DROIT & POLITIQUES HUMANITAIRES

Les menaces numériques dans les conflits armés : ce qui nous échappe et comment y remédier

octobre 2, 2023, Action humanitaire / Analysis / Artificial Intelligence and Armed Conflict / Cyber / Nouvelles technologies / Technology in Humanitarian Action

22 minutes de lecture

Joelle Rizk
Conseillère sur les menaces numériques, CICR

Sean Cordey
Chercheur sur les menaces numériques, CICR

Le développement et le recours à de nouvelles technologies numériques dans les conflits contemporains — des technologies de l'information aux cyberopérations, créent de nouvelles menaces et accroissent les risques qui existent déjà, de porter atteinte aux droits, à la vie, à la sécurité, à la dignité et à la résilience des populations civiles. À l'ère du numérique, la bonne compréhension de ces menaces est au cœur des activités de protection.

Dans ce billet, Joelle Rizk, conseillère du CICR sur les menaces numériques et Sean Cordey, chercheur sur les menaces numériques, mettent en exergue certaines des principales préoccupations relatives à la protection à l'ère du numérique et proposent la voie à suivre pour que les acteurs de la protection soient mieux préparés à répondre à ces défis.

La protection humanitaire se définit comme les mesures que les acteurs humanitaires mettent en place en période de conflit armé et dans d'autres situations de violence pour protéger la vie, la sécurité et la dignité des populations civiles. Dans cet objectif, les acteurs humanitaires et d'autres acteurs mènent des activités de protection afin de veiller à ce que les autorités et d'autres acteurs respectent leurs obligations et les droits des personnes, *conformément à la lettre et l'esprit des corpus de droits pertinents*. Ces activités visent à prévenir ou *mettre un terme aux violations manifestes ou alléguées* et à faire face à leurs conséquences. Le but fondamental des activités de protection est de limiter l'exposition aux risques et réduire les vulnérabilités par une aide matérielle et humanitaire, en soutenant

des mesures d'autoprotection, en sensibilisant aux risques et en fournissant les informations appropriées, etc. Les activités de protection nécessitent d'évaluer en permanence les risques auxquels les populations sont confrontées dans de telles situations.

Les activités de protection doivent constamment s'ajuster aux réalités versatiles des conflits, notamment au développement de nouvelles technologies qui façonnent la guerre. Dans une situation de conflit armé, l'emploi de nouvelles technologies numériques par divers acteurs – qu'il s'agisse d'États, d'acteurs non étatiques, de groupes criminels ou de sociétés privées (ci-après qualifiés d'acteurs des conflits), pour conduire des opérations cybernétiques et numériques, est l'une des évolutions contemporaines les plus importantes dans les conflits armés. S'il est rare que les opérations cybernétiques et numériques se *déroulent dans un contexte de vide juridique*, les *circonstances* prévues et attendues de l'emploi de technologies numériques qui sont susceptibles de faire peser de multiples risques, que l'on appelle les menaces numériques, sur la vie, la sécurité, la dignité et la résilience des populations civiles. Elles ont des conséquences néfastes qui viennent souvent s'ajouter aux ~~les~~ souffrances que des opérations cinétiques causent aux populations civiles.

La compréhension de l'ampleur des menaces numériques sur les civils dans un conflit fait encore défaut dans la réponse humanitaire. Il est donc urgent de documenter, évaluer et mieux comprendre la manière dont les nouvelles technologies numériques sont utilisées et les dommages qu'elles causent aussi bien dans la réalité physique que numérique. Actuellement, les menaces numériques peuvent être divisées en trois grandes catégories. Seules les deux dernières seront examinées dans cet article :

- Premièrement, les menaces numériques relatives à l'emploi de technologies numériques par des acteurs humanitaires à l'appui de leurs activités humanitaires et de protection, telles que l'utilisation de la biométrie;
- Deuxièmement, celles relatives à l'emploi de technologies numériques par des acteurs armés en complément d'opérations cinétiques ou indépendamment de celles-ci, par exemple des opérations d'information, des cyberopérations visant des populations ou des *infrastructures civiles*, ou un *usage abusif des données personnelles ou à caractère humanitaire*.
- Et troisièmement, celles qui visent à reprogrammer ou faire un double usage de technologies et d'infrastructures, permettant à des civils de *participer* à des actes en lien avec le conflit, tels que la *surveillance*, la collecte de renseignements ou encore des opérations d'information ou cybernétiques.

Ces technologies numériques et ces comportements peuvent avoir une influence transversale sur certains droits qu'ils restreignent, tels que la *liberté d'expression*, de *réunion* ou de *mouvement*, la *liberté et la sûreté*, *l'identité personnelle* et la *vie privée*. Toutefois, les plus préoccupants au regard de l'action conduite par le CICR dans les situations de conflit, sont ceux qui ont des conséquences néfastes sur la vie, la sécurité et l'intégrité physique et psychologique des populations affectées ainsi que sur leur dignité ; leur capacité à se protéger et à être résilients ; leurs moyens de subsistance ; et leur accès aux services humanitaires essentiels.

Si les acteurs humanitaires et les acteurs de la protection s'intéressent de plus en plus aux nouvelles technologies numériques en appui à leurs activités humanitaires et de protection ainsi que pour renforcer l'agentivité des personnes affectées par les conflits, leur objectif est de *ne pas nuire*. Cela est particulièrement vrai lorsque le développement de *technologies numériques dans le secteur humanitaire* dans les situations de conflit risque d'engendrer et d'exacerber des menaces qui peuvent, à leur tour, restreindre les droits fondamentaux des civils et saper leur confiance en l'action humanitaire. Ces menaces peuvent également engendrer *différents types de dommages*. Cet article porte sur le comportement et les modes d'action habituels des acteurs des conflits et non sur le comportement et le recours à des technologies numériques par des acteurs de la protection.

La « protection » à l'ère du numérique

Sans minimiser l'impact positif que les technologies peuvent avoir dans un conflit, lesquelles permettent notamment d'améliorer l'accès à des informations qui peuvent sauver des vies et limiter les dommages collatéraux, les activités de protection doivent, à l'ère du numérique, tenir compte des menaces. En d'autres termes, elles doivent intégrer la protection des droits des personnes lorsque leurs vies interagissent avec le monde numérique. Par exemple, en vertu du droit international humanitaire (DIH), les populations et les biens civils ne doivent pas être attaqués pendant un conflit armé, une obligation qui s'applique aux cyberopérations de la même manière qu'aux opérations numériques.

Au regard de la protection, les menaces numériques peuvent donc être en lien avec la protection des données ou d'autres ressources numériques, mais ne se limitent pas à ces questions. Elles portent aussi sur l'emploi de technologies numériques en période de conflit armé et sur la manière dont leur utilisation expose les civils à un risque, porte atteinte à leurs droits, leur sécurité et leur dignité (par exemple, l'emploi d'un *logiciel espion contre les civils*), y compris lorsqu'un usage abusif ou une violation se produisent exclusivement en ligne (comme c'est le cas des *discours de haine*). Autrement dit, il s'agit de toute menace déclenchée ou renforcée par des technologies numériques, qu'elle soit matérielle (par exemple, une menace sur des systèmes de soutien comme les satellites), logique ou informationnelle. En d'autres termes, les activités de protection devraient s'étendre aux violations et comportements issus d'interactions entre des êtres humains, entre des êtres humains et des machines et entre les machines (comme les cyberattaques qui *visent des civils ou une infrastructure à double-usage*).

L'exposition au risque et les préoccupations au regard de la protection

La protection à l'ère du numérique ne veut pas dire que les préoccupations au regard de la protection soient nouvelles. Toutefois, l'une de leurs particularités tient au fait que les préoccupations relatives à la protection face au numérique peuvent être moins visibles, moins tangibles, moins comprises (en particulier par les personnes affectées) et moins rapportées. De plus, en raison de la possible étendue des attaques ~~et~~ de la primauté des vulnérabilités, les menaces numériques peuvent *s'intensifier rapidement* et avoir des conséquences d'une vaste portée. Elles peuvent également évoluer au fur et à mesure que les technologies et les pratiques numériques progressent, susceptibles d'engendrer de nouvelles menaces et des risques imprévisibles que les acteurs de la protection doivent surveiller.

Les informations nuisibles en ligne

La diffusion d'informations nuisibles, comme la mésinformation, la désinformation et les discours de haine (MDH), peuvent *alimenter le conflit* et *compromettre* la sécurité et la dignité des populations. Les média et les plateformes d'information en ligne ont amplifié l'ampleur, l'étendue et la rapidité de la diffusion des MDH. Les systèmes d'information et de communication sont mis à profit par des *États* et des acteurs non étatiques pour exercer une influence, changer les comportements et atteindre des objectifs opérationnels. Dans cet environnement, les narratifs peuvent contribuer ou inciter à commettre des actes de violence contre des *personnes*, provoquer des souffrances ciblées et *psychologiques* à long-terme, mais aussi accentuer des vulnérabilités en raison de discriminations, d'une stigmatisation, empêcher l'accès à des services essentiels, compromettre une prise de conscience de la situation et des mesures d'autoprotection et perturber ou limiter les *opérations* des *acteurs de protection*. Le risque est d'autant plus grand que l'accès au contenu généré par des IA est aisé. En même temps, la manière dont les outils de la communication numérique ont été utilisés peuvent constituer des violations de certains droits et obligations, à l'instar de leur utilisation pour diffuser des informations nuisibles, en violation de l'interdiction de *recruter des enfants* ou de celle *d'exposer des prisonniers de guerre* à la *curiosité publique*.

Les activités cybernétiques qui visent des civils

Les civils sont également la cible directe d'activités cybernétiques qui peuvent être néfastes à leur bien-être et restreindre leurs droits. Par exemple, le développement de *logiciels espions* visant des civils peuvent conduire à un usage abusif des données personnelles *au détriment des individus* et peuvent avoir une influence plus large sur le conflit. Parallèlement, les populations déjà vulnérables en raison des conflits, comme les réfugiés en raison d'un conflit ou les personnes *déplacées*, pourraient être victimes d'une attaque en ligne par des acteurs criminels ou malveillants, ce qui pose la question du vol de l'identité, la fraude ou l'*escroquerie*.

Les cyberopérations visant des infrastructures civiles

Les acteurs des conflits mobilisent des moyens cybernétiques, tels que des *rançongiciels, des DDoS ou des wipers*, pour perturber ou empêcher le fonctionnement d'infrastructures civiles et de services essentiels, par exemple l'électricité, l'eau ou la santé, la gouvernance ou les services financiers. Ces opérations peuvent avoir un *coût humain* préoccupant et des conséquences humanitaires potentiellement *catastrophiques*, en portant atteinte à l'efficacité de la délivrance de services essentiels à des populations affectées par des crises, provoquant ainsi des dommages socio-économiques, sociétaux, *psychologique*s, voire entrainer la mort. Lorsque des cyberopérations visent des infrastructures à double-usage telles que des satellites, elles peuvent causer des dommages incidents dans la population civile.

L'usage abusif et la mauvaise gestion des données

Le développement et l'utilisation de technologies fondées sur les données, tels les capteurs, l'analyse prédictive et le *traitement de données biométriques*, posent toute une série de questions au regard des droits, de la sécurité et de la dignité des populations affectées par des crises. Par exemple, lorsqu'elles sont interceptées, notamment en passant par des demandes d'accès de prestataires tiers, le *piratage* ou la *fuite*, les données à caractère humanitaire peuvent être utilisées de manière abusive dans un objectif qui n'est pas humanitaire, comme à des fins de *maintien de l'ordre*, d'arrestations et de surveillance aux frontières. En même temps, les données personnelles et privées permettant d'identifier les personnes affectées, en particulier celles relatives à leur usage personnel de technologies numériques (par exemple, les réseaux sociaux) peuvent être utilisées pour les identifier et les attaquer (par exemple, par la désinformation, les escroqueries ou la violence).

Les données, l'IA et la prise de décision

Les acteurs des conflits intègrent des « systèmes d'aide à la décision » automatisés et fondés sur l'IA dans leur conduite de la guerre. Ce sont des outils logiciels qui fournissent des *analyses*, des *recommandations* et même des *prévisions* pour les décideurs militaires. Ceux-ci pourraient être utilisés à l'appui de toute une série de décisions militaires, à tous les niveaux de la chaine de commandement, par exemple pour « évaluer la menace » et identifier des cibles, ou de décisions relatives à la manière de conduire une opération militaire ou de toute autre décision qui a des conséquences sur les droits des populations comme la détention par exemple. Leur emploi est source de préoccupation, au regard, non seulement des moyens propres à garantir un contrôle humain, tant juridique que sur l'opération, mais aussi sur la capacité des utilisateurs à expliquer ces décisions et à les remettre en question, sans faire entièrement confiance à ces systèmes pilotés par des IA. D'autres craintes sont relatives à la transparence, aux possibles erreurs et biais de ces systèmes, à la non-discrimination de leurs attaques, mais aussi aux dommages qu'ils peuvent causer en raison d'attaques disproportionnées, lesquelles peuvent avoir des conséquences sur la vie, la dignité et les droits des personnes.

La perturbation des opérations humanitaires

Les opérations humanitaires sont de plus en plus *perturbées* par technologies numériques, qu'il s'agisse de campagnes d'information qui attaquent leur intégrité et leur neutralité, ~~ou~~ de *cyberopérations* ou de *piratages des données*. Cela peut avoir un impact sur la capacité d'action des acteurs humanitaires, leur accès aux populations affectées, la coordination avec d'autres acteurs, l'évaluation des besoins et la délivrance d'une aide aux populations affectées. Ceci peut également avoir des conséquences négatives sur la sécurité des personnes et sur la *confiance* qu'elles placent dans les acteurs et les opérations humanitaires. Par ailleurs, cela met en danger le *personnel humanitaire et en charge de l'aide*.

La perturbation de la connectivité des personnes

La perturbation de l'accès à internet et aux infrastructures de communication est une *pratique* de plus en plus répandue qui est employée par les acteurs des conflits pour contrôler l'information et / ou porter des objectifs politiques ou militaires. De telles pannes peuvent engendrer ou accentuer des conséquences humanitaires pour ceux qui se trouvent sur le terrain, dont certaines sont susceptibles de mettre en danger la vie des personnes. Par exemple, non seulement elles restreignent l'accès des personnes affectées par des crises à des informations essentielles pour survivre (par exemple, les humanitaires, la nourriture, des

abris, des *soins médicaux*) mais elles pourraient aussi accroitre le *risque de séparation* en raison de l'importance de la connectivité pour maintenir les liens familiaux et les restaurer. Parallèlement, elles peuvent aussi compromettre la résilience des civils et leur sensibilisation aux risques dans les situations de conflit, mais aussi leur capacité à se protéger, à *bénéficier d'opportunités économiques*, à parler et se réunir en toute liberté.

La participation de civils

La participation de plus en plus importante de civils et de *entreprises privées* aux actions sur le champ de bataille numérique peut non seulement porter atteinte aux individus, mais aussi porter atteinte au principe de *distinction* entre civils et combattants. En effet, les civils pourraient apporter un soutien direct aux acteurs des conflits, en participant à la *collecte de renseignements* militaires (par exemple, au moyen d'applications reprogrammées), en soutenant la cyberdéfense d'un belligérant ou en participant à des *cyberopérations* contre des objectifs ennemis, y compris contre d'autres objectifs, civils. Cette participation peut exposer les civils à de graves dommages : ils peuvent être attaqués par des militaires, leurs habitations peuvent être détruites, ils peuvent être détenus, voire *tués*. Cela peut aussi entrainer de fausses accusations et des soupçons qui causent d'autres préjudices.

Planification et activités de protection à l'ère du numérique

Tandis que les préoccupations au regard de la protection à l'ère du numérique continuent de gagner de l'ampleur, les acteurs humanitaires ont encore un long chemin à parcourir pour décortiquer les limites et les menaces des technologies numériques. L'interaction entre ce qui se trouve en ligne et ce qui est hors-ligne dans les conflits et les conséquences humanitaires qui en résultent, nécessitera que les humanitaires adaptent leurs savoir-faire, leurs méthodes et leurs approches, à différents égards :

1. Mettre en place un dialogue et des cadres de protection

Les guerres ont des limites, même dans l'espace numérique. Les activités de protection à l'ère du numérique doivent donc prendre en compte et si possible développer ces cadres de protection afin de protéger les droits, la sécurité et la dignité des personnes affectées par un conflit : que ce soit en poursuivant leur développement, en les faisant connaitre ou en dialoguant avec les États pour les promouvoir et les mettre en œuvre.

Les acteurs non étatiques tels que les entreprises de la tech et les cybergroupes sont devenus des parties prenantes dans les conflits armés et les opérations, ce qui ne fait qu'accroitre les menaces auxquelles sont confrontés les civils et les autres personnes protégées. Le dialogue avec les acteurs qui gravitent dans cet environnement devrait être favorisé. Parmi les sujets à aborder, on peut citer ceux relatifs à la gouvernance, à la prévention des dommages et des dommages causés incidemment, au respect du DIH et à la distinction entre des objectifs civils et militaires, à la coopération dans la délivrance et le renforcement des activités de protection, à des technologies fondées sur des principes et sur l'humain, *etc.* Ces questions pourraient reposer et se fonder sur des cadres protecteurs existants, tels que les *Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations Unies*. Parallèlement, le dialogue avec les États pourrait permettre de leur rappeler leurs obligations de s'assurer que *les entreprises privées respectent les règles du DIH* et du droit international des droits de l'homme.

Enfin et concomitamment, puisque les humanitaires recueillent des données personnelles et des données sensibles, il est indispensable qu'ils intègrent à leurs activités pratiques et des cadres relatifs à la protection des données. Ces pratiques peuvent consister à minimiser les données, à évaluer l'impact de la protection des données, à assurer la protection des données dès la conception et en prenant en compte les droits de la personne à laquelle elles appartiennent. Il faut saluer le fait qu'un travail considérable a déjà été réalisé ces dernières années pour un usage responsable des technologies et des données dans le secteur humanitaire. On peut citer le *manuel du CICR sur la protection des données*, la *Gestion de l'information relative à la protection* (PIM) ou les *Standards professionnels pour les activités de protection*.

2. Renforcer la résilience

Aujourd'hui, on a l'occasion d'introduire la culture numérique et des programmes et formations sur la sensibilisation aux risques numériques dans les activités de protection existantes, tant pour les populations affectées que pour les professionnels de l'humanitaire. Ces initiatives ne doivent pas, toutefois, aboutir à reporter le poids de la responsabilité sur les populations affectées. Tandis que de plus en plus d'organisations et d'acteurs privés recourent à des moyens de haute technologie et ouvrent la voie à la culture numérique et à la sensibilisation, il est important que les acteurs humanitaires et les acteurs de la protection aient une approche prudente, qui tienne compte des risques d'exclure des pans de la population ou des groupes, en instaurant *un faux sentiment de sécurité* et plus important encore, en faisant porter le poids de la responsabilité sur les plus vulnérables.

3. Renforcer les compétences

La sensibilisation aux risques au sein du secteur humanitaire reste parcellaire. Il y a un *fossé* considérable entre la compréhension et la connaissance du paysage des menaces numériques et des risques pour les populations affectées qui y sont associés et les comportements de divers acteurs dans des situations de conflit. Ainsi, les instruments permettant d'évaluer les menaces numériques devraient être élaborés et intégrés dans les activités de protection. De la même manière, les humanitaires devront *continuer* de renforcer leur coopération avec des experts universitaires, militaires et des spécialistes de la haute technologie pour disposer en temps opportun d'une réponse et d'une analyse d'ensemble de la protection, fondées sur des éléments probants.

De plus, pour mieux détecter, évaluer et réduire les menaces numériques, les acteurs de la protection devront élargir leurs connaissances pour se fonder sur des approches hybrides qui combinent des approches traditionnelles et de nouveaux outils. Cela inclut notamment une plus grande mobilisation et une meilleure intégration des informations en libre accès et une analyse des réseaux sociaux, lesquels peuvent fournir à la fois une plus grande visibilité et des éléments probants pour améliorer les activités de protection, ce qui va de la surveillance des incidents pour alimenter le dialogue relatif à la protection à une conception de la protection et du dialogue fondée sur les populations. Les acteurs de la protection devraient aussi être formés et soutenus pour être capables de prendre

conscience des conséquences des opérations numériques et des cyberopérations dans un conflit et de les signaler. Cela implique de dialoguer avec les populations, qui interagissent avec les technologies numériques dans leur vie quotidienne.

***

À l'ère du numérique, l'accroissement des *menaces numériques* aggravées par des informations nuisibles en ligne, des opérations de cyberdéfense, l'automatisation de systèmes militaires, l'usage abusif de données personnelles et humanitaires, des coupures de la connectivité ou la participation croissante de civils aux conflits *via* des moyens numériques, est une réalité des conflits. Leurs conséquences sur les droits, la sécurité, la dignité et la résilience des populations affectées par un conflit, sont une préoccupation qui ne peut être ignorée.

Alors que d'importants défis se posent au regard, par exemple, de la culture numérique, de la sensibilisation aux risques et de la capacité à générer des preuves des dommages engendrés, les acteurs de protection doivent s'employer à développer les cadres politiques et juridiques protecteurs en vigueur (y compris les cadres relatifs à la protection des données) ; instaurer un dialogue sur la protection contre les menaces numériques ; renforcer la résilience des populations affectées, par exemple par la sensibilisation et l'éducation aux risques ; construire leur propre expertise et renforcer leurs compétences pour détecter les risques et prévenir les dommages qui en découlent, ou y répondre.

Dans cet environnement numérique qui évolue rapidement, il est primordial de préserver l'espace humanitaire et une approche centrée sur la protection. Si les humanitaires continuent de décortiquer ce que cela implique pour leurs activités respectives, il est important de ne pas réinventer l'humanitaire, mais plutôt d'adapter les programmes existants. Répondre aux menaces numériques n'est pas « plaisant », mais il s'agit d'un impératif éthique et professionnel pour les humanitaires.

Cet article a été initialement publié en anglais le 27 juillet 2023.

Voir aussi :

- Tilman Rodenhäuser, Mauro Vignati, « *Vers un emblème numérique ? Cinq questions sur les enjeux juridiques, technologiques et politiques liés à une telle innovation* », 12 décembre 2023

Tags: action humanitaire, AI, conflit armé, cyber, cyberguerre, cyberwarfare, digital, digitalrisk, DIH, IA, intelligence artificielle, menaces numériques, numérique, protection

Ceci pourrait vous intéresser

De la désillusion à une culture universelle du respect du droit international humanitaire : l'enseignement du DIH « 2.0 »

17 minutes de lecture

Action humanitaire / Analysis / Artificial Intelligence and Armed Conflict / Cyber / Nouvelles technologies / Technology in Humanitarian Action

Etienne Kuster, Catherine Gribbin, Jonathan Somer & Charlotte Tocchio

L'opinion publique jouant un rôle essentiel dans la façon dont les décisions sont prises pendant ...

Au-dessus des décombres : la guerre en milieu urbain affecte les enfants, huit aspects négligés

20 minutes de lecture

Action humanitaire / Analysis / Artificial Intelligence and Armed Conflict / Cyber / Nouvelles technologies / Technology in Humanitarian Action

Dans les villes de Gaza, du Soudan et de l'Ukraine, les guerres en milieu urbain ...