Libre cours de Roula AZAR DOUGLAS

La cyberguerre est déclarée !

L'équipe de recherche de l'UIR en Web science du Cemam de l'USJ.

Guerre télaire (de la Toile), cyberespace, cyberarmes, cibles cybernétiques, cyberdéfense et cybersécurité. Vocabulaire de guerres bien réelles avec leurs lots de cybervictimes et de pertes matérielles. Aujourd'hui, plus que jamais, l'espace cybernétique est un terrain d'affrontements et de conflits. Dans ce contexte, l'Unité interdisciplinaire de recherche (UIR) en Web science du Centre d'études pour le monde arabe moderne de l'USJ a tenu le 22 mars un séminaire ouvert d'études avancées sur le thème : « Le Web à l'épreuve de la cyberguerre ».

Après une brève introduction de Stéphane Bazan, directeur de l'Unité des nouvelles technologies éducatives de la faculté des sciences de l'éducation, quatre étudiants, assistants de recherche ou stagiaires à l'UIR, tous diplômés en master de relations internationales, ont fait le tour du sujet – passionnant et d'actualité – de la guerre cybernétique. « La guerre de l'information désigne toute activité destinée à acquérir des données et des connaissances dans une finalité stratégique. La cyberguerre – qui représente la dimension technique de la guerre de l'information – désigne, elle, le recours aux capacités cybernétiques pour mener des opérations dites agressives, dans le cyberespace, contre des cibles militaires, un État ou des sociétés », explique Sabrine Saad.

Espionnage, sabotage, blocage, saturation, vols de données, déni de service, les types d'agressions dans l'espace cybernétique – exécutées dans un but menaçant d'attaque ou de déstabilisation – sont multiples. Malgré la fin de la guerre de Corée en 1953, « la cyberguerre entre les deux Corées bat son plein », affirme Sofia el-Amine. L'assistante de recherche évoque les attaques majeures de la guerre cybernétique entre les deux pays et la réponse tardive de la Corée du Sud, avant d'aborder la cyberguerre qui fait rage entre les États-Unis et la Chine, et l'attaque du *New York Yimes* par des hackers chinois au mois de janvier.

Que faire face aux cyberarmes ? « Face aux menaces cybernétiques, les États renforcent leurs mesures de cyberdéfense qui consiste à utiliser des moyens physiques et virtuels afin de contrer la cyberguerre », répond Addis Tesfa. Le jeune assistant de recherche mentionne l'Internet national iranien, dont le premier noyau, entièrement contrôlé par le régime et capable de fonctionner sans le Web mondial, a été achevé il y a quelques mois, suite aux attaques de 2010 visant le programme nucléaire iranien par le virus Stuxnet. « La cybersécurité englobe les usages offensifs et défensifs des systèmes d'informations. Ses acteurs sont les États et les entreprises », précise Saada Kalakech.

Stéphane Bazan conclut : « Aujourd'hui, on ne doit plus se demander si on a été victime d'une attaque informatique, mais plutôt s'interroger depuis quand, comment et pourquoi on l'a été. »