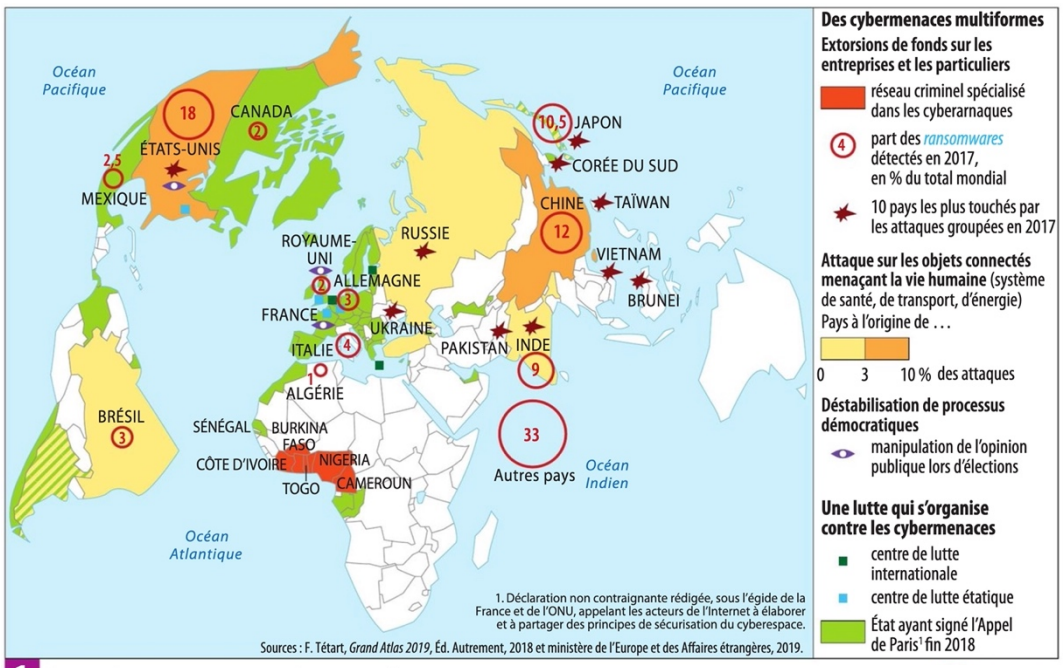
États et organisations internationales face à des cybermenaces croissantes

Comment États et organisations internationales s'organisent-ils pour sécuriser leur cyberespace ?

En 2007, l'Estonie, victime de la première cyberattaque, a vu son réseau informatique totalement paralysé. Depuis, les organisations criminelles, mais aussi certains États, ont fait du cyberespace un nouveau terrain de propagande et de criminalité.



1. Déclaration non contraignante rédigée, sous l'égide de la France et de l'ONU, appelant les acteurs de l'Internet à élaborer et à partager des principes de sécurisation du cyberespace.

Sources : F. Tétart, *Grand Atlas 2019*, Éd. Autrement, 2018 et ministère de l'Europe et des Affaires étrangères, 2019.

1 Les cyberattaques, un risque croissant

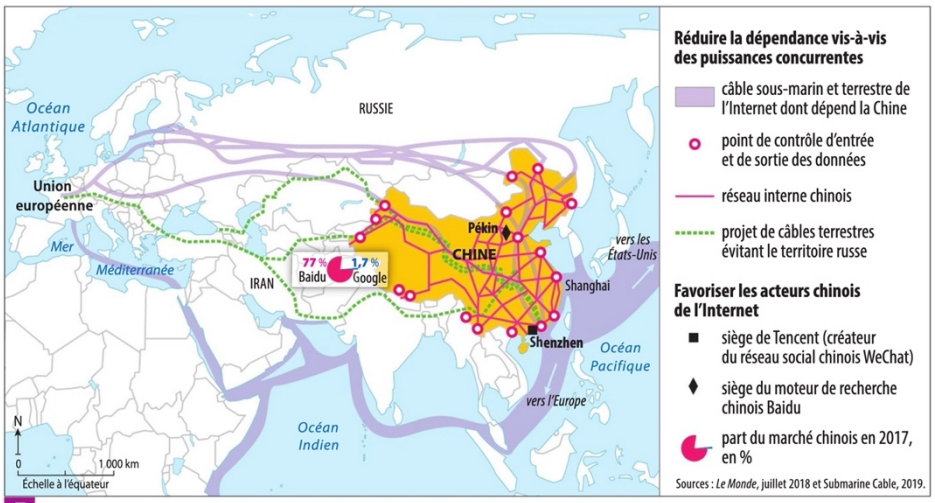
3 La cybersécurité, un enjeu pour les États

Affiche de l'édition 2018 du mois européen de la cybersécurité en France, Anssi. Depuis 2009, la France a mis en place l'Agence nationale de la sécurité des systèmes d'information qui mène des actions de sensibilisation à la cybersécurité.

2 Sécuriser les câbles, un enjeu géostratégique

En octobre 2015, l'Algérie s'est retrouvée privée de 80 % de ses capacités d'accès à Internet pendant près d'une semaine. La cause ? La simple bévue de l'équipage d'un navire qui avait jeté puis relevé son ancre là où passait un câble stratégique pour cet usage. Deux ans plus tard, en juillet 2017, le même scénario se reproduit au large de la Somalie, où un porte-conteneurs a privé accidentellement la Somalie d'Internet trois semaines durant. Et, dans un autre registre, lors de l'épisode du déploiement de forces russes en Crimée, en 2014, la péninsule avait été isolée du reste de l'Ukraine par la coupure physique des communications. Le risque terroriste n'est pas non plus absent : en 2007, Scotland Yard avait déjoué un projet d'Al-Qaïda qui visait des infrastructures vitales pour l'Internet au Royaume-Uni.

D'après J.-Y. Bouffet, « Géopolitique des câbles sous-marins », *Conflits*, avril-mai-juin 2018.



Sources : *Le Monde*, juillet 2018 et Submarine Cable, 2019.

5 La stratégie chinoise de cybersécurité : construire un intranet contrôlé

4 La stratégie européenne de cybersécurité : renforcer les coopérations

Dans un espace numérique globalisé, l'approche nationale ne semble plus suffisante. Premier succès majeur d'une action commune du FBI et d'Europol : deux des plus gros marchés criminels du darknet, AlphaBay et Hansa, ont été démantelés en juillet 2017, preuve de l'efficacité des actions coordonnées. Le 9 mai 2018, une première directive européenne est entrée en vigueur dans tous les États membres de l'Union européenne. Cette directive sur la sécurité des réseaux et des systèmes d'information vise à intensifier la coopération entre les États membres. L'actuelle agence européenne chargée de la sécurité des réseaux et de l'information basée en Grèce devrait ainsi voir ses compétences renforcées. Principale avancée de la fin d'année 2017, une équipe permanente d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne a également été créée, afin de répondre de manière coordonnée aux cyberattaques visant les institutions. Elle vient renforcer une *task force* existante depuis 2012.

Comité économique et social européen, 16 février 2018.

1. Quelles sont les menaces liées au développement d'Internet ? (doc. 1 et 2)

2. Montrez que la Chine, la France et l'Union européenne répondent à ces menaces par des stratégies différentes. (doc. 3, 4 et 5)

3. Pourquoi la coopération internationale est-elle nécessaire pour lutter contre les cybermenaces? (doc. 1 et 4)