54° SN AED Comité 1 IHEDN – NDU

RESUME

« How will cyber technologies innovation (Big Data, Internet of Thing, AI…) impact future battlefields ?"

L'emprise croissante du numérique sur la marche du monde trouve ses origines dans les avancées remarquables de l'informatique, de l'intelligence artificielle, de la robotique, de l'analyse de données et dans l'essor des réseaux. Elle se caractérise par une accélération spectaculaire des innovations et une mutation des comportements sociaux. Elle suscite de formidables opportunités mais induit aussi de nouvelles menaces comme l'illustrent les cyber-attaques en Estonie en 2007, « *Stuxnet* » en 2010, les actions d'influence via l'exploitation des réseaux sociaux lors des dernières campagnes présidentielles américaine et française, la robotisation du champ de bataille avec la généralisation des systèmes télé-opérés comme les drones et aujourd'hui, le spectre des systèmes d'armes autonomes létaux (SALA).

Certaines vulnérabilités des cyber-technologies ou le détournement de leurs usages peuvent menacer jusqu'à l'équilibre des puissances mondiales. Les forces armées occidentales ont pu, jusqu'à présent, s'appuyer sur leur supériorité opérationnelle et technologique. Toutefois, la large diffusion des technologies érode leur ascendant et fait apparaître des adversaires non étatiques capables de bouleverser l'ordre établi sur les différents champs de confrontation.

Ce rapport d'étude conjoint entre l'IHEDN et la National Defence University de Washington analyse, à l'horizon 2040, l'impact sur les futurs champs de bataille, de l'innovation dans les cyber-technologies (cyber-sécurité, Big Data, Intelligence Artificielle, objets connectés). Au cœur de ces travaux, trois fictions prospectives présentent les nouveaux modes de confrontation envisageables sur le champ de bataille traditionnel (terre, mer, air, espace), dans le cyberespace militaire et civil et sur les infrastructures critiques.

Construits à partir d'une réflexion sur les grandes tendances et ruptures associées, ces fictions mettent en scène trois aventures dont les personnages principaux se retrouvent dépassés par les événements au cœur d'une crise dont ils sont les protagonistes : « Domino effect, User Zero », « The end of the physical internet », « Blitzkrieg 4.0 ».

Cette étude propose enfin des recommandations à la communauté de défense, applicables en France et/ou aux États-Unis. Elles visent à adapter notre outil de défense aux nouveaux défis posés par les cyber-technologies sur le champ de bataille en intégrant aussi les aspects stratégiques et industriels. Pour maintenir leur supériorité, les armées occidentales devront intégrer les cyber-technologies dans leurs capacités et faire preuve de réactivité pour contrer les adversaires qui ne manqueront pas d'en faire aussi usage.

Le développement de la coopération avec les alliés sera essentiel pour préparer les futurs règlements ou accords internationaux portant sur la caractérisation des cyber-actions entre Etats, la recevabilité des preuves d'attribution des cyber-attaques et la codification des moyens d'intervention pour des réponses cyber ou militaires graduées et proportionnées. Adopter des méthodes d'acquisition agiles ou réactives présentera un double avantage, d'une part pour acquérir des équipements technologiques peu complexes dans une démarche « *good enough* » pour certains types d'opérations militaires et d'autre part favoriser l'utilisation de technologies grand public dans la conception de certains systèmes d'armes plus complexes, afin de réduire les coûts.

Face aux menaces que constitueraient des cyber-attaques massives dans une guerre totale, notre société, dans sa globalité, devra s'adapter. La Base Industrielle et Technologique de Défense devra poursuivre et renforcer son investissement dans l'innovation, la dualité civil/militaire et dans les technologies numériques. L'amélioration de la confiance accordée par le citoyen dans les technologies numériques ainsi qu'une cyber-résilience accrue aux attaques devront être recherchées.

Ainsi, loin d'une illusoire protection via l'interdiction des SALA par la communauté internationale et loin de la dangereuse certitude que notre outil de défense actuel saurait contrer ces chimères numériques, chaque nouvelle technologie du Cyberespace doit être considérée comme, à la fois, une opportunité et une menace. Sans certes prédire l'apocalyptique « Sky Net », les rapides et profondes évolutions apportées par le numérique continueront de métamorphoser les activités humaines et les conflits futurs. Envisager la conflictualité sans intégrer la dimension numérique - en mutation permanente - positionnerait le stratège dans la roue d'un hamster, voué à poursuivre les actuelles réflexions alors qu'il se doit d'envisager les ruptures technologiques et les surprises stratégiques.