La cybercoercition doit être combattue par une stratégie nationale et globale

La lutte contre les intrusions informatiques, qu'elles soient d'origine étatique ou criminelle, implique de combiner renseignement, protection, action internationale et capacité de riposte, soulignent **Bernard Barbier, Jean-Louis Gergorin et Edouard Guillaud,** anciens hauts responsables de la défense

Au début de l'année 2020, dans un monde qui n'imaginait pas encore à quel point la pandémie de Covid-19 le déstabiliserait, nous alertions sur l'ensemble des menaces cyber et appelions à la réflexion comme à l'action face à ce que nous avons baptisé la « cybercoercition » : toute intrusion informatique visant à intimider les dirigeants d'un Etat ou d'une entreprise pour obtenir des avantages politico-stratégiques dans un cas, une rançon financière dans l'autre. La lettre ouverte du Club informatique des grandes entreprises françaises (Cigref), le 18 novembre 2020, au premier ministre, Jean Castex, est un cri d'alarme des entreprises. Le nombre de cyberattaques réussies, notamment par des rançongiciels *(« ransomware »)* bloquant le système informatique d'une entreprise jusqu'au paiement d'une rançon, a encore quadruplé en un an. Les attaques sont de plus en plus sophistiquées et visent entreprises et services publics. Elles proviennent en quasi-totalité d'un écosystème criminel qui s'est développé dans des pays n'ayant pas ratifié la Convention de Budapest sur la cybercriminalité (2001).

En toute impunité, de puissants groupes pratiquent aussi bien la cyberextorsion directe que la vente à tout acheteur criminel des outils techniques permettant celle-ci : *« ransomware as a service »*. La tolérance intéressée des services officiels des Etats les abritant et l'importance de leurs gains font de la cyberpiraterie l'activité criminelle la plus rentable et la moins risquée de l'histoire humaine, ce qui explique sa croissance exponentielle. La pénétration, révélée fin 2020, des systèmes informatiques d'un millier d'entités publiques et privées américaines, dont la totalité des grands ministères, la NSA, Microsoft et la très performante société de cybersécurité FireEye, constitue une véritable *« rupture stratégique »*. Il s'agit de la modification non détectée d'une mise à jour d'un logiciel de gestion de réseaux. L'ajout d'un « cheval de Troie », nommé « Sunburst », de mars à mai, a permis de prépositionner au cœur des systèmes les plus critiques un implant, qui, à ce jour, ne paraît avoir été utilisé qu'à des fins d'espionnage. Il aurait pu tout aussi bien être un vecteur de sabotage.

Un plan de lutte en quatre volets

Jusqu'à la découverte récente et l'identification précise de Sunburst, l'Etat qui l'a créé – la Russie, selon la quasi-totalité des responsables officiels américains sauf Donald Trump – a disposé d'une *« capacité de première frappe numérique »* contre des infrastructures civiles et militaires critiques des Etats-Unis. Sunburst n'a été décelé que lorsque ses commanditaires ont volé les outils techniques offensifs de FireEye. Il est probable que cette capacité d'insérer un cheval de Troie indétectable dans une mise à jour de logiciel soit déjà exploitée ailleurs. La menace est donc critique. Dans ce contexte, la cybercoercition, qu'elle soit étatique ou criminelle, doit être combattue par une stratégie nationale d'anticoercition intégrée et globale. Elle comporterait quatre volets étroitement liés : renseignement, protection, action internationale et capacité de riposte. Le renseignement doit identifier les responsables des attaques et les signatures techniques de celles-ci. Pour ce faire, la coopération entre services de renseignement officiels, agences de cybersécurité et entreprises spécialisées de confiance est primordiale. La protection est une condition nécessaire mais non suffisante de la sécurité. A cet égard, l'attaque Sunburst est une alerte majeure sur la nécessité de ne plus s'en remettre aux seules certifications initiales des logiciels.

> VOULOIR ÉRADIQUER LA CYBERCRIMINALITÉ EST ILLUSOIRE ; LA RÉDUIRE EST À NOTRE PORTÉE

Des mécanismes de contrôle des mises à jour doivent être instaurés. Enfin, il est anormal que la France, exportatrice de cerveaux numériques, ne stimule pas mieux la création et le développement d'entreprises de logiciels de cybersécurité, mettant fin au duopole américano-israélien dominant le marché européen.

L'action internationale doit non seulement viser à réguler le cyberespace dans la suite de l'appel de Paris du président Macron, le 12 novembre 2018 *[discours d'inauguration de l'Internet Governance Forum, à l'Unesco]*, mais aussi utiliser tous les moyens bilatéraux et multilatéraux pour inciter les Etats auteurs ou protecteurs de cyberattaques à changer de comportement. Les sanctions individuelles ne sont que l'un des outils, à l'efficacité limitée ; le poids commercial de l'Union européenne offre des perspectives importantes. Enfin, la doctrine française de cyberdéfense doit prévoir la possibilité de riposte proportionnée à toute attaque contre des infrastructures jugées essentielles aussi bien civiles que militaires. Sous l'impulsion de Thierry Breton *[commissaire européen au marché intérieur]*, la Commission européenne vient d'annoncer de façon significative une nouvelle stratégie de cybersécurité.

Pour lutter au bon niveau, des objectifs ambitieux et atteignables doivent être fixés. Vouloir éradiquer la cybercriminalité est illusoire ; la réduire est à notre portée. La lutte cyber pourrait s'inspirer de l'opération Atalante contre la piraterie menée dans l'océan Indien depuis 2008, qui a vu l'Union européenne s'appuyer sur un premier pays, la France en l'espèce, pour allier rapidité et efficacité. Les ripostes d'anticoercition pourraient être effectuées par le ComCyber *[commandement interarmées de la lutte informatique, mis en place en 2017]* ou la direction générale de la sécurité extérieure (DGSE), ou par une équipe intégrée commune, comme en Grande-Bretagne, à l'échelon national ou en coopération avec des alliés. Sans l'évolution doctrinale déjà évoquée sur le caractère global de la cyberdéfense, il n'y aura aucun effet dissuasif et rien n'empêchera la répétition de ce que le CHU de Rouen a subi fen novembre 2019, frappé par une cyberattaque massive.

Face aux ruptures que représentent la croissance exponentielle des rançongiciels et l'opération « Sunburst », notre pays doit engager une réflexion stratégique et sortir de la logique incrémentale qui n'est plus adaptée au contexte. Il nous paraît indispensable que le président de la République puisse s'appuyer sur un coordonnateur national cyber (CNC), à l'instar du coordinateur national du renseignement de lutte contre le terrorisme (CNRLT), qui a montré son efficacité. ■

Bernard Barbier *a été directeur technique à la DGSE et directeur du Laboratoire d'électronique et de technologies de l'information (LETI). Il est membre de l'Académie des technologies* ; **Jean-Louis Gergorin,** *ancien chef du Centre d'analyse et de prévision du Quai d'Orsay, est coauteur de « Cyber. La guerre permanente » (Les éditions du cerf, 2018)* ; **l'amiral Edouard Guillaud** *est ancien chef d'état-major des armées*

Soldat « augmenté », humain minoré

Pour **les philosophes Bernadette Bensaude-Vincent et Emmuel Hirsch et le professeur de médecine Kostas Kostarelos,** la modification des caractéristiques humaines du combattant est injustifiable

Le 18 septembre, le comité d'éthique de la défense a remis à la ministre des armées, Florence Parly, un avis sur le « soldat augmenté », rendu public au début de décembre. Un tel avis appelle une discussion bien au-delà des cercles de la défense, comme le soulignait l'article que lui consacrait *Le Monde* daté du 5 décembre. Il soulève, en tout cas, des inquiétudes, car, sur cette question largement débattue depuis deux décennies, il adopte une position tranchée.

Le comité se prononce en faveur de la recherche sur les nouvelles techniques d'augmentation des capacités physiques et cognitives. Il le justifie par la nécessité d'adapter les performances de la combativité des militaires face à des adversaires faisant usage de technologies qui imposeraient de conformer l'homme à ces innovations. En d'autres termes, puisque d'autres pays ont fait le choix de modifier les caractéristiques humaines du soldat afin d'en faire un instrument intégré aux stratégies de la guerre technologique, nous ne disposerions d'aucune autre option que de nous soumettre aux impératifs de cette compétition. Convient-il de se résoudre à accepter cette mutation anthropologique, qui concerne l'intégrité de la personne, au nom de l'intérêt supérieur de la défense nationale ? Ne justifiait-elle pas une concertation, y compris au plan international, dès lors qu'elle a un impact sur les valeurs de dignité, de liberté et d'égalité affirmées dans la Déclaration universelle des droits de l'homme ?

> L'ARGUMENT DE LA SINGULARITÉ DES MISSIONS ASSURÉES PAR LES MILITAIRES NE JUSTIFIE PAS LE RELATIVISME ÉTHIQUE

Faut-il rappeler que les enjeux de la guerre ont suscité des controverses philosophiques et juridiques, par exemple sur le droit de tuer ? L'augmentation médicalisée des performances du soldat renouvelle les dilemmes soulevés par l'usage des drones, relatifs à la prise de décision dans un contexte modifié par les technologies. L'« art de la guerre » a toujours été un puissant moteur d'innovations techniques. Leurs implémentations dans la vie civile sont évidentes, ne serait-ce que dans les technologies de l'information et de la communication. On doit donc être attentifs à la signification et aux effets de cette augmentation de l'humain sur nos représentations et nos pratiques sociales. Il paraît discutable de limiter la réflexion à la délibération d'un comité d'éthique dédié à la défense, alors que son avis relatif au soldat augmenté concerne nos principes d'humanité dans l'ensemble de la société.

Puisque l'armée est, par vocation, engagée dans des rapports de forces, ce comité estime légitime de doter les troupes des moyens les mieux adaptés aux circonstances. Aussi, tenant compte d'un principe de réalité, se borne-t-il à fixer quelques seuils ou limites qu'il conviendrait de ne pas outrepasser, en insistant sur l'importance de la proportionnalité et de la réversibilité des dispositifs médicaux à mettre en œuvre. Il énonce la liste connue des risques liés aux techniques d'augmentation (en particulier l'addiction) et recommande une évaluation bénéfices/risques au cas par cas. Au bilan, augmenter la *« capacité opérationnelle »* des soldats semble s'imposer comme un moyen en vue d'une fin : permettre aux militaires d'assumer leurs missions dans les conditions les mieux adaptées aux contraintes du terrain. Il s'agit également d'atténuer d'autres risques psychologiques comme le stress et les symptômes post-traumatiques suite à des violences. En fait, le recours aux technologies biomédicales vise à compenser et à diminuer la vulnérabilité et la sensibilité humaines. Le paradoxe serait que pour augmenter les performances du soldat il conviendrait de diminuer ce qui fait son humanité.

En même temps, l'avis rappelle que les militaires ayant devoir d'obéissance, y compris jusqu'au sacrifice, aucun principe ne s'opposerait à leur imposer le recours à des interventions sur leur corps ou leur psychisme ayant pour justification et objectif d'accroître leurs performances. On n'ose imaginer les manipulations auxquelles pareille licence pourrait inciter les autorités militaires, dès lors qu'un intérêt supérieur les exonérerait d'un principe éthique fondamental depuis le code de Nuremberg : celui du consentement libre, éclairé et exprès !

Pour une réflexion politique

L'argument de la singularité des missions assurées par les militaires, parfois dans des contextes extrêmes, ne justifie pas le relativisme éthique là où les valeurs de dignité humaine sont engagées. Car ces transgressions, ne serait-ce que par exception dans un premier temps et demain de manière routinière, compromettent nos principes dès lors qu'une personne est instrumentalisée en fonction d'objectifs qui révoquent ses droits fondamentaux. L'impératif supérieur invoqué n'est pas de renforcer ses capacités à préserver sa vie, mais d'en faire un combattant augmenté en occultant ses facultés humaines de jugement, de discernement, sa capacité d'apprécier en conscience les risques, y compris ceux auxquels il serait exposé. Dans le contexte de numérisation de l'humain et de virtualisation du monde, la prudence aurait été plutôt de renforcer la compétence du militaire à assumer ses éminentes fonctions en conscience et en responsabilité. L'éthique médicale ne doit pas s'adapter aux règles d'une guerre assimilable à un jeu vidéo, car les conséquences des décisions d'un combat réel ne s'évaluent pas à l'aune du score d'un engagement virtuel.

Nous attendons d'un comité d'éthique de la défense qu'il éclaire les décisions sensibles sans renoncer à considérer comme son obligation de préserver les valeurs inconditionnelles auxquelles nos démocraties sont attachées. Celles précisément dont sont garantes nos armées. Dans le contexte de menaces géopolitiques, de terrorisme, d'exactions commises y compris par des armées régulières, ne convient-il pas d'opposer nos valeurs d'humanité à ceux qui s'y opposent ? Nous ne sommes pas naïfs au point de ne pas comprendre les impératifs que les autorités militaires doivent intégrer à leurs stratégies. Mais admettre qu'il conviendrait de sacrifier l'humanité d'une personne afin de lui conférer des capacités augmentées pour défendre notre société appelle une réflexion éthique et politique qui mérite mieux que l'avis d'un comité. Une concertation au sein de notre représentation nationale est nécessaire, de même qu'une réflexion au plan international en vue de la rédaction d'un texte qui encadrerait ces interventions biomédicales sur le soldat. Car nos valeurs morales, celles de nos sociétés y sont engagées. ■

Bernadette Bensaude-Vincent *est professeure émérite de l'université Paris-I-Panthéon-Sorbonne et membre de l'Académie des technologies*
Emmanuel Hirsch *est professeur d'éthique médicale et président du Conseil pour l'éthique de la recherche et l'intégrité scientifique (Poléthis) de l'université Paris-Saclay*
Kostas Kostarelos *est professeur de nanomédecine à l'université de Manchester et à l'Institut catalan de nanoscience et nanotechnologie de Barcelone*