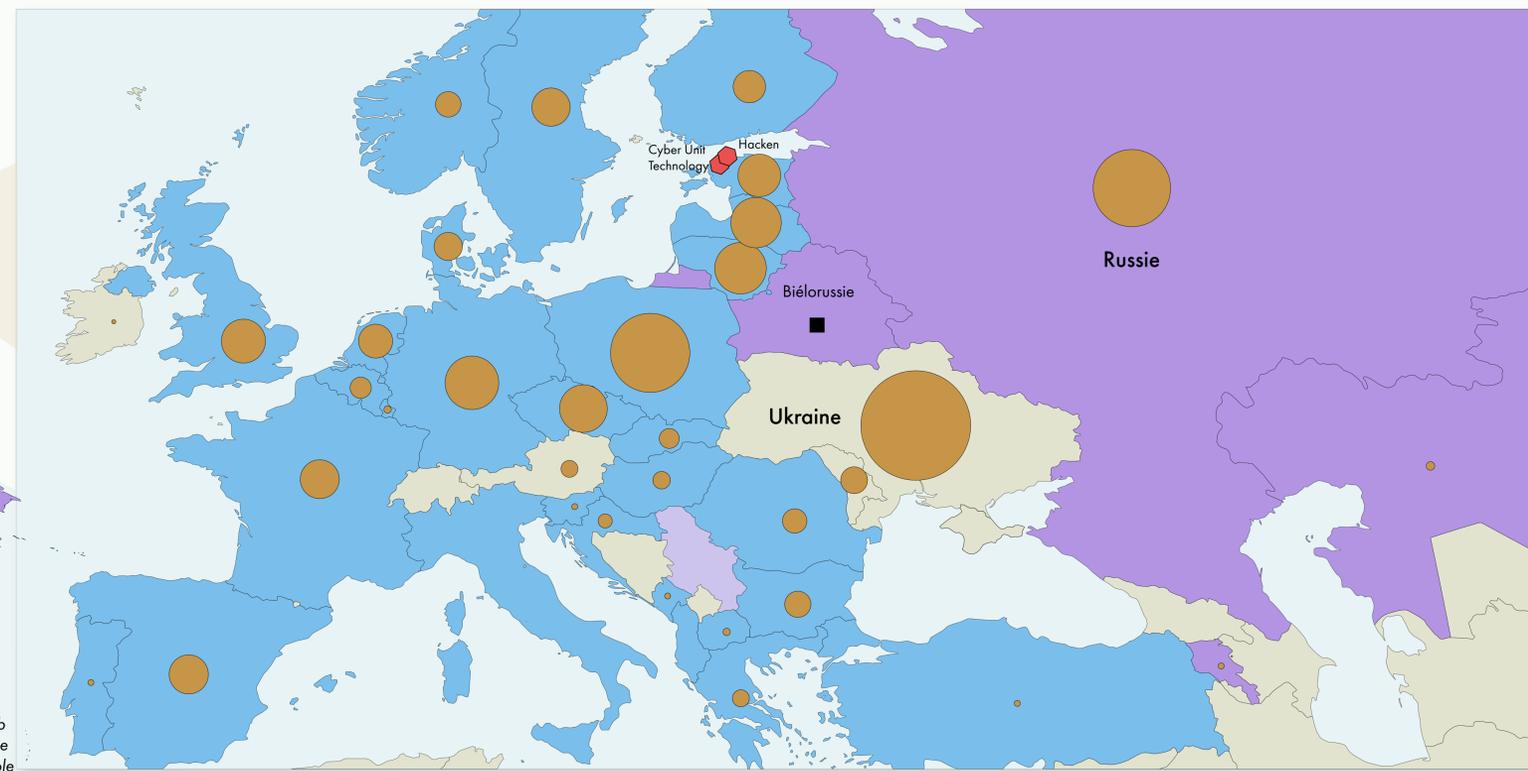
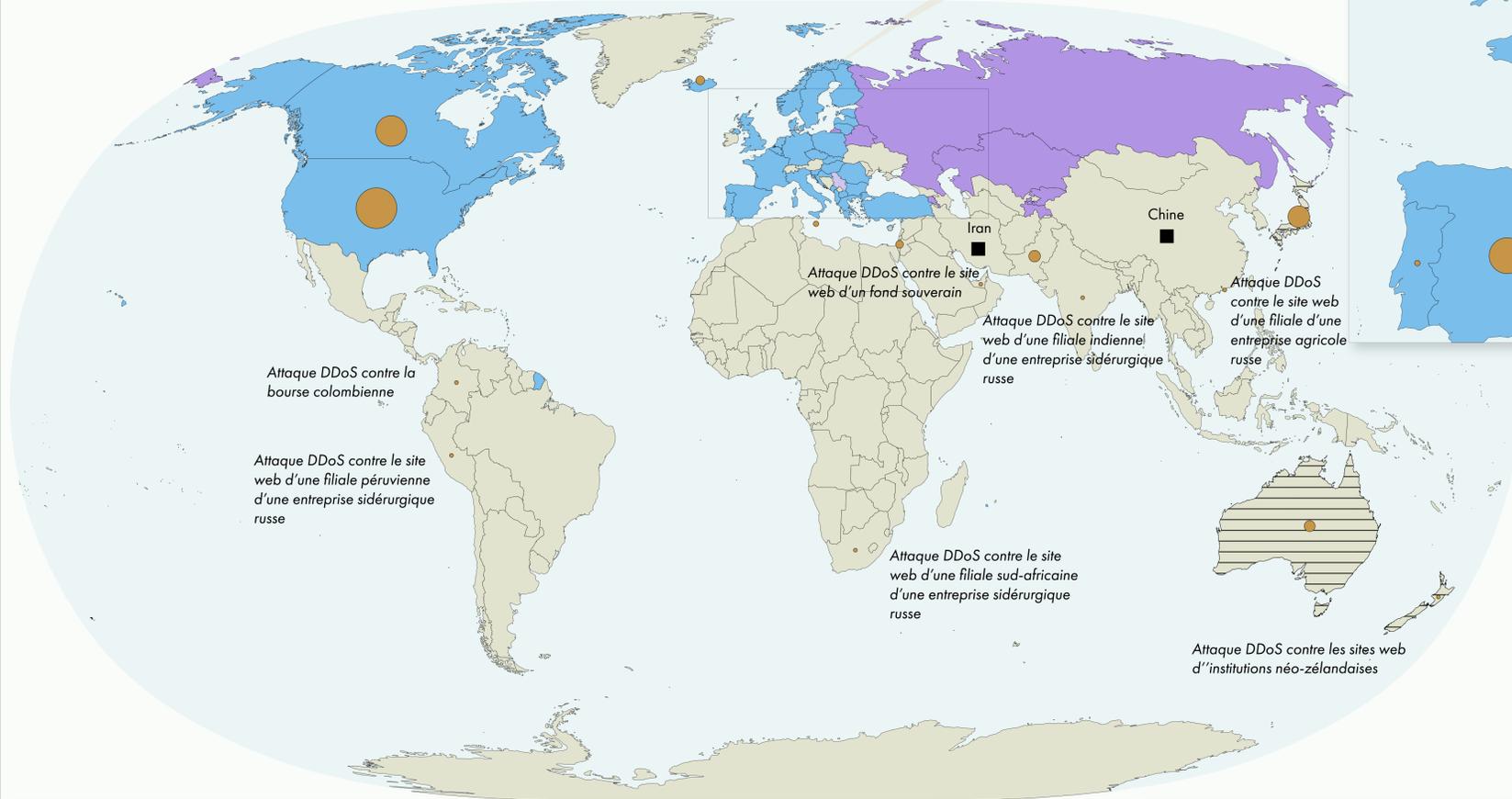


# Russie - Ukraine : la cyberguerre, caractère de la guerre hybride

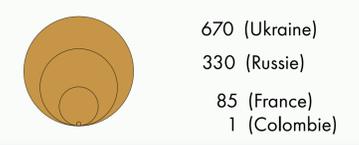
Les cyberattaques liées au conflit russo-ukrainien entre 2022 et 2023 selon l'ONG CyberPeace Institute

« 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 membre de l'Organisation du Traité de sécurité collective (OTSC)	
	Pays apportant une aide financière à l'Ukraine hors des pays membres de l'OTAN		État observateur de l'Organisation du Traité de sécurité collective (OTSC)	
	Siège d'entreprises privées ukrainiennes mandatées par le ministère de la transformation numérique ukrainien pour travailler sur les failles informatiques d'entreprises russes			Soutien à la Russie dans la lutte informationnelle

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



### Des acteurs au coeur de la cyberguerre

<h4>Acteurs Publics</h4> <p><b>Institutions et services d'État</b></p> <ul style="list-style-type: none"> <li>GRU Service de renseignement de l'état-major de l'armée russe</li> <li>SVR Service des renseignements extérieurs</li> <li>FSB Service fédéral de sécurité</li> </ul> <p>Ministère de la transformation numérique</p> <p>Service de renseignement extérieur d'Ukraine</p> <p>Service de cyberdéfense (DSSZZI)</p> <p><b>OIG</b></p> <p>Alliance des «Five Eyes» (États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande pour le partage du renseignement et la sécurité)</p>	<h4>Acteurs Privés</h4> <p><b>Entreprises</b></p> <ul style="list-style-type: none"> <li>Entreprises privées de technologie et cybersécurité</li> <li>Les GAFAM contribuent à la protection informatique de l'Ukraine et des pays alliés</li> </ul> <p><b>Groupes informels - Hactivistes</b></p> <ul style="list-style-type: none"> <li>ATP 28 ou Fancy Bear</li> <li>Internet Research Agency (IRA)</li> <li>IT Army of Ukraine</li> <li>Mouvance Anonymous</li> </ul>
---	--

### 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
- Jun 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