Hostile Influence campaigns and attacks on reputation are the new normal

Itai Yonat, july 2022

While the war in Ukraine is still far from over, there is already one clear lesson to be learned. Influence operations are an integral part of the 21st century, and public opinion manipulation has never been more evident. In this new reality, the business sector has become an active participant both as an influencer and as a target. This situation forces companies to prepare in advance relevant capabilities to detect, block, and recover from hostile influence campaigns.

Modern Hostile Influence Campaigns (HICs) are the 21st incarnation of the propaganda /psychological warfare /disinformation operations of the 20th century. Similarly, HICs aim to shape perception, mobilize the crowds, influence decision-making and more. However modern HICs are easier to execute and more impactful for several reasons: Short time frame from idea to execution, high connectivity of the crowds (mainly over social media), lower technical skills needed, new technologies enabling high quality of counterfeits (e.g. deep fake).

This ease of execution has made HICs a common practice not only for countries' but to the private sector as well. Companies offer hostile influence campaigns as a service (HICaas) to anyone with enough money. This is bad news to everyone, but for the private sector it means double risk: a business risk of being attacked by an aggressive competitor, and being targeted by a country for political or military gains.

HICs typically attack through a combination of social media outlets (such as TikTok), fake websites, cyber-attacks aimed at influence (Cyfluence), paid advertisements, and more.

In the Russia-Ukraine war, for example, both sides applied aggressive HICs on companies. Russia aimed to deter companies from shutting down operations in Russia, by a combination of internal influence operations on the Russian population and cyber- attacks on companies that decided to exit Russia. Ukraine aimed at enhancing the economic sanctions on Russia and damaging its international reputation by forcing companies to leave Russia.

Companies that were both quick to identify the threat and reacted quickly were able to determine their own terms of exit, without suffering any consequences. For example, early in the war, McDonald's issued statements that they were freezing their activity in Russia. Nothing was sold, no employee was fired, the entire move was

reversible[1], yet McDonald's was cheered up. In comparison, Toyota was slower in decision-making, and lacked an understanding of the Ukraine modus operandi. As a result, Toyota was hit by both Russian cyber-attack[2] and a Ukraine influence campaign calling the company to exit the Russian market[3]. But Toyota's case is not the worst one. Renault[4] is an example of late understanding of the situation, combined with zigzag decision making which both damaged the company's reputation and forced it to fire-sell its assets in Russia.

The fight over influence and hegemony between Russia, China, and the west, is a fertile ground for an unprecedented wave of hostile influence campaigns. In addition, the HICaaS makes attacks on reputation highly affordable. As a result, in the past year, we, in Intercept 9500, doubled the number of incident response cases we had in the private sector. The bottom line is that **companies must realize that influence attacks are the new normal.**

Intercept 9500 provides companies with the most effective defense from HICs. Our services are based on a unique approach combined with cutting-edge technologies. We identify and prevent HICs before they cause actual damage, and provide Incident response and recovery services in cases where the attack has already begun.

[1] McDonalds decided to fully exit the Russian market only 2.5 months into the war.
[2] Actually it was a sub-contractor of Toyota, but the effect was as if Toyota were attacked directly.
[3] In our opinion, the Ukrainian supporters missed the fact that Toyota has already exited the Russian market because Toyota did not /mis communicate that fact over social media.
[4] The French carmaker.