naïveté, on peut lui reprocher un optimisme excessif quant aux effets possibles d'une telle dérégulation. Enfin, on peut raisonnablement douter de la réception d'une telle proposition par les décideurs militaires, tant elle s'oppose à la culture dominante et aussi aux intérêts propres de ces derniers.

Stéphane Taillat

CYBER WAR WILL NOT TAKE PLACE

Thomas Rid
Londres, Hurst, 2013, 256 pages

Clin d'œil au célèbre *La Guerre de Troie n'aura pas lieu* de Jean Giraudoux, le livre de Thomas Rid apporte une réflexion essentielle sur la menace d'une hypothétique cyberguerre. Précis et richement documenté, il explore les dimensions stratégiques, politiques, historiques, culturelles et techniques en vue de déterminer si une « guerre » a(ura) lieu dans le cyberespace.

S'appuyant en détail sur ce qu'il considère comme les mythes fondateurs et ce qu'il nomme les Cassandre[1] de la « cyberguerre », son livre est découpé en huit chapitres comme autant de mythes à déconstruire. Ainsi, le deuxième chapitre, consacré à la violence, est le pivot de son argumentation. Se plaçant dans le droit fil du traité de stratégie militaire *De la guerre* de Clausewitz, il considère qu'il n'y a pas et il n'y aura pas de cyberguerre, même s'il reconnaît que se déroule une intense activité conflictuelle dans le cyberespace. Pour cela, il s'attache à démontrer que si la plupart des cyberattaques sont susceptibles d'être violentes, elles ne peuvent l'être qu'indirectement. La violence administrée par un code informatique offensif, complexe et puissant comme Stuxnet apparaît finalement limitée, non émotionnelle et symbolique.

Une cyberattaque, en particulier consacrée au sabotage ou à l'espionnage, posséderait même un certain caractère éthique, permettant d'atteindre un objectif politique par l'utilisation d'une moindre violence. Dans cette acception, la subversion pose, elle, problème par ses effets psychologiques potentiels. En prime, sa capacité à altérer la confiance qu'incarne la cible, souvent étatique, peut se révéler efficace et produire des effets durables. L'opération Orchard d'Israël contre une installation nucléaire expérimentale en Syrie fournit une illustration convaincante.

S'intéressant dans le septième chapitre au problème de l'attribution des cyberattaques, T. Rid affirme qu'il s'agit davantage d'une question de volonté politique et de moyens associés que d'impossibilités techniques de traçabilité. Des éléments de preuves supplémentaires non techniques, notamment psychosociaux et culturels, et du renseignement, sont nécessaires pour atteindre un niveau d'estimation « probable » ou « presque certain », pour permettre une décision politique en vue de réagir. Le huitième chapitre vient récapituler les idées fortes développées au cours du livre, en insistant sur les présupposés avantages d'une cyberattaque : efficace tant qu'elle reste discrète, elle devient plus difficilement répétable dès lors qu'elle devient visible. La menace potentielle qu'elle représentait perd alors en crédibilité.

Finalement, la cyberguerre a une valeur plus métaphorique que descriptive, et son concept même apparaît exagéré, un « cyber-Hiroshima » demeurant « très peu vraisemblable ». Pour T. Rid, ce

1. SCADA – URSS 1982, Estonie avril-mai 2007, opération Orchard septembre 2007, Géorgie août 2008, Stuxnet 2010.

n’est pas le cyberespace qui est militarisé, c’est le débat ; sans doute biaisé et confisqué au travers de mythes savamment construits et entretenus. Débat que son ouvrage permet de maintenir ouvert en démontant les rouages essentiels exposés. Ainsi donc, *La Cyberguerre n'aura pas lieu* est, comme son quasi éponyme, déjà un classique, s’adressant autant au spécialiste qu’au néophyte.

Éric Hazane