# Dynamiques cyber et géopolitique de la guerre russo-ukrainienne

## 2nde édition

Citalid

Frise chronologique comparée du
23 mars au 13 avril 2022

www.citalid.com

# DYNAMIQUES CYBER ET GÉOPOLITIQUE DE LA GUERRE RUSSO-UKRAINIENNE

Frise chronologique comparée du 23 mars au 13 avril 2022

## Rappel du contexte

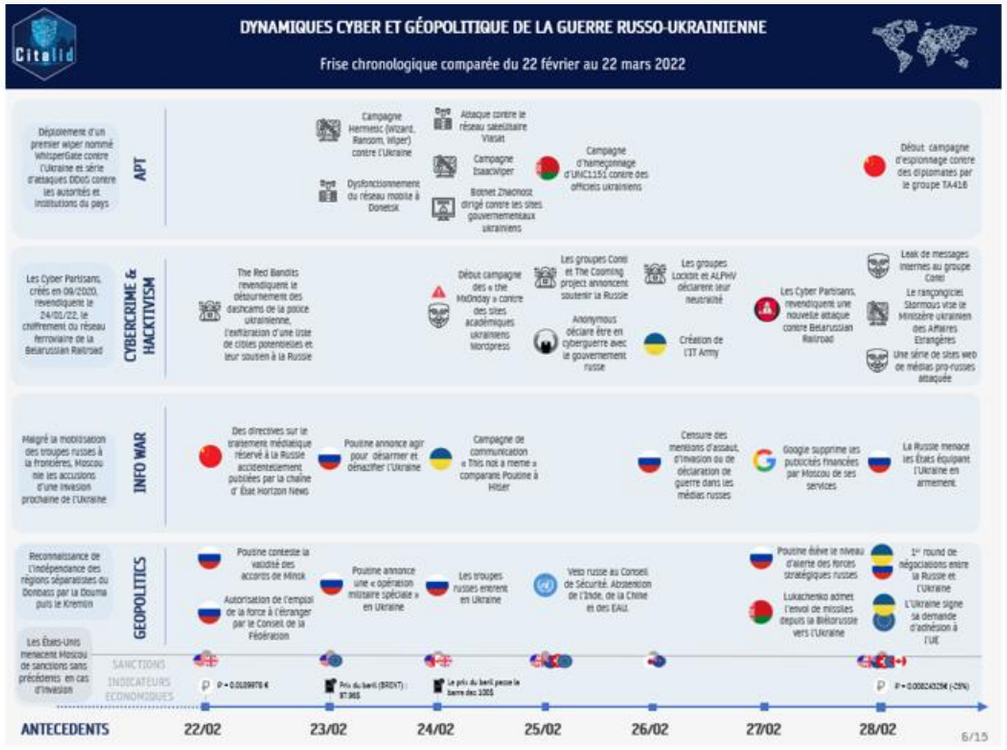
Dans la nuit du **23 au 24 février 2022**, les **troupes russes entrent en Ukraine** par les fronts Est, Nord (russe et biélorusse) et Sud (Crimée) au motif d'une opération de « maintien de la paix » selon le gouvernement russe. L'invasion survient quelques jours après la **reconnaissance par le Kremlin de l'indépendance des régions séparatistes du Donbass** (Luhansk et Donetsk).

Le conflit éclate alors que **Kiev fait état d'une volonté d'indépendance croissante vis-à-vis de Moscou** (révolution orange de 2004, révolution de Maïdan de 2014) et d'un **rapprochement progressif avec les puissances occidentales** (Union européenne et OTAN). Cette double dynamique avait été le catalyseur de l'annexion de la Crimée en 2014 après la destitution et l'exil du président ukrainien pro-russe Viktor Ianoukovytch.

L'Ukraine reste le **théâtre d'une lutte d'influence entre l'OTAN et la Russie** qui y projette ses ambitions de puissance régionale. L'extension de l'OTAN et l'installation de bases militaires vers l'Est est ainsi désignée par la Russie comme une **menace directe à ses intérêts vitaux** et une trahison des engagements pris par les États-Unis en février 1990 (non élargissement de l'OTAN vers l'Est). Les tensions s'accélèrent en avril 2021 lorsque **la Russie rassemble ses forces armées à la frontière ukrainienne**. Leur nombre atteint 100 000 hommes en fin d'année. La machine diplomatique s'enlise après le **refus par l'OTAN des gages de sécurité proposés par la Russie** (non adhésion de l'Ukraine à l'OTAN et limitation du personnel et de l'équipement déployés en Europe de l'Est).

*Si vous avez manqué la première édition de notre frise chronologique comparée, nous vous invitons à la consulter directement ici :*
*https://citalid.com/blog/dynamiques-cyber-et-geopolitique-de-la-guerre-russo-ukrainienne/*





## Démarche

- Visualiser la progression des positions des acteurs intervenant dans le cadre de la guerre russo-ukrainienne
- Dégager les modalités d'implémentation de la dimension cyber au sein de dynamiques conflictuelles interétatiques
- Identifier les tendances propres ou partagées des acteurs et moyens impliqués dans le conflit
- Quatre entrées thématiques dans la frise chronologique :

**1. APT :** Représentation des attaques informatiques d'ampleur, persistantes et avancées, *a priori* conduites ou soutenues par des États.
**2. CYBERCRIME & HACKTIVISM :** Représentations des attaques informatiques aux fins de revendications politiques et/ou à finalité lucrative.
**3. INFOWAR :** Représentation des manœuvres informationnelles de source officielle.
**4. GEOPOLITICS :** Evènements et prises de positions étatiques (unilatérales, bilatérales et multilatérales)
**4.1. SANCTIONS :** Représentation chronologique des États émetteurs de sanctions contre la Russie.

## Avertissements liminaires

- Le travail présenté ci-dessous rend compte de l'état des informations disponibles en sources ouvertes au **13 avril 2022**.
- Les éléments présentés ci-dessous n'ont pas vocation à être exhaustifs, ils relèvent d'une sélection d'évènements significatifs et représentatifs des dynamiques géopolitiques et cybernétiques à l'œuvre dans le cadre de la guerre russo-ukrainienne.
- Les mesures humanitaires, les livraisons d'équipements militaires ou toute autre forme de soutien logistique ainsi que le suivi des opérations militaires ne sont pas traités.
- La coïncidence chronologique des évènements listés ne vaut pas nécessairement leur corrélation.
- L'attribution formelle d'attaques informatiques à un acteurs ou un pays, et les liens qui peuvent être faits entre elles, demeure un exercice incertain et périlleux. Les liens entre Mode Opératoire d'Attaque et acteurs s'appuient sur des attributions fondées sur des faisceaux d'indices réalisés par des éditeurs de solutions de cybersécurité.
- La démarche proposée ici vise à l'objectivité ; toutefois des biais persistent dans le cadre des manœuvres informationnelles menées par les parties au conflit affectant certaines des informations et des données rapportées.

# Tendances identifiées 1/2

Tendance vérifiée et stable
Nouvelle tendance
Tendance en hausse
Tendance en baisse

## Essoufflement apparent des opérations de sabotage et des cyber-attaques majeures

La période étudiée n'a pas permis de relever une inflexion volumétrique dans la conduite d'opérations cybernétiques d'ampleur. A ce titre, l'essentiel des cyber-attaques majeures ont été conduites avant ou lors du début de l'invasion russe. Toutefois, les cas de pré-positionnement russe, découverts et mis en échec par l'Ukraine et les États-Unis, doivent amener à tempérer ce constat.

## Forte capacité de nuisance et montée en intensité d'opérations hacktivistes

Les offensives revendiquées hacktivistes restent diffuses et continuent de gagner en intensité. Les opérations de sabotage (cf. NB65) et menées contre des cibles stratégiques (cf. TheBlackRabbitWorld) se multiplient. L'impunité contextuelle dont bénéficie les Modes Opératoires d'Attaque (MOA) hacktivistes alimente la surenchère et la démonstration de force. Cette dynamique pourrait tendre à faciliter la conduite d'opérations étatiques majeures sous couvert de fausses revendications hacktivistes.

## Internationalisation du conflit cybernétique

Les opérations offensives hacktivistes élargissent le spectre de leur ciblage en visant des organisations et des gouvernements étrangers alliés de la Russie. De leur côté, les entreprises et institutions occidentales toujours en lien avec Moscou sont désormais largement exposées dans la mesure où les mouvances hacktivistes se sont montrées réceptives aux incitations au boycott formulées par le président Zelensky. Côté russe, la projection connue du conflit cybernétique à l'international reste principalement limitée à la conduite d'opérations d'espionnage contre les gouvernements occidentaux.

## Émergence d'une conflictualité inter-hacktivistes

La montée en intensité des opérations offensives hacktivistes alimente une rivalité entre groupes adverses. A ce titre, les opérations de doxxing menées par ATW/Blue Hornet contre des groupes rivaux et des Advanced Persistent Threats (APT) adverses caractérisent l'émergence d'une conflictualité inter-hacktiviste. Cette tendance n'a toutefois pas vertu à se développer en raison de l'asymétrie du rapport de force (en faveur de l'Ukraine) des groupes hacktivistes parties au conflit. Elle ne pourra tout au mieux que dissuader la conduite d'opérations pro-russes contre le camp occidental.

# Tendances identifiées 2/2

## Sous-exploitation apparente du levier cyber

Si les cyber-attaques sont nombreuses, beaucoup d'entre elles restent de faible à moyenne intensité et sont mises en échec (CERT-UA). Sur le plan opérationnel, la poursuite d'une victoire stratégique sur l'adversaire se fait principalement au moyen d'armes dites cinétiques ou conventionnelles. La neutralisation de certaines infrastructures de communications ukrainiennes par frappes aériennes tend à entériner ce constat.

## Mobilisation stratégique du renseignement déclassifié

Les États-Unis gardent la main sur le volet informationnel du conflit par l'adoption d'une posture préemptive. Cette stratégie conduit Moscou et ses alliés à s'abstenir d'agir dans le sens prédit pour donner tort à Washington ou à admettre la véracité des prédictions américaines sur les prochaines manœuvres adverses. Sur le plan cyber, la mise en lumière d'opérations de défense active menées contre la Russie témoigne d'une rupture entre les doctrines Biden et Obama (marquée par une discontinuité du discours et des pratiques).

## Accélération de la consolidation côté occidental

L'invasion russe accélère la réhabilitation de la légitimité et de l'attractivité de l'OTAN. Alors que la Finlande et la Suède envisagent la sortie de leur statut de neutralité pour rejoindre l'Organisation, les pays membres revendiquent l'unité retrouvée de l'alliance face à la Russie. Dans ce contexte, il ne peut pas être exclu que la Russie conduise des cyber-attaques contre la Suède, la Finlande et les pays baltes. Parallèlement, l'effort commun d'isolement politique, économique et commercial de Moscou et de ses alliés trouve son écho au sein des institutions internationales (ONU, OMC, CPI).

## Radicalisation des discours

Alors que les appels au respect et à l'application du droit international humanitaire restent le paradigme dominant, les discours s'endurcissent.
Les États-Unis et la Pologne ont rallié l'Ukraine dans le narratif des pratiques génocidaires russes tandis que Zelensky multiplie les interventions auprès des audiences occidentales et les dénonciations expresses à l'égard de Poutine et de son gouvernement. Ces dynamiques narratives participent à une ostracisation des élites russes auprès de l'opinion publique et d'un système international jusqu'à présent mis en défaut. De son côté, la Russie poursuit ses efforts de légitimation d'un *casus belli* désignant l'Ukraine comme l'auteur d'exactions imputées à Moscou et des frappes conduites en territoire russe.

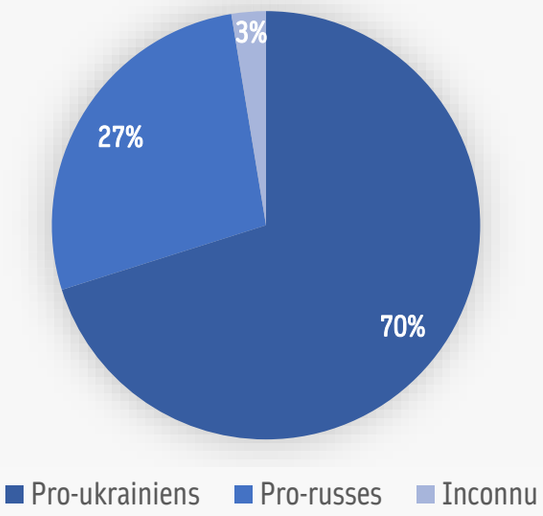
# DYNAMIQUES CYBER ET GÉOPOLITIQUE DE LA GUERRE RUSSO-UKRAINIENNE

Frise chronologique comparée du 23 mars au 13 avril 2022

## Etat-Nation

| Nom | Soutien | Attribution |
|---|---|---|
| GhostWriter | Russie | Biélorussie |
| SandWorm | Russie | Russie |
| Gamaredon | Russie | Russie |
| DEV-0586 APT | Russie | Russie |
| DEV-0665 APT | Russie | Russie |
| FancyBear | Russie | Russie |
| IT Army of Ukraine | Ukraine | Ukraine |
| Internet Forces of Ukraine | Ukraine | Ukraine |
| IT Army of Ukraine Psyops | Ukraine | Ukraine |
| MustangPanda | Inconnu | Chine |
| Curious George | Inconnu | Chine |

### 77 MOA actifs sur la période




## Affiliés Anonymous

| Nom | Soutien | Provenance |
|---|---|---|
| BlackHawks | Ukraine | Georgie |
| LiteMods | Ukraine | Inconnue |
| ShadowS3c | Ukraine | Puerto Rico |
| N3UR0515 | Ukraine | Inconnue |
| PuckArks | Ukraine | Inconnue |
| GrenXPaRTa_9haan | Ukraine | Indonésie |
| YourAnonNews | Ukraine | Inconnue |
| DeepNetAnon | Ukraine | Inconnue |
| Anonymous Younes | Ukraine | Inconnue |
| 0xAnonLeet | Ukraine | Inconnue |
| AnonGh0st | Ukraine | Inconnue |
| Anonymous Romania | Ukraine | Roumanie |
| Shadow_Xor | Ukraine | Inconnue |
| PuckArks | Ukraine | Inconnue |
| Squad303 | Ukraine | Pologne |
| Synthynt | Ukraine | Inconnue |
| DDoS Secrets | Ukraine | Inconnue |
| V0g3lSec | Ukraine | Inconnue |
| Anonwolf3467 | Ukraine | Italie |
| DoomSec | Ukraine | Inconnue |
| CyberNinja Security Team | Ukraine | Inconnue |
| ReaperSec | Ukraine | Inconnue |
| HAL9000 | Ukraine | Inconnue |
| RedCult | Ukraine | Inconnue |
| The Black Rabbit World | Ukraine | Inconnue |
| NB65 | Ukraine | Etats-Unis |
| GhostSec | Ukraine | Inconnue |
| Wh1t3sh4d0w | Ukraine | Inconnue |

## Pro-Ukraine

| Nom | Provenance |
|---|---|
| BlueHornet ATW | Inconnue |
| KelvinSecurity Hacking Team | Inconnue |
| GNG | Géorgie |
| GhostClan | Inconnue |
| 1LevelCrew | Inconnue |
| Spot | Inconnue |
| Hydra UG | Inconnue |
| SecJuice | Inconnue |
| Ring3API | Ukraine |
| Belarusian Cyber-Partisans | Biélorussie |
| Monarch Turkish Hacktivists | Turquie |
| Shadow_Xor | Inconnue |
| The Connections | Inconnue |
| RabbitTwo | Inconnue |
| SecDet | Etats-Unis |
| BeeHive Cybersecurity | Inconnue |
| HackenClub | Ukraine |
| Cyber_legion_hackers | Inconnue |
| Stand for Ukraine | Ukraine |
| BrazenEagle ATW | Inconnue |
| Bandera Hackers | Inconnue |
| Spectre123 | Inconnue |
| Ghost Security Group | Etats-Unis |

## Pro-Russie

| Nom | Provenance |
|---|---|
| The RedBandits | Russie |
| STORMOUS ransomware | Inconnue |
| Hydra | Russie |
| RaHDit | Russie |
| Xaknet | Russie |
| KillNet | Russie |
| 404 Cyber Defense | Inconnue |
| WeretheGoons | Russie |
| Conti ransomware | Russie |
| punisher_346 | Inconnue |
| SaintBear/Lorec53 | Russie |
| DDoS Hacktivist Team | Russie |
| Cyberwar_world | Russie |
| Zsecnet | Russie |
| DivisionZ | Russie |

Source de données : Curated intel & iiyonite (ajouts et modifications apportées par CITALID)

# Modes Opératoires d'Attaque notables sur la période du 23 mars au 13 avril 2022

## Network Battalion 65

**Soutien :**
**Provenance :**
**Affiliation :** Anonymous

**Premiers signes d'activité :** février 2022

**Type(s) d'opérations :** Divulgation de données à finalité d'agitation et ransomware à finalité de neutralisation

**Victimologie :** Entreprises (transport, média, construction, services) et agences gouvernementales russes (espace)

**Opérations notables :** Exfiltration et chiffrement des données de VGTRK, Roscosmos, JSC Mosexpertiza, et de Gazregion SSK

## UAC-0056/SaintBear

**Attribution :** (Crowdstrike)
**Affiliation :** Inconnue

**Premiers signes d'activité :** début 2021

**Type(s) d'opérations :** Espionnage stratégique, Sabotage à finalité de destruction

**Victimologie :** Gouvernement ukrainien, gouvernement géorgien et secteur de l'énergie ukrainien

**Opérations notables :** Wiper WhisperGate contre les autorités ukrainiennes, campagne Saintbot et Outsteel contre le secteur énergétique ukrainien, campagnes Cobalt Strike, Graphsteel et Grimplant

## ATW/Blue Hornet

**Soutien :**
**Provenance :** Inconnue
**Affiliation :** Inconnue

**Premiers signes d'activité :** mars 2022 (annonce de la fin des activités le 13 avril 2022)

**Type(s) d'opérations :** Divulgation de données à finalité d'agitation, Doxxing d'adversaires, Pentesting défensif

**Victimologie :** Entreprises et agences gouvernementales russes (services en ligne), chinoises (finance, justice, services cloud), iraniennes (télécom), groupes adverses

**Opérations notables :** Divulgations des données de MyBank, Doxxing Killnet, Doxxing APT29, Compromission du logiciel ATM de Bank of China

## Sandworm Team

**Attribution :** (FireEye)
**Affiliation :** GRU - unité 74455

**Premiers signes d'activité :** 2009

**Type(s) d'opérations :** Sabotage à finalité de destruction

**Victimologie :** Ukraine, secteur de l'énergie ukrainien

**Opérations notables :** Industroyer2 et CaddyWiper contre les réseaux électriques ukrainiens (échec), BlackEnergy3 (2015), Industroyer (2016), NotPetya (2017)

MITRE

## UAC-0010/Gamaredon

**Attribution :** (SSU)
**Affiliation :** FSB

**Premiers signes d'activité :** 2013

**Type(s) d'opérations :** Espionnage stratégique

**Victimologie :** Gouvernement et officiels ukrainiens, autorités européennes

**Opérations notables :** Multiples campagnes d'hameçonnage ciblées visant les autorités ukrainiennes et européennes (principalement baltes)

MITRE

## The Black Rabbit World

**Soutien :**
**Provenance :** Inconnue
**Affiliation :** Anonymous

**Premiers signes d'activité :** décembre 2021

**Type(s) d'opérations :** Divulgation de données à finalité d'agitation, attaque en déni de service

**Victimologie :** Russie (secteur bancaire, militaire, nucléaire, gouvernemental)

**Opérations notables :** Leak des données de la Banque centrale russe, diffusion flux du réseau CCTV du Kremlin, Leak des données de Rosatom

## Légende

Activité criminelle

Activité hacktiviste non-affiliée

Attaque par chiffrement et/ou wiper

Attaque par déni de service

Diffusion de code malveillant

Campagne ou opération d'espionnage

Type d'attaque non-spécifiée à finalité de sabotage

Revendications de la mouvance Anonymous

Revendications d'ATW/Blue Hornet

Revendications de Killnet

Revendications de Conti

Confiance limitée dans la qualification

Action ou déclaration de l'Allemagne

Action ou déclaration de la Turquie

Action ou déclaration de la Biélorussie

Action ou déclaration du Canada

Action ou déclaration de la Chine

Action ou déclaration du Conseil de l'Europe

Action ou déclaration des États-Unis

Action ou déclaration d'Israël

Action ou déclaration de la Hongrie

Action ou déclaration de l'OTAN

Action ou déclaration de la Pologne

Action ou déclaration du Royaume-Uni

Action ou déclaration de la Russie

Action ou déclaration de la Suède

Action ou déclaration de l'Inde

Action ou déclaration de l'OSCE

Vote à l'Organisation des Nations Unies

Action ou déclaration de l'UE

Action ou déclaration de la Banque mondiale

Action ou déclaration de l'OMC

Action ou déclaration de Twitter

Action ou déclaration de Meta

Action ou déclaration de Youtube

Déclaration relative au groupe Wagner

# DYNAMIQUES CYBER ET GÉOPOLITIQUE DE LA GUERRE RUSSO-UKRAINIENNE

## Frise chronologique comparée du 23 mars au 13 avril 2022

### APT

- Le CERT-UA avertit de l'usage de DoubleZero contre les entreprises ukrainiennes
- Sentinel Labs attribue les activités d'UAC-0026 à Scarab
- Ghostwriter cible les officiels ukrainiens via Cobalt Strike Beacon
- Une campagne d'espionnage via un variant de Quasat RAT découvert par Lab52
- Ukretelecom impactée par une attaque contre son infrastructure centrale
- Le FBI affirme que que la Russie procède à des opérations de reconnaissance contre le secteur énergétique américain
- Identification de campagnes de COLDRIVER et Curious George en Europe de l'Est et contre l'OTAN

### CYBERCRIME & HACKTIVISM

- AnonGhost revendique une attaque contre le système d'éclairage de rue russe et démontre la compromission du système industriel de Moxa
- Georgia's Society of Hackers revendique la compromission du serveur mail.ru
- Black Rabbit World leak 28GB de données de la Banque centrale russe
- 65To de données et emails de la société Rosaviatsiya auraient été effacés
- Killnet revendique une série de DDoS contre la Pologne
- Divulgation de 110GB de données de la société russe Mashoil
- Killnet revendique une attaque contre l'US Bradley Airport
- Ghostsec divulgue les données de Shambala casino (Russie)
- Conti attaque la filiale britannique de la société japonaise Konica Minolta
- Anonymous attaque les sites d'Auchan, Leroy Merlin et Décathlon
- Twitter ferme 4 comptes affiliés Anonymous
- Divulgation de 2,4GB de mails de la compagnie russe RosProekt
- ATW cible des sociétés et le gouvernement chinois
- L'infostealer Mars Stealer est déployé contre la société civile ukrainienne
- Défiguration du site web de Gazprom
- BeeHive Cybersecurity affirme mener une campagne ransomware contre des cibles russes
- Killnet cible la Pologne et l'OTAN
- Nb65 divulgue les données de la chaîne d'Etat russe VGTRK
- Nb65 revendique l'attaque contre JSC Mosexpertiza; 450GB de données exfiltrées
- Des sites Wordpress compromis engendrent des DDoS contre des sites ukrainiens
- ATW divulgue les données d'Alibaba cloud et du ministère chinois de la Justice

### INFO WAR

- Zelensky s'exprime en anglais dans son discours quotidien à la nation pour la première fois
- Lors du sommet de l'Organisation; Biden affirme que l'OTAN n'a jamais été aussi unie
- Erdoğan affirme que la Russie et l'Ukraine sont parvenues à un consensus sur 2/3 de leurs différends
- L'Ukraine conteste les résultats annoncés par Erdoğan
- Biden à propos de Poutine : « For God's sake, this man cannot remain in power »
- Macron avertit des risques d'escalade verbale après les propos tenu par Biden à l'égard de Poutine
- L'Ukraine dévoile la potentielle identité de 620 agents du FSB
- Les services de sécurité ferment 5 botfarms gérant 100 000 comptes actifs sur les réseaux sociaux
- Shoigu annonce le succès de la première étape de l'opération russe en Ukraine : les forces navales, aériennes et anti-aériennes adverses seraient détruites
- Selon les États-Unis, Poutine est délibérément mal informé sur l'état du terrain et de ses troupes en Ukraine

### GEOPOLITICS

- Zelensky appelle au boycott des sociétés occidentales toujours en activité en Russie
- Zelensky s'exprime face à l'UE et l'OTAN par appel vidéo
- La Hongrie rejette la demande de l'Ukraine de transit d'armes via son territoire
- A Varsovie, Biden réaffirme l'engagement « sacré » des États-Unis envers l'article 5 du Traité de l'Atlantique Nord
- La France réaffirme la nécessaire application du droit international humanitaire
- Le Royaume-Uni affirme que le groupe Wagner est présent en Ukraine
- L'Ukraine envisage la neutralité mais refuse un compromis sur sa souveraineté et son intégrité territoriale
- Zelensky livre un discours historique devant le parlement norvégien
- Biden en visite en Europe
- Le Conseil de sécurité rejette le projet russe de résolution sur la situation humanitaire en Ukraine
- Les occidentaux se prononcent contre l'adhésion de la Biélorussie à l'OMC
- La Chine suspend les négociations autour d'un projet d'investissement pétrochimique en Russie
- Bennett réaffirme un soutien politique et humanitaire à l'Ukraine
- Biden menace la Russie de représailles non spécifiées en cas d'utilisation d'armes chimiques
- Reprise des pourparlers entre l'Ukraine et la Russie à Istanbul
- Lavrov en visite en Chine
- Explosion d'un dépôt de munitions dans la région de Belgorod

SANCTIONS

23/03 | 24/03 | 25/03 | 26/03 | 27/03 | 28/03 | 29/03 | 30/03

# DYNAMIQUES CYBER ET GÉOPOLITIQUE DE LA GUERRE RUSSO-UKRAINIENNE

## Frise chronologique comparée du 23 mars au 13 avril 2022

### APT

- Spear-phishing délivrant Elephant contre des organisations ukrainiennes dont ICTV attribué à SaintBear
- Découverte du wiper AcidRain déployé précédemment contre le réseau Viasat
- Spear-phishing contre des officiels via Telegram attribué à Gamaredon par le CERT-UA
- Découverte de deux campagnes menées par Gamaredon contre les organisations gouvernementales ukrainiennes et européennes
- Exploitation du sujet du conflit par les MOA Lyceum (Iran), SideWinder (Inde), El Machete (Amérique latine)
- Le Département de la Justice annonce le succès d'une opération du FBI contre Cyclops Blinks
- Microsoft saisit 7 domaines utilisés par APT28
- Ghostwriter compromet les comptes FB de soldats ukrainiens pour diffuser des incitations à déposer les armes

### CYBERCRIME & HACKTIVISM

- Divulgation de mails des sociétés russes Thozi corp et Marathon Group
- Nordex localisé à Hambourg et Rostock attaqué
- Xaknet menace le camp ukrainien et divulgue 638 MB de documents du ministère ukrainien des affaires étrangères
- Wh13sh4d0w attaque la société russe Capital Legal Services
- Divulgation de 15GB de données de l'Église orthodoxe russe
- Wh13sh4d0w divulgue 25GB de données de l'usine russe de Lipetsk
- Défiguration du site du constructeur aéronautique russe Sukhoi
- Spectre123 divulgue des données de l'armée indienne
- ATW divulgue des informations sur les MOA APT3, APT40, APT38 et APT28
- ATW dévoile l'identité alléguée d'un membre clé du groupe Killnet
- Divulgation de données de l'agence fédérale russe de gestion des biens d'État
- Nb65 revendique l'attaque contre le constructeur d'équipement gazier russe SSK
- L'identité alléguée de 120 000 soldats russes dévoilée
- RedbanditsRU interfèrent avec l'outil Liberator utilisé pour conduire des DDoS contre la Russie
- Divulgation de 82GB de mails de la société russe Korolevskiy
- Panasonic Canada ciblé par Conti
- STORMOUS menace d'intégrer la France à sa liste de cibles
- Compromission du système CCTV du Kremlin par The Black Rabbit World
- Divulgation de mails des sociétés russes Petrovsky Fort, Aerogas et Forest
- ATW revendique la compromission et la divulgation de données de la société russe Rabotut

### INFO WAR

- Moscou rassemble 134000 conscrits mais nie leur déploiement en Ukraine
- Pour Washington le repositionnement russe dans le Donbass démontre l'incapacité de Moscou à prendre Kiev
- Le gouverneur de Belgorod accuse l'Ukraine d'une attaque en territoire russe
- Le Kremlin annonce que les négociations seront entravées par les frappes ukrainiennes en Russie
- Le maire de Kiev qualifie la situation à Boucha de génocide
- Le ministre de la défense dénonce une campagne médiatique coordonnée à Boucha
- Zelensky accuse la Russie de génocide lors d'un discours diffusé aux Grammy Awards
- Le Roskomnadzor demande à Wikipédia de supprimer les informations traitant de la guerre en Ukraine
- Dmitri Medvedev qualifie les incidents de Boucha de fake news
- La Russie accuse l'Ukraine de préparer une opération au chlore à Pervomaiskyi sous faux drapeau
- L'Ukraine accuse Orban d'aider Poutine
- Meta ferme 200 comptes pro-russes pour mass-reporting

### GEOPOLITICS

- Rencontre entre le ministre de la défense polonais et le ministre des affaires étrangères ukrainien
- Lavrov en visite en Inde
- Poutine annonce le paiement du gaz russe en roubles pour les États déclarés hostiles
- Kiev dénonce la conscription de citoyens ukrainiens par la Russie en territoires occupés
- Frappes contre un dépôt de carburant à Belgorod
- La Commission européenne et le Canada lancent l'initiative de financement #StandupforUkraine
- Le Royaume-Uni annonce soutenir l'enquête de la CPI pour des crimes de guerre en Ukraine
- Le Belgique et les Pays-Bas expulsent 38 diplomates russes
- Macron appelle à la condamnation des autorités russes en réaction à la situation à Boucha
- L'Allemagne qualifie les exactions commises à Boucha de crimes de guerre
- Orban désigne Zelensky comme un adversaire
- Paris annonce l'expulsion de 35 diplomates russes
- Vilnius expulse l'ambassadeur russe et rappelle son homologue lithuanien
- Zelensky demande l'exclusion du la Russie du Conseil de Sécurité
- 87 diplomates russes expulsés par 4 pays européens
- La France et la Suède ouvrent des enquêtes pour crimes de guerre en Ukraine
- Appel téléphonique entre Poutine et Orban sur l'Ukraine
- Le Conseil de l'Europe qualifie les évènements de Boucha de crimes de guerre
- La Russie refuse de discuter le cas de la Crimée et du Donbass avec l'Ukraine
- La Russie suspendue du Conseil des droits de l'Homme

SANCTIONS

31/03 | 01/04 | 02/04 | 03/04 | 04/04 | 05/04 | 06/04 | 07/04

# DYNAMIQUES CYBER ET GÉOPOLITIQUE DE LA GUERRE RUSSO-UKRAINIENNE

## Frise chronologique comparée du 23 mars au 13 avril 2022

### APT

- DDoS contre les ministères finlandais de la défense et des affaires étrangères
- Annonce de l'échec du sabotage (via Industroyer 2 et CaddyWiper) attribué à Sandworm, contre les réseaux électriques ukrainiens
- DDoS contre le FAI McLaut, impacts sur la région de Cherkasy (Ukraine)

### CYBERCRIME & HACKTIVISM

- ATW revendique la compromission d'ATM de la Bank of China
- ATW divulgue les données de la banque chinoise en ligne MyBank
- Compromission des données de la Luna Glob mission de Roskosmos par Vlog3lsec
- Syncthe et AnonZeus fusionnent pour former ReaperSec
- Bandera Hackers diffusent des articles dénonçant les exactions russes en Ukraine sur le site du CADDPI russe
- Campagne de recrutement du groupe pro-russe Zsecnet
- Divulgation de 230 000 mails du ministère de la culture russe
- Wh1t3sh4d0w divulgue 130 000 mails du gouverneur de Tver et son équipe
- Divulgation de 250 000 mails du Département de l'éducation de Strezhevoy (Russie)
- ATW annonce l'arrêt de l'activité du groupe et sa reconversion en white hat
- Divulgation de 440GB de mails de la société russe Technotec

### INFO WAR

- La France qualifie le bombardement de la station de Kramatorsk de crime contre l'humanité
- Le Ministre de la défense russe affirme que les missiles Tochka-U sont uniquement utilisés par l'Ukraine
- Le gouverneur de Kursk dénonce des tirs de mortiers à proximité d'Elizovetovka
- Youtube ferme la chaîne officielle de la Douma sur son site
- Le vice-ministre de l'économie assure que la Russie a suffisamment de ressources pour assurer sa dette
- L'UE accuse la Russie d'aggraver une crise alimentaire mondiale
- Lukachenko désigne la Grande-Bretagne comme responsable des exactions commises à Boucha
- Biden accuse la Russie de crime de génocide en Ukraine
- Accusations contre la Russie d'emploi d'armes chimiques (phosphore) à Marioupol
- La Russie annonce le bombardement d'un poste de contrôle frontalier de la région de Koursk

### GEOPOLITICS

- Von der Leyen et Borrel se rendent à Boucha
- Remise du questionnaire d'adhésion à l'UE à Zelensky
- 1 000 mercenaires recensés dans le Donbass
- Le président allemand appelle à la création d'un tribunal de guerre contre Poutine et Lavrov
- Rencontre entre Johnson et Zelensky à Kiev
- L'ambassadeur russe aux États-Unis avertit d'une possible confrontation militaire entre Moscou et Washington
- La Banque mondiale prévoit une baisse respective de 45% et 11% de l'économie ukrainienne et russe en 2022
- L'Inde propose à la Russie une rencontre entre Poutine et Zelensky
- La France expulse 6 diplomates russes accusés d'espionnage
- Rencontre entre les présidents polonais, lituanien, estonien et letton à Rzeszów en soutien à l'Ukraine
- Rencontre entre Poutine et Loukachenko
- La Russie considère les livraisons d'armes par les États-Unis et l'OTAN comme cibles militaires légitimes
- Le rapport de l'OSCE relève des violations répétées au droit international humanitaire par la Russie
- Les présidents des pays baltes et polonais rencontrent Zelensky à Kiev

SANCTIONS

08/04 09/04 10/04 11/04 12/04 13/04

# Principales Sources

Curated Intel/Ukraine-Cyber-Operation, BushidoUK, 23/02/2022, Github
https://github.com/curated-intel/Ukraine-Cyber-Operations

Threat Table
https://www.threatable.io/

Liveuamap
https://liveuamap.com/

Reuteurs sanctions tracker
https://graphics.reuters.com/UKRAINE-CRISIS/SANCTIONS/byvrjenzmve/

Correctiv
https://correctiv.org/en/latest-stories/2022/03/01/sanctions-tracker-live-monitoring-of-all-sanctions-against-russia/

Peterson Institute of International Economics
https://www.piie.com/blogs/realtime-economic-issues-watch/russias-war-ukraine-sanctions-timeline

Cyber Peace Institute
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/

Russia the Silent Conflict (3/4-9/4) - Security Affairs
https://securityaffairs.co/wordpress/130057/cyber-warfare-2/apr-03-apr-09-ukraine-russia-cyber-conflict.html

Russia the Silent Conflict (27/3-2/4) - Security Affairs
https://securityaffairs.co/wordpress/129768/cyber-warfare-2/mar-27-apr-02-ukraine-russia-cyber-conflict.html

Russia the Silent Conflict (20/3-26/2) - Security Affairs
https://securityaffairs.co/wordpress/129518/cyber-warfare-2/mar-20-26-ukraine-russia-cyber-conflict.html

Russia-linked cyberattacks on Ukraine: A timeline – CSO
https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html?page=2

Live Updates: Russia/Ukraine Conflict - Cyber Threats and Attacks  - Cyware
https://cyware.com/blog/live-updates-russiaukraine-conflict-cyber-threats-and-attacks-3d68

CERT-UA
https://cert.gov.ua/

Malpedia
https://malpedia.caad.fkie.fraunhofer.de/

Distributed Denial of Secrets
https://ddosecrets.com/wiki/Distributed_Denial_of_Secrets

## Crédits

Cyber attack icons created by Freepik – Flaticon - Ransomware icons created by wanicon – Flaticon - Hacker icons created by Freepik – Flaticon - Propaganda icons created by Freepik – Flaticon - Ddos icons created by Freepik – Flaticon - Ddos icons created by juicy_fish – Flaticon – Rise icon by Freepik – Flaticon – Spyware icon by Freepik – Flaticon – New icon by Freepik – Flaticon – Checked icon by Roundicon – Flaticon – Warning icon by Pixelmeetup - Flaticon

## Contact Citalid

Mail : sales@citalid.com
Site : www.citalid.com
Twitter : https://twitter.com/citalid
LinkedIn : https://fr.linkedin.com/company/citalid
Adresse : 120, rue Jean Jaurès 92 300 Levallois-Perret