Le pouvoir de l'humanité
XXXIVe Conférence internationale
de la Croix-Rouge et du Croissant-Rouge
28-31 octobre 2024, Genève

Protéger les civils, ainsi que les autres personnes et biens protégés, contre les cyberopérations et les opérations d'information dans les situations de conflit armé

AVANT-PROJET DE RÉSOLUTION

Avril 2024

FR
34IC/24/DRX.X
Original : anglais
Projet

Document établi par le Comité international de la Croix-Rouge en consultation avec
la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge

AVANT-PROJET DE RÉSOLUTION

Protéger les civils, ainsi que les autres personnes et biens protégés, contre les cyberopérations et les opérations d'information dans les situations de conflit armé

La XXXIV[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge,

reconnaissant que nous vivons dans un monde de plus en plus numérisé et connecté, ce qui ouvre des perspectives dans les domaines économique, social, du développement ainsi que de l'information et de la communication, et peut contribuer à sauver des vies et à améliorer les conditions d'existence, y compris dans les situations de conflit armé,

soulignant l'importance des technologies de l'information et de la communication (ou technologies numériques) pour assurer la fourniture de services essentiels – en particulier de services médicaux et humanitaires – à la population civile, et pour permettre aux civils de savoir où trouver un lieu sûr ou des biens indispensables à leur survie ainsi que de rester en contact avec leurs proches, y compris dans les situations de conflit armé,

notant que des capacités numériques sont utilisées comme moyens ou méthodes de guerre dans les conflits armés actuels et qu'il est de plus en plus probable qu'elles soient utilisées de la sorte dans des conflits futurs,

notant avec inquiétude qu'une telle utilisation des capacités numériques dans les situations de conflit armé risque de causer des dommages aux civils et aux autres personnes et biens protégés, en particulier si les cyberopérations visent, ou touchent incidemment, des systèmes informatiques intégrés à des infrastructures civiles et des services essentiels ou utilisés par ces infrastructures et services,

reconnaissant que les États et les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge qui disposent de capacités numériques réduites peuvent être particulièrement vulnérables aux cyberopérations,

exprimant des inquiétudes face à l'ampleur, à la vitesse de propagation et à la portée de la désinformation et des discours de haine véhiculés au moyen des technologies numériques, ainsi que face aux différents dommages que ces opérations d'information risquent d'infliger aux personnes touchées par un conflit armé, notamment celles qui ont des besoins particuliers, comme les femmes, les enfants ou les personnes en situation de handicap,

notant que les technologies numériques sont utilisées pour permettre à des civils de mener ou de soutenir des cyberopérations ou des opérations d'information dans des situations de conflit armé, ou pour les encourager à mener ou à soutenir de telles opérations, et *s'inquiétant* de ce que les civils ne soient pas toujours au fait des risques encourus et des limites applicables à leur conduite,

rappelant que les entreprises privées du secteur de la technologie fournissent tout un éventail de produits, de services et d'infrastructures numériques dont dépendent les civils, les gouvernements et les organisations humanitaires, y compris dans les situations de conflit armé,

reconnaissant que les technologies numériques sont essentielles pour la conduite d'opérations humanitaires efficaces et efficientes, et *exprimant de vives inquiétudes* quant aux conséquences que les cyberopérations, notamment le piratage de données, et les opérations d'information conçues pour s'ingérer dans le travail des organisations humanitaires ou nuire à leur action risquent d'avoir sur ces dernières et sur leur personnel, perturbant la fourniture des services humanitaires aux personnes qu'elles s'efforcent d'aider,

rappelant la valeur juridique et protectrice des emblèmes et signaux distinctifs, le cas échéant, et *saluant* les recherches et consultations menées par le Comité international de la Croix-Rouge (CICR), en collaboration avec des établissements universitaires et d'autres composantes du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement), sur la finalité, les paramètres et la faisabilité d'un « emblème numérique[1] »,

réaffirmant la résolution 4 adoptée par la XXXIII[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale) et intitulée « Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles », et *soulignant* que les questions abordées dans cette résolution sont importantes également du point de vue de la protection des autres données humanitaires,

prenant note de la résolution 12 adoptée par le Conseil des Délégués de 2022 et intitulée « La protection des données humanitaires », et *saluant* les engagements pris par le Mouvement en ce qui concerne la protection de ses données humanitaires,

reconnaissant le travail accompli par les États dans le cadre du Groupe de travail de l'Organisation des Nations Unies à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), en particulier en relation avec le droit international,

réaffirmant la conviction qu'aucune disposition du droit international humanitaire (DIH) ne peut être interprétée comme légitimant ou autorisant tout acte d'agression ou tout autre emploi de la force incompatible avec la Charte des Nations Unies, et *soulignant* que le rappel des règles et principes du DIH ne légitime ni n'encourage en aucun cas les conflits,

soulignant le fait que les personnes, ainsi que les organisations médicales et humanitaires, risquent de subir des dommages également lorsque des cyberopérations ou des opérations d'information sont menées dans des situations d'urgence autres que des conflits armés, *appelant* les États à prendre appui sur cette résolution pour mettre en place des mesures efficaces visant à assurer leur protection conformément aux cadres juridiques applicables, et *demandant* au Mouvement de prendre des mesures appropriées pour assurer en tout temps la cybersécurité et la protection des données,

1. *exprime* la volonté commune à tous les membres de la Conférence internationale de protéger les civils ainsi que les autres personnes et biens protégés dans les situations de conflit armé, y compris contre les dangers résultant des cyberopérations et des opérations d'information ;

2. *rappelle* que le DIH s'applique uniquement aux situations de conflit armé, de même que les principes reconnus du droit international que sont l'humanité, la nécessité, la proportionnalité et la distinction, et *précise* que, même dans les situations de conflit armé, le DIH ne s'applique qu'aux actes ayant un lien avec le conflit ;

[1] Voir CICR, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions, 3 novembre 2022.

3. *reconnaît* la nécessité d'examiner plus avant de quelle manière et dans quelles circonstances ces principes s'appliquent à l'utilisation des technologies numériques, notamment aux cyberopérations et aux opérations d'information ;

4. *réitère* que, dans les situations de conflit armé, les règles et principes du DIH – notamment le principe de distinction, l'interdiction de lancer des attaques indiscriminées ou disproportionnées, l'obligation de veiller en permanence à éviter, ou du moins à réduire autant que possible, les dommages civils et de prendre toutes les précautions pratiquement possibles à cet effet, l'interdiction d'encourager les violations du DIH, et l'interdiction de répandre la terreur parmi la population civile – contribuent à protéger les civils ainsi que les autres personnes et biens protégés, notamment contre les dangers résultant des cyberopérations et des opérations d'information ;

5. *appelle* les parties aux conflits armés à respecter et protéger en toutes circonstances le personnel médical ainsi que les unités et moyens de transport sanitaires accomplissant exclusivement des tâches médicales, y compris lors de cyberopérations et d'opérations d'information qui pourraient indûment entraver leur mission médicale ;

6. *appelle* les États et les parties aux conflits armés à autoriser et faciliter, dans les situations de conflit armé, la conduite d'activités humanitaires impartiales, notamment celles reposant sur des technologies numériques, et à respecter et protéger le personnel et les biens humanitaires, y compris lors de cyberopérations et d'opérations d'information qui pourraient indûment entraver leur action humanitaire ;

7. *demande* aux États et aux parties aux conflits armés de s'acquitter des obligations qui leur incombent en période de conflit armé au titre du droit international de manière à assurer une protection efficace aux civils et aux autres personnes et biens protégés ;

8. *insiste* sur le fait que, dans les situations de conflit armé, les acteurs non étatiques doivent se conformer aux règles applicables du droit interne et du droit international qui protègent les civils ainsi que les autres personnes et biens protégés, et *appelle* les États à diffuser ces règles aussi largement que possible sur leur territoire, ainsi qu'à poursuivre et sanctionner les auteurs d'éventuelles violations ;

9. *encourage* toutes les composantes du Mouvement à tenir compte des dommages que les cyberopérations et les opérations d'information peuvent causer aux civils ainsi qu'aux autres personnes et biens protégés, *demande instamment* à toutes les composantes de renforcer leur préparation et leur capacité à faire face aux risques liés à ces opérations, par exemple en améliorant leur capacité à détecter ces risques et à déployer des activités de protection en faveur des populations affectées, et *invite* les États à soutenir le Mouvement dans ces efforts ;

10. *encourage* les États et les composantes du Mouvement à discuter avec les entreprises privées du secteur de la technologie des implications qu'a, au regard du droit interne et du droit international, la prestation de services numériques dans les situations de conflit armé, et à établir un dialogue avec ces entreprises pour s'assurer que leurs politiques sont conformes au droit applicable dans les situations de conflit armé, que leur personnel respecte ses obligations juridiques, et qu'elles ont mis en place des mesures appropriées pour protéger leur personnel et leurs clients civils contre d'éventuels dommages ;

11. *se félicite* des résultats des recherches et des tests en cours autour d'un emblème numérique, et *encourage* le CICR à poursuivre ses recherches et ses tests, en consultation avec les États et les composantes du Mouvement, afin d'établir plus précisément la finalité spécifique et la faisabilité technique d'un tel emblème, ainsi qu'à

mener des consultations avec les États sur les procédures qui devraient être mises en place pour l'intégrer dans le droit international ;

12. *engage* les composantes du Mouvement à prendre des mesures appropriées, dans les limites de leurs mandats, possibilités et besoins opérationnels respectifs, pour renforcer leur capacité à assurer un niveau adéquat de cybersécurité et de protection des données, conformément à la résolution 12 adoptée par le Conseil des Délégués de 2022 et intitulée « La protection des données humanitaires », et *invite* les États à soutenir le Mouvement dans ces efforts ;

13. *rappelle* que les composantes du Mouvement doivent traiter des données personnelles pour pouvoir s'acquitter de leurs mandats, notamment au titre du DIH, lorsqu'il s'applique, et des Statuts du Mouvement, et que ce traitement est nécessaire et justifié par des motifs importants d'intérêt public ainsi que par les intérêts vitaux des personnes concernées, et *engage instamment* les États et le Mouvement à coopérer pour veiller à ce que ces données ne soient pas sollicitées ni utilisées à des fins incompatibles avec la nature humanitaire de l'action du Mouvement ou d'une manière susceptible de nuire à la confiance des personnes auxquelles il vient en aide ou à l'indépendance, l'impartialité et la neutralité de ses opérations ;

14. *encourage* les composantes du Mouvement à échanger connaissances et meilleures pratiques sur la cybersécurité, la protection des données, le droit international et la protection des civils, ainsi que des autres personnes et biens protégés, contre les dangers résultant des cyberopérations et des opérations d'information, en tenant compte des disparités qui existent au niveau des ressources dont disposent les composantes du Mouvement, et *invite* les États à soutenir ces activités.