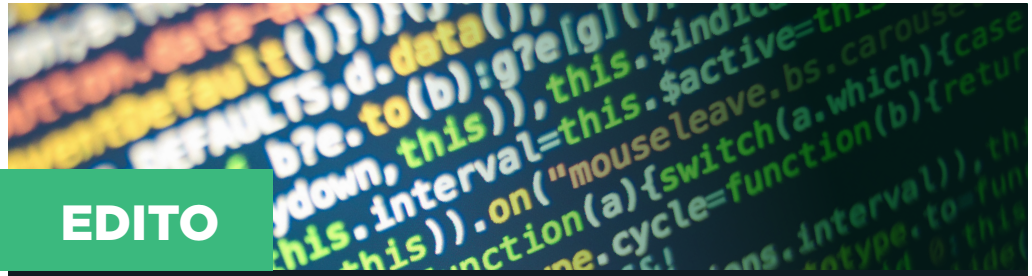
2 JUILLET 2019

SÉMINAIRE

CYBERDÉFENSE & STRATÉGIE

ET SI INTERNET S'EFFONDRAIT ?

CERCLE NATIONAL
DES ARMÉES



EDITO

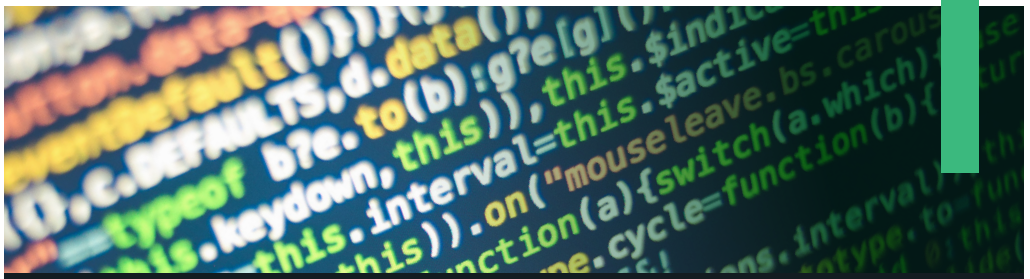
INTERNET : FAUT-IL CRAINDRE UN “BLACK-OUT” MASSIF ?

Depuis 20 ans, Internet a montré sa résilience. Même si quelques attaques ou erreurs de manipulation ont provoqué des ralentissements ou coupures ponctuelles et localisées, les infrastructures internet ont tenu bon face à l'adversité. Elles ont d'abord résisté à l'erreur humaine, à l'image du routage BGP, véritable «ciment» du réseau, régulièrement fragilisé par des erreurs de manipulation. Elles ont ensuite résisté à toutes sortes d'attaques malveillantes, comme celle ayant affecté l'ICANN et le système DNS en février 2019 ou bien encore les nombreux «dénis de service distribués» (DDoS) générés par le botnet Mirai, qui a notamment coupé le Libéria du reste du monde en 2016. Elles ont enfin résisté à l'explosion des utilisateurs, des usages, des données et du trafic (près de 40% d'augmentation chaque année). Alors est-il vraiment utile de se faire peur ?

La réponse est oui ! C'est justement parce que Internet est devenue une «commodité» et les données le nouvel «or noir», que l'on a une fâcheuse tendance à oublier les câbles, les points d'échange, les protocoles de routage et d'adressage, les datacenters, bref les infrastructures qui sous-tendent cette évolution, qu'il faut craindre une panne massive pour mieux s'y préparer.

A contrario, c'est aussi parce que certains États, Russie en tête, s'entrainent à couper leur « portion » d'internet du reste du réseau et que « l'arsenalisation » de l'espace numérique est de plus en plus assumée, que la question mérite d'être posée. L'hyperconnectivité, qui deviendra la norme avec la 5G, et l'immixtion de l'IoT dans tous les domaines de l'activité humaine renforcent encore cette exigence. D'autant que la concentration des infrastructures et la faible diversité «génétique» de certains équipements renforcent le caractère systémique des risques, non seulement en matière de confidentialité mais également de disponibilité.

Quels sont aujourd'hui les principaux talons d'Achille des infrastructures Internet en termes de vulnérabilités et de menaces ? Quelles sont les réponses politiques, juridiques, techniques et technologiques pour faire face à ces défis ? Doit-on revoir les protocoles clés du réseau ? Faut-il imaginer au plan juridique une protection spécifique du «coeur public» d'internet ? A l'heure du retour des Etats-puissance et d'une montée de l'unilatéralisme, quel système de sécurité collective peut-on imaginer ?



PROGRAMME

14H30 – 14H40
ALLOCUTION D'OUVERTURE
Général Olivier Bonnet de Paillerets, Commandant de la Cyberdéfense

14H40 – 15H15
PRÉSENTATION D'UN SCÉNARIO D'ATTAQUE,
Guillaume Prigent et Adrien Barchapt, Diateam

15H15 – 15H35
DÉMONSTRATION TECHNIQUE : SÉCURISER LES LOGICIELS CLÉS DES CŒURS DE RÉSEAU.
Julien Signoles, CEA List

15H35 – 15H45
PITCHES DE PROJETS DE THÈSE OU DE RECHERCHE.
Avec Florent Kirchner, CEA List, et Thomas Clédel, IMT-Atlantique

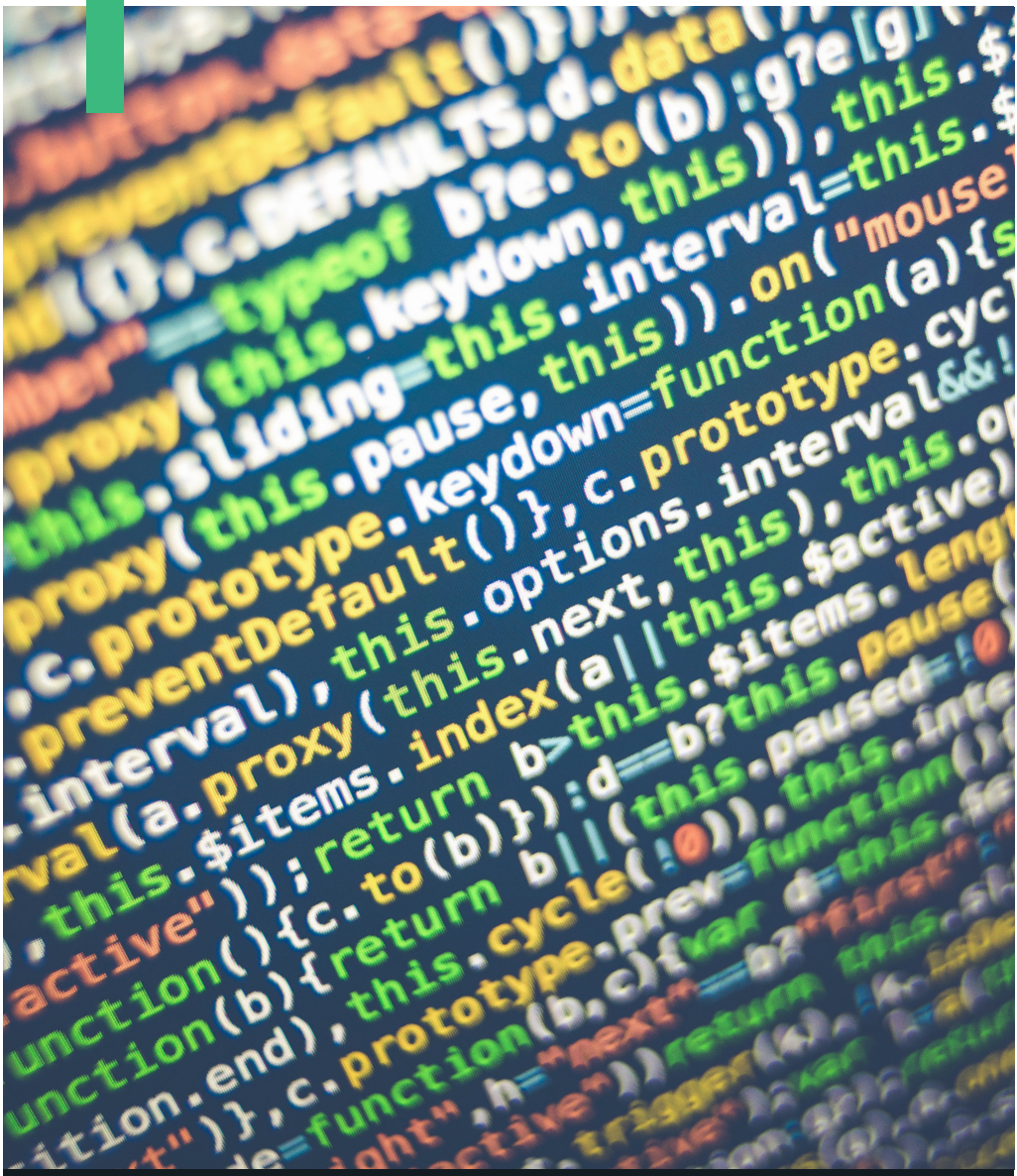
15H45 – 16H00
Pause Café

16H00 – 16H20
TÉMOIGNAGE SUR UNE GESTION DE CRISE RÉUSSIE

16H20 – 16H40
LES BONNES PRATIQUES EN MATIÈRE DE COMMUNICATION DE CRISE,
Stéphanie Ledoux, ALCYCONIE

16H45 – 17H30
TABLE RONDE : “DOIT-ON S'ENTRAINER À LA DÉCONNEXION”
Avec François-Bernard Huygue, IRIS, Xavier Hartout, Adenium, La Chaire IMT sur la cybersécurité des infrastructures critiques,

17H30 – 17H50
Conclusion



ORGANISÉ ET ANIMÉ PAR :

ceis

POUR LE COMPTE :

COMCYBER COMMANDEMENT DE LA CYBERDÉFENSE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

Dans le cadre du contrat-cadre n°2018-02 intitulé : « défense, sécurité et actions dans l'espace numérique : enjeux, environnement, menaces, défis ».