



La guerre en Ukraine ne respecte pas les normes de la cyberguerre

0 • 0

La guerre en Ukraine ne respecte pas les normes de la cyberguerre

Crédits : Matej Moderc/iStock

« *L'invasion russe a dangereusement déstabilisé les normes de cybersécurité* », **titre** The Register, relayant les craintes exprimées à Black Hat par Kim Zetter, journaliste experte des questions de cybersécurité.

Elle rappelle qu'en 2015, les Nations Unies avaient chargé 20 pays, dont les États-Unis, le Royaume-Uni, la Chine et la Russie, d'élaborer les lignes directrices du droit international dans le cyberspace, en prévision des cyberattaques qui accompagneraient les conflits et guerre à venir.

« *Ils ont convenu que les États ne devraient pas intentionnellement endommager les infrastructures critiques d'autres États ou autrement entraver le fonctionnement des infrastructures critiques qui fournissent des services publics* », a récapitulé Zetter :

« *Ils ont également convenu que les États ne devraient pas autoriser l'utilisation de leur territoire pour des cyberattaques contre d'autres États et devraient prendre des mesures pour atténuer les activités malveillantes émanant de leur territoire lorsqu'elles visent les infrastructures critiques d'autres États.* »

Au-delà des cyberattaques émanant des Russes et des Ukrainiens, Zetter évoque également un programme de bug bounty **lancé** par une entreprise estonienne afin de confier à des hacktivistes ukrainiens des vulnérabilités dans les systèmes d'infrastructure critiques russes.

« *Si une entreprise russe située en Allemagne organisait un programme offensif de primes aux bugs ciblant les infrastructures critiques ukrainiennes et partageait les vulnérabilités découvertes avec la communauté du renseignement russe ? Berlin, Bruxelles et Washington jugeraient-ils ce comportement acceptable de la part du secteur privé ?* », s'interroge Kim Zetter.

Victor Zhora, chef adjoint de l'agence ukrainienne de cybersécurité défensive, a de son côté qualifié de « *cybercrimes de guerre* » certaines des cyberattaques dont son pays a fait l'objet, **relève** Motherboard :

« *La plupart des opérations cinétiques [russes] se sont concentrées sur les infrastructures civiles, et les cyberopérations qui les soutiennent frappent les infrastructures informatiques civiles, nous pouvons [donc] les traiter comme des crimes de guerre dans le cyberspace.* »



