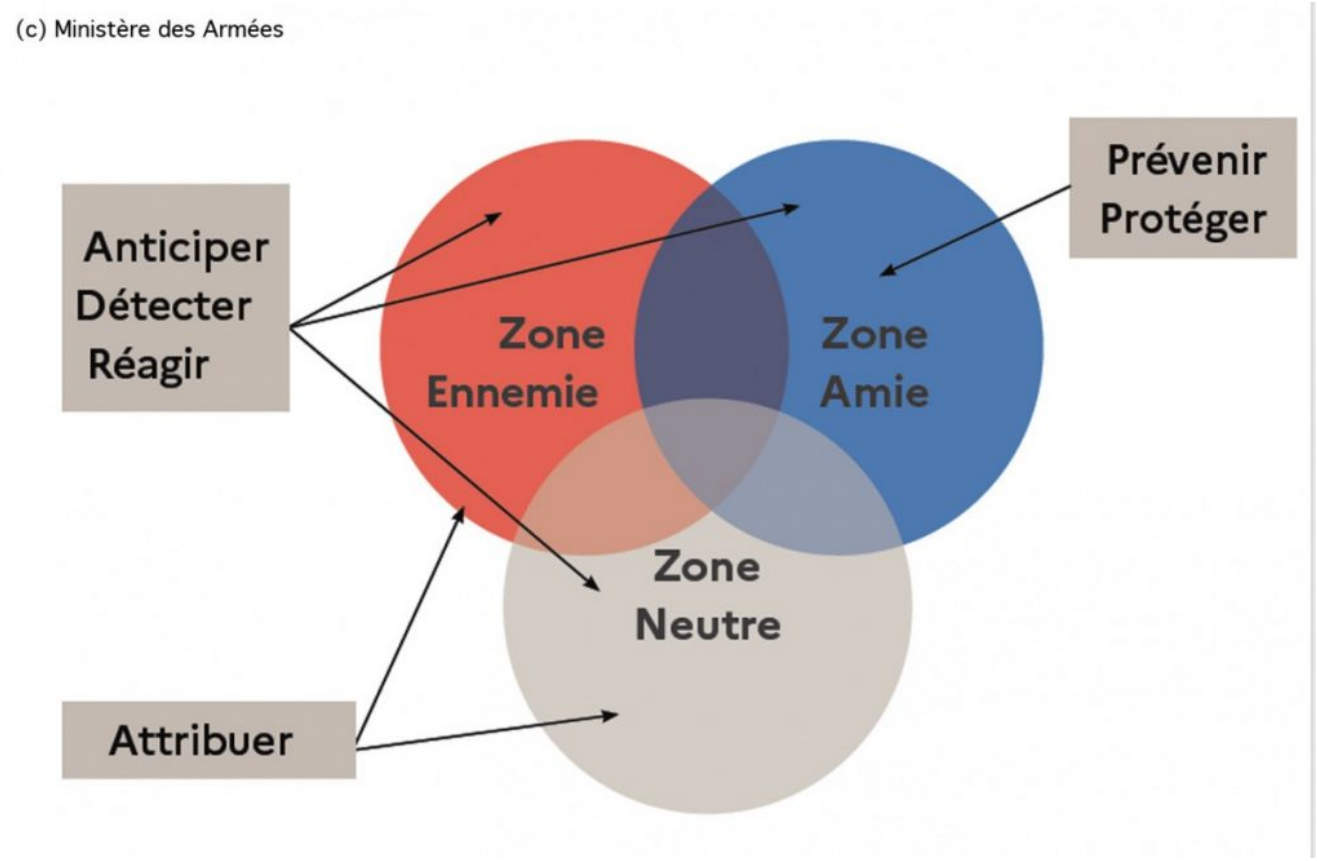
Défense : le cyber, de la conflictualité à la guerre froide



Les attaques dans le cyberespace au-dessous du seuil de l'acte de guerre et la centralisation des flux numériques d'information par certains Etats rappellent la Guerre froide (1947-1991), mais sans mécanismes de désescalade.

Citant la Chine, l'Iran et la Corée du Nord, la ministre des Armées, Florence Parly, a constaté « *une asymétrie entre les autocraties déshinibées et les démocraties libérales* », lors de son intervention le 8 septembre 2021 au Forum international de la cybersécurité, tenu à Lille du 7 au 9 septembre.

« Cybercombattants ». Pour la période 2019-2025, le ministère des Armées dispose d'un budget de 1,6 Md€ pour la cyberdéfense et prévoit d'en augmenter le recrutement à 1.900 personnels pour soutenir les missions de renseignement, de protection, de défense et d'action. Recrutés sous statut militaire, civil ou réserviste, les guerriers du cyber occupent des postes d'expert ou de cadre, effectuent leur premier emploi ou diversifient leur parcours professionnel. Leurs activités portent sur : l'ingénierie logicielle (expression du besoin, conception et développement) ; l'administration système et sécurité ; la sécurité des systèmes

d’information (assistance, conseil et expertise) ; l’évaluation des systèmes par audit, test d’intrusion, « Red Team » (hackers) et « Blue Team » (défenseurs) ; lutte informatique défensive par l’évaluation de la menace, l’analyse de traces et la supervision dans les « SOC » (systèmes de détection d’intrusion), « forensic » (analyse du système après intrusion pour récupérer les fichiers) et « reverse engineering » (analyse des bogues d’un programme) ; veille sur les réseaux sociaux. Des postes spécifiques seront créés au sein des armées, à la Direction générale de la sécurité extérieure et à la Direction générale de l’armement, qui développe de nouveaux équipements. Les personnels à recruter renforceront le vivier de compétences à la disposition du Commandement de la cyberdéfense (Comcyber), qui devrait disposer de 5.000 cybercombattants d’ici à 2025. Placé sous l’autorité directe du chef d’état-major des armées et implanté à Paris et Rennes, le Comcyber a pour missions : la protection des systèmes d’information de l’Etat-major des armées et du ministère des Armées ; la conception, la planification et la conduite des opérations militaires offensives et défensives dans le cyber ; la contribution à la préparation de l’avenir du domaine de la cyberdéfense.

Unités militaires spécialisées. L’armée de Terre, particulièrement exposée aux cyberattaques, s’est dotée des moyens pour s’en protéger. A Rennes, le Commandement des systèmes d’information et de communication contribue aux missions cyber et à la préparation à l’engagement des forces en opérations. La 807ème Compagnie de transmissions, spécialisée dans la défense des systèmes d’information (SI) projette en permanence des personnels en opérations extérieures. La 785ème Compagnie de guerre électronique (CGE) effectue des audits de sécurité informatique. Le Centre technique de lutte informatique défensive assure la surveillance et la défense des systèmes métiers déployés en métropole. A Paris, la Cellule de coordination de lutte informatique défense assure la veille de l’empreinte numérique (SI et sites internet). Enfin, le Commandement du renseignement des forces terrestres regroupe la 785ème CGE, le 44ème Régiment de transmissions (renseignement d’origine électromagnétique), le 54ème Régiment de transmissions (guerre électronique) et le Centre du renseignement terre (analyse et exploitation).

Loïc Salmon

Défense : détecter les cyberattaques et réagir vite

Cyber : nouvelle doctrine pour la lutte informatique

Cyber : instrument de la puissance russe en Baltique