

GUERRE HYBRIDE

Assemblée des Parlementaires Francophones
Pristina, 10–12 novembre 2024

Didier Danet (PhD, HDR)

Consultant Cyberdéfense

Chercheur associé GEODE, Université Paris 8

didier.Danet@gmail.com

GUERRE HYBRIDE

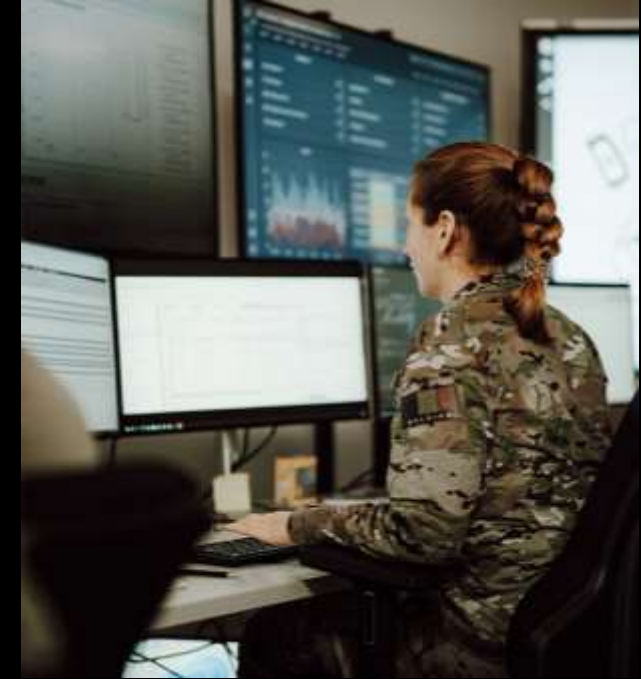
INTRODUCTION



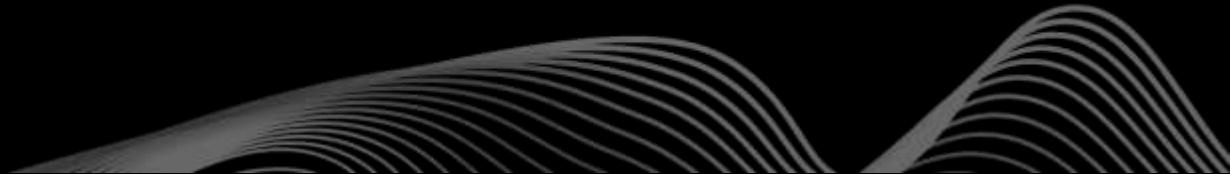
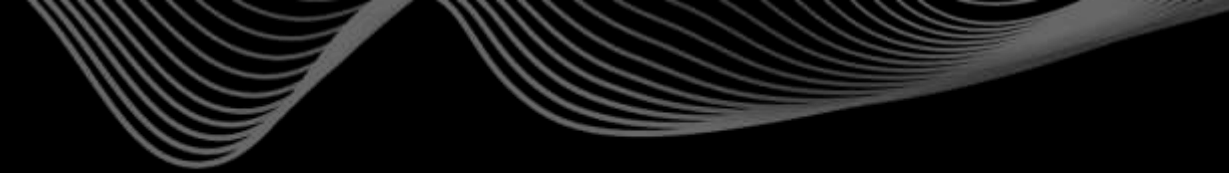
De quoi s'agit-il ?



La guerre hybride et le cyberspace



Les acteurs de la guerre hybride



1.

UN CONCEPT DYNAMIQUE

La mutation des formes de la guerre



LA GUERRE, UNE DÉFINITION

- Lutte armée entre Etats, considérée comme un phénomène historique et social qui s'oppose à la paix.
- Le Robert
- A state of usually open and declared armed hostile conflict between states or nations.
- Merriam-Webster



LA GUERRE HYBRIDE (2005)

Contexte : Afghanistan & Moyen-Orient

Un nouveau défi : des acteurs non étatiques (Hezbollah, Hamas), agissant selon des procédés irréguliers, ont accès à des capacités militaires sophistiquées.

Franck G. Hoffman, Conflict in the 21 st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, Arlington, 2005 (p.28)

LA GUERRE HYBRIDE (2024)

Contexte : Ukraine

Attribution à la Russie d'actes hostiles de différentes sortes : incendies volontaires et manipulation des migrants (Pologne), fake news et achats de vote lors du référendum sur l'adhésion à l'UE (Moldavie), colis piégés à l'encontre de DHL (Allemagne, Royaume-Uni)...



Fermeture du consulat de Russie à Poznan : le ministre des affaires étrangères appelle la Russie à cesser la guerre hybride contre la Pologne et ses alliés.



La Moldavie face à son destin européen, entre achats de votes, désinformation et pots-de-vin.

LA GUERRE HYBRIDE (2024)

GUERRE HYBRIDE ; CONCEPT



Définition : mélange des techniques de guerre conventionnelle avec des stratégies non militaires, telles que les cyberattaques, la désinformation, la guerre économique, et les manipulations politiques.

Une triple extension :

Dans le temps : Paix / guerre → Coopération / Contestation / Affrontement

Dans les champs : Matériel (Cinétique) → Immatériel (Cyber / Informationnel)

Dans les dimensions : Militaire → PESTEL

2. GUERRE HYBRIDE
ET CYBER
CONFLICTUALITÉ

L'importance de la dimension immatérielle dans la guerre hybride contemporaine

Les 3 macro-couches constitutives du cyberspace

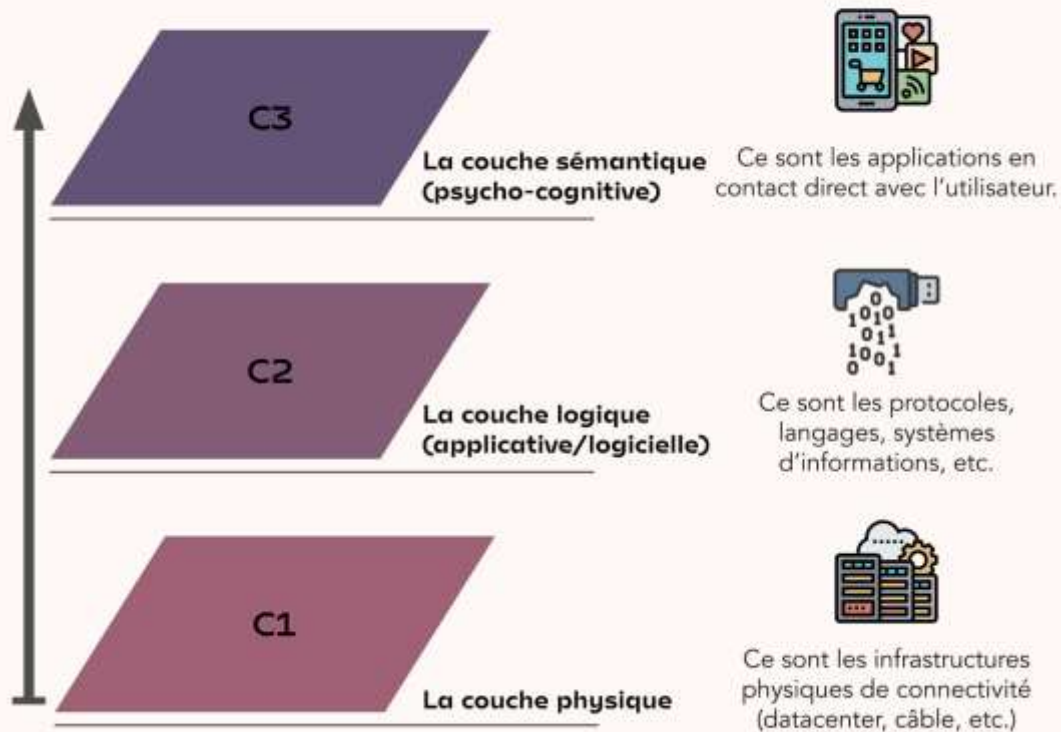


Illustration adaptée du tableau de Daniel Ventre, *Cyberspace et acteurs du cyberconflits*, éditions Hermès Lavoisier, Paris, 2011.

LE CYBERESPACE, UN TERRAIN D'AFFRONTEMENT

- Dans le cyberspace, l'affrontement prend deux formes complémentaires :
- L'atteinte à la couche physique → Lutte informatique défensive et offensive
- L'atteinte à la couche sémantique → Lutte informatique d'influence

LE CYBERESPACE, UN TERRAIN PRIVILÉGIÉ POUR LA GUERRE HYBRIDE



Interconnexion généralisée des systèmes d'information → accessibilité des cibles + failles de sécurité



Caractéristiques du cyberspace (instantanéité / ubiquité / anonymat relatif / faible coût) → ambiguïté + sous le seuil du conflit armé



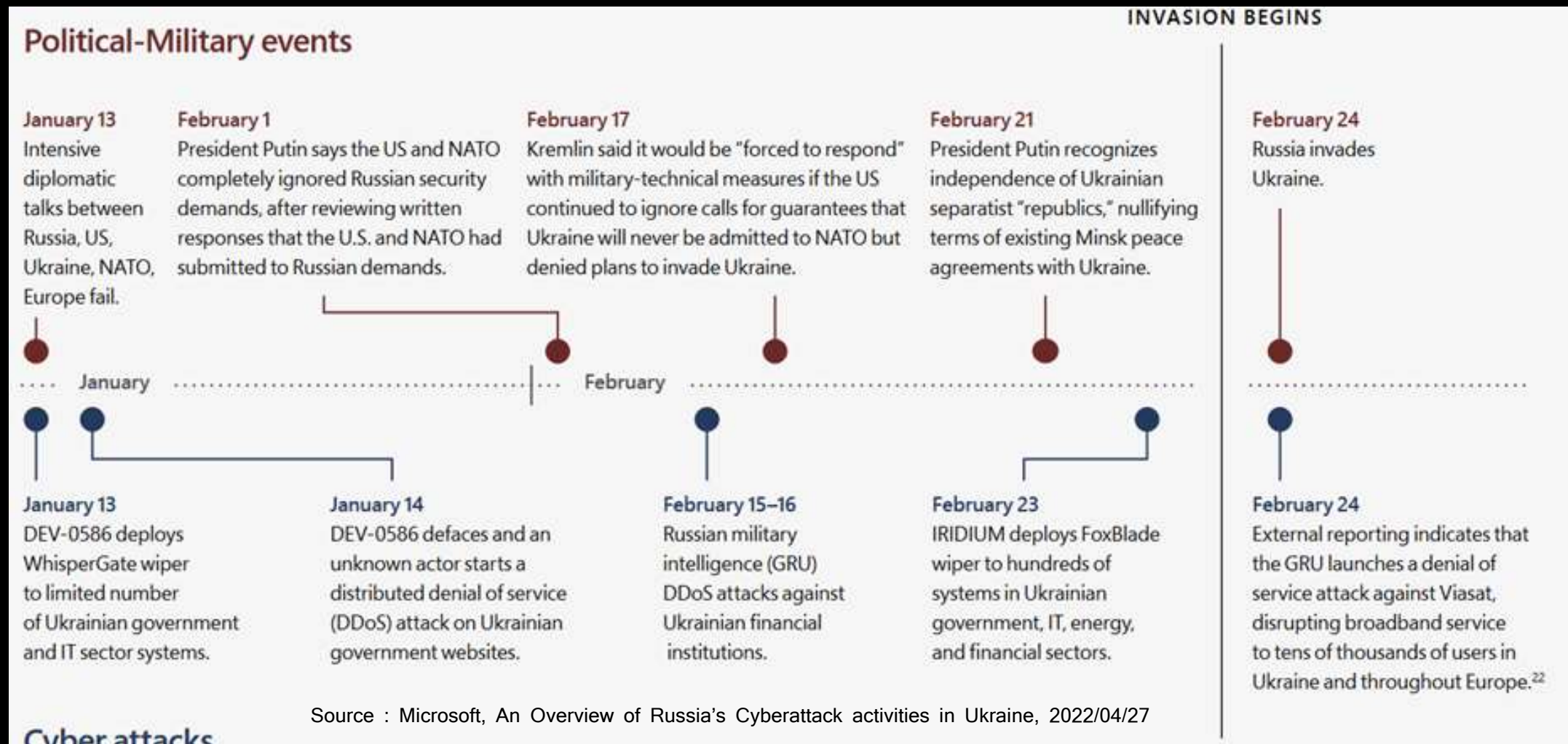
Pluralité des objectifs et des effets (matériels / immatériels) dans les trois univers (compétition / contestation / affrontement)

L'UTILITÉ DU CYBER

Objectif	Logique	Mécanisme	Modes d'action militaires	Utilité du cyber
Compétition	Obtention de gains relatifs	Recherche de supériorité matérielle ou informationnelle	Pré-positionnement stratégique	Faible
			Renseignement	Élevé
Subversion	Affaiblissement de la cible	Exploitation des vulnérabilités	Sabotage	Intermédiaire
			Propagande	Élevé
Dissuasion	Empêcher la cible d'agir	Menace de coûts	Représailles	Faible
			Déni	Élevé
Contrainte	Forcer la cible à changer de comportement	Imposition de coûts	Diplomatie coercitive	Intermédiaire
			Guerre	Intermédiaire

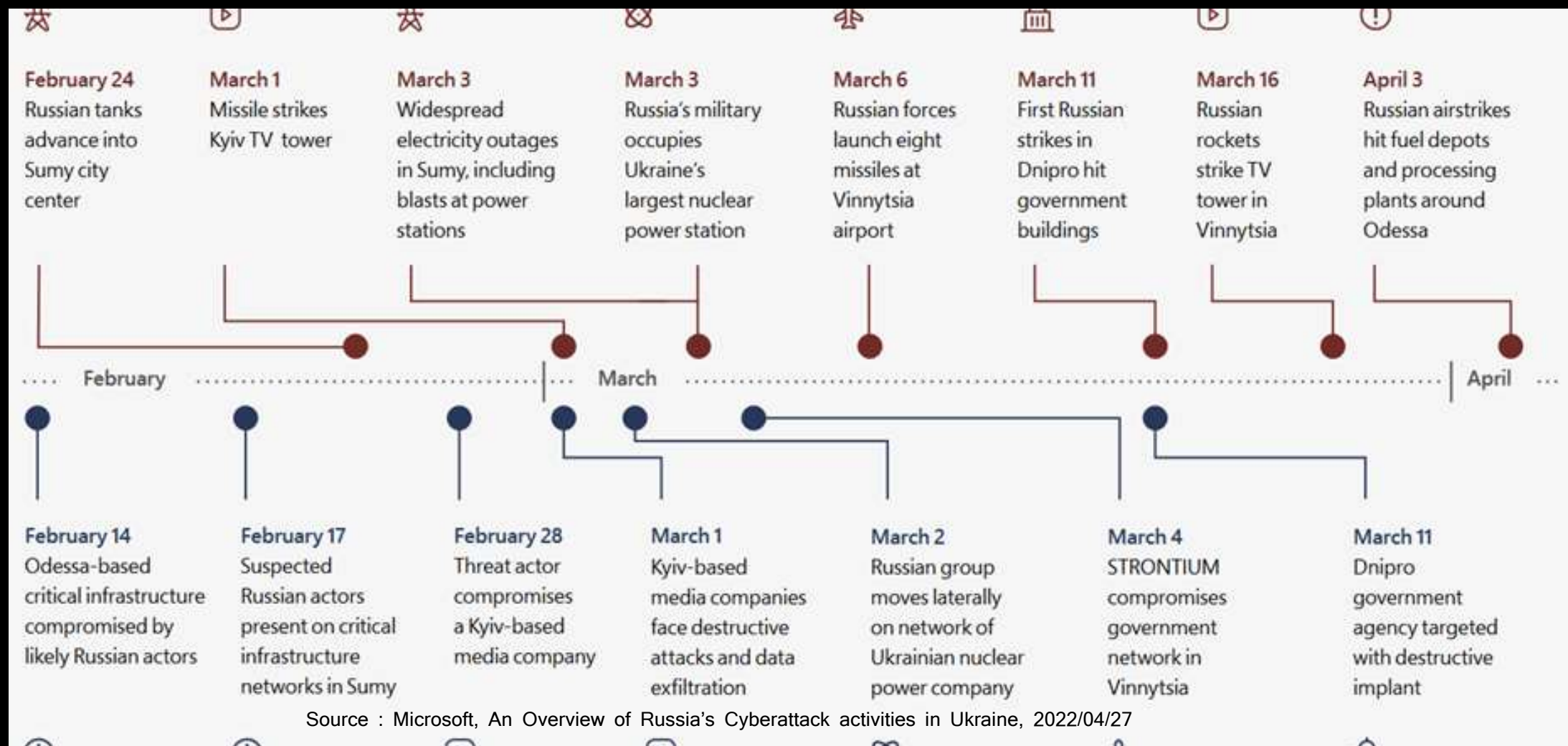
L'utilité spécifique des opérations cyber réside dans la possibilité d'agir avant l'affrontement pour conforter sa position (espionnage), affaiblir l'adversaire (propagande, voire sabotage) ou l'empêcher d'agir (déni)

UKRAINE : LA PRÉPARATION DE L'INVASION



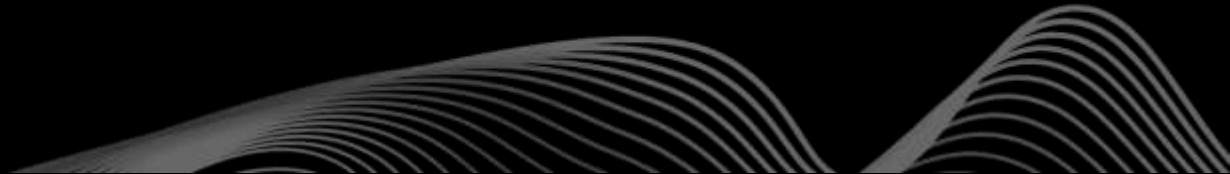
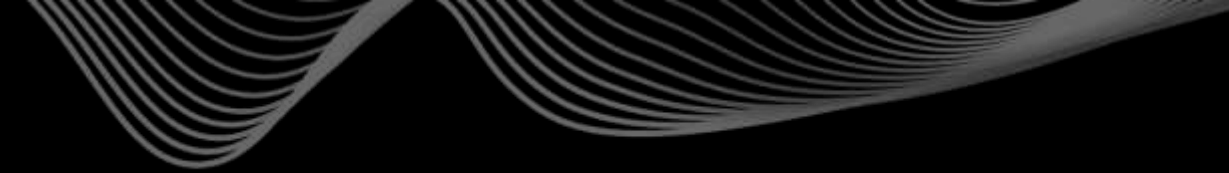
Deux mois avant l'invasion, combinaison d'actions contre les infrastructures (wipers) et contre la confiance dans les institutions publiques et privées (DDoS)

UKRAINE : LA PARTICIPATION À L'INVASION



Source : Microsoft, An Overview of Russia's Cyberattack activities in Ukraine, 2022/04/27

Pendant l'invasion, multiplication d'actions de sabotage (réseaux télécoms, médias, énergie, sites gouvernementaux)



3. LES ACTEURS DES CYBERCONFLITS

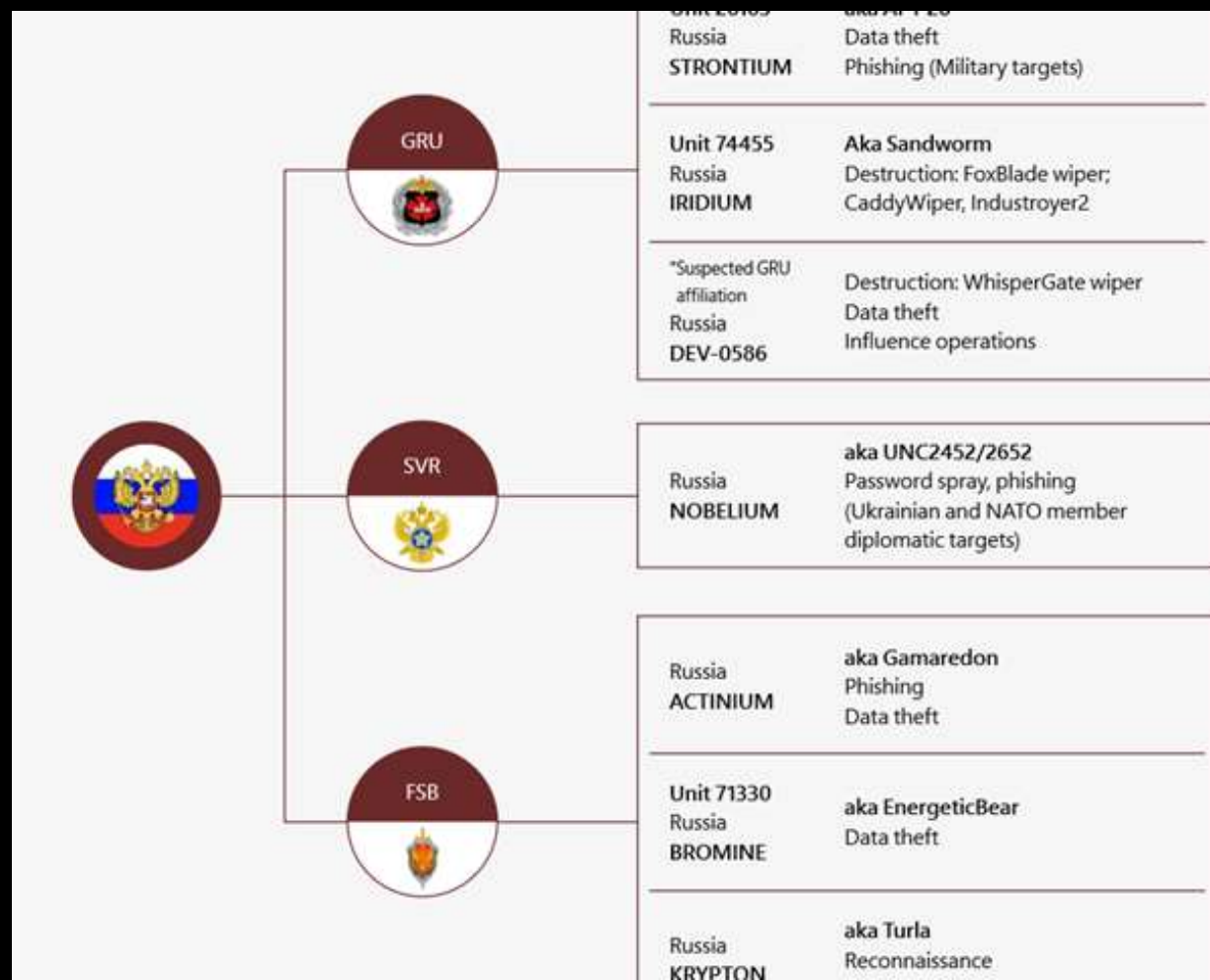
Des Etats aux citoyens, la multiplication des acteurs de la guerre hybride



LE CAS VIASAT

- Le jour de l'invasion (24/02/2022), un wiper détruit les modems des utilisateurs du satellite Viasat.
- L'attaque vise directement à désorganiser les communications militaires de l'Ukraine et à perturber la distribution d'électricité du pays.
- Elle touche également des milliers de modems utilisés par les entreprises d'électricité en Pologne ou en Allemagne.

LES ATTAQUANTS : SERVICES DE RENSEIGNEMENT



Unités cyber affiliées au GRU (rens.mil.) → Strontium (pré-positionnement par phishing) & DEV-0586 (conception du wiper)

LES ATTAQUANTS : GROUPE CRIMINELS



Après l'éclatement de Conti entre pro-russes et pro-ukrainiens, les premiers prennent l'initiative d'opérations contre l'Ukraine.

Ils utilisent leurs outils (ransomware visant les banques) en se faisant passer pour Starlink et inciter les utilisateurs à télécharger une mise à jour contenant le ransomware

Pas de coordination explicite avec le GRU mais possible action sous la contrainte (cf Revil)

LES DÉFENSEURS : ACTEURS ÉTATIQUES



Min.Déf.Ukrainien bascule vers systèmes de communication alternatifs ;

Services de renseignement américains et européens collectent des preuves et attribuent la cyberattaque ;

ENISA identifie les vulnérabilités et lutte contre les effets collatéraux dans l'UE

LES DÉFENSEURS : ACTEURS PRIVÉS DES TELECOMS



Viasat remplace les Modems détruits en renforçant les mesures de sécurité contre les cyberattaques → Restauration partielle du service

Starlink fournit rapidement des kits et étend la couverture satellitaire à l'Ukraine.

LES DÉFENSEURS : ACTEURS PRIVÉS DE LA CYBERSÉCURITÉ

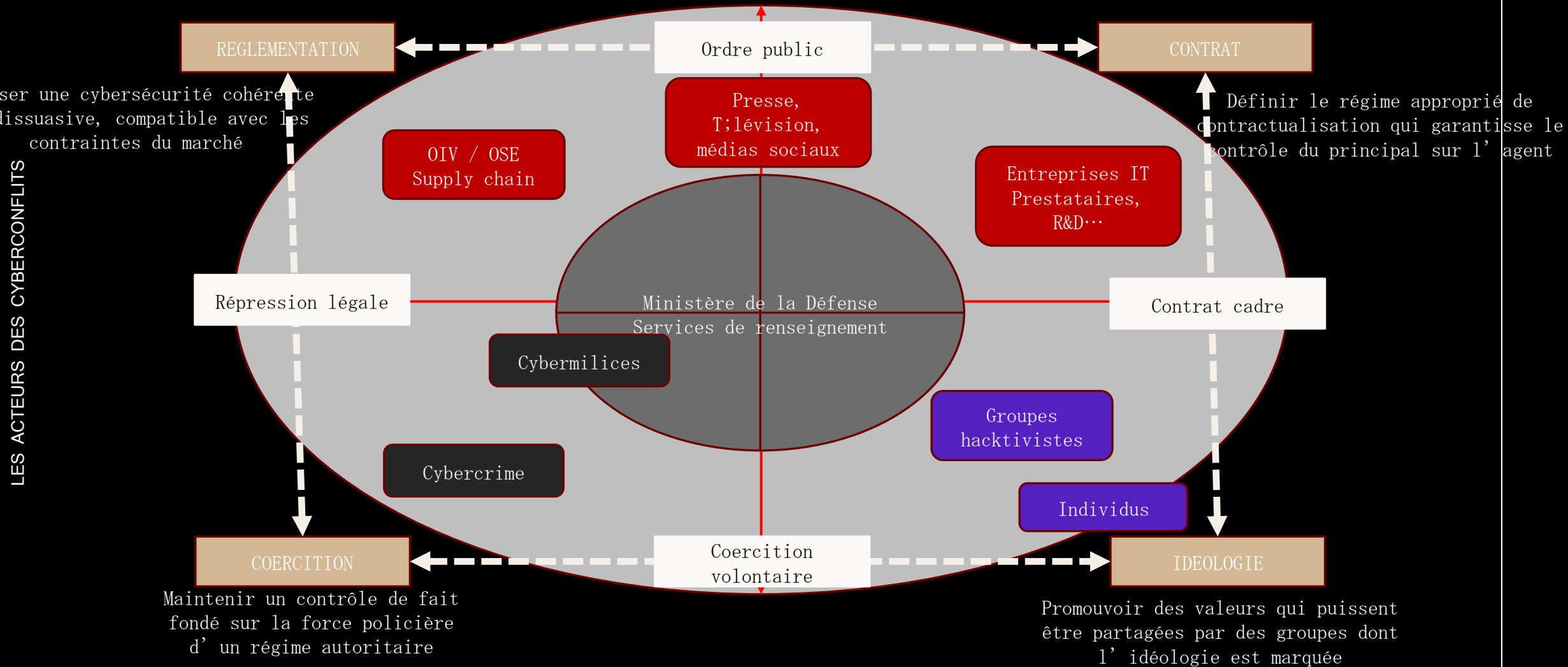


Mandiant (filiale Google) analyse les techniques, tactiques et procédures utilisées par les attaquants ; elle contribue à attribuer l'attaque et à lutter contre ses effets.

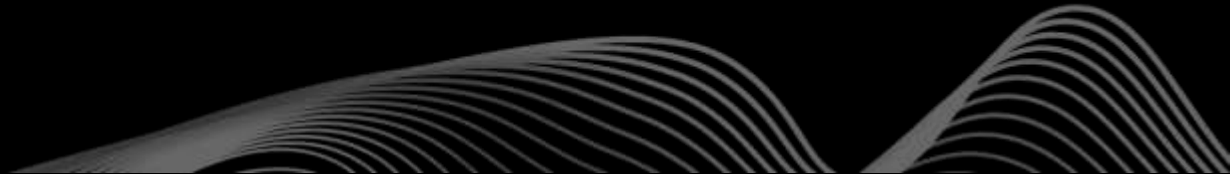
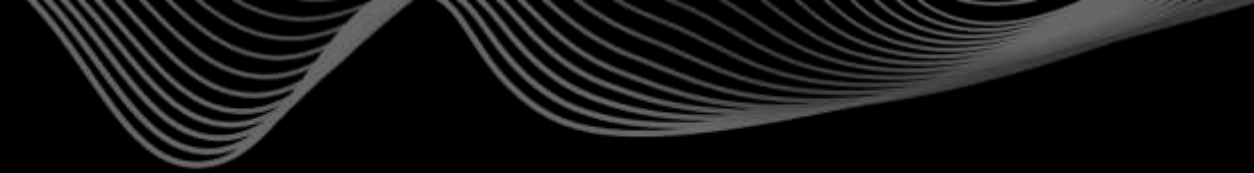
Microsoft contribue au renforcement de la cyberdéfense ukrainienne.

LA COORDINATION DES ACTEURS

:



La multiplication des acteurs de la cyberconflictualité suppose une diversification des modes de coordination reposant sur quatre mécanismes (Coercition / Réglementation / Contrat / Idéologie) Chaque pays se caractérise par une configuration spécifique en fonction de ses valeurs et de ses capacités.

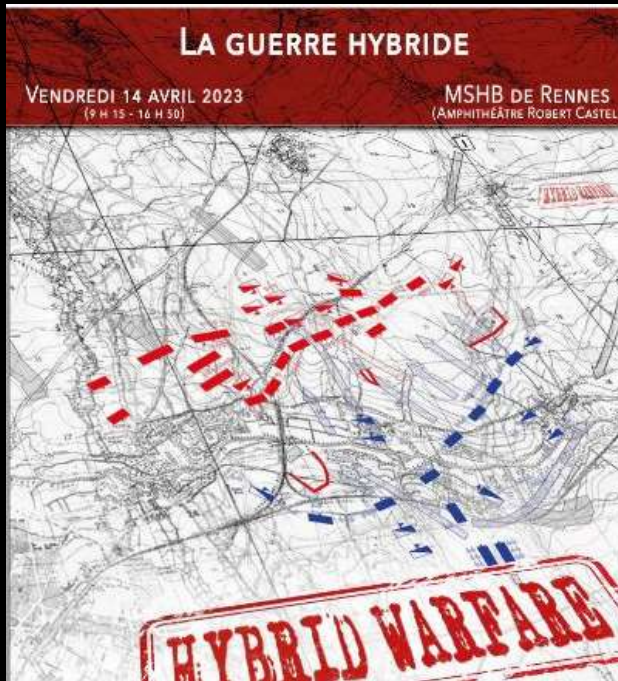


CONCLUSION

Des Etats aux citoyens, la multiplication des acteurs de la guerre hybride

CONCLUSION

CONCLUSION



Guerre hybride : gagner la guerre avant la guerre → espionner, subvertir et dissuader pour prendre l'avantage en restant sous le seuil du conflit armé.



Le cyberspace, un terrain privilégié de la guerre hybride où se déploient des opérations dans les couches physiques (infrastructures) et sémantiques (FIMI)



La guerre hybride implique la multiplication voulue ou non des acteurs qu'il s'agit de coordonner pour renforcer la résilience des démocraties visées.