



Guerre hybride en Ukraine :
quels rôles les entreprises
technologiques jouent-elles
dans le conflit et quels défis
sont à relever dans l'avenir ?

Quang-Minh Lepescheux

Directeur, Affaires Publiques Européennes

Microsoft



Contexte de cybersécurité



78 trillions

de signaux chaque jour

600 millions

d'attaques chaque jour

34 000

ingénieurs dédiés

15 000

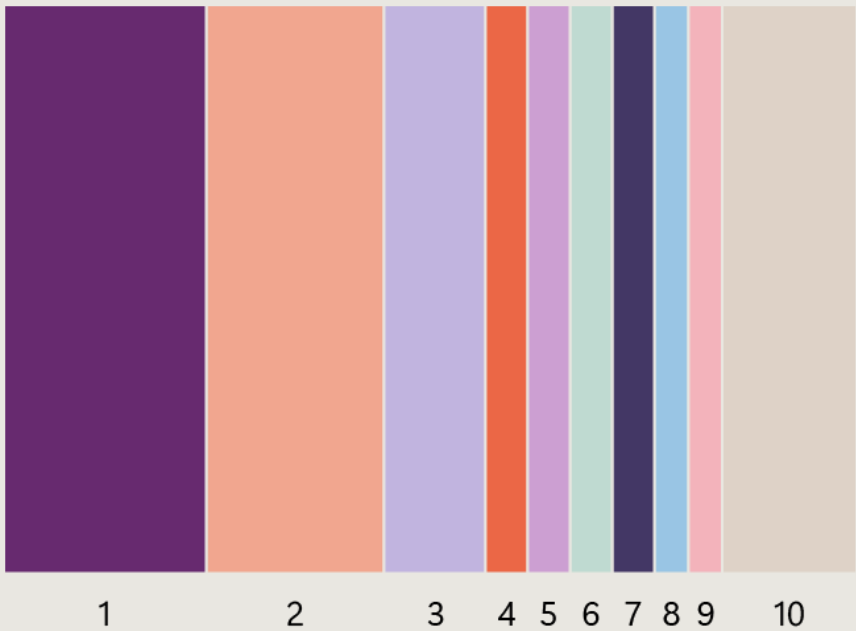
partenaires spécialisés

partenaires spécialisés

12 000

Menaces cyber conduites par des Etat-nations

Top 10 targeted sectors worldwide



Sector		Percentage
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Source: Microsoft Threat Intelligence, nation-state notification data

Targeting by region



Sector	Percentage
1 Europe & Central Asia	68%
2 North America	20%
3 Middle East & North Africa	5%
4 East Asia & Pacific	3%
5 Latin America & Caribbean	3%
6 South Asia	1%
7 Sub-Saharan Africa	1%

Most targeted sectors



Sector	Percentage
1 Government	33%
2 IT	15%
3 Think tanks and NGOs	15%
4 Education and Research	9%
5 Inter-governmental organization	4%
6 Defense Industry	4%
7 Transportation	3%
8 Energy	2%
9 Media	2%
10 All others	13%

Une pléthore d'acteurs

- 01 **États** : Agents au sein du gouvernement d'un pays, y compris, par exemple, les agences militaires et de renseignement qui dirigent les cyber-opérations dans le cadre de la conduite plus large de la politique étrangère.
- 02 **Cybercriminels** : Acteurs non étatiques, individus et groupes, qui mènent des cyber-opérations principalement motivées par le profit.
- 03 **Hacktivistes** : Acteurs non étatiques ayant des motivations politiques, qui limitent leur activisme au domaine cybernétique. Ils peuvent ou non avoir de la sympathie pour un État particulier.
- 04 **Groupes terroristes** : Acteurs non étatiques qui sont motivés par des idéologies et cherchent souvent à semer la discorde ou à diffuser des campagnes d'influence parallèlement aux attaques physiques.
- 05 **Cyber-mercenaires** : cyber-agents privés pour compte d'autrui qui sont engagés par un acteur étatique ou non étatique pour une opération spécifique ou pour la vente d'une technologie spécifique.

La première guerre
hybride à grande
échelle



Engagement du secteur privé

01 Protéger le personnel en Ukraine et en Russie

02 Dons philanthropiques

03 Soutenir la migration vers le cloud

04 Partage de renseignements sur les cybermenaces

MANDIANT



SOPHOS



NOKIA



La stratégie Cyber russe

Cyber-attaques
destructrices

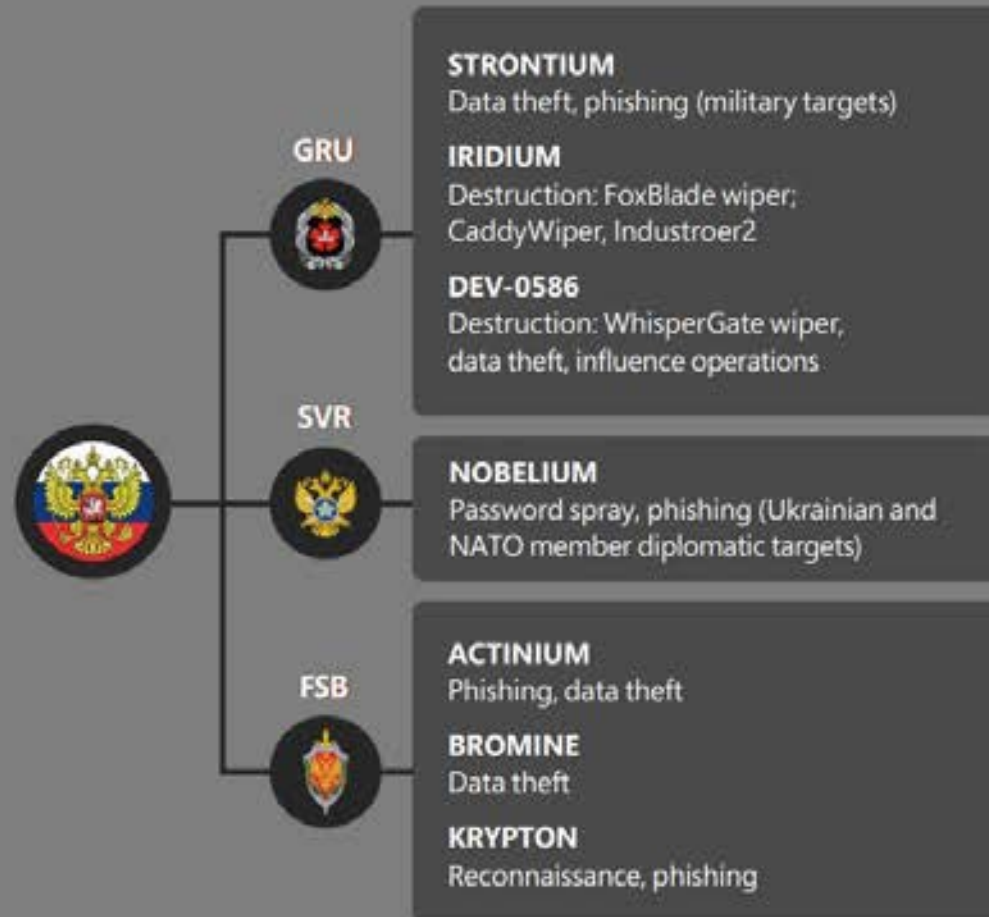
Cyber-espionnage

Cyber-influence

The background is a dark, teal-toned digital illustration. On the left, a person wearing a hoodie is shown from the side, looking down. The background is filled with faint binary code (0s and 1s) and several stylized virus or malware icons with spikes. A laptop is visible at the bottom center, and a large, glowing virus icon is prominent on the right side.

Cyber-attaques destrucrices

Entités gouvernementales russes responsables des cyber-attaques



Attaques cyber et militaires coordonnées



Attaques cyber et militaires coordonnées

Frappes militaires

October 8

Crimean Kerch Bridge damaged by truck bomb, disrupting Russian supply route. Putin calls it a "terrorist attack" and blames Ukrainian forces.

October 10

Missile strikes against residential targets in Zaporizhzhia.

October 12

Missile strikes against residential targets in Mykolaiv.

October 12

Massive drone strikes in Kyiv destroyed civilian and energy infrastructure

October 17

Missile strikes against power and water in Dnipetrovsk.

October 22

Missile strikes against critical infrastructure throughout Ukraine, including Kyiv.

October 31

Missile strikes against hydroelectric plants and energy infrastructure in Kyiv and 10 other regions, leaving about 80% of residents in Kyiv without water.

Octobre

October 3

FoxBlade wiper malware staged on critical infrastructure in Dnipetrovsk region.

October 11

Caddywiper malware staged on critical infrastructure in Mykolaiv.

October 11

Caddywiper malware staged in two critical infrastructure organizations in Kyiv region.

October 11

Seashell Blizzard deploys Prestige ransomware against 3 transportation and logistics companies, 1 Polish, 2 Ukrainian.

October 16

Destructive attack against critical infrastructure along the Dniester and Dnieper rivers.

Cibles :

- Energie
- Eau
- Habitation

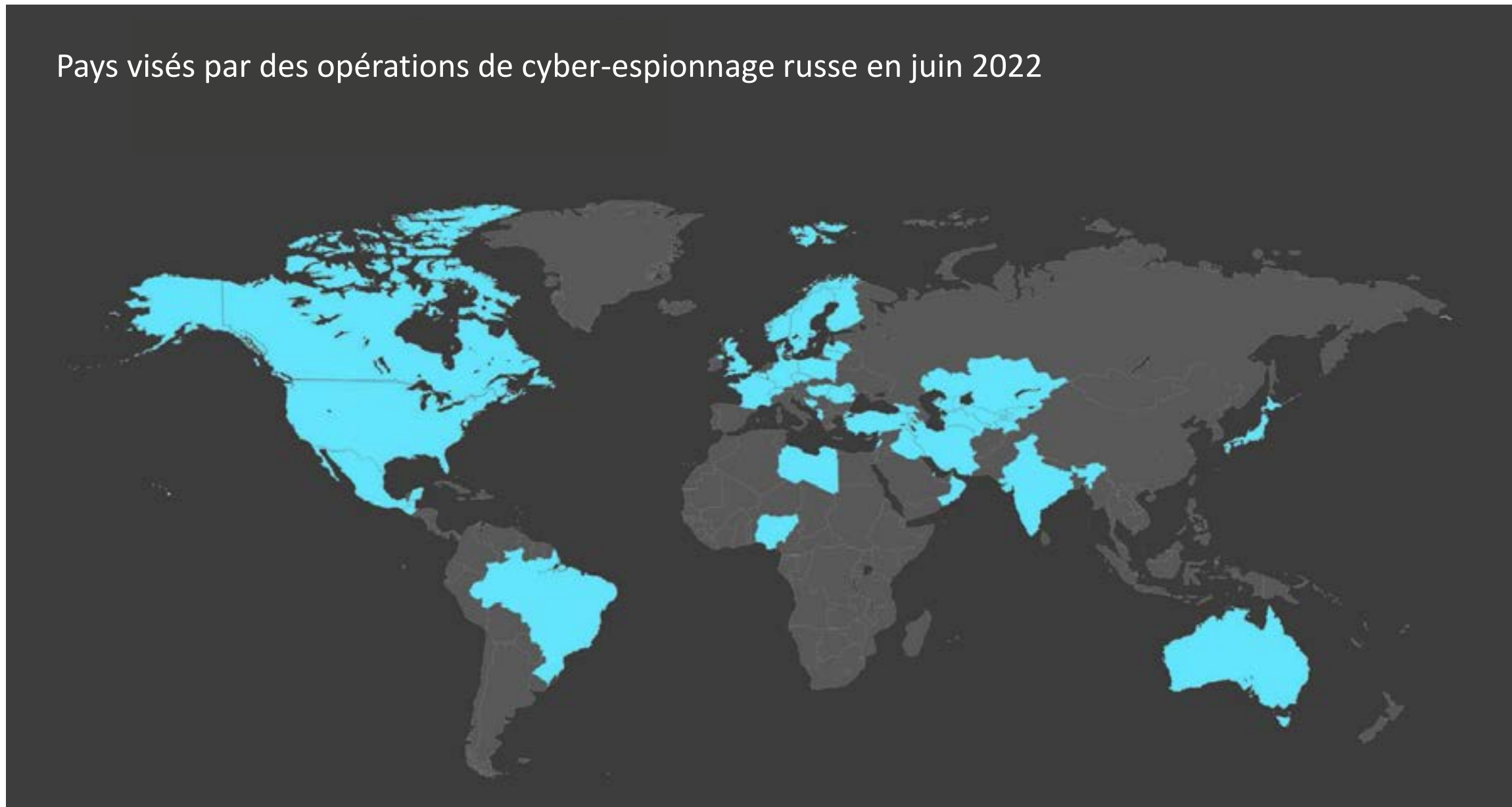
Cyber-attaques

LEGEND (!) Critical Infrastructure ⚡ Electrical Infrastructure 🚰 Water infrastructure 🚂 Transportation/Logistics 🏠 Residential area

A person wearing a black balaclava and a dark jacket is holding binoculars to their eyes. The lenses of the binoculars are filled with a pattern of white binary code (0s and 1s). The background is solid black.

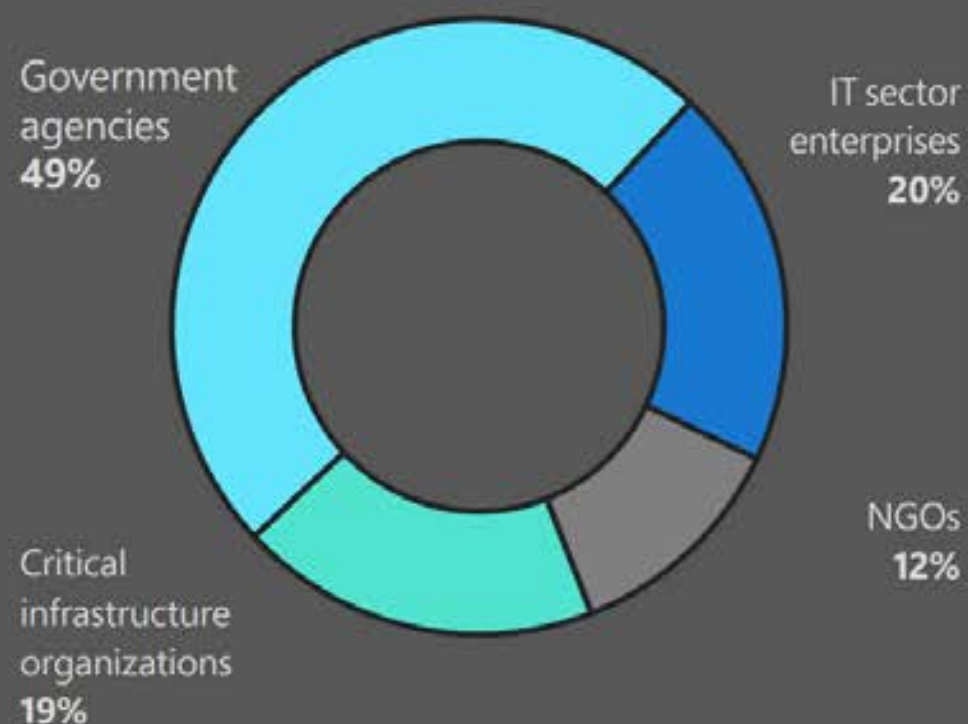
Cyber-espionnage

Pays visés par des opérations de cyber-espionnage russe en juin 2022



Pénétrations russes et cyber-espionnage à l'extérieur de l'Ukraine (Juin 2022)

Russian network intrusion targets



128 Pénétrations russes

42 Pays

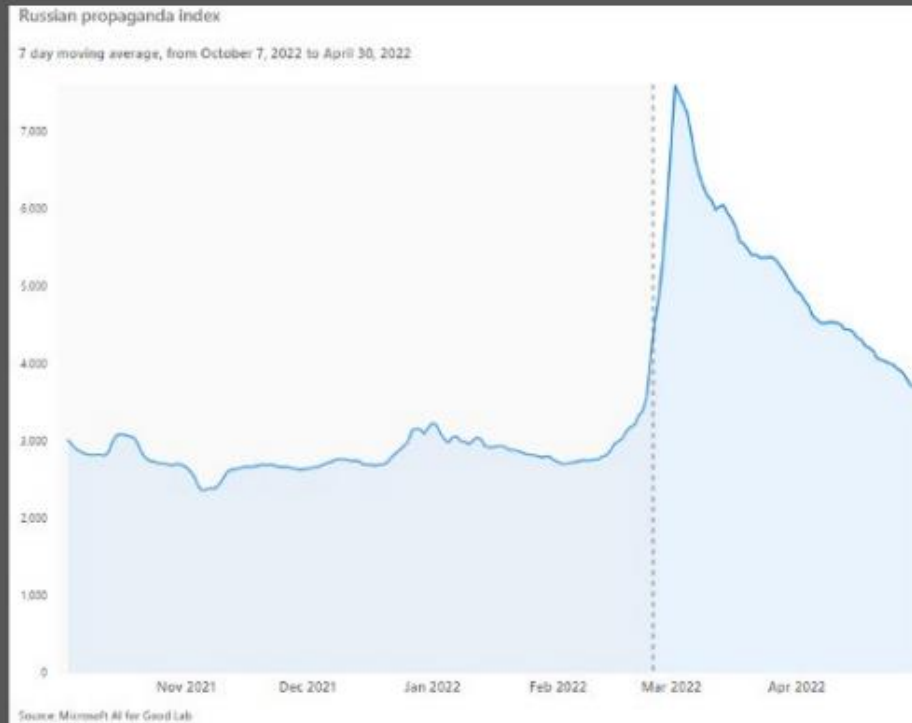
29% Taux de succès

In most instances the victims were operating on premises, not in the cloud.

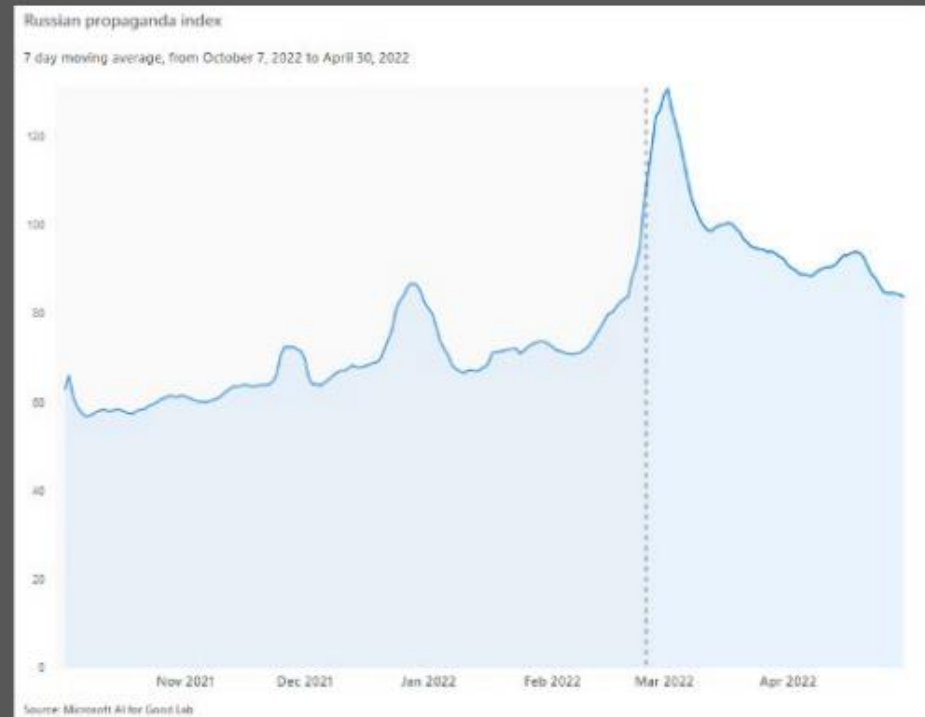
Cyber-influence

Russian Propaganda Index (RPI)

Russian propaganda consumption in Ukraine



Russian propaganda consumption in the US



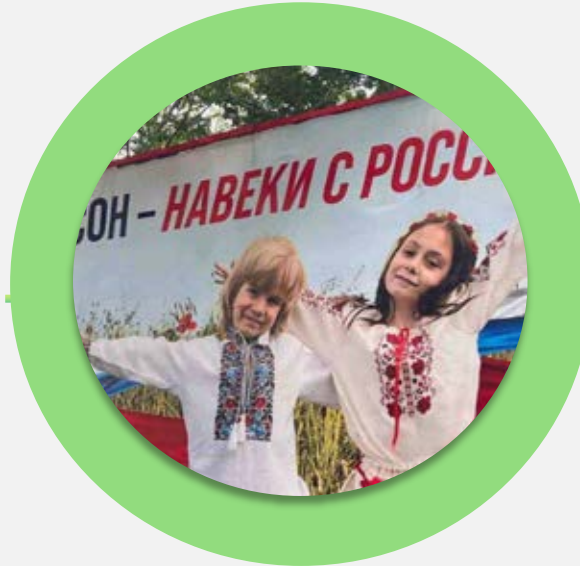
Propagande anti-Ukraine

À l'intérieur
de la Russie



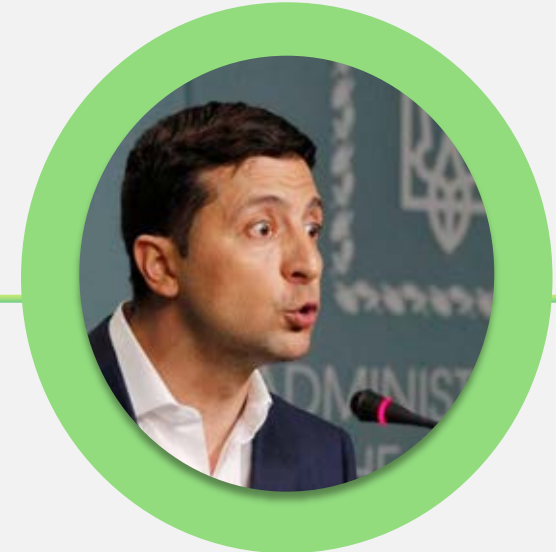
La Russie contre
le monde

À l'intérieur de
l'Ukraine



L'Ukraine est russe
pour toujours

Reste du monde



Délégitimer
l'Ukraine



IA et désinformation

Développement des deepfakes

Cibles : élections, partis politiques, candidats, dirigeants politiques

Solutions existantes





Principaux
enseignements

4 principaux enseignements

1. IA et transformation numérique
2. Interopérabilité du cloud et des données
3. Cyber-dissuasion
4. Coopération public-privé



Tendances

Cyber

- Augmentation des attaques de cyber-espionnage
- Les attaques wiper se poursuivent
- Déploiement de nouvelles variantes de ransomware

Influence indirecte

- Seashell Blizzard (IRIDIUM, Sandworm) se coordonne probablement avec le groupe d'hacktivistes pro-russe Cyber Army of Russia
- Groupes Xaknet et InfoCenter ayant des liens possibles avec les services de renseignement russes
- Utilisation de cyber-proxies

Influence

- Autres campagnes de propagande visant la diaspora ukrainienne en Europe
- Déplacement de l'influence de l'Ukraine vers l'Europe au sens large
- La Russie courtise un public réceptif dans les pays du Sud et dans les Balkans

Merci !

Quang-Minh Lepescheux
quangle@microsoft.com

Microsoft Threat Analysis Center

<https://blogs.microsoft.com/on-the-issues/tag/mtac/>

Microsoft Digital Defense Report 2024

<https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024#modal-dialog>