿均将通过"战火中的人道"网站公开发布。**
• The consultation will be recorded, but the recording will not be made public.	• 咨商会议将进行录像，但录像不会公开。
# Agenda	# 会议议程
Upholding International Humanitarian Law in the Use of Information and Communication Technologies During Armed Conflict	**武装冲突期间使用信息和通信技术时维护国际人道法**
(ICT Workstream)	**（信通技术工作领域）**
Second Round of Consultations	**第二轮咨商**
9:00–18:00, 24 November 2025	2025 年 11 月 24，9:00-18:00
ICRC Humanitarium, 17 avenue de la Paix, 1202 Geneva	红十字国际委员会人道中心（17 avenue de la Paix, 1202 Geneva）
* *Depending on the number of statements given, all times set out below are subject to change..*	*以下所有时间安排将依据发言数量进行调整。

Registration and coffee / Login and connection	8:30–9:00
Opening of the meeting and introduction	9:00–9:30
Panel discussion: Key legal and humanitarian issues arising from the use of ICTs during armed conflict	9:30–10:30

现场注册和茶叙/线上登录和接入会议	8:30–9:00
会议开幕、情况概述	9:00–9:30
专家讨论会：武装冲突期间使用信通技术所带来的关键法律和人道问题	9:30–10:30

Session 1: Practical measures to ensure compliance with IHL and protect civilians in the use of ICTs during armed conflict	10:30–11:30	**第 1 部分：武装冲突期间使用信通技术时确保遵守国际人道法并保护平民的实际措施**	10:30–11:30
Guiding questions 1. What legal and operational measures has your state adopted, or is considering adopting, to ensure compliance with IHL and prevent or mitigate civilian harm when conducting ICT activities during armed conflict? How do these measures – because of the specific characteristics of ICT operations – differ from those applied to kinetic operations, and how can these characteristics be addressed? 2. What measures does your state take, or has considered taking, to prevent and suppress IHL violations committed through or related to ICT activities? 3. What forms of capacity-building or international cooperation would be most useful for supporting states in strengthening compliance and sharing practical measures in this area?		**引导性问题** 4. 贵国已经采取，或正在考虑采取哪些法律和行动措施，以确保在武装冲突期间实施信通技术活动时遵守国际人道法并防止或减轻平民伤害？ 鉴于信通技术行动的特性，这些措施与适用于动能行动的措施有何不同，以及应如何应对这些特性带来的问题？ 5. 贵国采取或已经考虑采取哪些措施，以防止并遏制通过信通技术活动或相关活动实施的违反国际人道法的行为？ 6. 何种形式的能力建设或国际合作最有助于支持各国在该领域加强遵守法律并分享实际措施？	
Coffee break	11:30–12:00	茶歇	11:30–12:00
Session 2: Safeguarding civilians and other protected persons and objects against the dangers arising from ICT activities during armed conflict	12:00–13:00	**第 2 部分：武装冲突期间保护平民和其他受保护人员及物体免受信通技术活动所带来的危害**	12:00–13:00
Guiding questions 1. What are the human costs and the IHL implications of ICT operations that result in non-			

physical effects, such as disabling the targeted system?

Consider an ICT operation, conducted in the context of an armed conflict, against a civilian object, for example the server of a transport provider, an internet service provider or a bank. At the time of the operation, this server is not being used in a manner that would qualify it as a military objective. As a result of the operation, the targeted object no longer provides the service it normally does; however, it is not physically damaged. How does your state assess the lawfulness of the ICT operation? Would your assessment change if physical damage took place as a result of the foreseeable direct or indirect effects of the ICT operation?

2. How do you address the protection, under IHL, of civilian and other data against, for example, tampering, damage, deletion, or extraction and publication without authorization? Does your state distinguish between different categories of data (medical, biometric, financial, etc.) when assessing their protection under IHL?

   Consider an ICT operation, conducted in the context of an armed conflict, to delete civilian data (such as medical data, social-security data, bank accounts, tax records, or client data of civilian companies). How does your state assess the lawfulness of such ICT operations? What IHL rules limit tampering with, damaging or destroying civilian or other protected data

引导性问题

4. 造成非物理性影响（如目标系统丧失功能）的信通技术行动会带来哪些人类代价并对国际人道法及其适用带来何种影响？

   请思考：假设在武装冲突期间实施了一项针对民用物体的信通技术行动，例如对运输服务提供方、网络服务提供方或银行的服务器发动攻击。在行动之时，该服务器的用途不足以使其被认定为军事目标。由于该行动，受到攻击的物体无法再继续提供正常服务；然而，该物体未受到物理损害。贵国如何评估该信通技术活动的合法性？如果因为该信通技术行动可预见的直接或间接影响造成了物理损害，贵国的评估结果是否会发生变化？

5. 依据国际人道法，贵国如何保护民用数据和其他数据，例如免遭篡改、破坏、删除、或提取及未经授权的发布？在评估国际人道法对不同类别的数据（医疗数据、生物数据、财务数据等）所提供的保护时，贵国是否对这些数据进行区分？
   请思考：假设在武装冲突期间实施了一项信通技术行动，删除了民用数据（例如医疗数据、社会保障数据、银行账户、税收记录或民用公司的客户数据）。贵国如何评估此类信通技术活动的合法性？对于武装冲突期间篡改、破坏或销毁民用或其他受保护数据的行为，哪些国际人道法规则对此进行了限制？对于在未经授权的情况下复制、获取甚至公开民用或其他受保护数据的行为，国际人道法提供了何种保护？
6. 对于依据国际人道法不构成“攻击”的信通技术行动，哪些国际人道法规则为平民和民用物体免受此类行动影响提供了保障？例如，当开展信通技术活动时，必须采取哪些实际措施，以履行在进行军事行动时应经常注意不损害平民居民、平民和民用物体的义务？

in times of armed conflict? What protection does IHL provide against the unauthorized copying, seizing and potential publication of civilian or other protected data? 3. What IHL rules safeguard civilians and civilian objects from ICT operations that do not qualify as an 'attack' under IHL? For example, what practical measures must be taken when carrying out ICT activities to implement the obligation to take constant care to spare the civilian population, civilians and civilian objects in the conduct of military operations?	
Lunch (not provided)	13:00–14:00
Session 3: Operationalizing specific protections for persons, objects and activities against the effects of the use of ICTs during armed conflict	14:00–15:00
Guiding questions 1. What practical measures does your state take, or is considering taking, to ensure that ICT activities during armed conflict do not damage or disrupt the functioning of medical services, humanitarian activities or objects indispensable for the survival of the civilian population, including their ICT systems and data? And what precautions does your state take, or is considering taking, to protect these specifically protected objects against harm, including harm caused through ICT activities? 2. Regarding the specific protection for medical	

午餐（自理）	13:00–14:00
第 3 部分：落实武装冲突期间对人员、物体和活动的特别保护，使其免受信通技术使用的影响	14:00–15:00
引导性问题 4. 贵国已采取或正在考虑采取哪些实际措施，以确保防止武装冲突期间的信通技术活动对医疗服务运转、人道行动或对平民居民生存不可或缺的物体（包括其信通技术系统和数据）造成损害或致其中断？此外，贵国已采取或正在考虑采取哪些预防措施，以保护此类受到特别保护的物体免受损害，包括信通技术活动造成的损害？ 5. 关于对医疗机构和医务人员的特别保护，请思考：假设在武装冲突期间冲突一方实施了一项信通技术行动，以访问一所位于敌方领土内的医疗机构的服务器。该方收集了在该机构接受治疗的武装部队人员的医疗数据，随后对所有病患档案进行加密，导致医务人员无法获取档案。对于医疗机构运作中所访问、收集、处理并存储的数据，医疗机构享有的特别保护在何	

facilities and personnel, consider an ICT operation, in the context of an armed conflict, by a party to gain access to the servers of a medical facility in an adversary's territory. The party concerned collects medical data of members of the armed forces treated there, and then encrypts all patient files, making them unavailable to medical staff. To what extent does the specific protection of medical facilities encompass the confidentiality, integrity, and availability of the data they access, collect, process, and store for their operations? Similarly, how does such protection apply to the data accessed, collected, processed, and stored by humanitarian personnel and objects used for humanitarian operations? 3. What specific risks arise from ICT activities with respect to the prohibition of sexual violence and/or the unlawful recruitment or use of children in hostilities? What practical measures has your state adopted, or considered adopting, to prevent and respond to such unlawful acts?		种程度上适用于此类数据的保密性、完整性和可用性？ 同样，此类特别保护在何种程度上适用于由人道工作者和用于人道行动的物体所访问、收集、处理和存储的数据？ 6. 就禁止性暴力和/或禁止在敌对行动中非法征募或使用儿童兵而言，信通技术活动带来了哪些具体风险？贵国已采取或已考虑采取哪些实际措施，以防止并应对此类非法行为？	
Session 4: Safeguarding civilians, and others protected under IHL, against information spread in violation of IHL during armed conflict	15:00–16:00	**第 4 部分：武装冲突期间保护平民及其他受国际人道法保护人员免遭违反国际人道法的信息传播活动之害**	15:00–16:00
Guiding questions 1. What limits does IHL impose on the spread of information through ICT activities during armed conflict? Consider, for example, an information campaign by a		**引导性问题** 4. 对于武装冲突期间通过信通技术活动传播信息的行为，国际人道法对其施加了哪些限制？ 请思考：例如，假设武装冲突一方实施的信息活动包含下列内容：	

party to an armed conflict that entails:

- posting online images of prisoners of war and their treatment
- fabricating, and disseminating on social-media platforms, messages that inflame tensions between local communities, increasing the risk of violence.

What safeguards or oversight mechanisms has your state established, or considered establishing, to prevent ICT activities from exposing persons deprived of their liberty to public curiosity? And how does your state determine whether ICT-enabled information operations constitute prohibited incitement or encouragement of IHL violations, or spreading terror among the civilian population?

2. How does your state address the risk that ICT-enabled spreading of disinformation could obstruct medical services or humanitarian operations during armed conflict?

   Consider an online campaign circulating fabricated images and fake social-media posts that falsely claim that a hospital is a combatant stronghold. This disinformation provokes distrust in the local population and disrupts access for medical staff; in addition, staff entering the facility become the objects of growing incitement or intimidation. What IHL rules protect medical services and humanitarian operations against digital disinformation?

- 在网上发布战俘及其所受待遇的图片
- 在社交媒体平台上编造并传播激化当地社区之间紧张关系的信息，从而加剧暴力风险。

贵国已经设立或已经考虑设立哪些保障或监督机制，以防止信通技术活动将被剥夺自由者暴露于公众好奇心之下？贵国如何确定由信通技术支持的信息行动是否构成受禁止的煽动或鼓励违反国际人道法的行为，或构成在平民居民中散布恐怖？

5. 由信通技术支持的虚假信息传播活动可能会在武装冲突期间对医疗服务或人道行动造成阻碍，贵国如何应对此种风险？

   请思考：假设一项网络活动在网上传播伪造图像及虚假社交媒体帖文，谎称一家医院是战斗员据点。这一虚假信息引发了当地民众的不信任，并阻碍医务人员通行；此外，进入医院的工作人员还成为日益加剧的煽动或恐吓行为的对象。哪些国际人道法规则为医疗服务和人道行为提供保护，使其免受数字虚假信息的影响？贵国已经采取或已经考虑采取哪些法律或行动措施，以应对此类风险？

6. 贵国已经采取或已经考虑采取哪些其他措施，以防止利用信通技术（包括通过社交媒体）传播违反国际人道法的信息？

What legal or operational measures has your state adopted, or considered adopting, to address these risks? 3. What other measures has your state taken, or considered taking, to prevent the use of ICTs, including through social media, to spread information in violation of IHL?	
Coffee break	16:00–16:30

茶歇	16:00–16:30

Session 5: Addressing the risk of harm arising from the military use of civilian ICT infrastructure, and from the involvement of civilians in ICT activities, during armed conflict	16:30–17:30		**第 5 部分：武装冲突期间应对民用信通技术基础设施用于军事用途和平民参与信通技术活动所带来的伤害风险**	16:30–17:30	
Guiding questions 1. What are the human costs and the IHL implications of the military use of civilian ICT infrastructure, and what measures grounded in IHL need to be taken to mitigate the associated risks of harm to civilians and essential civilian services? Consider a commercial data centre, on the territory of a state party to an armed conflict, hosting military data and applications as well as data of civilian populations and applications used in the provision of essential civilian services. • How does your state apply IHL principles and rules such as distinction, proportionality and precautions when assessing an ICT operation against such ICT infrastructure? If a particular part of the ICT infrastructure, such as a cloud server, becomes a military objective, how should the effects on its civilian uses be considered when planning and conducting an ICT operation against it? • What precautionary measures can and should the state conducting the ICT operation take to protect civilian			**引导性问题** 4. 民用信通技术基础设施用于军事用途会带来哪些人类代价并对国际人道法及其适用带来何种影响？以及依据国际人道法需采取哪些措施来减轻对平民和基本民用服务的相关伤害风险？ 请思考：假设在参与武装冲突的一国领土上存在一个数据中心，该中心存有军事数据及军事应用程序，以及平民居民的数据和用于提供基本民用服务的应用程序。 • 在评估一项针对此类信通技术基础设施发动的信通技术行动时，贵国如何适用国际人道法原则和规则，例如区分原则、比例原则和预防措施原则？如果该信通技术基础设施的某一特定部分（例如云服务器）构成军事目标，那么在规划并实施对其发动的信通技术活动时，应如何评估对其民用用途产生的影响？ • 实施该信通技术行动的国家能够且应该采取哪些预防措施，以保护依赖被攻击的信通技术基础设施的平民居民以及基本民用服务？ • 数据中心所在国能够且应该采取哪些预防措施，以保护在其控制下的平民居民和民用物体，免受针对该数据中心的信通技术行动的影响？ • 拥有或运营数据中心的公司能够且应该采取哪些预防措施，以防止针对军事数据及应用程序的信通技术行动波及同设施内的民用数据？		

populations and essential civilian services relying on the ICT infrastructure being targeted? • What precautions can and should the state that is home to the data centre take to protect the civilian population and civilian objects under its control from the effects of ICT operations against the data centre? • What precautions can and should the company that owns or operates the data centre take to prevent civilian data from being affected by ICT operations directed against the military data and applications hosted in the same facility? 2. How might civilians be endangered by their involvement in ICT activities during armed conflict, and what measures grounded in IHL need to be taken to mitigate the risks to them? Consider civilian hackers on the territory of one of the belligerents conducting ICT operations, in the context of an armed conflict, that are designed to disrupt military communications or damage the ICT infrastructure of private companies, in order to weaken the enemy state's economy and lower morale among its people. • What legal obligations, under IHL, do civilian hackers have to fulfil when conducting any of these ICT operations?			5. 武装冲突期间参与信通技术活动的平民面临何种危险，以及依据国际人道法需要采取哪些措施来减轻此种风险？ 请思考：假设在武装冲突期间，位于交战一方领土上的平民黑客实施了信通技术行动，旨在破坏军事通信或损害私营企业的信通技术基础设施，以削弱敌国经济水平并打击国民士气。 • 依据国际人道法，平民黑客在实施任何此类信通技术行动时，须履行哪些法律义务？ • 受影响国家可以采取哪些措施，应对此类信通技术行动？ 6. 贵国已经采取或已经考虑采取哪些实际措施，以确保其管辖或控制下的平民（如实施与武装冲突相关的信通技术活动的平民黑客、黑客团体或技术公司员工）了解并遵守国际人道法，了解其行为的相关风险，并尽可能受到保护免受此类风险的影响？	
			总结发言	17:30–18:00

• What measures may the affected state take against these ICT operations? 3. What practical measures has your state taken, or considered taking, to ensure that civilians within its jurisdiction or under its control – such as civilian hackers, hacker groups or tech company employees conducting ICT activities related to an armed conflict – are aware of IHL and comply with it, and are aware of, and protected to the maximum extent possible against, the risks associated with their actions?			
Concluding remarks	17:30–18:00		