# Cyber : les défis de demain

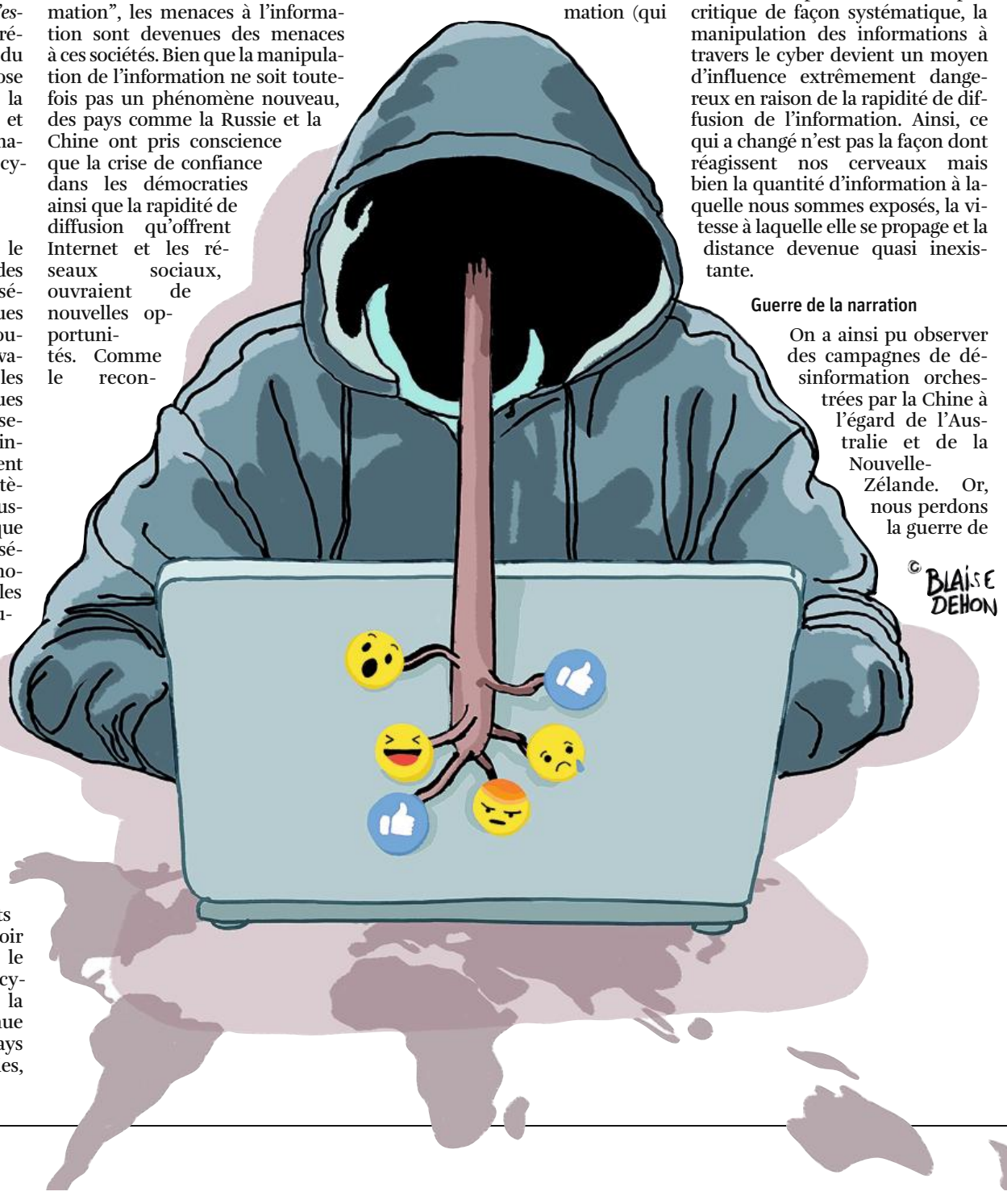
En mai 2019, le secrétaire général de l'Otan Jens Stoltenberg déclarait: *"Plus nos infrastructures critiques seront protégées et résilientes, plus nos ennemis se concentreront sur l'esprit de nos sociétés."* Cette phrase résume assez bien la complexité du cyberespace. En effet, celui-ci pose aujourd'hui trois défis majeurs: la vulnérabilité des infrastructures et des données, la guerre de l'information dans le cyberespace, et la cybersouveraineté.

### Paralyser l'économie

Le premier, et probablement le plus connu, concerne la sécurité des infrastructures et par conséquent les dimensions physiques (ordinateurs, serveurs, routeurs, etc.) et logistiques (softwares, etc.) du cyberespace. Malgré les récents exemples de cyberattaques de type hard, les investissements restent, dans notre pays, insuffisants. Les risques que courent les infrastructures de nos ministères et entreprises sont souvent sous-évalués alors qu'une cyberattaque pourrait avoir pour conséquence la paralysie de notre économie. Parallèlement, et bien que les cyberattaques DDoS (Distributed Denial of Service) subies par l'Estonie en 2007 aient tout de même alerté la communauté internationale sur le potentiel du cyberespace, tout un pan du danger est souvent négligé.

### Menaces à l'information

C'est sur ce dernier que reposent les deux défis suivants, souvent sous-estimés alors qu'ils touchent aux fondements de nos démocraties: à savoir la guerre de l'information dans le cyberespace et la logique de la cybersouveraineté défendue par la Chine. L'information est devenue un moyen pour déstabiliser les pays et en particulier les démocraties, aussi bien par des acteurs externes mais également de plus en plus internes. Pour nos sociétés de plus en plus connectées et considérées comme des "sociétés de l'information", les menaces à l'information sont devenues des menaces à ces sociétés. Bien que la manipulation de l'information ne soit toutefois pas un phénomène nouveau, des pays comme la Russie et la Chine ont pris conscience que la crise de confiance dans les démocraties ainsi que la rapidité de diffusion qu'offrent Internet et les réseaux sociaux, ouvraient de nouvelles opportunités. Comme le reconnaît le neuroscientifique Giordano, *"le cerveau humain est devenu le champ de bataille du XXIe siècle"*. En s'appuyant sur des failles cognitives humaines comme le biais de confirmation (qui fait que nous avons tendance à privilégier les informations confirmant nos hypothèses) ou notre paresse intellectuelle naturelle qui consiste à ne pas exercer son esprit critique de façon systématique, la manipulation des informations à travers le cyber devient un moyen d'influence extrêmement dangereux en raison de la rapidité de diffusion de l'information. Ainsi, ce qui a changé n'est pas la façon dont réagissent nos cerveaux mais bien la quantité d'information à laquelle nous sommes exposés, la vitesse à laquelle elle se propage et la distance devenue quasi inexistante.




### Guerre de la narration

On a ainsi pu observer des campagnes de désinformation orchestrées par la Chine à l'égard de l'Australie et de la Nouvelle-Zélande. Or, nous perdons la guerre de