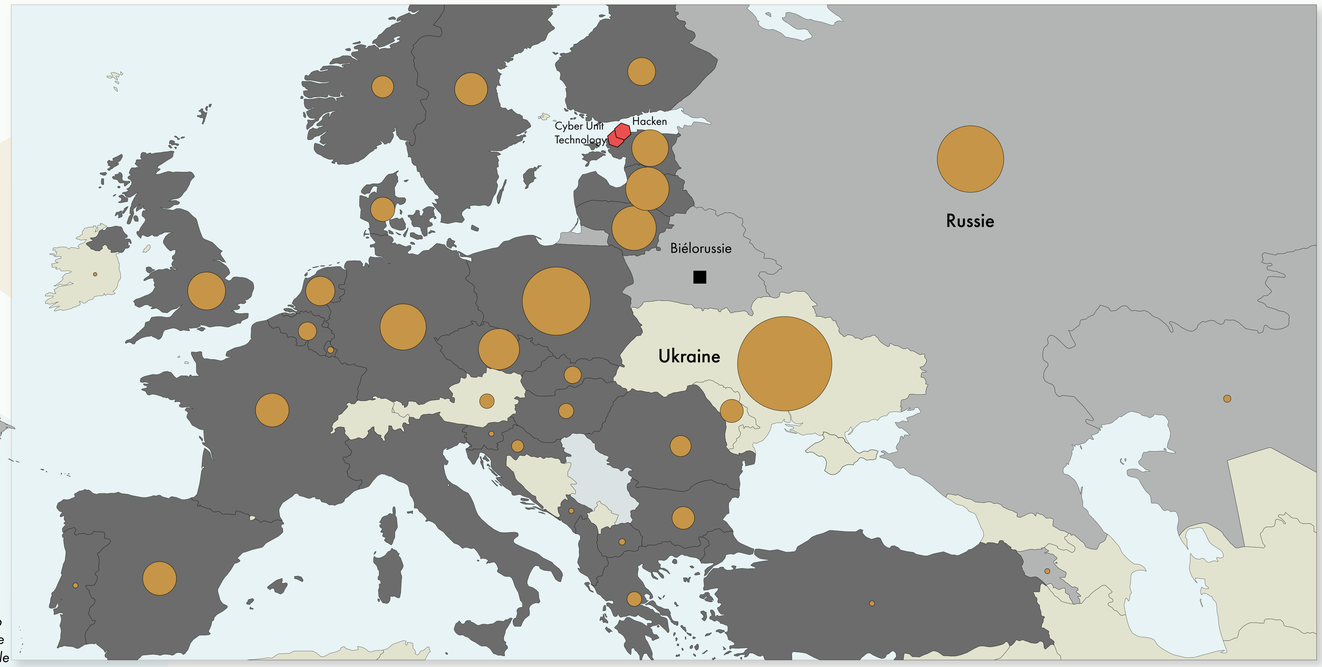
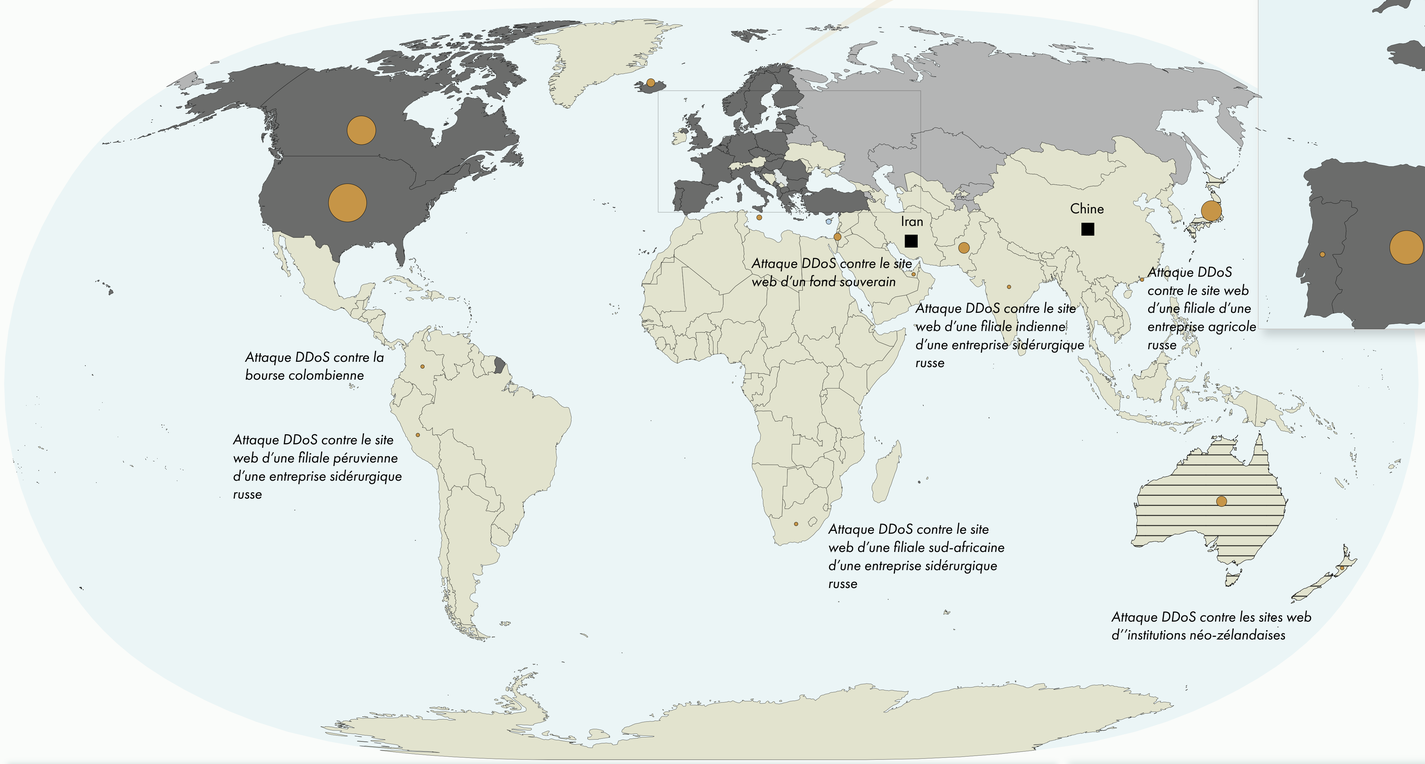
Russie - Ukraine : la cyberguerre, caractère de la guerre hybride

Les cyberattaques liées au conflit russo-ukrainien entre 2022 et 2023 selon l'ONG CyberPeace Institute

« On ne saurait tenir les troupes longtemps en campagne, sans porter un très grand préjudice à l'État et sans donner une atteinte mortelle à sa propre réputation » (Sun Tzu, «L'Art de la guerre»)





Pays membre de l'Organisation du Traité de l'Atlantique Nord (OTAN)

Pays apportant une aide financière à l'Ukraine hors des pays membres de l'OTAN

Siège d'entreprises privées ukrainiennes mandatées par le ministère de la transformation numérique ukrainien pour travailler sur les failles informatiques d'entreprises russes

Pays membre de l'Organisation du Traité de sécurité collective (OTSC)

État observateur de l'Organisation du Traité de sécurité collective (OTSC)

Soutien à la Russie dans la lutte informationnelle

Nombre d'attaques subies et identifiées par l'ONG (janvier 2022 – décembre 2023)

670 (Ukraine)
330 (Russie)
85 (France)
1 (Colombie)

Des acteurs au coeur de la cyberguerre

Acteurs Publics

Institutions et services d'État

GRU Service de renseignement de l'état-major de l'armée russe

SVR Service des renseignements extérieurs

FSB Service fédéral de sécurité

Ministère de la transformation numérique

Service de renseignement extérieur d'Ukraine

Service de cyberdéfense (DSSZZI)

OIG

Alliance des «**Five Eyes**» (États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande pour le partage du renseignement et la sécurité

Acteurs Privés

Entreprises

Entreprises privées de technologie et cybersécurité

Les GAFAM contribuent à la protection informatique de l'Ukraine et des pays alliés

Groupes informels - Hacktivistes

ATP 28 ou Fancy Bear

IT Army of Ukraine

Internet Research Agency (IRA)

Mouvance Anonymous

La cyberguerre débute avant 2022

Janv 2014 - «**Secondary Infektion**» : campagne de désinformation contre l'Ukraine lancée par la Russie

Fév 2014 - Occupation russe de la Crimée

Avril 2014 - Début de la guerre du Donbass

Déc 2015 - Attaque russe «**Black Energy**» qui prive 1.5 million d'ukrainiens d'électricité

Déc 2016 - Attaque russe «**Industroyer**» prive Kiev d'électricité pendant une heure

Juin 2017 - Offensive russe : le virus «**NotPetya**» paralyse banques, infrastructures de transport à Kiev (métro, aéroport), des médias, des hôpitaux ainsi que des fournisseurs d'énergie. 1 ordinateur sur 10 est inutilisable, 55.000 machines sont paralysées en 7 mn. L'attaque fait plus de 9 milliards d'euros de dégats

Fév 2022 - Offensive russe et début de l'invasion de l'Ukraine. Elle s'accompagne d'un blitz numérique contre un réseau contrôlé par la société américaine de satellites Viasat

JC Fichet - Cartolycée

Sources: nato.int ; cyberpeaceinstitute.org ; Vincent Lamigeon, *Ukraine : comment la Russie mène sa cyberguerre*, challenges.fr, 19/05/2022 ; Martin Untersinger, *Guerre en Ukraine : les cyberattaques contre la Russie, le « cri de colère » d'une armée de volontaires*, Le Monde, 25/03/2022 ; Ministère des armées, *L'arme cyber en Ukraine : les trois enseignements à retenir*, 12/01/2023 ; Sophy Caulier, *La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques, Le Monde*, 12/02/2023 ; reuters.com