MASTER 2 SECURITE INTERNATIONALE,
CYBERSECURITE ET DEFENSE

Sujet de mémoire : L'utilisation des nouvelles technologies (cyberattaques, drones, intelligence artificielle) au prisme du respect du jus contra bellum et du jus in bello dans le conflit russo-ukrainien.

Yessine Mhiri

Dirigé par : Pr. Thierry Garcia

Année 2024 – 2025

BIBLIOGRAPHIE

I. Ouvrages

- CROIZET FONTANE (R.), *Le cyberespace dans la guerre d'Ukraine : enseignements d'une nouvelle ère de conflictualité numérique*, Paris, Édit. IEGA / DGRIS, 30 janvier 2025, 48 p.
- DESPAIRIES (B.), *Les drones aériens dans la guerre russo-ukrainienne : missions, limites et enseignements*, Paris, L'Harmattan, 2023, 221 p.
- PEJIC (J.), « Le ciblage extraterritorial au moyen des drones armés : quelques conséquences juridiques », *Revue internationale de la Croix-Rouge*, vol. 96, 2014, 101 p.
- ROSCINI (M.), *Cyber Operations and the Use of Force in International Law*, Oxford, Oxford University Press, 2014, 307 p.
- SCHMITT (M.N.) (éd.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013, 282 p.
- SCHMITT (M.N.) (éd.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017, 598 p.

II. Articles

- BANNELIER (K.), "Obligations de diligence dans le cyberespace : qui a peur de la Cyber-diligence?", *RBDI*, 2018.
- BANNELIER (K.), "Rien que la *Lex Lata* ? Etude critique du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations", *AFDI*, 2018.
- BANNELIER (K.), « *Is the Principle of Distinction Still Relevant in Cyberwarfare? From Doctrinal Discourse to States' Practice* », in TSAGOURIAS (N.) & BUCHAN (R.) (dir.), *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 2021, pp. 427-456.
- BANNELIER (K.), CHRISTAKIS (T.), *Cyberattaques – Prévention–Réactions : Rôles des États et des acteurs privés*, Les Cahiers de la Revue Défense Nationale, Paris, 2017, 92 p.
- BANNELIER-CHRISTAKIS (Karine), *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?*, *Baltic Yearbook of International Law*, vol. 14, 2014, pp. 1–15.
- BOYLE (Michael J.), « The Costs and Consequences of Drone Warfare », *International Affairs*, vol. 89, n° 1, janvier 2013, p. 22.

- BUCHAN (R.), « Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? », *Journal of Conflict & Security Law*, Vol. 17, n° 2, 2012, pp. 211-228.
- FÉREY (A.), ROUCY-ROCHEGONDE (L.), *De l'Ukraine à Gaza : l'Intelligence artificielle en guerre*, édit. IFRI, *Politique étrangère*, vol. 89, n° 3, automne 2024, pp. 39-50.
- HOLLIS (D.), « An e-SOS for Cyberspace », *Harvard International Law Journal*, Vol. 52, 2011, pp. 373-432.
- IVANOV (E.), « Combating Cyberterrorism under International Law », *Baltic Yearbook of International Law*, Vol. 14, 2014, pp. 23-39.
- KOZIK (A.), « The Concept of Sovereignty as a Foundation for Determining the Legality of the Conduct of States in Cyberspace », *Baltic Yearbook of International Law*, Vol. 14, 2014, pp. 93-103.
- O'CONNELL (M.), « Cyber Security without Cyber War », *Journal of Conflict & Security Law*, Vol. 17, n° 2, 2012, pp. 187-201.
- REUCHERON (G.), *L'emploi des drones dans la guerre en Ukraine*, La note du CESA, 2022. https://operationnels.com/wp-content/uploads/2022/05/Note-CESA-emploi-des-drones-en-Ukraine.pdf
- SCHMITT (M.), « Classification of Cyber Conflict », *Journal of Conflict & Security Law*, Vol. 17, n° 2, 2012, pp. 245-260.
- SCHMITT (M.), PITTS (C.), « Cyber Countermeasures and Effects on Third Parties: The International Legal Regime », *Baltic Yearbook of International Law*, Vol. 14, 2014, pp. 1-21.
- TSAGOURIAS (N.), « Cyber-attacks, self-defence and the problem of attribution », *Journal of Conflict & Security Law*, Vol. 17, n° 2, 2012, pp. 229-244.
- TURNS (D.), « Cyber Warfare and the Notion of Direct Participation in Hostilities », *Journal of Conflict & Security Law*, Vol. 17, n° 2, 2012, pp. 279-297.
- WATTS (S.), « Low-Intensity Cyber Operations and the Principle of Non-Intervention », *Baltic Yearbook of International Law*, Vol. 14, 2014, pp. 137-161.

III. Documents officiels

- Assemblée nationale. « Compte rendu n°27 : Commission de la défense nationale et des forces armées », 7 décembre 2022.

https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2223027_compte-rendu

- Charte des Nations Unies, 24 octobre 1945,1 RTNU XVI
- CICR/ICRC, expert meeting, autonomous weapon systems technical, military, legal and humanitarian aspects, mars 2014, 91 p.
- CICR/ICRC, Position paper, International humanitarian law and cyber operations during armed conflicts, November 28, 2019, https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl_and_cyber_operations_during_armed_conflict_fr.pdf
- Commission du droit international, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, novembre 2001, Supplément n° 10, doc. ONU A/56/10, novembre 2001
- CONSEIL DE L'EUROPE, Convention sur la cybercriminalité, Budapest, 2001, https://rm.coe.int/168008156d
- « ENISA Threat Landscape 2023 », 19 octobre 2023. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
- « ENISA Threat Landscape 2024 », 19 septembre 2024. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
- FRANCE, ministère des Armées, Droit international appliqué aux opérations dans le cyberespace, 2019 (https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf)
- FRANCE, SGDSN, Revue Stratégique de cyberdéfense (2018), http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
- FRANCE, Stratégie internationale de la France pour le numérique (2017), (https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/strategie-internationale-de-la-france-pour-le-numerique/)
- « Microsoft Digital Defense Report 2024 ». Microsoft Threat Intelligence Report, 2024.
- ONU, Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, Projet de convention des Nations Unies contre la cybercriminalité

Renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication de preuves sous forme électronique d'infractions graves, 7 août 2024, A/AC.291/L.15.

- ONU, Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale), Rapport de 2015, Note du Secrétaire général, A/70/174, 22 juillet 2015 (site ONU) https://documents.un.org/doc/undoc/gen/v24/055/07/pdf/v2405507.pdf
- ONU, Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, March 10, 2021 (11 p.) https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
- Projet de convention des Nations Unies contre la cybercriminalité, Assemblée générale de l'ONU 7 aout 2024

IV. Jurisprudence

- CIJ, Affaire des activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda), Arrêt du 19 décembre 2005, CIJ Recueil 2005.
- CIJ, Affaire du Détroit de Corfou, Arrêt du 4 avril 1949, CIJ Recueil 1949.
- CIJ, Affaire du personnel diplomatique et consulaire des États-Unis à Téhéran (États-Unis c. Iran), Arrêt du 24 mai 1980, CIJ Recueil 1980.
- CIJ, Affaire relative à l'application de la convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro), Arrêt du 26 février 2007, Recueil CIJ 2007.
- CIJ, Activités militaires et paramilitaires au Nicaragua et contre celui-ci, Arrêt du 27 juin 1986, Rec. 1986.
- CIJ, Avis consultatif du 8 juillet 1996, Licéité de la menace ou de l'emploi des armes nucléaires.
- CIJ, Avis consultatif du 9 juillet 2004, Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé.

INTRODUCTION

L'art de la guerre n'a jamais cessé d'évoluer au fil du temps en adaptant en permanence ses moyens de combat aux exigences stratégiques de chaque époque. De l'Antiquité à l'âge classique, la confrontation directe prédominait, et les combats reposaient principalement sur les capacités physiques individuelles, avec l'épée, la lance ou l'arc comme armes essentielles. La fin du Moyen Âge constitue un tournant avec l'invention de la poudre à canon, engendrant une militarisation accrue des sociétés européennes et marquant l'essor de l'artillerie et des armes à feu. Le XXe siècle marque un une nouvelle étape, celle de l'industrialisation de la guerre et de ses moyens. Les deux conflits mondiaux ont accéléré cette transformation avec un renforcement massif des armées et des technologies. L'introduction généralisée des chars, le développement massif de l'aviation militaire, l'importance stratégique prise par les flottes navales modernes et l'usage intensif de l'artillerie lourde bouleversent totalement la façon de faire la guerre, causant des pertes humaines inédites (plus de 20 millions pour la Première Guerre mondiale et environ 60 millions pour la Seconde). Cette escalade technologique atteint son point culminant avec l'arme nucléaire, utilisée en 1945 à Hiroshima et Nagasaki. Dès lors, la victoire militaire cesse d'être le seul objectif : la dissuasion nucléaire devient centrale, fondée sur la menace d'une destruction totale et mutuelle. Ainsi, la guerre peut potentiellement entraîner l'anéantissement de civilisations entières. Avec le XXI^{e} siècle apparaît une nouvelle forme de rupture stratégique. Ce ne sont plus seulement la puissance de feu et l'effet destructeur direct qui définissent l'évolution des armes, mais leur caractère immatériel, autonome et invisible. L'émergence des cyberattaques, des drones armés et de l'intelligence artificielle bouleverse encore une fois le champ de bataille. Désormais, la guerre dépasse largement les terrains physiques traditionnels au profit des réseaux informatiques, les systèmes de communication et les infrastructures numériques. Sa dangerosité ne réside plus seulement dans la destruction matérielle directe, mais dans la capacité à déstabiliser, désorganiser et manipuler grâce à des outils numériques sophistiqués.

Le conflit russo-ukrainien illustre parfaitement cette nouvelle réalité. Déclenché en 2014 et intensifié par l'invasion russe de février 2022, il est devenu un véritable laboratoire des nouvelles technologies de guerre. Drones armés, cyberattaques massives, intelligence artificielle intégrée aux systèmes de commandement, et recours à des groupes hybrides : tout concourt à transformer le champ de bataille. La Russie, pour contourner la puissance militaire de l'OTAN, mise largement sur ces technologies. De l'autre côté, l'Ukraine, soutenue par ses

alliés occidentaux, utilise elle aussi des moyens technologiques avancés, souvent fournis par des entreprises privées telles que Microsoft, Palantir ou Starlink pour se défendre. Ce conflit apparaît donc comme un terrain d'expérimentation, où les innovations militaires sont testées et perfectionnées en temps réel.

Cette évolution soulève une interrogation de savoir si ces technologies sont réellement développées dans un but de protection des populations, ou si elles constituent de nouveaux vecteurs d'influence et de puissance dans un système international toujours marqué par l'anarchie. Le courant réaliste des relations internationales offre une interprétation particulièrement pertinente pour comprendre la relation entre l'innovation technologique et la quête de puissance. Hans Morgenthau et Kenneth Waltz soulignent que, dans un système international anarchique, les États cherchent à maximiser leur sécurité et leur puissance. L'innovation militaire devient ainsi un levier stratégique destiné à compenser des retards technologiques, dissuader les adversaires et garantir la survie de l'État. L'usage des drones, des cyberarmes et de l'intelligence artificielle illustre pleinement cette logique : ces outils sont développés et déployés dans une dynamique de rivalité permanente et de quête de supériorité technologique et de puissance afin de s'affirmer sur la scène internationale. À l'inverse, les théories libérales et constructivistes fondées sur la coopération internationale et les représentations que les décideurs se font des relations interétatiques, peinent à expliquer la constance des rivalités et la dynamique ininterrompue de la course technologique. En effet, ces visions se heurtent à la réalité des rivalités stratégiques croissantes et à la faiblesse des engagements contraignants.

Dans ce sens, l'objet d'étude de ce mémoire est de répondre à la question de savoir dans quelle mesure l'usage croissant des nouvelles technologies dans le conflit russo-ukrainien respecte-t-il les exigences du droit international et que révèle-t-il de ses insuffisances actuelles ?

Une première partie sera donc dédiée à la conformité de l'utilisation opérationnelle des drones et de l'intelligence artificielle dans le conflit russo-ukrainien au droit international, en tant que technologies produisant des effets cinétiques et posant des défis croissants à l'application des principes du *jus in bello* (I). Puis, une seconde partie analysera l'arme cybernétique, envisagée comme une forme de conflictualité non conventionnelle, souvent dépourvue d'effets matériels immédiats mais générant des conséquences stratégiques majeures, et dont l'encadrement par les normes du *jus contra bellum* et du droit international humanitaire est incertaine (II)

I. L'efficacité opérationnelle des drones et l'IA dans le conflit russo-ukrainien face à l'applicabilité du droit international

Pour une analyse approfondie de cette partie, il convient, dans un premier temps, d'examiner l'usage opérationnel des drones et de l'intelligence artificielle dans le conflit russo-ukrainien (A), afin d'en comprendre les modalités concrètes de déploiement sur le terrain pour ensuite évaluer les effets cinétiques que ces technologies sont susceptibles de produire, ouvrant ainsi la voie à une application du droit international humanitaire et du jus contra bellum (B).

A. Les drones et l'IA dans le conflit russo-ukrainien : une révolution des hostilités

La généralisation tactique et stratégique des drones :

Le ministère des Armées français définit un drone comme « *un engin mobile terrestre, aérien ou naval, sans équipage embarqué, programmé ou télécommandé et réutilisable* » et que « *les drones militaires sont équipés de systèmes d'armes ou de collecte d'informations* »[1]. De son côté, le Department of Defense américain les définit comme des « *véhicules pilotés à distance ou contrôlés automatiquement* »[2]. Ces définitions ne couvrent pas l'ensemble des catégories de drones utilisés aujourd'hui car elles ne prennent pas en compte les drones dits « kamikazes » ou « suicides », qui sont conçus pour une utilisation unique.

Si l'idée d'un appareil piloté à distance remonte aux années 1920, les premiers drones militaires, qualifiés alors de « robots volants »[3], apparaissent dans les années 1960-1970, essentiellement à des fins de reconnaissance et de guidage d'artillerie. Progressivement, ces appareils sont dotés de capacités offensives. Dans les années 1990, les États-Unis mettent en service les célèbres drones armés « Predator » et « Reaper », avec des portées respectives de 1240 et 1850 km[4]. Ces drones, réutilisables et équipés d'une importante capacité de frappe, sont employés à la fois pour des frappes à distance et pour des missions de renseignement. Jusqu'en 2020, l'usage des drones militaires reste principalement cantonné à la lutte contre le terrorisme et n'occupe qu'une place secondaire dans les conflits interétatiques. Ils ont été largement utilisés dans plusieurs conflits, notamment en Lybie, Syrie, Yémen mais surtout au

[1] Glossaire interarmée de terminologie opérationnelle (GIATO), 2013. https://www.defense.gouv.fr/sites/default/files/cicde/20131216-NP-CICDE-DC-004-GIATO-2013-AM-01-06-2015.pdf
[2] https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=1769
[3] Desparairies p.18.
[4] Armée de l'air américaine : https://www.af.mil/about-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/ & https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104469/mq-1b-predator/

Haut-Karabakh. Cependant, Le conflit Russo-ukrainien débuté en 2022, a mis en avant l'utilisation fréquente de cette technologie. Il convient de relever, à cet égard, que les défenses anti-aériennes russes, jugées peu efficaces contre les drones armés en Libye et lors du conflit du Haut-Karabakh, semblent en revanche avoir fait preuve d'une meilleure efficacité sur le théâtre ukrainien.

L'efficacité des drones militaires fait l'objet de nombreux débats sur la scène internationale. Certains considèrent cette technologie comme une véritable révolution, capable de modifier en profondeur le cours des batailles, en particulier grâce à la difficulté qu'ont les radars à détecter ces engins. Depuis les travaux de Clausewitz, il est admis qu'un équilibre entre l'offensive et la défensive est nécessaire à la conduite des opérations militaires. En effet, combattre en territoire adverse expose les armées à de nombreuses contraintes : immersion dans une population hostile, éloignement des lignes de ravitaillement et difficultés liées à l'absence de préparation défensive du terrain. Dans ces conditions, enchaîner des manœuvres d'abord offensives puis défensives devient plus complexe et risqué qu'adopter une stratégie défensive-offensive[5]. Hors l'utilisation des drones permet de changer le cours de cette réflexion en portant une attention particulière à l'offensive au profit de la défensive en limitant les risques pour les forces engagées. D'autres experts relativisent l'impact stratégique des drones en mettant en avant leurs limites opérationnelles, telles que leur dépendance aux réseaux de communication et leur efficacité réduite face à des défenses anti-aériennes modernes et bien coordonnées. Selon eux bien que ces technologies offrent des avantages tactiques indéniables, elles ne suffisent pas à garantir une supériorité sur le long terme.

Ainsi, les drones apparaissent comme des outils capables de rééquilibrer temporairement les rapports de force entre belligérants, en neutralisant des équipements plus coûteux et sophistiqués grâce à leur autonomie et leur faible détectabilité. Mais cette capacité à prolonger les combats sans issue décisive pose la question d'un risque d'instabilité chronique. Le conflit russo-ukrainien en est l'illustration : malgré des prévisions défavorables, l'Ukraine résiste et met en échec, la supériorité militaire russe, en grande partie grâce à l'emploi de ces technologies.

[5] Cf. Clausewitz, *De la Guerre*, op. cit., pp. 409, 663-664
« *tout plan d'attaque stratégique devra, dès le début, porter une attention spéciale à ce point, c'est-à-dire, à la défensive qui lui fera suite* »

L'utilisation des drones dans la guerre Russo-Ukrainienne :

Face à la supériorité numérique et technologique de l'armée russe, l'Ukraine a su tirer parti de ces nouvelles technologies pour rééquilibrer le rapport de forces. Deux stratégies complémentaires se dégagent : l'utilisation des drones Bayraktar TB2 fournis par la Turquie et une forme de « techno-guérilla » reposant sur l'emploi de drones tactiques et commerciaux.

Les drones Bayraktar TB2 se sont avérés déterminants en frappant des cibles stratégiques comme des centres de commandement, des convois logistiques et des batteries antiaériennes russes. Leurs tactiques efficaces d'évitement de radar et leurs frappes de précision ont largement contribué à leur succès opérationnel. Avec 27 heures d'autonomie, un rayon d'action de 150 km, une altitude opérationnelle de 5 000 à 8 000 mètres et une capacité d'armement de 150 kg incluant des bombes guidées MAM[6], ces drones ont même servi d'appâts pour attirer les forces russes vers des zones couvertes par l'artillerie ukrainienne.

En parallèle, des unités mobiles comme Aerorozvidka ont utilisé des drones civils modifiés (Mavic, Punisher, R-18) pour mener des actions perturbant les lignes logistiques russes et fixant les troupes adverses, notamment autour de Kiev. Cette stratégie a permis de freiner significativement l'avancée russe au début du conflit.

Outre les effets militaires immédiats, l'Ukraine a également conduit avec succès une guerre informationnelle, en diffusant massivement sur les réseaux sociaux les images des frappes de drones. Cette communication a renforcé le moral de la population ukrainienne tout en sapant celui des soldats russes, véhiculant une image d'une Ukraine technologiquement avancée et déterminée, soutenue notamment par des acteurs civils comme Starlink, qui a garanti des communications efficaces entre les unités au sol.

De son côté, la Russie, malgré ses importantes capacités industrielles en matière de drones (Orlan-10, Orion, ou munitions rôdeuses ZALA KUB-BLA), a adopté une approche plus traditionnelle. Ses drones servent principalement à des missions de reconnaissance, de surveillance et au guidage de l'artillerie, conformément à une doctrine militaire privilégiant l'artillerie lourde. Moscou mise, par ailleurs, sur sa supériorité dans le domaine de la guerre électronique pour neutraliser les drones ukrainiens, en utilisant notamment le système AeroScope développé par l'entreprise chinoise DJI, capable de détecter et localiser en temps

[6] Zaman, Amberin, « Turkish drones boost Ukrainian spirits amid fears of Russian invasion », *Al-Monitor,* 27/01/2022

réel les drones civils employés par Kiev[7]. Ces capacités de détection sont complétées par des dispositifs avancés de brouillage électronique, capables de perturber voire interrompre les communications entre les drones et leurs opérateurs

Ainsi, la question de l'intégration de l'intelligence artificielle dans les systèmes de drones devient centrale, tant pour déjouer les stratégies de brouillage que pour améliorer l'autonomie décisionnelle des appareils

L'utilisation de l'intelligence artificielle dans les conflits armés et l'intégration de cet outil dans les drones militaires :

Face à la supériorité militaire conventionnelle de la Russie, Kiev a misé sur l'IA pour favoriser l'exploitation des solutions avancées de traitement de données, d'aide à la décision et de ciblage, réduisant l'écart capacitaire par l'innovation technologique. Cette stratégie s'appuie notamment sur des partenariats avec des entreprises telles que Palantir, Microsoft, Amazon, Google et Starlink, transformant l'Ukraine en un véritable laboratoire expérimental de l'IA militaire[8].

Les systèmes comme Skykit, basés sur la plateforme MetaConstellation de Palantir, ont permis l'élaboration de plans de frappe en analysant en temps réel des images satellites et en croisant ces données avec celles provenant des drones et des réseaux sociaux. Cette capacité accélère considérablement le cycle décisionnel dit OODA (Observer, Orienter, Décider, et Agir), réduisant ainsi le délai entre l'identification d'une menace et la prise de décision pour engager le feu. Grâce à l'IA, l'armée ukrainienne peut également traiter d'immenses volumes de données collectées par ses drones, ce qui était auparavant un défi majeur pour les armées. Pour mémoire, en Afghanistan, en 2009, les drones américains avaient produit tellement d'images qu'il aurait fallu 24 ans pour les analyser sans assistance algorithmique. Aujourd'hui, ces flux de données sont traités en temps réel, permettant un ciblage plus précis, une meilleure reconnaissance des objectifs et une anticipation plus fine des mouvements ennemis. L'IA ouvre également la voie à de nouvelles approches tactiques, en particulier le déploiement d'essaims de drones autonomes. Ces petits drones multicoptères sont capables de communiquer entre eux et de définir de manière indépendante les meilleures stratégies d'attaque, réduisant le besoin

[7] Sean Hollister, « DJI drones, Ukraine, and Russia. What we know about AeroScope », *The Verge*, 23/03/2022.

[8] V. Bergengruen, « How Tech Giants Turned Ukraine Into an AI War Lab », Time, 8 février 2024.

d'intervention humaine tout en multipliant les vecteurs d'assaut à moindre coût. Ce concept a d'ailleurs été expérimenté avec succès par Tsahal à Gaza. [9]

L'intégration de l'IA dans les systèmes de drones n'est toutefois pas dénuée de risques. D'un point de vue juridique, elle soulève des interrogations fondamentales quant au respect du droit international humanitaire, en particulier des principes de distinction, de proportionnalité et de précaution. La délégation croissante de la prise de décision à des algorithmes contribue à diluer les responsabilités en cas d'erreurs ou de frappes sur des civils. L'exemple du recours à la reconnaissance faciale développée par Clearview AI, utilisée pour identifier des soldats russes, illustre bien ces dérives et les menaces qu'elles font peser sur les droits fondamentaux[10]. Sur le plan stratégique, l'autonomisation croissante des systèmes de combat ouvre également la voie à une vulnérabilité accrue face aux cyberattaques et à la guerre électronique. Enfin, cette mutation du champ de bataille accélère l'entrée dans l'ère de la « hyperwar », caractérisée par l'extrême rapidité des engagements et l'automatisation des processus décisionnels, ce qui rend presque impossible toute forme de désescalade ou de médiation avant que les frappes ne soient déclenchées

Ainsi, l'intégration de l'intelligence artificielle dans les conflits armés, et plus particulièrement dans les drones militaires, modifie en profondeur les équilibres stratégiques et les rapports de force. Elle impose désormais une réflexion sur l'encadrement juridique de ces technologies et sur la nécessité de préserver, dans ce nouveau contexte, un minimum de contrôle humain, garant d'un usage éthique et conforme au droit des conflits armés.

B. Un encadrement juridique partiel limité aux effets cinétiques

L'encadrement juridique des drones et de l'intelligence artificielle, doit être analysé selon deux contextes : d'une part, leur utilisation dans des opérations produisant des effets cinétiques (pertes en vies humaines, destructions matérielles etc.), d'autre part, leur emploi dans des opérations sans effets cinétiques, notamment dans les missions de renseignement ou de surveillance.

L'application du jus contra bellum et du jus in bello face aux effets cinétiques :

[9] Z. Kallenborn, « Israel's Drone Swarm Over Gaza Should Worry Everyone », Defense One, 7 juillet 2021, disponible sur : https://www.defenseone.com/ideas/2021/07/israels-drone-swarm-over-gaza-should-worry-everyone/183156/
[10] V. Bergengruen, « Ukraine's "Secret Weapon" Against Russia Is a Controversial U.S. Tech Company », Time, 14 novembre 2023

Lorsqu'il s'agit d'opérations entraînant des effets matériels, la qualification juridique ne suscite aucun débat. Toute intervention armée provenant de ces technologies constitue une utilisation de la force armée au sens de l'article 2§4 de la Charte des Nations Unies. Une telle action illicite, peut donc justifier la mise en œuvre du droit de légitime défense prévue à l'article 51 de la Charte.

Sur le terrain du jus in bello, cette même logique s'applique mais des défis relatifs à ces nouvelles technologies persistent. En effet, Dès lors que l'emploi de ces technologies produit des effets matériels, l'application des règles du droit international humanitaire, issus du droit de La Haye, des Conventions de Genève et de leurs Protocoles additionnels ainsi que de la coutume s'imposent aux parties. Trois principes fondamentaux encadrent ces situations. D'abord, Le principe de distinction impose de différencier en tout temps les civils des combattants, et les biens civils des objectifs militaires[11]. Toutefois, les technologies autonomes compliquent fortement l'application de ce principe, car elles rencontrent des difficultés à identifier clairement les cibles légitimes, en particulier lorsqu'il s'agit d'infrastructures ou d'individus ayant des fonctions duales civiles et militaires. Ensuite, le principe de nécessité militaire interdit toute violence inutile : seules les actions absolument nécessaires à la victoire sont autorisées[12]. Or, l'automatisation des systèmes de décision militaire tend à accélérer les frappes sans permettre une évaluation humaine adéquate, augmentant ainsi les risques d'erreurs et de dommages collatéraux. Enfin, le principe de proportionnalité interdit les attaques qui causeraient des dommages civils disproportionnés par rapport à l'objectif militaire poursuivi[13]. Ici encore, l'intelligence artificielle et les drones montrent leurs limites, car ces systèmes autonomes peinent à intégrer des critères qualitatifs et moraux nécessaires pour juger correctement la proportionnalité d'une attaque dans son contexte opérationnel précis

A ces difficultés d'applications structurelles s'ajoutent des enjeux éthiques et psychologiques majeures. En effet, l'éloignement physique des opérateurs crée une forme de déshumanisation de l'acte létal appelé « syndrome playstation »[14]. L'opérateur, éloigné du champ de bataille, agit dans un environnement déconnecté de la réalité humaine du conflit ce qui réduit sa

[11] L'article 48 du Protocole I de 1977 interdit d'attaquer des civils ou des biens civils
L'art 51 du Protocole I : interdit les attaques indiscriminées, qui toucheraient sans distinction objectifs militaires et civils
L'article 52 du protocole I pose une présomption du caractère civil de certains biens (lieu de culte, maison, école, hôpitaux etc.) et définit l'objectif militaire comme tout objectif permettant de procurer un avantage militaire particulier.
[12] Codifié pour la première fois dans le code Lieber de 1863 (interdit les attaques inutiles), il a été repris par la Déclaration de Saint-Pétersbourg en 1868 avant d'être repris par les conventions de la Haye de 1899 et 1907.
[13] Évoqué implicitement pour la première fois dans le code Lieber de 1863, il a été codifié à l'article 51 et 57 du Protocole additionnel I aux conventions de Genève de 1977.
[14] J.B. J. Vilmer, "Not so remote drone warfare". *International Politics*, June 2021, p. 1-22.

perception des conséquences humaines de ses actes et favorise une banalisation de l'usage de la force. Par ailleurs, La dilution des responsabilités juridiques, revêt également une difficulté importante. En effet, Lorsqu'un drone doté d'un système d'IA décide du ciblage et de l'engagement, la question de l'imputabilité de la responsabilité devient complexe : cette responsabilité serait-elle celle de l'opérateur humain, réduit à un rôle de supervision ? Au supérieur hiérarchique qui a autorisé l'opération ? À l'entreprise ayant conçu l'algorithme ou même à l'État détenteur de ces technologies ?

Ainsi, si l'usage de ces technologies produit en général des effets cinétiques, justifiant l'application du DIH sans difficulté conceptuelle, c'est leur application pratique et effective qui est remise en cause par la complexité des mécanismes de responsabilité et le manque de contrôle humain sur l'usage de la force.

Le vide juridique quant à l'encadrement des activités sans effets cinétiques :

La situation est encore plus délicate pour les usages ne produisant pas d'effets cinétiques, tels que les missions de renseignement, de surveillance ou de guerre électronique.

Sur le plan du jus contra bellum, la question est de savoir si de telles opérations, même sans usage direct de la force armée, peuvent constituer une violation de la souveraineté d'un État, voire un acte d'agression imputable à un État ?

Sur le plan du jus in bello, l'absence d'effets matériels pose la question de l'applicabilité des règles du DIH. En l'absence de destruction ou de perte en vies humaines, peut-on considérer que le seuil de conflictualité justifiant l'application du DIH est atteint ?

Cette question trouve une résonance particulière dans le domaine des cyberconflits, caractérisés par l'absence d'effets cinétiques et fera l'objet d'une réflexion spécifique dans la partie suivante.

II. La guerre cybernétique à l'épreuve du droit international : une invisibilité stratégique créant un certain vide juridique

Pour analyser cette nouvelle forme de conflictualité, il convient de s'interroger sur la manière dont le droit international appréhende la guerre cybernétique, caractérisée par son invisibilité stratégique, l'absence fréquente d'effets matériels immédiats, et la difficulté à en identifier clairement les auteurs. A ce titre, il conviendra, dans un premier temps, de mettre en évidence

l'omniprésence du cyberespace dans les conflits contemporains, en particulier dans la guerre russo-ukrainienne (A). Dans un second temps, l'étude portera sur les lacunes normatives et les défis juridiques posés par l'usage de l'arme cyber (B)

A. Une cyberguerre omniprésente mais juridiquement insaisissable

L'Ukraine comme un laboratoire d'une intensification sans précédent des cyberattaques visant les infrastructures critiques :

Depuis le début de l'invasion russe en février 2022, l'Ukraine est devenue un terrain privilégié d'expérimentation pour les cyberattaques à grande échelle. Entre 2000 et novembre 2024, environ 369 incidents cybernétiques impliquant près de 86 groupes de menaces ont été recensées[15]. Bien que ces attaques soient généralement menées conjointement avec des opérations militaires classiques, ce qui limite leur qualification en tant qu'armes autonomes, leur impact opérationnel reste considérable. Ces opérations visent essentiellement à perturber les structures de commandement, les infrastructures critiques ainsi que les chaînes d'approvisionnement militaires.

Parmi les cas les plus notables de cyberattaques dans ce conflit, figurent l'attaque Whispergate contre les systèmes gouvernementaux ukrainiens en janvier 2022 et HermeticWiper, qui a frappé les secteurs financier et énergétique juste avant l'offensive russe en février 2022. De même, en mars 2022, le groupe russe BROMINE a réussi à pénétrer les systèmes informatiques des centrales nucléaires de Tchernobyl et Zaporijjia. Cette stratégie cybernétique russe ne constitue pas une nouveauté, mais prolonge une politique mise en place dès 2014, notamment en Crimée et dans le Donbass. À titre d'exemple, en 2015 et 2016, le groupe Sandworm, lié au renseignement militaire russe GRU, avait déjà mené des cyberattaques de grande ampleur contre les infrastructures électriques ukrainiennes, provoquant des coupures prolongées aux conséquences graves pour la population civile.

L'une des tactiques les plus utilisées dans ce conflit est celle des attaques par déni de service (DDoS), visant à saturer les serveurs et à rendre les systèmes inaccessibles. En 2023, elles représentaient 89 % des cyber-incidents signalés en Ukraine, et 99,4 % à l'échelle mondiale[16]. C'est dans ce contexte que s'inscrit l'attaque lancée le 24 février 2022, jour même de

[15] « European Repository of Cyber Incidents (EuRepoC) », Stiftung Wissenschaft und Politik (SWP), consulté le 15 novembre 2024, https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc.
[16] 101 CyberPeace Institute, « Cyber Dimensions of the Armed Conflict in Ukraine ».

l'invasion, qui a paralysé le réseau de communication européen Viasat, affectant non seulement l'Ukraine, mais également plusieurs États membres de l'Union européenne.

Les cibles privilégiées de ces offensives sont les infrastructures critiques : réseaux d'énergie, de transport, de télécommunications, mais aussi médias, services bancaires et institutions gouvernementales. Durant les deux premiers mois du conflit, 350 cyberattaques russes ont été recensées, dont 40 % visaient directement des infrastructures jugées vitales pour le fonctionnement de l'État, de l'économie ou de la défense. Par ailleurs, 30 % de ces cyberattaques ont directement visé les administrations publiques ukrainiennes à tous les niveaux (national, régional, local), avec des conséquences opérationnelles immédiates. Par exemple, en mars 2022, des cyberattaques contre les sociétés logistiques ukrainiennes ont considérablement perturbé l'acheminement de l'aide humanitaire et militaire. Plus tard, en décembre 2022, le groupe IRIDIUM a déclenché une cyberattaque majeure contre le réseau électrique national, plongeant plusieurs régions ukrainiennes dans l'obscurité en pleine période hivernale, exacerbant ainsi la crise humanitaire déjà critique.

Ces attaques ciblées ont contribué à affaiblir la population civile, en coupant l'accès aux services essentiels, en isolant certaines régions, et en renforçant la précarité des populations déjà vulnérables.

Une diversité d'acteurs et le rôle déterminant des entreprises privées dans la cyberdéfense :

La guerre cybernétique est caractérisée par la multitude des acteurs en jeux. Cela s'applique dans la guerre russo-ukrainienne, où hormis les offensives menées par les agences de renseignement (GRU, FSB, SVR), plusieurs groupes hybrides mêlant cybercriminels, hacktivistes et acteurs privés interviennent activement. Plusieurs opérations ont été menés par des groupes mixtes avec un collaboration entre des groupes étatiques et cybercriminels. Des groupes comme Sandworm et Storm-2049 ont par exemple mené des opérations conjuguant sabotage et espionnage[17]. Ainsi, Les services russes semblent avoir externalisé plusieurs de leurs opérations, notamment de cyber espionnage, à des groupes criminels. Cela a été notamment démontré en juin 2024, lorsqu'un groupe suspecté de cybercriminalité a utilisé des logiciels malveillants pour compromettre au moins 50 appareils militaires ukrainiens. Dans ce contexte, le groupe Google threat intelligence a publié un rapport exposant les opérations

[17] Microsoft Digital Defense Report 2024.

hybrides d'espionnage et d'influence dans le cadre d'une compagne menée par des groupes de hackers soutenus par la Russie (UNC5812) visant à diffuser des contenus anti-mobilisation et des logiciels malveillants en Ukraine[18].

Par ailleurs, La sophistication des outils employés s'est accrue, avec l'utilisation de malwares avancés tels que Cobalt Strike pour des campagnes de renseignement massif. Les groupes non étatiques tels que Killnet et Anonymous Russia ont intensifié les campagnes de DDoS et de désinformation à l'échelle mondiale, bien que leur impact stratégique demeure limité. Killnet a par exemple visé des pays ayant imposé des sanctions contre la Russie, perturbant des sites gouvernementaux et privés en Roumanie, Italie, Norvège, Japon et États-Unis[19].

D'un point de vue géographique, l'intensification des cyberopérations russes à partir de 2021 a non seulement visé l'Ukraine mais aussi ses alliés. Dès 2022, cette dynamique s'est traduite par une augmentation de 250 % des attaques dirigées contre les utilisateurs situés en Ukraine par rapport à 2020, tandis que le ciblage des États membres de l'OTAN enregistrait une hausse de plus de 300 %. Si 75 % des cyberattaques russes ont été dirigées contre l'Ukraine et ses alliés occidentaux, les attaques ont également concerné des acteurs non gouvernementaux situés en dehors du théâtre direct des opérations comme les *think tanks*, les organisations humanitaires ou les entreprises informatiques. 49 % des entités visées étaient des agences gouvernementales, en particulier au sein des institutions des États de l'OTAN et 12 % des cibles étaient des organisations non gouvernementales Au total, 128 cibles réparties dans 42 pays tiers ont été visées, illustrant une volonté d'élargir la pression stratégique sur les soutiens politiques, économiques et humanitaires de Kiev.

Face à cette intensification des menaces, les entreprises privées se sont révélées essentielles dans la préservation des capacités numériques ukrainiennes. Ainsi, Starlink a assuré la continuité des communications stratégiques malgré la destruction des réseaux traditionnels, tandis que des acteurs tels que Microsoft et Google ont apporté un soutien logistique et technologique, en renforçant les défenses des systèmes ukrainiens et en luttant contre les campagnes de désinformation.

[18] Kat Duffy et al., « Cyber Week in Review: November 1, 2024 » (Council on Foreign Relations, 1 novembre 2024), https://www.cfr.org/blog/cyber-week-review-november-1-2024.« Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives », GoogleCloud Blog, consulté le 18 novembre 2024, https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives
[19] « ENISA Thrat landscape 2023 », 2023.

Cette collaboration public-privé représente une innovation stratégique majeure, posant la question du rôle croissant des entreprises privées dans la sécurité des États et de leur implication directe dans les conflits armés.

L'inefficacité des cyber opérations russes face à la primauté du conventionnel :

Malgré l'intensité et la sophistication des cyberopérations menées par la Russie, celles-ci se sont révélées largement inefficaces sur le plan stratégique. En effet, aucune des 28 grandes campagnes cyber recensées n'a permis d'obtenir un avantage décisif sur le terrain. Ces offensives, principalement orientées vers des actions de harcèlement numérique et de désorganisation, n'ont jamais atteint le seuil critique d'une victoire stratégique. Sur une échelle d'évaluation des dégâts des cyberattaques allant de 1 à 15, les attaques russes affichent une intensité moyenne plafonnant à 2,38[20].

Cette inefficacité s'explique par plusieurs facteurs cumulatifs. D'abord l'absence de coordination étroite entre les cyberopérations et les actions militaires conventionnelles a considérablement réduit l'impact des offensives numériques. À la différence de la guerre en Géorgie en 2008, où la Russie avait su synchroniser ses moyens cyber et cinétiques, le conflit ukrainien a révélé une désorganisation stratégique manifeste. Ensuite, La croyance initiale dans une victoire rapide a conduit à une mauvaise préparation des opérations cyber intégrées. En conséquence, les cyberattaques, lorsqu'elles n'étaient pas directement accompagnées d'actions militaires physiques, ont échoué à produire des effets stratégiques durables. Par ailleurs, les opérations russes ont souffert de la fragmentation de leurs acteurs. En effet, une large part des actions cyber a été menée par des groupes semi-autonomes pro-russes, notamment des hacktivistes, opérant sans réelle coordination avec les organes étatiques, conduisant à une absence de contrôle stratégique et à une dispersion des objectifs. À ces facteurs s'ajoute l'efficacité des mesures de défense adoptées par l'Ukraine et ses alliés puisque suite aux enseignements tirés des cyberattaques précédentes, notamment l'opération NotPetya en 2017, les Ukrainiens ont considérablement renforcé leurs capacités de cyberdéfense, Grâce à une mobilisation rapide des entreprises privées, des ONG spécialisées et des experts en cybersécurité. De plus, sur le plan technologique, les cyberattaques russes se sont révélées majoritairement disruptives plutôt que destructrices. Seuls 29 % des incidents documentés relèvent de véritables attaques de dégradation. Le recours massif aux attaques de type DDoS,

[20] « European Repository of Cyber Incidents (EuRepoC) »

représentant 89 % des incidents en Ukraine en 2023 confirme cette tendance à privilégier des opérations à faible impact technologique et stratégique. Enfin, cette faiblesse des capacités offensives cyber russe peut également s'expliquer par les contraintes économiques et techniques inhérentes à la mise en œuvre de cyberattaques sophistiquées.

Face à ces limites, la doctrine militaire russe a progressivement réorienté ses priorités vers l'usage des moyens conventionnels. Dès 2023, une baisse significative de l'intensité des opérations cyber a été observée, marquant un retour à des stratégies plus traditionnelles, où la supériorité sur le terrain est acquise essentiellement par la puissance de feu. La prévalence accordée aux armes conventionnelles relègue alors les cyberattaques à un rôle secondaire, « *quand la poudre parle, la lutte informatique offensive trouve ses limites* »[21].

Cette inefficacité opérationnelle, conjuguée à la multiplicité des acteurs impliqués, et l'absence d'effets cinétiques immédiats contribue à renforcer la complexité d'établir un cadre juridique international.

B. Un encadrement lacunaire face à un outil de guerre non conventionnel.

Les divergences quant à l'engagement de la responsabilité de l'État :

La responsabilité d'un État ne peut être engagée que lorsqu'un acte internationalement illicite lui est juridiquement attribuable. La qualification de l'acte illicite ne pose pas de difficultés lorsqu'il y a violation de la souveraineté d'un autre État. Ce principe, consacré dès les traités de Westphalie de 1648, repose sur deux piliers : le principe de non-intervention (respect de l'intégrité territoriale) et celui de la non-ingérence dans les affaires internes de celui-ci. Cette violation peut être commise par commission (par exemple en cas d'acte d'agression armée) ou par omission, dans le cas où un État laisserait utiliser son territoire pour permettre un acte d'agression qu'il aurait pu empêcher. Il s'agit du principe de due diligence, consacré par l'arrêt de la CIJ, détroit de Corfu de 1949 et repris à plusieurs reprises par d'autres arrêts de la CIJ[22]. C'est un devoir de protéger à l'intérieur du territoire, les droits des autres États par une vigilance d'un bon gouvernement. Ainsi, tout État doit contrôler les activités qui se développent

[21] Mueller et al., « Cyber Operations during the Russo-Ukrainian War ».
[22] CIJ, Affaire des activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda), Arrêt du 19 décembre 2005, CIJ Recueil 2005.
CIJ, Affaire relative à l'application de la convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro), Arrêt du 26 février 2007, Recueil CIJ 2007

sur son territoire[23], et en matière de cybersécurité, ce principe implique que les États doivent protéger leurs infrastructures critiques et prendre les mesures nécessaires pour faire cesser la violation s'ils ont connaissance d'activités illicites initiées depuis leur territoire.

Ainsi, pour qu'un État puisse invoquer le droit à la légitime défense en application de l'article 51 de la Charte des Nations Unies, il est nécessaire que la cyberattaque soit à la fois qualifiée d'agression armée au sens de l'article 2 § 4 de la Charte et qu'elle puisse être juridiquement attribuée à un État. Or, les profondes divergences sur ces deux critères expliquent en grande partie l'absence d'un cadre juridique clair et consensuel en la matière.

Une cyberattaque est définie par le CICR comme : « *une opération dirigée contre un ordinateur ou un réseau informatique, ou par le biais d'un système informatique pour collecter, altérer ou encrypter des données pour déclencher, détourner ou manipuler des processus* ». Dans ce sens, pour qu'une cyberattaque soit qualifiée d'acte internationalement illicite, elle doit nécessairement constituer une violation de la souveraineté d'un État. Selon le manuel Tallinn 2.0 cette violation est caractérisée si elle provoque des dommages physiques ou des blessures, une perte de fonctionnalité d'infrastructure critique cyber nationale ou dans le cas d'une nécessité de réparation ou de remplacement d'équipements. Cet instrument n'étant pas contraignant, plusieurs divergences sont persistent quant à la qualification d'agression armée d'une cyberattaque. La position majoritaire établi un critère de gravité des effets de l'attaque qui doivent être similaires à ceux qui résultent d'une attaque classique. Dès lors, les cyberattaques aux effets limités, qui représentent la grande majorité des incidents observés (comme démontré précédemment), ne remplissent pas ce critère et ne peuvent être qualifiées d'agression armée. Au-delà de cette première difficulté, il faut encore que la cyberattaque soit attribuable à un État. Cette question suscite également d'importantes divergences au niveau international, notamment depuis les attentats du 11 septembre 2001, qui ont ravivé le débat sur la possibilité pour des acteurs non étatiques de commettre des actes d'agression. Mais la position jurisprudentielle reste claire : seuls les États peuvent être considérés comme auteurs d'un acte d'agression armée[24]. Or, il est particulièrement difficile de prouver de manière certaine l'implication directe d'un État dans une opération cyber. Ces attaques reposent fréquemment sur des techniques sophistiquées de dissimulation (spoofing, utilisation de proxies, recours à des serveurs tiers), rendant complexe l'établissement d'un lien de causalité

[23] CIJ, Affaire relative à l'application de la convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro), Arrêt du 26 février 2007, Recueil CIJ 2007
[24] CIJ, Avis consultatif du 9 juillet 2004, Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé

entre l'acte illicite et l'État présumé responsable. Depuis l'affaire « *Activités militaires et paramilitaires au Nicaragua »* (1986), pour qu'une attaque soit attribuée à un état il faut établir contrôle effectif. Un État ne peut être tenu responsable des actes commis par un acteur non étatique que s'il a exercé un contrôle direct sur ces activités, par le biais de directives ou d'instructions. Ce principe a été repris par la Commission du droit international (CDI) dans son Projet d'articles sur la responsabilité de l'État (2001), à son article 8.

Les divergences sur l'application du DIH dans le cadre des cyberattaques à cause de l'absence des effets cinétiques.

Les règles du droit international humanitaire s'appliquent aux conflits armés, quelles que soient les formes de guerre ou les armes employées, actuelles ou futures[25]. Elles s'appliquent donc à l'arme cyber qualifiée en 2009 par Barack Obama comme « *« une arme de destruction massive par perturbation* ». Cela a été confirmé par Le rapport des groupes d'experts gouvernementaux de l'ONU[26] qui soutient que les principes du DIH s'appliquent aux opérations cybernétiques, notamment les principes d'humanité, de nécessité, de proportionnalité et de distinction.

Dès lors, il est légitime de se demander si les règles du DIH, et en particulier le principe de distinction, initialement conçues pour les armes classiques, sont réellement applicables à des opérations cybernétiques immatérielles, souvent dénuées d'effets immédiats sur les civils.

L'article 49 du Protocole Additionnel I de 1977, définit les attaques comme « *des actes de violence contre l'adversaire, qu'ils soient offensifs ou défensifs* ». Sur cette base, certains États, à l'instar de la France, estiment qu'une cyberopération peut être qualifiée d'attaque si elle entraîne des effets violents, même sans recours à la force armée traditionnelle. D'autres États adoptent une position plus restrictive. L'Australie et le Danemark, par exemple, considèrent qu'une cyberattaque ne peut être juridiquement qualifiée d'attaque que si elle produit des effets physiques comparables à une attaque cinétique : pertes en vies humaines, blessures ou destructions matérielles. Cette approche rejoint les conclusions du Manuel de Tallinn, qui exige l'existence d'effets matériels pour qualifier une cyberopération d'attaque du point de vue du DIH. Cependant, cette interprétation cinétique présente des limites, notamment l'exclusion du champ d'application du DIH les cyberopérations qui, sans causer de destructions physiques,

[25] CIJ, Avis consultatif du 8 juillet 1996, Licéité de la menace ou de l'emploi des armes nucléaires
[26] ONU, Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale), Rapport de 2015, Note du Secrétaire général, A/70/174, 22 juillet 2015 (site ONU) https://documents.un.org/doc/undoc/gen/v24/055/07/pdf/v2405507.pdf

peuvent avoir des conséquences dramatiques sur les populations civiles. Par exemple, L'interruption d'un réseau électrique, comme lors du blackout de 2003 aux États-Unis, peut avoir des conséquences humaines et économiques graves, sans destruction matérielle directe. Face à cela, plusieurs États, dont la France et la Nouvelle-Zélande, soutiennent une approche élargie, prenant en compte les effets indirects et prévisibles des cyberopérations. Le CICR appuie cette interprétation en affirmant que ces effets doivent être intégrés à l'analyse de la licéité d'une opération au regard du DIH. Cette approche est également conforme à l'article 52 § 2 du Protocole additionnel I, qui admet que la neutralisation d'un objectif militaire constitue une attaque, même sans destruction physique.

Par ailleurs, La question de la protection des données illustre également les difficultés d'adaptation du DIH. Dans un environnement de plus en plus dématérialisé, les données jouent un rôle central dans la gestion des services essentiels : santé, finance, énergie, transports. La qualification des données comme « objets » au sens du DIH fait l'objet de vifs débats. Tandis que le Tallinn Manual et Israël considèrent que seuls les objets matériels sont protégés par le principe de distinction, la France et le CICR estiment que les données essentielles, en particulier médicales et bancaires, doivent bénéficier d'une protection équivalente à celle des biens matériels. Exclure ces données du champ de protection reviendrait à créer un vide juridique dangereux, permettant de mener des cyberopérations aux conséquences humanitaires graves sans tomber sous le coup des interdictions du DIH.

En outre, la distinction entre objectif militaire et civil dans le cyberspace particulièrement complexe par la prévalence de ciblage des objets à double usage : les infrastructures de télécommunication, les réseaux électriques, ou encore les systèmes de gestion de l'eau et des transports. Si la France plaide pour une analyse au cas par cas, le manuel Tallinn 2.0 considère qu'un objet servant à des fins tant civiles que militaires doit être considéré comme un objectif militaire légitime. Ce flou juridique risque de conduire à une interprétation extensive du concept d'objectif militaire, au détriment de la protection des populations civiles.

Enfin, la participation directe des civils aux hostilités dans le cyberespace complique l'application du principe de distinction. Selon l'article 51§3 du Protocole Additionnel I, les civils bénéficient d'une protection contre les attaques sauf lorsqu'ils participent directement aux hostilités. Le CICR a précisé les critères de cette participation directe : un seuil de dommage prévisible, une causalité directe et un lien belliqueux avec les hostilités. Ainsi, les civils qui participent à des opérations de piratage de réseaux militaires ou à l'installation de

malwares visant des objectifs militaires peuvent perdre leur protection. Cette règle pose la question du moment où ces hostilités commencent et se terminent dans un environnement dématérialisé, où les actions sont souvent éphémères et à effets différés.

Ainsi, l'application des principes du droit international humanitaire, notamment celui de distinction, rencontre des obstacles à la fois pratiques et conceptuels dans le cyberespace dues à l'absence d'effets cinétiques. Cette logique se transpose également pour les autres nouvelles technologies laissant le cadre juridique international flou. Dans ce sens, cette difficulté conduit à une réflexion plus large sur la nature des réactions que les États et les acteurs privés peuvent légitimement adopter en cas de cyberattaque. C'est précisément dans ce cadre qu'émerge la problématique du hack-back, également appelé « cyberdéfense active ». Cette méthode consiste pour une entité victime d'une cyberattaque à riposter directement contre l'auteur présumé, en utilisant des moyens offensifs semblables. Elle soulève des inquiétudes majeures en raison du vide juridique dans lequel elle s'inscrit, ainsi que des interrogations sur sa compatibilité avec le droit international.

Le principe de hack-back : l'absence de cadre juridique dangereuse.

Le recours à la cyberdéfense active découle principalement du constat d'une incapacité des États à assurer une protection rapide et efficace des entités privées face aux cybermenaces sophistiquées, souvent transfrontalières. Face aux limites des défenses passives traditionnelles, ces acteurs privés se tournent vers des stratégies offensives, facilitées par l'absence d'un cadre juridique clairement établi. Ces pratiques de riposte comprennent la neutralisation des botnets adverses, l'infiltration de leurs systèmes informatiques et l'introduction de logiciels malveillants destinés à endommager durablement leurs infrastructures, voire à les désactiver.

Souvent justifié sous couvert de légitime défense, ce glissement vers une riposte privée immédiate est pourtant incompatible avec le droit international, qui ne reconnaît la légitime défense qu'aux États. En effet, Le hack-back ne bénéficie d'aucune reconnaissance formelle en droit international. Ni la Charte des Nations Unies, ni les instruments régionaux ou internationaux, tels que la Convention de Budapest (2001) ou le projet de convention des Nations Unies contre la cybercriminalité (2024), ne consacrent un droit au hack-back. Bien au contraire, ces textes imposent aux États de pénaliser les intrusions informatiques et de protéger l'intégrité des systèmes d'information, sans prévoir d'exception pour des contre-mesures prises par des acteurs privés. En France, par exemple, les articles L.2321-1 et L.2321-2 du Code de

la Défense réservent expressément les mesures de cyberdéfense offensive à l'État et à ses services spécialisés. Le droit international coutumier réaffirme également le monopole étatique de la contrainte légitime, s'opposant à toute reconnaissance d'un droit d'autodéfense privée dans le cyberespace. Ainsi une action offensive menée par une entreprise ou un acteur privé, même avec l'autorisation d'un État, ne saurait s'inscrire dans ce cadre sans violer les règles fondamentales du droit international.

Malgré ces interdictions, certains États envisagent cependant une régulation encadrée de cette pratique, en s'appuyant sur les entreprises militaires et de sécurité privées (EMSP). Ces acteurs, bien qu'ayant suscité de nombreuses critiques pour leurs exactions sur les théâtres d'opérations extérieures, ont démontré l'existence d'un marché de la sécurité parallèle, qui pourrait également s'étendre à la sphère cyber. Toutefois, l'expérience des EMSP, marquée par des dérives, comme dans l'affaire Blackwater en Irak, met en lumière les risques de perte de contrôle lié à l'externalisation de la sécurité.

Face à ces enjeux, il apparaît nécessaire de promouvoir un encadrement international des pratiques de cyberdéfense active. À défaut, le risque est grand de voir se multiplier les actions unilatérales, échappant à tout contrôle institutionnel, et compromettant les efforts en matière de sécurité collective. Dans ce cadre, le développement de normes contraignantes sur la cyberdéfense et l'adoption d'un code de conduite international sur l'usage du hack-back apparaissent comme des étapes indispensables pour éviter l'anarchie numérique et assurer une régulation efficace de cette nouvelle dimension des relations internationales.

CONCLUSION

Le conflit russo-ukrainien constitue une rupture profonde dans l'évolution des conflits modernes, marquée par une utilisation massive et inédite des nouvelles technologies militaires telles que les drones armés, l'intelligence artificielle et les cyberattaques. Cette guerre inaugure ainsi une époque où la supériorité stratégique ne dépend plus uniquement des capacités militaires traditionnelles, mais repose de plus en plus sur la maîtrise technologique et informationnelle.

Face à ces bouleversements, le droit international existant montre rapidement ses limites. Conçu initialement pour réguler des conflits conventionnels, il peine aujourd'hui à encadrer efficacement ces nouvelles formes de guerre, notamment les cyberattaques et les armes autonomes. Bien que des solutions provisoires, comme celles proposées par le Manuel de Tallinn, apportent quelques réponses, elles restent insuffisantes face à l'ampleur des défis juridiques posés. Il est donc impératif de réformer en profondeur le cadre juridique international afin de combler ces vides normatifs, de clarifier les régimes de responsabilité, et d'assurer une régulation efficace de l'usage des nouvelles technologies dans les conflits armés.

Au-delà des enjeux purement juridiques, cette guerre amène aussi à s'interroger sur les futurs équilibres stratégiques mondiaux. Ces nouvelles technologies risquent en effet d'accentuer l'asymétrie des conflits, d'abaisser les seuils de déclenchement des hostilités et de multiplier les affrontements hybrides, rendant la frontière entre paix et guerre particulièrement difficile à cerner.

Enfin, il est important de souligner que l'élaboration de nouvelles normes internationales, même ambitieuses, ne suffit pas en elle-même à assurer leur respect dans un contexte international dépourvu de réels mécanismes contraignants. L'histoire démontre que les engagements juridiques internationaux restent souvent conditionnés par les intérêts propres et la volonté politique des États. Le non-respect fréquent du droit international par certains États, malgré l'existence de traités formellement contraignants, confirme cette réalité.

La guerre en Ukraine constitue ainsi un véritable laboratoire des conflits à venir. Face à ce constat, la communauté internationale porte la responsabilité historique de repenser le droit international pour préserver autant que possible les principes d'humanité, dans un contexte où la technologie tend à déshumaniser toujours davantage la guerre.