Éthique et threat intelligence

kaspersky

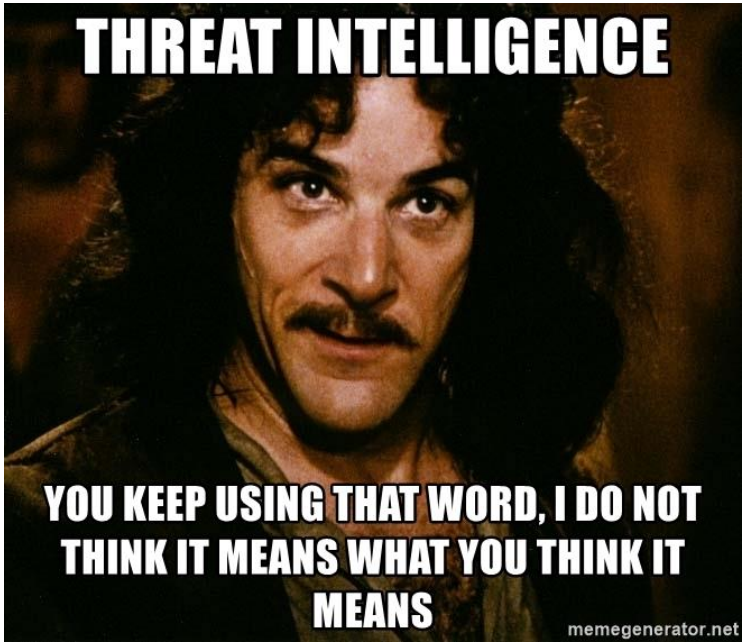
Ivan Kwiatkowski
Senior Security Researcher
Kaspersky
@JusticeRage

Résumé des épisodes précédents

Nécessité d’avoir un dialogue sur l’éthique dans la cybersécurité

Reconnaissance de ses dilemmes moraux intrinsèques

Discussion sur les incitations structurelles de manquer à l’éthique



Intelligence

Les revendeurs de TI sont des sociétés de renseignement privé

Y a-t-il du renseignement neutre ? Apolitique ?

Les entités

Chercheurs

Pouvoir sur

Sociétés

Pouvoir sur

Gouvernements

Petit pouvoir sur

Dilemme #0 : la threat intelligence est vendue aux attaquants

Les APT conduisent des attaques

Les revendeurs de threat intel écrivent des rapports

Les APT achètent les rapports

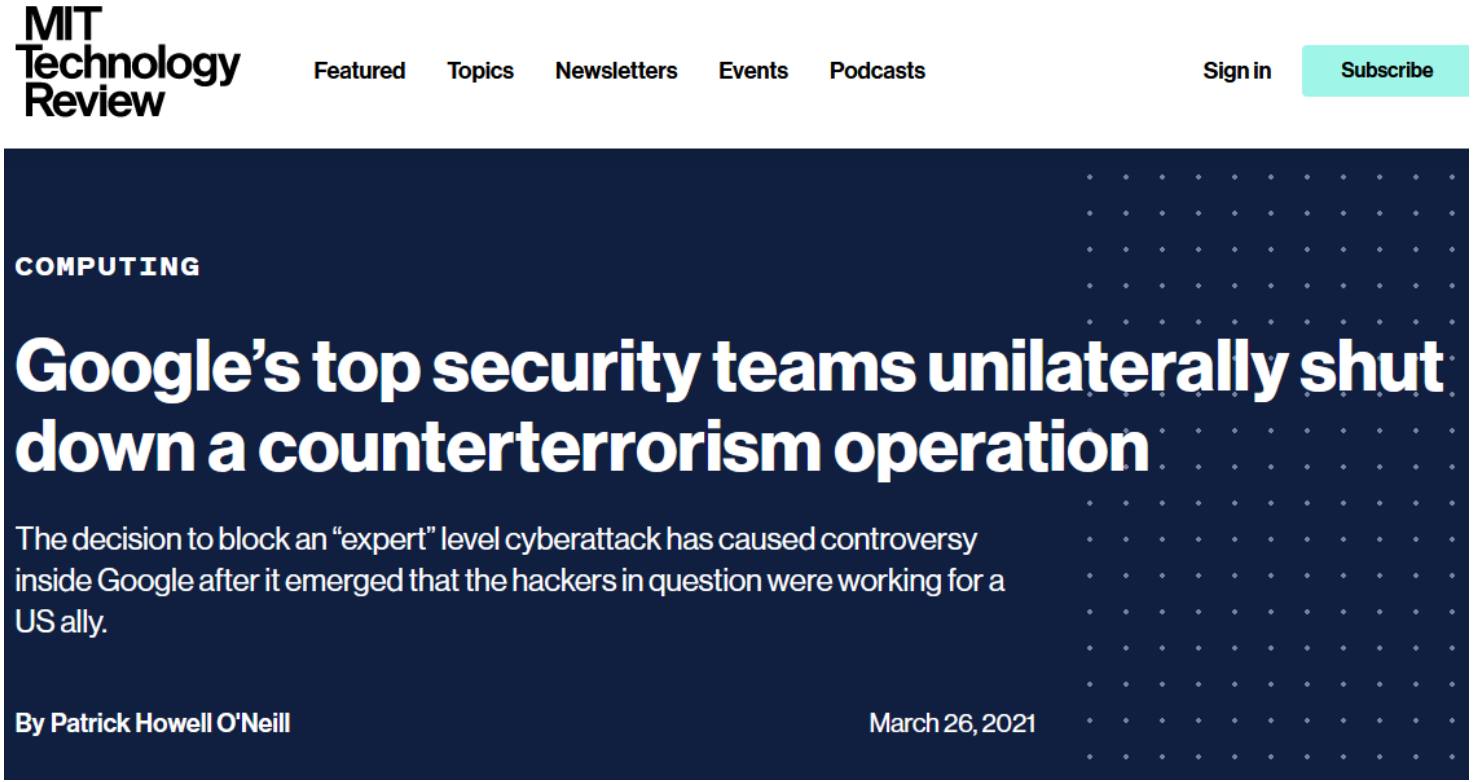
Faire face à la menace existentielle

Mise en place de stratégies d’évitement

Migration vers des publications privées

Alignement avec un bloc, de gré ou de force

Dilemme #1 : des attaques légitimes ?



MIT Technology Review

Featured Topics Newsletters Events Podcasts Sign in Subscribe

COMPUTING

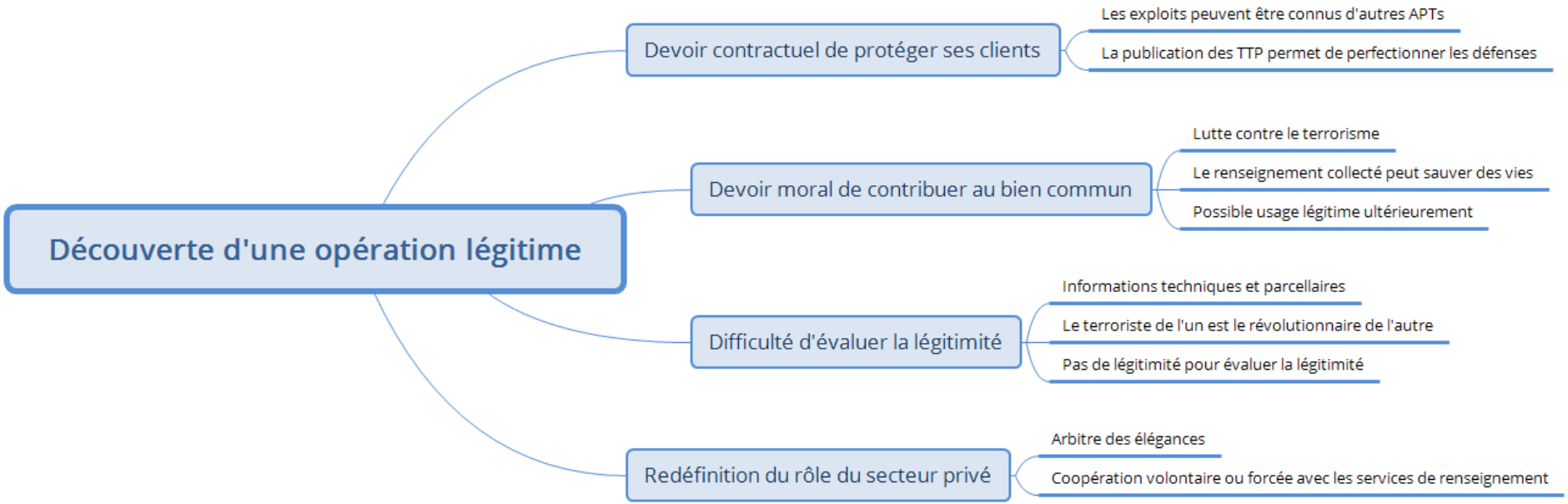
Google's top security teams unilaterally shut down a counterterrorism operation

The decision to block an "expert" level cyberattack has caused controversy inside Google after it emerged that the hackers in question were working for a US ally.

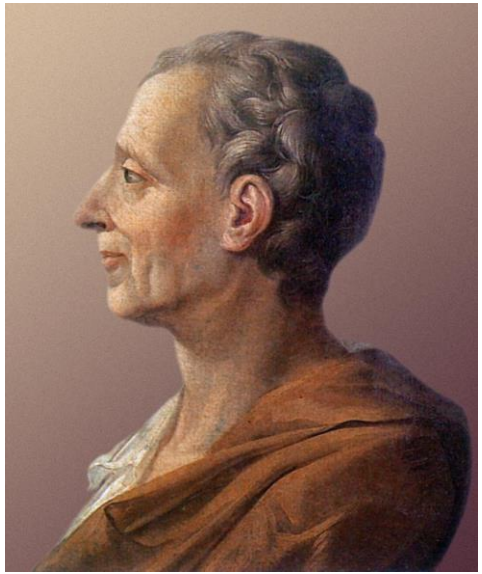
By Patrick Howell O'Neill

March 26, 2021

Dilemme #1 : des attaques légitimes ?



La threat intelligence est un (petit) contre-pouvoir



« Pour qu'on ne puisse abuser du pouvoir, il faut que par la disposition des choses le pouvoir arrête le pouvoir. »
– Montesquieu, *L'Esprit des Lois* (1748)

Dilemme #1 Reloaded : toutes les attaques sont-elles égales ?

La raison d’état est « un moyen entre ce que la conscience permet et les affaires exigent. »
– Jean de Silhon (1596 - 1667)

Ca c’est Richelieu, mais de Silhon bossait pour lui

Assembling the Russian Nesting Doll: UNC2452 Merged into APT29

This conclusion matches attribution statements previously made by the U.S. Government that the SolarWinds supply chain compromise was conducted by APT29, a Russia-based espionage group assessed to be sponsored by the Russian Foreign Intelligence Service (SVR). Our evaluation is based on firsthand data gathered by [redacted] and is the result of an extensive comparison and review of UNC2452 and our detailed knowledge of APT29.

Dilemme #2 : recherches reproductibles

Replying to @JusticeRage

This is an interesting question. Let's say I can attribute an attacker to say North Korea but can't share the exact technical details of how I made that conclusion publicly, don't people still want to know? Better than silence?

3:49 AM · Apr 28, 2022 · Twitter Web App

Quel est notre rôle ?

Trusted party

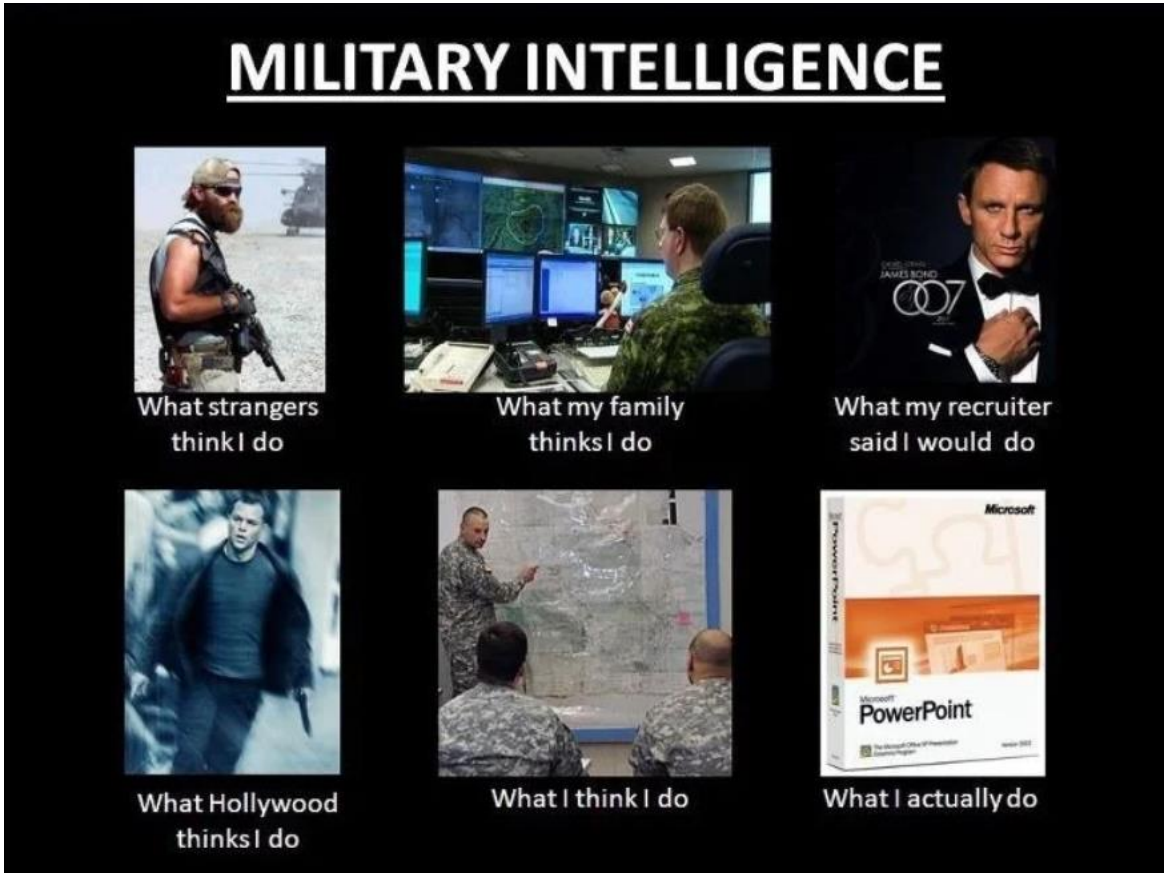
Chercheurs

Technical Evidence Indicates Operators Located in Minsk, Possible Connection to the Belarusian Government.

Sensitively sourced technical evidence indicates that the operators behind UNC1151 are likely located in Minsk, Belarus. This assessment is based on multiple sources that have linked this activity to individuals located in Belarus. In addition, separate technical evidence supports a link between the operators behind UNC1151 and the Belarusian military.

- Evidence for the location in Belarus and connection to the Belarusian Military has been directly observed by [redacted].
- These connections have been confirmed with separate sources.

Dilemme #3 : blanchiment d'informations



« La moralité d’un acte peut être évaluée en fonction de la perception qu’on en aurait s’il était commis par une société russe. »

– Rasoir de Kwiatkowski

Un coup de rasoir

Dilemme #1 : des attaques légitimes ?

Dilemme #2 : recherches reproductibles

Dilemme #3 : blanchiment d'informations

Rating - Rasoir de Kwiatkowski

Conclusion

Ivan Kwiatkowski
Senior Security Researcher
@JusticeRage