WEBINAIRE #6

Conflit Russie Ukraine

Menaces cyber

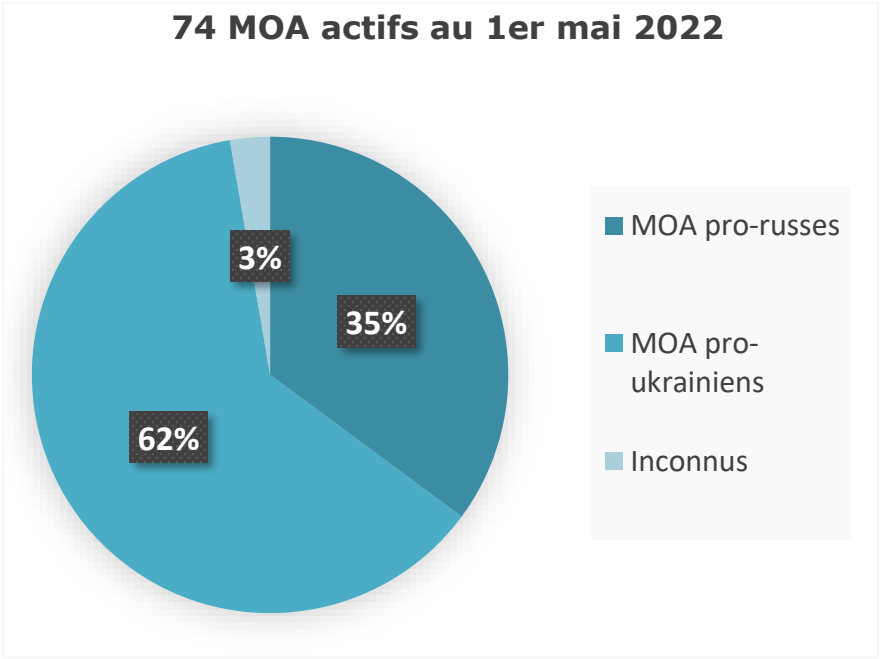
13/05/2022

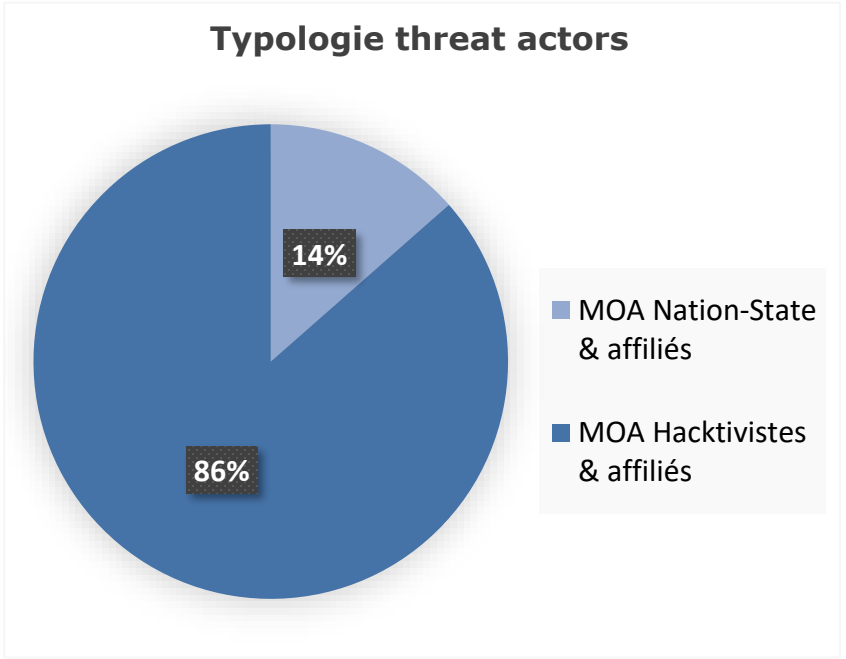
Modérateur : Philippe Cotelle, administrateur de l'AMRAE et président de la Commission Cyber.

Intervenants :

- **Robin Evans**, cyber threat intelligence analyst, Citalid.
- **Vladimir Rostan d'Ancezune**, avocat associé, DAC Beachcroft France, membre du Comité scientifique de l'AMRAE.

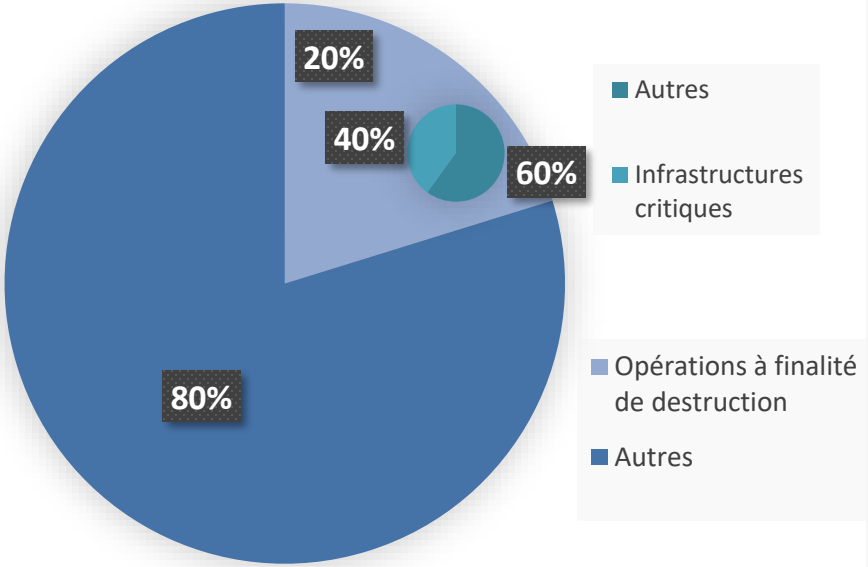
I. Guerre russo-ukrainienne et menace cyber : quelles dynamiques ?





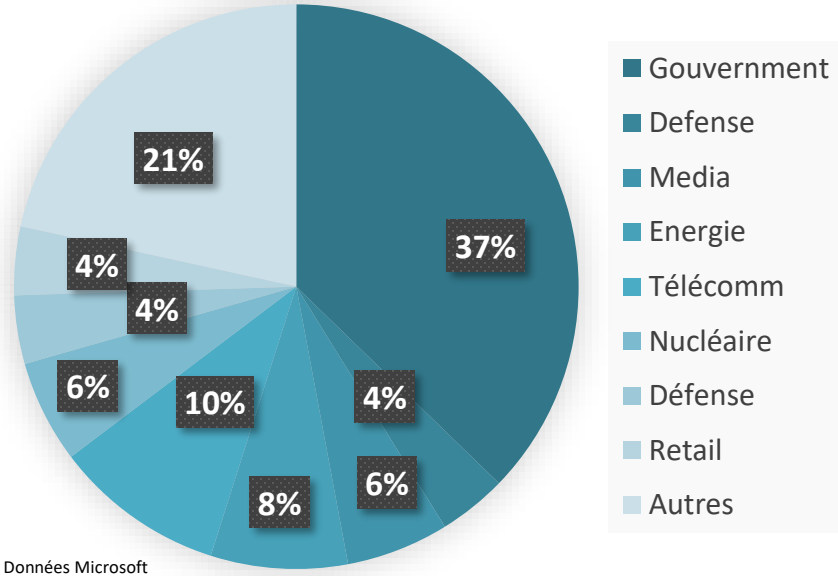
I. Guerre russo-ukrainienne et menace cyber : quelles dynamiques ?

Opérations de destruction réputées russes en Ukraine (février-mars 2022)



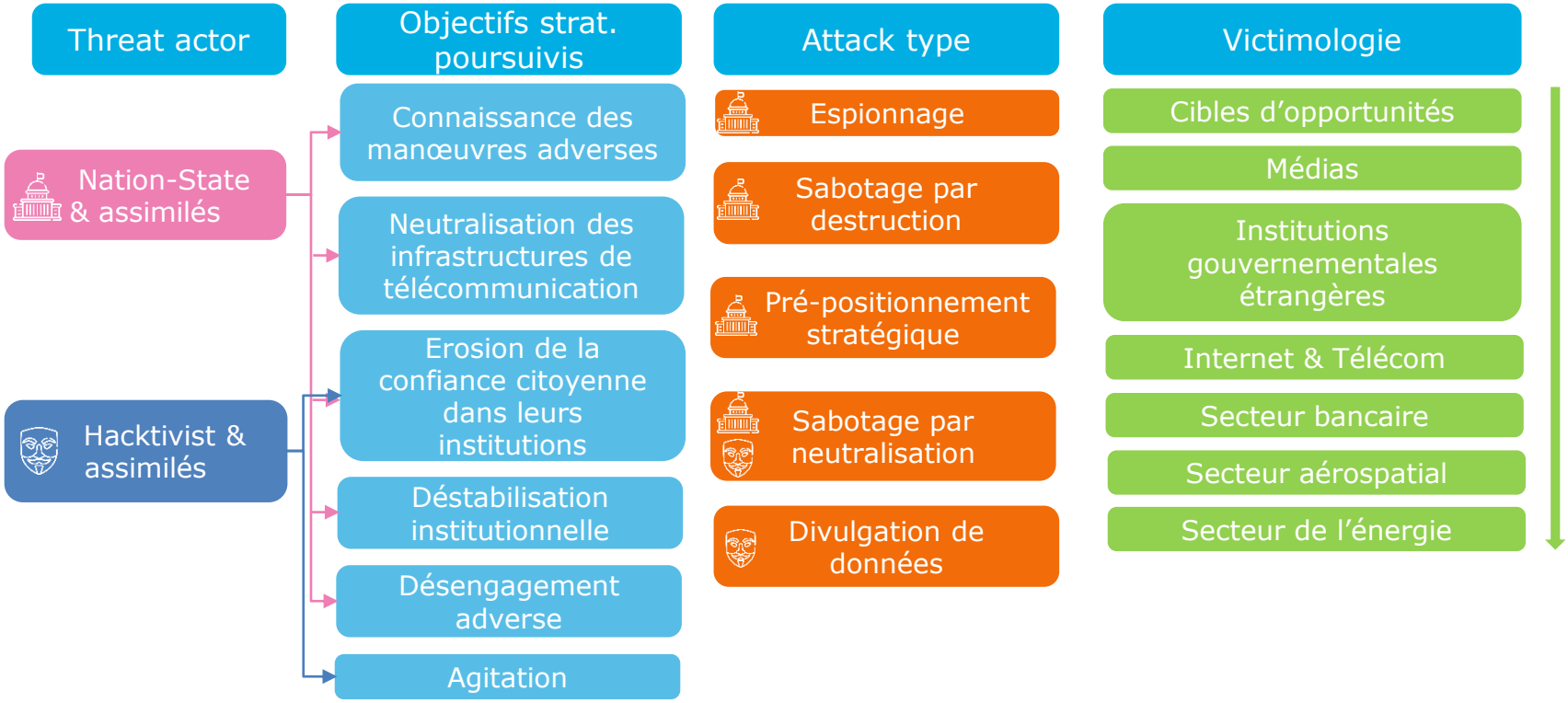
Données Microsoft

Échantillon ciblage réputé russe en Ukraine (23/02-08/04)

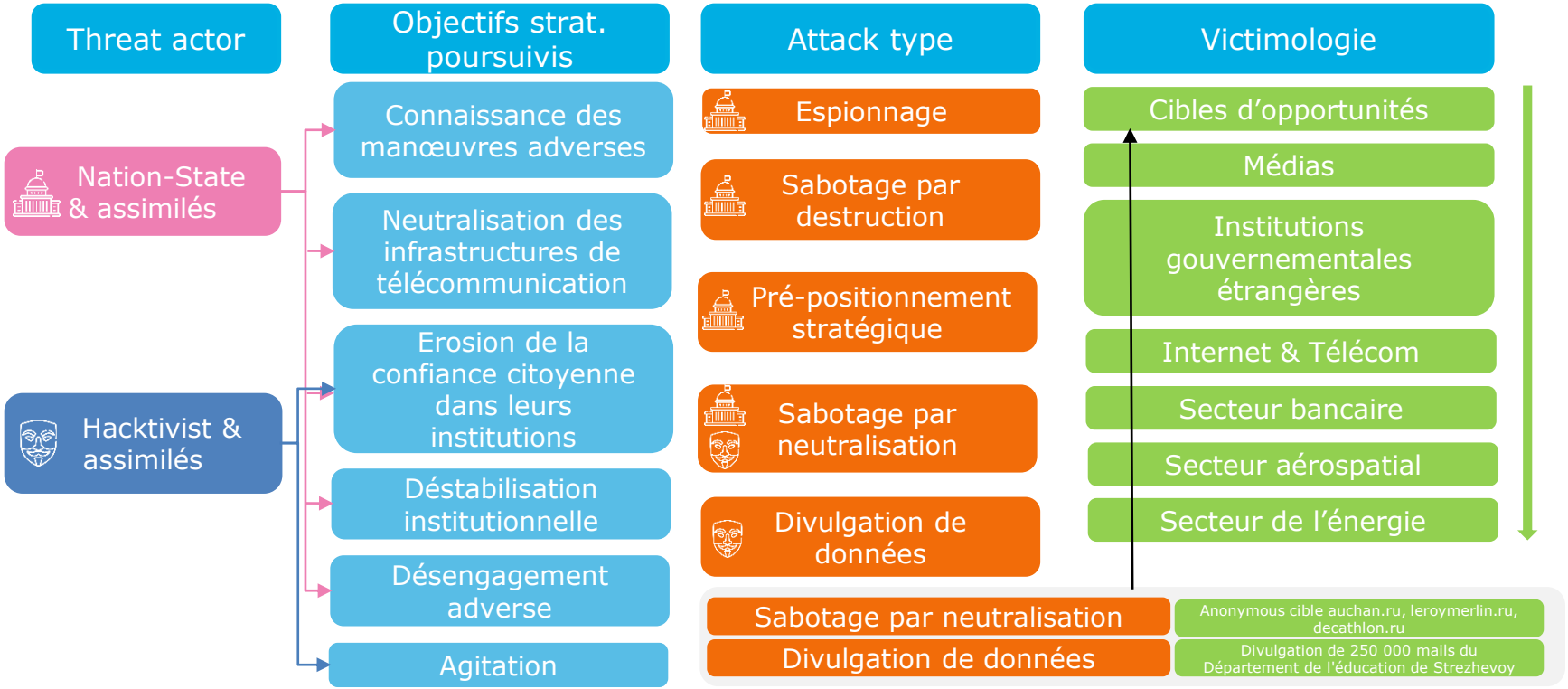


Données Microsoft

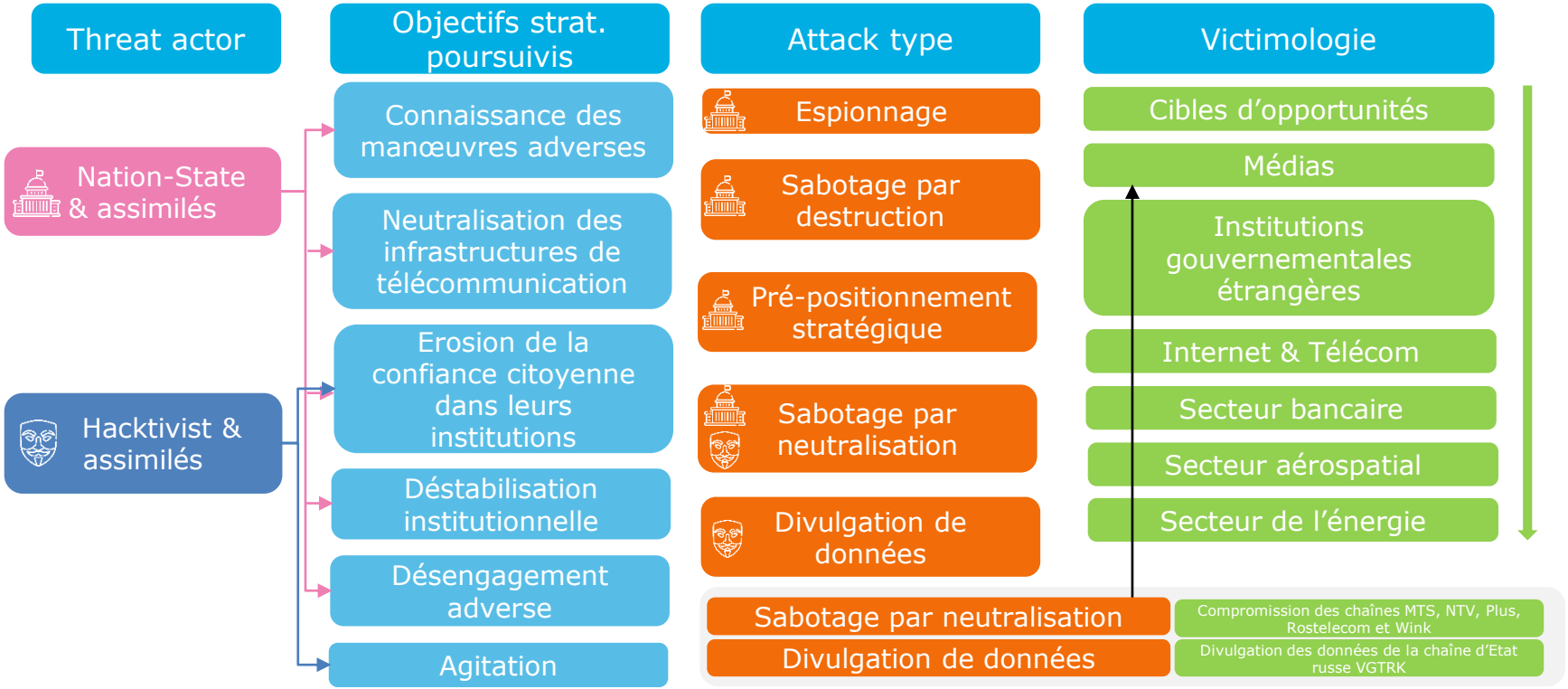
1. Anatomie de la menace



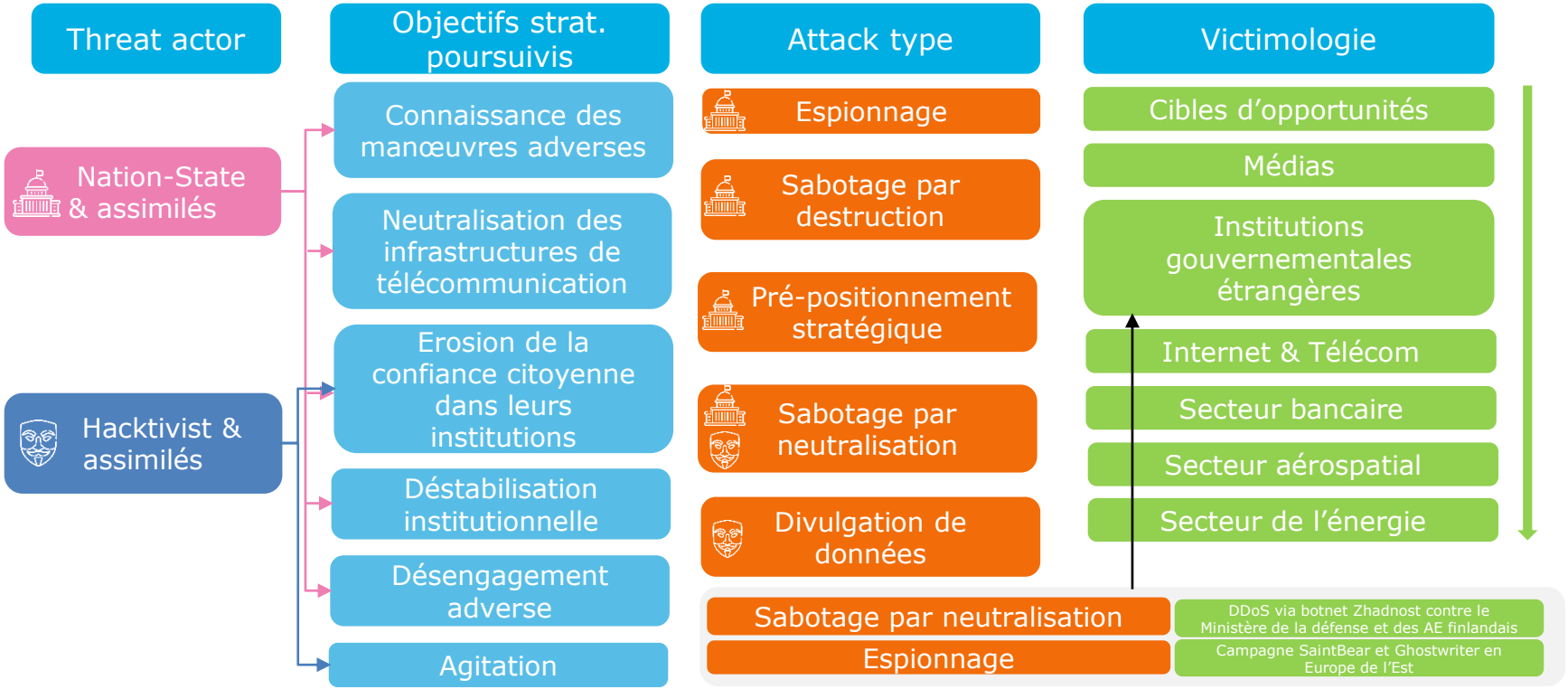
1. Anatomie de la menace



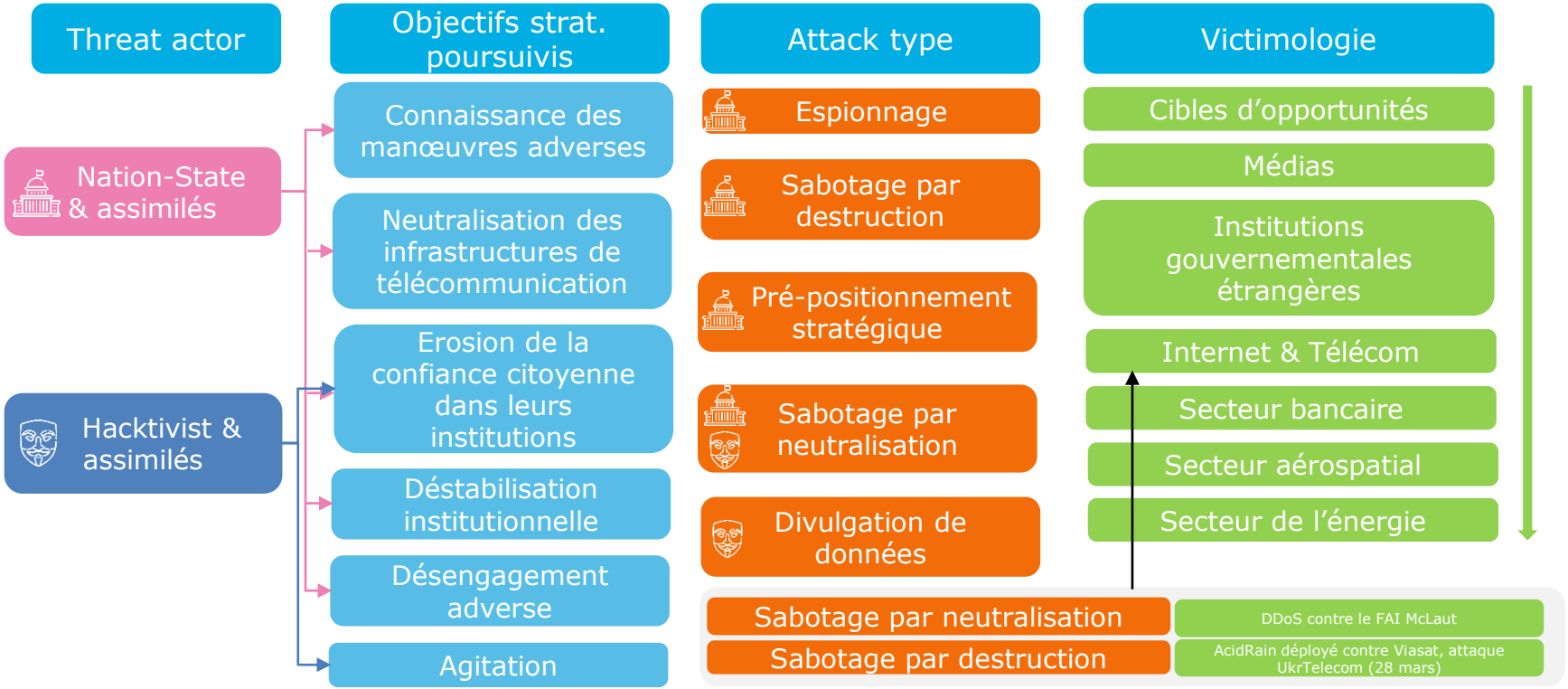
1. Anatomie de la menace



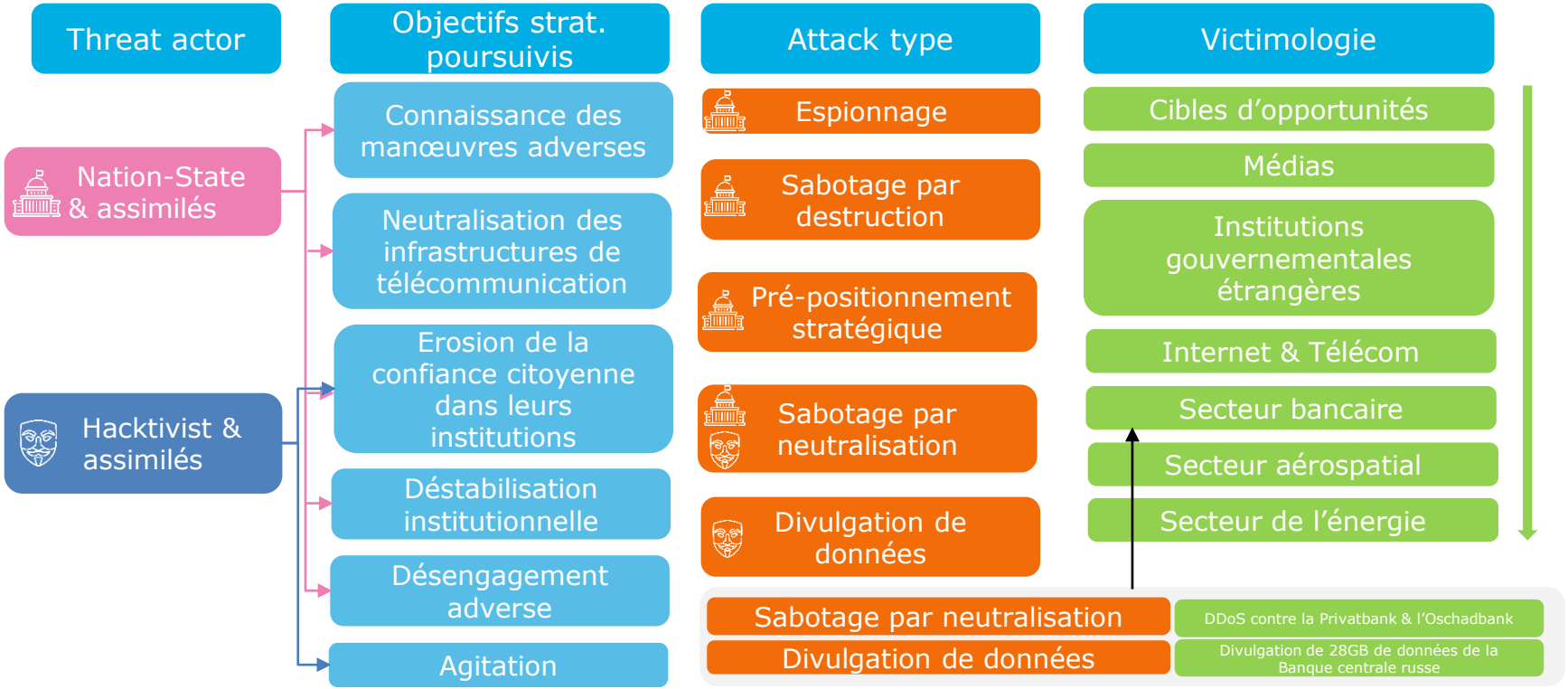
1. Anatomie de la menace



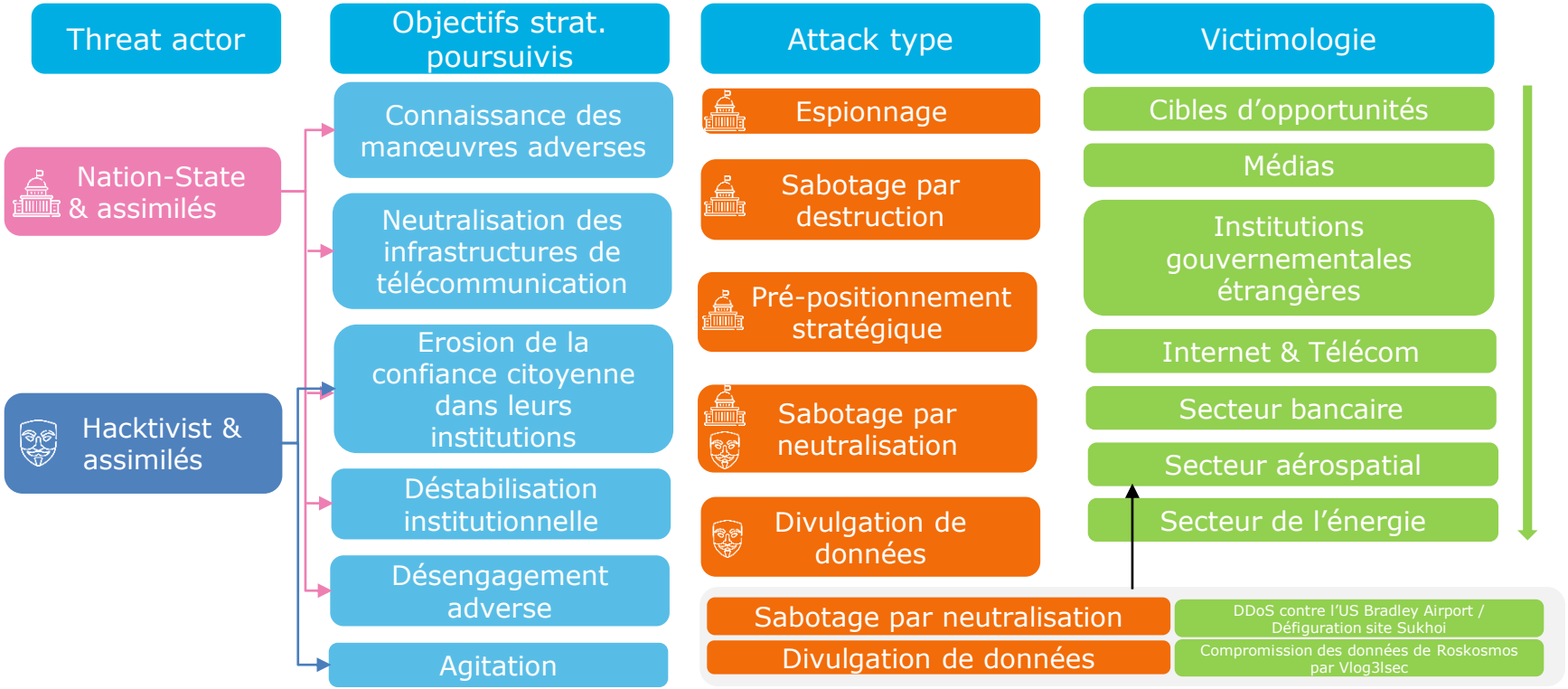
1. Anatomie de la menace



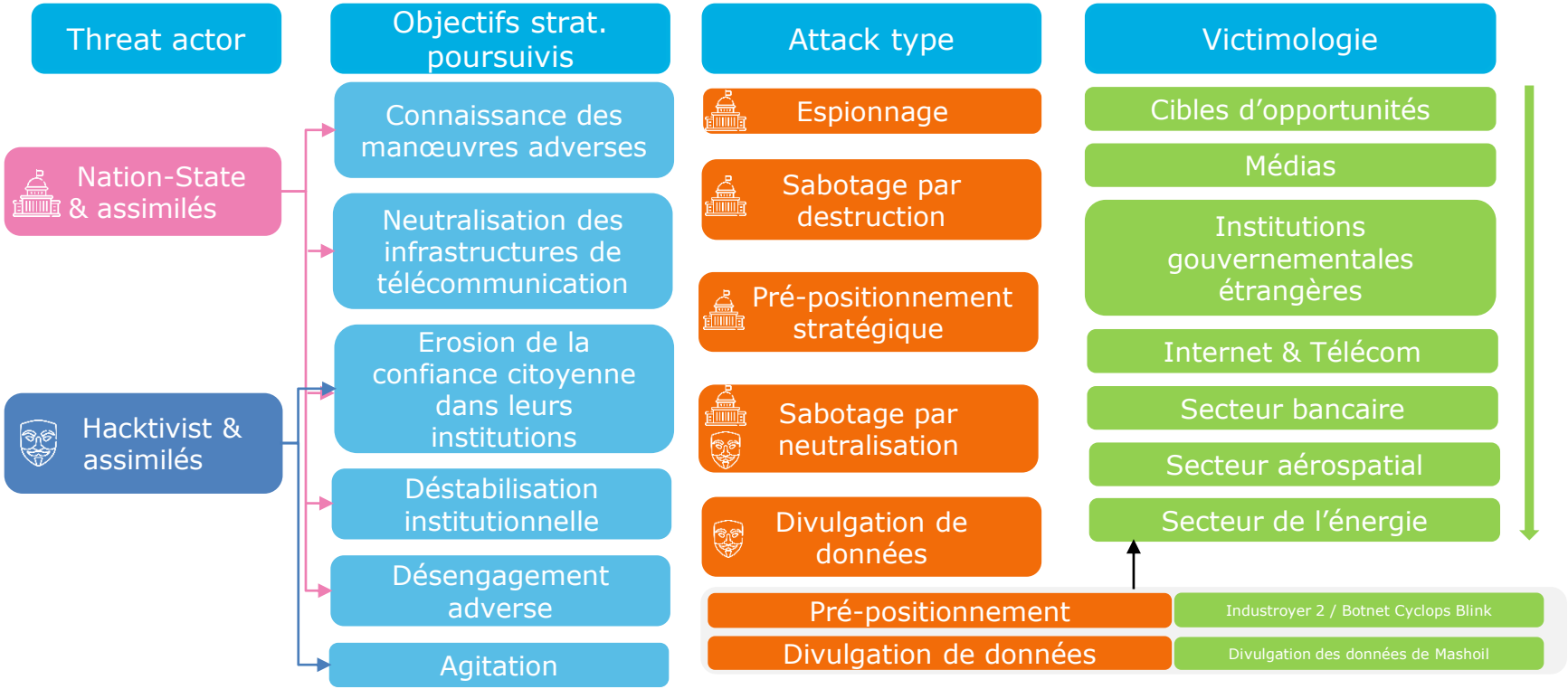
1. Anatomie de la menace



1. Anatomie de la menace



1. Anatomie de la menace



2. Rythmes et tendances conflictuelles

Sous-exploitation apparente du levier cyber

- Cyber-attaques **nombreuses**, restent majoritairement de **faible à moyenne intensité** et **mises en échec** (CERT-UA).
- **Victoire stratégique** sur l'adversaire principalement au **moyen d'armes conventionnelles**

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

- **Appui aux opérations militaires** et/ou visent à **simuler la défaillance de l'État** ukrainien
- Attaques ciblant les **infrastructures de communications** restent nombreuses (3000 DDoS entre le 15 février et le 16 mars – *données du Ministère de la Défense Ukrainien-*)
- Cas de **pré-positionnement russe**, découverts et mis en échec par l'Ukraine et les États-Unis, doivent amener à **tempérer ce constat**

Ambiguïté de l'articulation entre opérations cybernétiques et conventionnelles

- Principale difficulté émerge en considération des deux tendances précédentes
- Le levier cybernétique dispose-t-il de ses **objectifs et cibles stratégiques propres** ou recoupe-t-il avec le levier conventionnel ?

→ Volet **local, régional et international** du conflit : disjonction entre les deux modalités conflictuelles s'accroit en passant à l'échelle

2. Rythmes et tendances conflictuelles

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

- Offensives hacktivistes sont **diffuses**, **nombreuses** et **intenses**,
- Opérations de sabotage et menées contre des cibles stratégiques se multiplient.
- L'impunité contextuelle dont bénéficie les MOA hacktivistes alimente la surenchère et la démonstration de force

Quelles projections ?

- Accentuation consolidation côté occidental → Poursuite opérations espionnage et opérations de **sabotage par neutralisation** à redouter
- Vers un désengagement occidental → Opérations de **pré-positionnement** à redouter

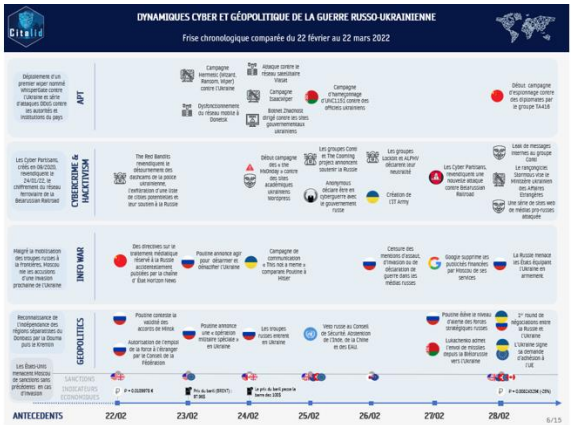
Internationalisation du conflit cybernétique

- Opérations offensives hacktivistes élargissent le spectre de leur ciblage :
  - **Organisations et des gouvernements étrangers** alliés de la Russie
  - **Entreprises et institutions occidentales** toujours **en lien avec Moscou**
- Côté russe, projection concentrée sur des **opérations d'espionnage contre les gouvernements occidentaux**
  - Opérations de **pré-positionnement contre des infrastructures critiques** étrangères probables
  - Mobilisation **hacktiviste pro-russe** concentrée sur la **zone d'influence historique russe**

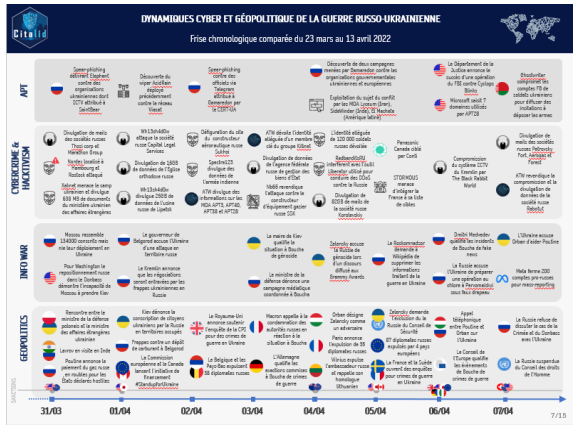
Citalid suit l'évolution de la menace liée au conflit au jour le jour

→ Pour un suivi des dynamiques conflictuelles et de la menace liée au conflit, Citalid propose une série de timelines contextualisées :

La 1ère édition (22 février – 22 mars 2022) ici



2ème édition (23 mars-13 avril 2022) ici



→ Notre 3ème édition (14 avril – 24 mai 2022) sortira le 26 mai prochain

https://citalid.com

II. La cyber-guerre : Enjeux et état des lieux

1. Constats et problématisation

Les cyber-attaques ne sont **pas prises en considération** par le droit des conflits armés

→ Initiative : le **Manuel de Tallin 2.0** (2013)

- Application du droit international public aux cyber-opérations
- Transposition du droit des conflits armés à certains types d'opérations

Les cyber-attaques évoluent en zone grise :

- « Prolongement de la politique par d'autres moyens »,
- **Coercition**,
- **Limitations** des coûts humains, matériels, politiques et **juridiques** d'une agression armée

Décalage entre une **réalité conflictuelle** et une **mauvaise assimilation juridique & sémantique** du phénomène

II. La cyber-guerre : Enjeux et état des lieux

1. Constats et problématisation

→ Face à une confusion juridico-terminologique, l'entreprise et ses risques :

- *Merck & Co., Inc. et al. v. Ace American Ins. Co. et al.* (1,3 mrds USD)
- *Mondelez International, Inc. v. Zurich American Insurance* Company (100 mil. USD)

Quelles définitions ? Quels critères ? Quels seuils d'applicabilité ? Quels types d'attaques ? Quel(s) type(s) d'attaquants ?

Contexte :

- Opérateur économique infecté par NotPetya
- Opération attribuée au Sandworm Group (GRU -unité 74455-)
- Clause d'exclusion des actes de guerre
- « Un outil utilisé par le gouvernement russe dans son conflit avec l'Ukraine »

Contexte :

- Clause d'exclusion des actes de guerre & assimilés (« hostile or warlike acts »)
- Couverture des « pertes ou dommages physiques aux données, programmes ou logiciels électroniques, y compris les pertes ou dommages physiques »

2. Identifier le conflit armé et ses composantes

Opérateur économique touché

Par une organisation privée
- Art. 8 PAREFII
- « Contrôle effectif »

Par l'Etat ou l'un de ses organes

CIJ, avis, *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, 9 juillet 2004, §139 :

« L'article 51 de la Charte reconnaît ainsi l'existence d'un droit naturel de légitime défense en cas **d'agression armée par un Etat contre un autre Etat**. Toutefois, Israël ne prétend pas que les violences dont il est victime soient imputables à un Etat étranger. »

2. Identifier le conflit armé et ses composantes

Opérateur économique touché

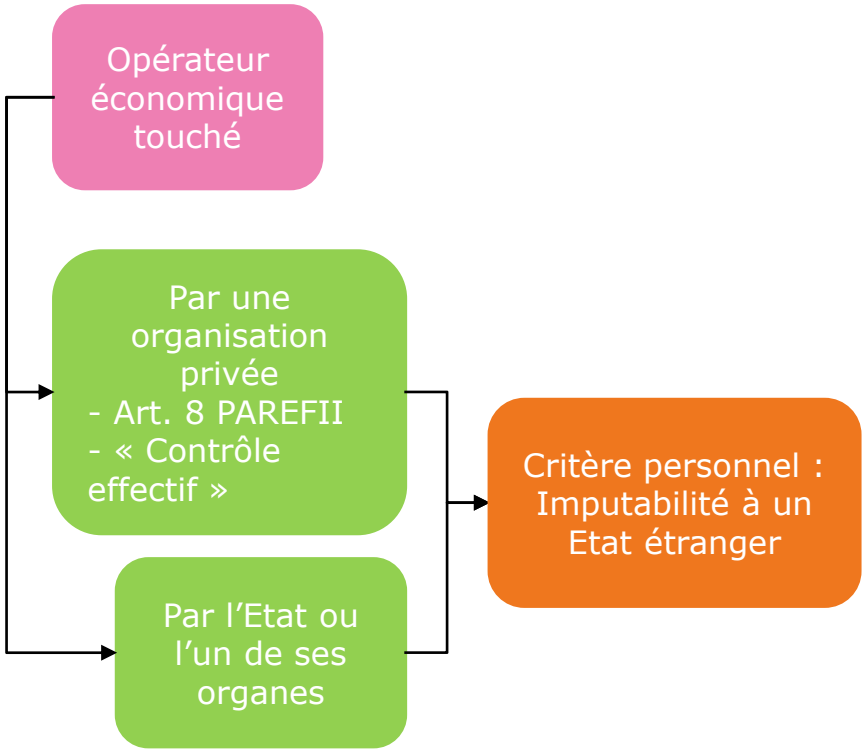
Par une organisation privée
- Art. 8 PAREFII
- « Contrôle effectif »

Par l'Etat ou l'un de ses organes

CDI, *Projet d'articles sur la responsabilité de l'Etat pour fait internationalement illicite*, 2001, Article 8 :
« Le comportement d'une personne ou d'un groupe de personnes est considéré comme un fait de l'Etat d'après le droit international si cette personne ou ce groupe de personnes, en adoptant ce comportement, **agit en fait sur les instructions ou les directives ou sous le contrôle de cet Etat. »**

CIJ , *Activités militaires et paramilitaires des Etats-Unis au Nicaragua et contre celui-ci*, arrêt du 27 juin 1986, §115 :
Pour que la responsabilité juridique de ces derniers soit engagée, il devrait en principe être établi qu'ils avaient **le contrôle effectif des opérations** militaires ou paramilitaires au cours desquelles les violations en question se seraient produites.
→ Confirmé par : CIJ, *Application de la convention pour la prévention et la répression du crime de génocide*, arrêt du 26 février 2007, §377-415

2. Identifier le conflit armé et ses composantes



2. Identifier le conflit armé et ses composantes

Opérateur économique touché

Par une organisation privée
- Art. 8 PAREFII
- « Contrôle effectif »

Par l'Etat ou l'un de ses organes

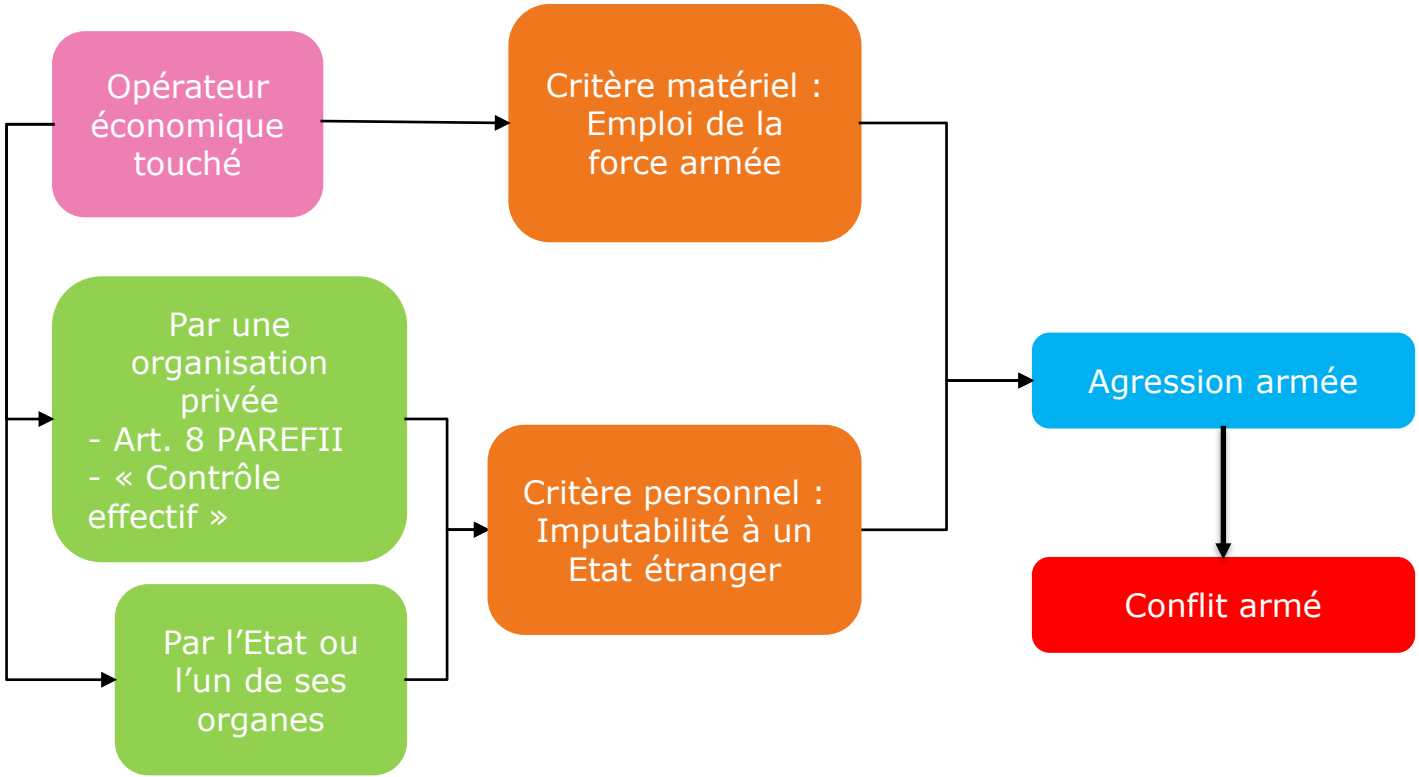
Critère matériel : Emploi de la force armée

Critère personnel : Imputabilité à un Etat étranger

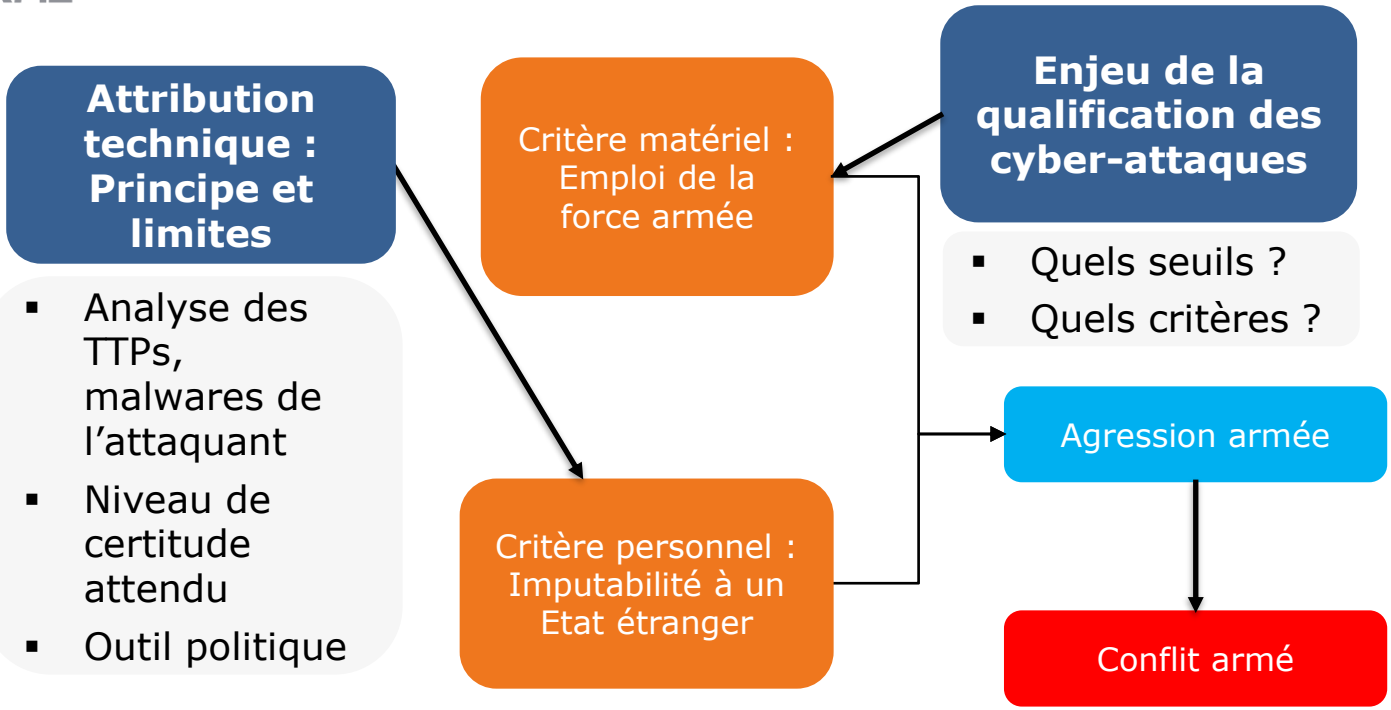
Assemblée Générale des Nations-Unies, rés. 3314 (XXIX), 14 décembre 1974 :

« L'agression est **l'emploi de la force armée par un Etat** contre la **souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre Etat**, ou de toute autre manière incompatible avec la Charte des Nations Unies. »

2. Identifier le conflit armé et ses composantes



2. Identifier le conflit armé et ses composantes



Citalid, de la threat intelligence au pilotage des risques par la quantification financière de la menace cyber

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

Quels impacts sur l’assurance cyber ?

La sinistralité de la cybercriminalité

- Les risques cyber existent par le seul recours aux technologies de l'information et de la communication utilisant des réseaux tel qu'Internet.
- 2021: **le coût total a dépassé les 6.000 milliards de dollars**.
- 1/5ème de ces attaques a visé l'Europe.
- Primes collectées: environ 10 milliards $.
- Augmentation de 42% du coût des rançons par rapport à 2020.
- 1er semestre 2021: 60% du total 2011-2020.

Enjeux et contradictions

- Besoin d'hyper sélectivité
- Politique Cyber et investissement
- Souscription de nouveaux risques limités
- PME et ETI françaises:
  - Taux d'équipement dérisoire > 8%;
  - 43% des attaques cyber;
  - 71 % ne se remettent pas d'une attaque.
- Dans une monde de pénurie, des entreprises a priori non stratégiques deviennent des cibles possibles de déstabilisation.
- Un marché de l'assurance cyber peu attractif pour les assureurs.

Perspectives sectorielles

- Combattre le sous-équipement : de quelques mois à plusieurs années.
- Plus de 50% des entreprises UE manquent d'experts cyber.
- Pendant l'implémentation de solutions, nouvelles attaques qui rendent les solutions obsolètes et non satisfaisantes au regard des nouveaux standards des assureurs.

Risques : actes de guerre et cyberguerre

- Acte de guerre
  - Définition pratique
  - Définition en droit international public

- Cyberguerre.

Dématérialisation de la guerre

- Une dématérialisation considérée en droit international
- Une dématérialisation considérée en doctrine.

Variété d'attaques cyber

- Extorsion de fonds (rançongiciels) : Petya (rançon);
- Espionnage industriel;
- Atteinte à l'image / vol;
- …

Détruire, déstabiliser, désorganiser

La couverture du risque de guerre

- **Une exclusion de principe** :
  - En France.
  - Marchés de Londres et US

- **Une couverture possible**

Précédents jurisprudentiels

- Mondelez International v. Zurich
- Merck & Co. Inc. vs. ACE

L’absence de couverture des « attaques soutenues par un Etat »

- Marché de Londres
- Hors marché de Londres

Le critère de l’attribution

Concept central du nouveau cadre : qui attribue ? Qui est visé par l’attribution?

- **L’autorité attributrice**
- **La source de l’attaque**

« *Actes commis par ou avec la participation d'un Etat et invoqué comme tel par un autre Etat* »

Concept central du nouveau cadre : qui attribue ? Qui est visé par l'attribution?

- Terrain probatoire
- Un certain flou
- L'intention de non-couverture
- Les contours des nouvelles exclusions