ARTICLE D'ALAIN BAUER DANS LA REVUE DE CEA

"Le cyberrisque n'est pas près de disparaître"

Dans cet article rédigé par **Professeur Alain Bauer**, Directeur de l'équipe PSDR3C, met en lumière le fait que les cyber-risques ne sont pas près de disparaître et explique pourquoi il pense que c'est le cas.

DOSSIER | MENACES

« Le cyberrisque n'est pas près de disparaître »

L'avis de... Alain Bauer
professeur de criminologie et responsable du pôle sécurité défense renseignement criminologie cybermenaces et crises au Cnam

Depuis les années 1970, les experts et les criminologues mettent en garde contre cet autre *Big One*, un tremblement de terre numérique porté par la cyberguerre et son lot de cybermenaces, aussi destructeur qu'un crash géologique. Sans même imaginer que toute une zoologie d'événements se cumulerait pour créer un effet de chaos considérable : falsification d'e-mails de compagnies d'électricité ou de banques, *ransomwares*, blanchiment d'argent au moyen de cartes bancaires prépayées, sans oublier l'immense système de Ponzi né de la spéculation sur les cryptomonnaies ou les cyberattaques militaires régulières contre l'Ukraine, l'Otan, la Corée du Sud, les États-Unis.

Les criminels sont à la fois des hackers sociaux, politiques ou économiques, des racketteurs proposant leur protection, des agents d'influence, des espions d'États et des militants. Ces mercenaires des réseaux agissent, de plus en plus souvent, dans un espace de « libre échange » et pour le compte du plus offrant, parfois en conservant, à l'instar du collectif de hackers *Anonymous*, un véritable attachement aux valeurs qu'ils revendiquent.

Ces pirates considèrent les i
tures, les plateformes, les fo
de logiciels et les développe
des vecteurs d'entrée dans
nistrations, les entrepri
infrastructures critiques. L
malveillants placent des
tout au long de la chaîne
sionnement en logiciels,
dans les codes sources pro
les référentiels des dévelo
bibliothèques *open source*,

Le problème réside dans la
générale dans laquelle s'eng
prédation criminelle, l'espi
brouillage de serveurs, le
données ou leur destruction
existe une logique spécifiq
chacune de ces actions ou t

Pourtant, nous analysons
l'essentiel alors que c'est l
réseau et ses parties « c
comme les points d'échang
centres névralgiques perm
cès au web mondial, qui co
plus. Serveurs racines, ali
électrique, refroidisseme
sous-marins, hangars, les i
tures *brick and mortar* s
vulnérables que le soft. Et l
verte des opérations militai
depuis le début de la nouv
du conflit en Ukraine l'a so
pelé à tous.

L'enjeu est d'autant plus i
que la gestion des serve
confiée à des organismes
considèrent la sécurité co
affaire confidentielle, si bi
pays n'ont d'autre choix q
confiance à une entité sur l
n'ont aucun contrôle alors
dépositaire de tous leurs
communication électroni

L'espionnage des organisati
les communications est e
une menace majeure. De
services de l'État admetten
qu'un nombre croissant d
de Troie sont installés et a
des réseaux dont le trafic co
quantité considérable de

10 octobre 2023