Ethics in ~~cyber~~war times

cyber

kaspersky

Ivan Kwiatkowski
Senior Security Researcher
Kaspersky
@JusticeRage

War

"Truth is the first casualty of war"

Threat intelligence is about truth

Everyone is forced to pick a side

Goran Marby
President and Chief Executive Officer, ICANN

Dear Mr. President and Chief Executive Officer,

I am sending you this letter on behalf of the People of Ukraine to ask you to address an urgent need to introduce strict sanctions against the Russian Federation in the field of DNS regulation in response to its acts of aggression towards Ukraine and its citizens.

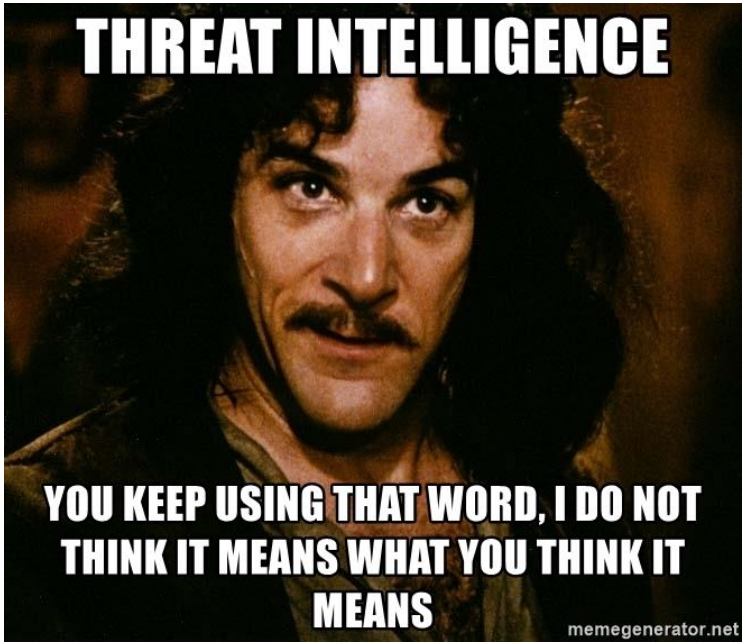
On the 24th of February 2022 the army of the Russian Federation engaged in a full-scale war against Ukraine and breached its territorial integrity, leading to casualties among both military staff and civilians.

By proceeding to a so-called "military operation" aiming at "denazifying" and "demilitarizing" Ukraine under the pretext of its own national security, the Russian Federation breached numerous provisions of International Law. Russia's invasion of Ukraine is a clear act of aggression and a manifest violation of Article 2.4 of the UN Charter, which prohibits the "use of force against the territorial integrity or political independence of any State". Also Russia is using it's weapon to target civilian infrastructure such as residential apartments, kindergartens, hospitals etc., which is prohibited by the Article 51(3) of Additional Protocol I and Article 13(3) of Additional Protocol II to the Geneva Conventions.

In a first, Israel responds to Hamas hackers with an air strike

Israel military said it bombed building housing Hamas cyber forces.

Written by **Catalin Cimpanu, Contributor** on **May 5, 2019**



Intelligence

TI resellers are intelligence brokers

Can there be neutral intelligence? Apolitical intelligence?

The structure of our ecosystem

Researchers

Power over

Companies

Power over

Governments

Tiny power over

Dilemma #0 : threat intelligence is sold to attackers

APTs conduct attacks

↓

Threat intelligence companies write reports

↓

APTs buy these reports

↑

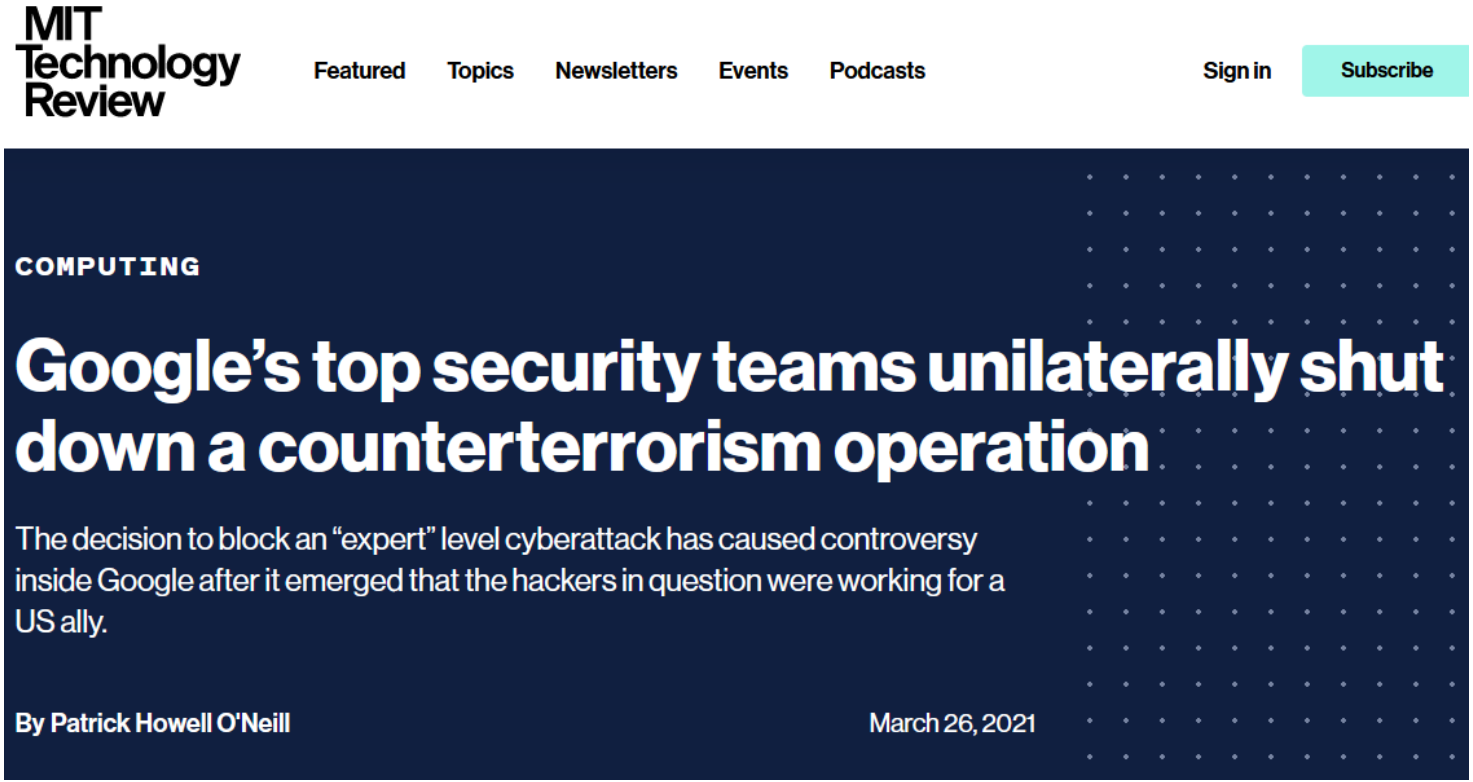
Facing the existential threat

Adopting avoidance strategies

Switch to private reports

Align with a block, whether you want it or not

Dilemma #1 : legitimate attacks?



MIT Technology Review

Featured Topics Newsletters Events Podcasts Sign in Subscribe

COMPUTING

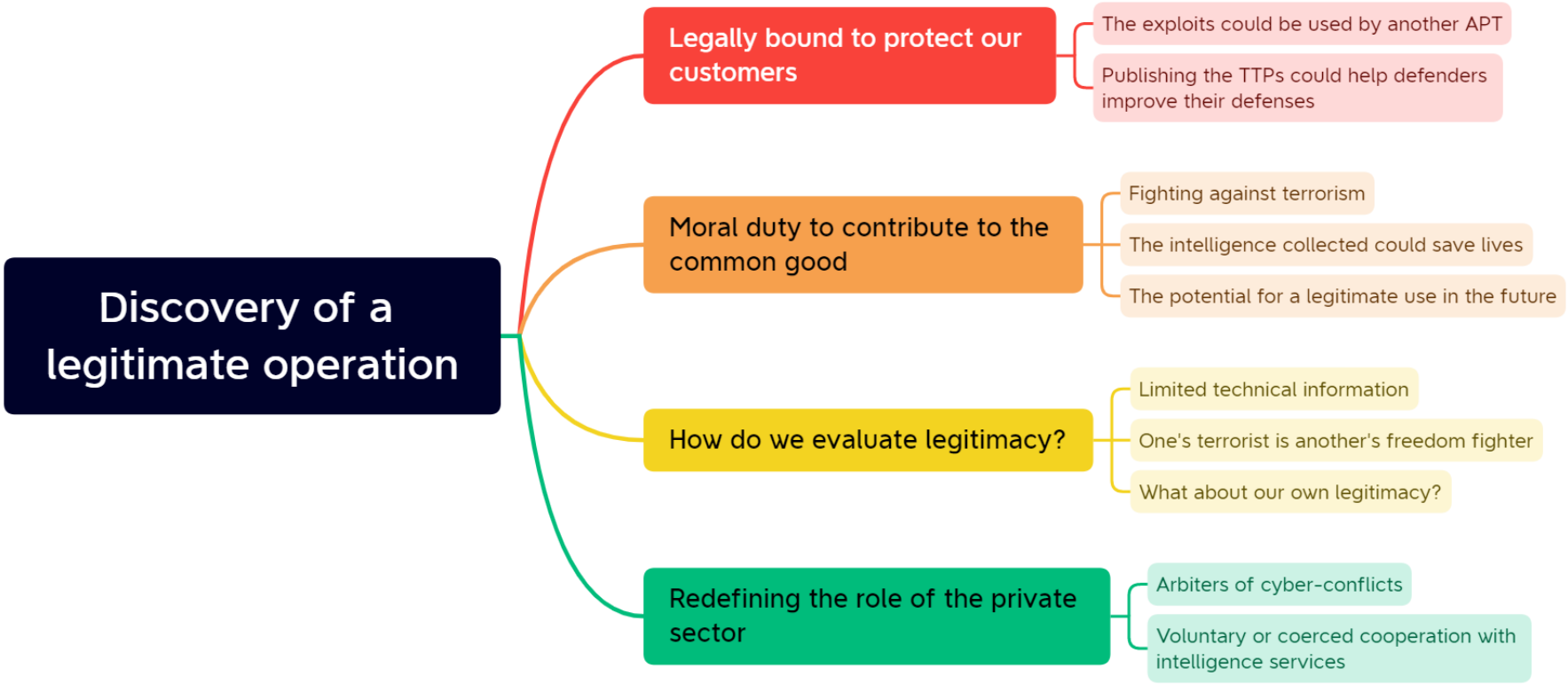
Google's top security teams unilaterally shut down a counterterrorism operation

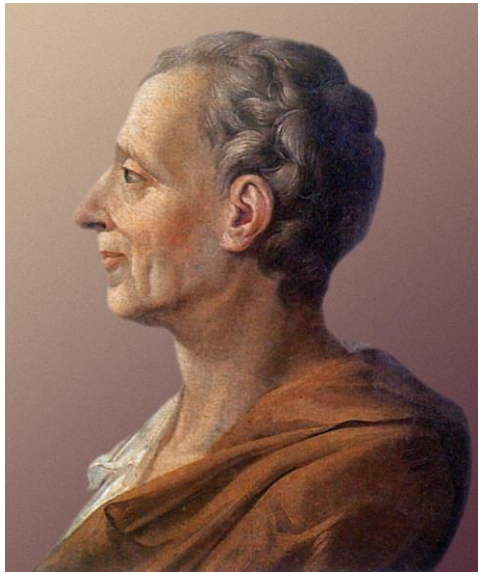
The decision to block an "expert" level cyberattack has caused controversy inside Google after it emerged that the hackers in question were working for a US ally.

By Patrick Howell O'Neill

March 26, 2021

Dilemma #1 : legitimate attacks?





“In order for power not to be abused, it is necessary that, by the disposition of things, power stops power.”
– Montesquieu, *The Spirit of the Laws* (1748)

Dilemma #1 Reloaded – Are all attackers equal?

Dilemma #1 Rereloaded – Are all cyberattacks equal?

The reason of state is “a mean between that which conscience permits and affairs require”.
– Jean de Silhon (1596 - 1667)

That’s actually Richelieu, Silhon’s boss.

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.

Dilemma #2: reproducible research

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

What is our role?

Trusted party

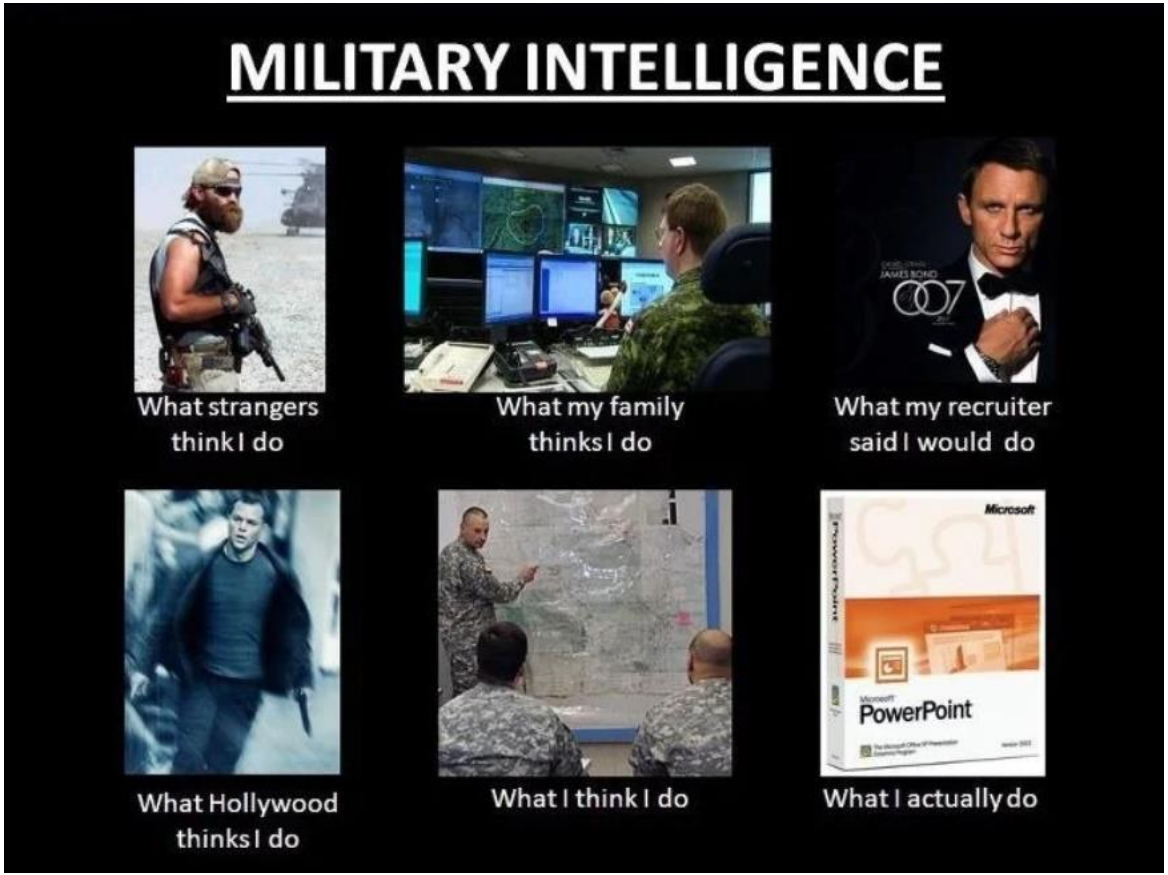
Researchers

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.

Dilemma #3: information laundering



“An act is only as moral as it would be perceived if it were committed by a Russian company”

–Kwiatkowski’s razor

The razor in action

Dilemma #1 : legitimate attacks?

Dilemma #2: reproducible research

Dilemma #3: information laundering

Kwiatkowski's razor rating

Conclusion

Ivan Kwiatkowski
Senior Security Researcher
@JusticeRage