

10-June-2021



9500
GROUP

Cyber based
influence campaigns





Information Operations

Cyber based influence campaigns H2 May 2021 Report

10-June-2021



Table of Contents

| | |
|--|----|
| Introduction | 3 |
| Glossary | 4 |
| Report Highlights | 6 |
| Hostile influence campaigns | 7 |
| Social media platforms | 7 |
| Facebook Threat Report: Combating Influence Operations | 7 |
| Google TAG Bulletin: Q2 2021 | 8 |
| State actors | 9 |
| Russia | 9 |
| Suspected Russian Cyber Campaign Targets German Politician | 9 |
| Surge of Pro-Kremlin Disinformation in Czech Republic | 9 |
| Pro-Kremlin Outlets Target Defender Europe 2021 and Ukraine in One Go | 10 |
| China | 10 |
| China’s US Foreign Influence Operation Budget Centered on TV and Media | 10 |
| China’s Influence in Eastern Europe Weakens | 11 |
| Troubling Trends in Chinese Cyber Campaigns | 11 |
| Private Sector Activity? | 12 |
| COVID-19 related influence activity | 13 |
| Influencers Offered Money to Vilify Vaccine | 13 |
| General Reports | 14 |
| Are the Middle East's 'electronic armies' the most dangerous of all? | 14 |
| Bogus Fact-Checking Site Amplified on Social Media | 15 |
| Case Study – Malaysian Netizens Vs Israel | 16 |
| From Disinformation to Hashtag Poisoning and Cyber Attacks | 16 |



Introduction

Cyber-based hostile influence campaigns are aimed at influencing target audiences by promoting information and/or disinformation over the internet, sometimes combined with cyber-attacks which enhance their effect (hence force Cyfluence, as opposed to cyber activities that aim to steal information, extort money, etc.) Such hostile influence campaigns and "operations" can be considered an epistemological branch of Information Operations (IO) or Information warfare.

Typically, and as customary during the last decade, the information is spread throughout various internet platforms, which are the different elements of the hostile influence campaign, and as such, connectivity and repetitiveness of content between several elements are the main core characteristics of influence campaigns.

Cyber-attacks are abundant these days. A multitude of attacks and malicious activities are launched daily against individuals, corporations, and governments, requiring constant vigil from cyber security teams and experts in both governmental and private sectors as they attempt to thwart these attacks. In tandem, **hostile influence campaigns** have also become a tool for rival nations and corporations to damage reputation or achieve various business, political or ideological goals. Much like in the cyber security arena, PR professionals and government agencies are responding to negative publicity and disinformation shared over the news and social media.

We use the term **cyber based** hostile influence campaigns, as we include in this definition also cyber-attacks aimed at influencing (such as hack and leak during election time), while we exclude of this term other types of more traditional kinds of influence such as diplomatic, economic, military etc.

During the 2nd half of May 2021 we observed, collected and analyzed endpoints of information related to **cyber based** hostile influence campaigns (including Cyfluence attacks). The following report is a summary of what we regard as the main events while informing which are based on news outlets, specialized websites and research centers. Some of the mentioned campaigns have to do with social media and news outlets solemnly, while others leverage cyber-attack capabilities.



Glossary

Information Operations - the employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making." Information Operations (IO) are actions taken to affect adversary information and information systems. IO can sometimes be considered as a part of Soft Warfare.

Hybrid Warfare - a known strategy which blends conventional warfare (kinetic), irregular warfare and cyber-warfare with other Soft Warfare parts like influencing methods, fake news dissemination, diplomacy, lawfare and foreign electoral intervention, to mention a few.

Cyber Warfare – commonly known as the use of digital attacks to cause harm and/or disrupt vital computer and information systems. There is a debate among experts regarding the definition of cyber warfare, and even if such a thing exists.

Cyfluence Attack – a cyberattack that aims to amplify or enhance an influence effort, as opposed to cyber-attack that aim to steal information, extort money, damage military capability etc.

Soft Warfare – all warfare disciplines that are not kinetic (i.e. no physical attack of sort of shooting, using explosives, poisoning etc.), such as cyber warfare, economic warfare, diplomatic warfare, legal warfare (lawfare), psychological warfare and more.

Misinformation - false, inaccurate, or misleading information that is communicated regardless with intention to deceive. Examples of misinformation are false rumors or straight-out lies or dissemination of known conspiracy theories – on purpose.

Disinformation - false or misleading information that is spread and distributed deliberately to deceive. This is a subset of misinformation. The words "misinformation" and "disinformation" have often been associated with the concept of "fake news", which some scholars define as "fabricated information that mimics news media content in form but not in organizational process or intent".

Hostile Influence Campaign (HIC) - An information operation sought to influence targeted audience for a hostile cause.



Digital Impact on Discourse (DID) – a non-hostile effort to influence discourse. Usually used in marketing articles. Here used to illustrate the opposite of the HIC.

Inauthentic Behavior – defined by Facebook as “the use of Facebook or Instagram assets (accounts, pages, groups or events), to mislead people or Facebook: about the identity, purpose or origin of the entity that they represent; about the popularity of Facebook or Instagram content or assets; about the purpose of an audience or community; about the source or origin of content; to evade enforcement under our Community Standards“. We have broadened this term to encompass all social media platforms, mutatis mutandis.

Fake users – a generic term describing all types of users which are not a legitimate social media user, i.e. are bots or operated by humans but not under their real identity, or are operated by humans under real identity but for the sole purpose of promoting an agenda that is not theirs.

Unidentified users – a generic term used to describe users on social networks that are allowed to keep their real identity undisclosed (like on Twitter, for example).

Fake website – a website designed for fraudulent or scam activity, hiding its real purpose.

Sockpuppet accounts - A sock puppet or sockpuppet is an online identity used for deception.



Report Highlights

- [Facebook](#) has published a strategic Threat Report that covers Coordinated Inauthentic Behavior activities from 2017 through 2020. The report draws several evolvment landmarks of influence campaigns over the years, while also providing researchers detailed statistics and listing of enforcements against such activities by Facebook.
- [DFRLab](#) reports that pro-Kremlin media spread different narratives claiming that Defender Europe 21, an annual NATO military exercise, will serve as a pretext for NATO troop deployment near Crimea. These stories are spread on YouTube and several media outlets.
- [Council on Foreign Relations](#) has analyzed the Chinese APT 'Evil Eye' campaign targeting Uyghur activists and journalists living abroad on various platforms. The campaign is a blend of an influence operation with cyber means.
- [Graphika](#) has identified and analyzed a network of social media accounts related to Chinese businessman Guo Wengui. The network spreads disinformation and promoted real-world harassment campaigns.
- [DW](#) covers Middle East's 'electronic armies', detailing upsurges of disinformation across social media that eventually led even to murders. Regulatory blind of social media companies in content in Arabic allows thriving of such incidents.



Hostile influence campaigns

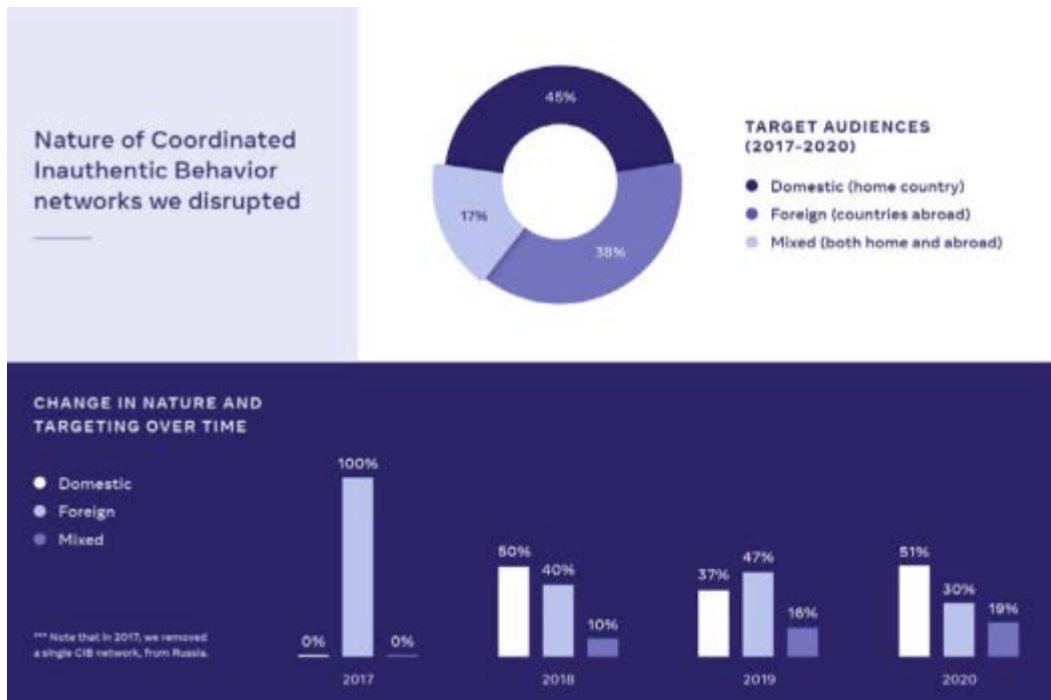
Social media platforms

Facebook Threat Report: Combating Influence Operations

[Facebook](#) has published a strategic Threat Report on Influence Operations that covers its Coordinated Inauthentic Behavior (CIB) enforcements from 2017 through 2020. The threat report draws on its existing public disclosures and its internal threat analysis to do four things: first, it defines how CIB manifests on FB platform and beyond; second, it analyzes the latest adversarial trends; third, it uses the US 2020 elections to examine how threat actors adapted in response to better detection and enforcement; and fourth, it offers mitigation strategies that seems to be effective against influence operations.

Facebook marks several threat trends:

1. A shift from “wholesale” to “retail” influence operations.
2. Blurring of the lines between authentic public debate and manipulation.
3. Perception hacking - for instance, create the false perception of widespread manipulation of electoral systems, even if there is no evidence.
4. Influence operations as a service.
5. Increased operational security and identity obfuscation.
6. Platform diversification.





Facebook also shared a comprehensive [table](#) that includes each CIB takedown it has reported since September 2017.

Google TAG Bulletin: Q2 2021

[Google](#) has published a report about coordinated influence operation campaigns terminated on its platforms in Q2 2021:

- 3 YouTube channels as part of an investigation into coordinated influence operations linked to El Salvador. This campaign uploaded content in Spanish focusing on a mayoral race in the Santa Tecla municipality.
- 43 YouTube channels as part of an investigation into coordinated influence operations linked to Albania. This campaign uploaded content in Farsi that criticized Iran's government and was supportive of the Mojahedin-e Khalq.
- 728 YouTube channels as part of an ongoing investigation into coordinated influence operations linked to China. These channels mostly uploaded spammy content in Chinese about music, entertainment, and lifestyle. A very small subset uploaded content in Chinese and English about protests in Hong Kong and criticism of the USA response to the COVID-19 pandemic.



State actors

Russia

Suspected Russian Cyber Campaign Targets German Politician

[The Guardian](#) reports on a suspected Russia-led cyber campaign targeting Germany's Green party leader Annalena Baerbock after she voiced opposition to a gas pipeline project between Russia and Europe. The campaign on social media has included fake images purporting to show her naked, in which the body depicted is that of a Russian model, and a photograph of her standing next to the billionaire financier George Soros that has been used to claim she is part of a worldwide Jewish conspiracy of which the far right believe he is the mastermind. The tabloid newspaper Bild said security experts, including NATO specialists, believed "Moscow has pressed the anti-Baerbock button".

Surge of Pro-Kremlin Disinformation in Czech Republic

[Semantic Visions](#), a Czech private intelligence firm, is reporting that there has been a dramatic surge in pro-Kremlin disinformation following the diplomatic clash between Prague and Moscow over alleged Russian intelligence-linked terrorist attacks in the Czech Republic. This follows the Czech Republic's accusation of Russia of being responsible for a deadly 2014 warehouse blast and expulsion of 18 Russian diplomats over the incident, which caused the death of two people.

According to the firm, Czech disinformation sources are pushing staunchly pro-Kremlin coverage of the GRU scandal, in line with their established history of Kremlin-aligned and anti-Western agitation. These sources frequently amplify Russian disinformation narratives and official Kremlin talking points, and support domestic political actors that advocate populist, pro-Kremlin positions, like the far-right SPD party, the Communist Party (KSČM), and the Putin-friendly Czech president, Miloš Zeman. However, despite their pro-Kremlin orientation, the majority of the sites have no evident links to the Russian state, and do not produce content in coordination with Russian media. Their primary drivers are profit (i.e., ad revenues) and social influence.

The Russian disinformation response to the disclosure of the GRU's role in Vrbětice was immediate and has followed the same blueprint as in other cases where Russia's activity has been exposed. Russian officials and pro-government media deny any Russian involvement in the explosion and dismiss the Czech government's response as an attempt to score points in Washington's "war of sanctions".

The [DFRLab](#) analysis of pro-Kremlin media outlets showed that these outlets spread four main false narratives about the arms depot blast and the ensuing investigation.



Pro-Kremlin Outlets Target Defender Europe 2021 and Ukraine in One Go

[DFRLab](#) reports that amid the tense situation at the Russian-Ukrainian border, pro-Kremlin media spread stories claiming that Defender Europe 21, an annual NATO military exercise, will serve as a pretext for NATO troop deployment near Crimea.

According to these various stories and social media posts, Defender Europe 21 will be used as an excuse to amass NATO troops on the border with Crimea and afford NATO allies the opportunity to practice with Ukraine for a war with Russia. To send this message, three overarching sub-narratives were used. One claimed that Kyiv and NATO are preparing to take back Crimea; a second claimed that the Kremlin is extending its warning signs not to “wake up the Russian bear”; and a third called Ukraine a free training ground for NATO troops. These narratives serve as a tool for domestic fearmongering targeting two of Russia’s enemies simultaneously — Ukraine and NATO.

The stories were published on YouTube channels, RIA.ru, IZ.ru, lenta.ru and more. Most of the stories received moderate engagement online. The original stories published in the larger pro-Kremlin media outlets garnered thousands of engagements, while the smaller outlets managed to receive engagement in the dozens, sometimes hundreds.

China

China’s US Foreign Influence Operation Budget Centered on TV and Media

[VOA News](#) reports that China's big-budget foreign influence operation in the USA is heavily tilted toward television broadcasting and other media activities, according to newly disclosed Foreign Agents Registration Act (FARA) filings. The country's state-owned China Global Television Network (CGTN) spent more than \$50 million on its USA operations last year, accounting for nearly 80% of total Chinese spending on influencing U.S. public opinion and policy. In total, China spent nearly \$64 million on propaganda and lobbying in the United States last year.

Counting its television broadcasting operations, China spent more money on influencing U.S. public opinion than any other country. Qatar came in second, reporting nearly \$50 million, and Russia ranked No. 3, with \$42 million in spending.

Of the \$64 million spent by China on influence operations, nearly \$10 million came from nongovernmental entities. Telecom conglomerate Huawei Technologies was the top nongovernmental spender, reporting nearly \$3.5 million in lobbying expenditure.



China's Influence in Eastern Europe Weakens

[International Politics and Society](#) is reporting on China's weakening influence in Eastern Europe, arguing that with Sino-American tensions rising, Chinese activities in the region are being increasingly restricted. According to an International Politics and Society report, the activities of Chinese investors are increasingly being restricted in Central and Eastern Europe countries. For instance, in May 2020, Romania cancelled a deal with China to build two new nuclear reactors. Following Washington's lead, Poland, the Czech Republic, Romania, and Estonia all plan to restrict Huawei's operations in their countries. The region is also voicing stronger criticism of China's policy on national minorities, Hong Kong and human rights in general. Ukraine's decision regarding the nationalization of the Motor Sich Joint Stock Company can be considered in keeping with the overall regional trend. The European market is of great interest to China, and the countries of Central Asia and Eastern Europe are important as routes and corridors. But in the changing geopolitical realities, the price of political issues is dramatically increasing — including the very issues which China is doing its best not to raise.

Troubling Trends in Chinese Cyber Campaigns

[Council on Foreign Relations](#) points out several trends that can be concluded based on the latest campaign by the Chinese APT 'Evil Eye' on Facebook and other websites targeting Uyghur activists and journalists living abroad with malware. Evil Eye's campaign was clearly motivated by a political goal that China frequently uses a blend of information operations and cyber means to accomplish: the disruption of dissidents, especially those who raise awareness of China's human rights violations against its ethnic minorities.

Social media companies should be cognizant of three trends from this incident. **First**, Facebook was just one part in a larger APT campaign. **Second**, the ease of opening new accounts on Facebook and other social media outlets remains a critical vulnerability with the fake user accounts easily weaponized. Evil Eye used social engineering to access targeted individuals and have them install and pass on exploits for prepared malware. The fake accounts were also used to conduct psychological damage and identity theft. **Third**, social media companies have an ever-increasing need for information sharing with relevant cybersecurity partners; in this incident, Facebook should be commended for collaborating with FireEye.



Private Sector Activity?

[Graphika](#) released a report focused on Guo Wengui's Online 'Whistleblower Movement'. Chinese businessman Guo Wengui is at the center of a vast network of interrelated media entities which have disseminated online disinformation and promoted real-world harassment campaigns. Graphika has identified thousands of mostly-authentic social media accounts associated with this network which are active across platforms. In the last year, this network has promoted harassment campaigns against anti-CCP Chinese dissidents, activists, and other perceived enemies in six countries. These campaigns have been linked to multiple violent incidents.

Graphika has noted multiple instances of what appear to be coordinated authentic behavior, with real supporters posting with the singular purpose of amplifying Guo-related content. The network acts as a prolific producer and amplifier of mis- and disinformation, including claims of voter fraud in the USA, false information about Covid-19, and QAnon narratives. Accounts in the network have used centrally-coordinated tactics to evade enforcement actions by social media platforms.



COVID-19 related influence activity

Influencers Offered Money to Vilify Vaccine

According to [Info Security](#), a public relations agency in the UK has allegedly offered social media influencers money to portray the Covid-19 vaccine created by Pfizer-BioNTech as highly dangerous. Fazze allegedly offered to pay French and German bloggers, influencers and YouTubers to tell their followers that the vaccine had caused hundreds of deaths. It is alleged that Fazze contacted several French health and science YouTubers last week, asking them to share the false claim that the Pfizer vaccine is three times more deadly than the COVID-19 vaccine developed by AstraZeneca. It is alleged that Fazze told the influencers to tell their followers that the dangers of the Pfizer vaccine were being ignored by mainstream media and to question the wisdom of governments who purchased it.

The full investigation is available on [The Guardian](#) and on [Medium](#).



General Reports

Are the Middle East's 'electronic armies' the most dangerous of all?

[DW](#) covers the Middle East's 'electronic armies', groups of people assume false identities in order to participate in internet forums and social media to send — or suppress — a specific message. However, these messages might lead to a murder in the Middle East. For instance, Iraqi activist Riham Yaqoob was assassinated in August 2020, following videos that purported to show her leading protests were actually not of her and a widely shared conspiracy theory that accused a group of young locals "of being agents in a US plot to orchestrate violent protests in Basra."

In Iraq, local activists say the largest and most active electronic armies are those working on behalf of the country's paramilitary groups, known as the Popular Mobilization Forces, or PMF. Many of these pledge loyalty to Iran because Iran's leadership provides them with financial, military and logistical support.

Perhaps the highest-profile example of such online harassment relates to the case of Saudi journalist and dissident Jamal Khashoggi, who was murdered inside the Saudi Embassy in Turkey in 2018. An analysis of threats made against him on Arabic-language social media in 2020 indicated a pattern of coordinated intimidation and abuse, much of which could be traced back to Saudi Arabia, investigators from the Soufan Group, a US-based security consultancy, have argued.

In its 2020 list of digital predators, Reporters without Borders pointed out that the Algerian administration has paid online "trolls" to discredit journalists reporting on anti-government protests and that Sudanese intelligence services were also thought to be behind similar disinformation campaigns. Some cases may be clear, but it is often difficult to know exactly who is paying or controlling the electronic armies.

The Middle East's problem with electronic armies may also have to do with language. In Arabic, disinformation seems to thrive. Part of the reason for this is a regulatory blind spot when it comes to the social media companies, who are less inclined to take action against accounts who aren't speaking English, or that aren't impacting directly on US interests. When they are being encouraged by politicians or governments, and then also find that social media platforms are letting them loose without any genuine or swift action to rein them in, electronic armies thrive in the absence of the rule of law.



Bogus Fact-Checking Site Amplified on Social Media

[DFRLab](#) reports that “Press Media”, a Canada-based communications firm, created India Vs. Disinformation, a website presenting itself as an Indian media outlet and fact-checking site. It then used the website to promote narratives supporting the Indian government. Articles from the website, written to influence public perception in favor of the Modi government and against its opponents, were amplified by verified social media accounts of dozens of Indian embassies and consulates on Twitter and Facebook.

The firm used India Vs. Disinformation to amplify and aggregate pro-government content while simultaneously publishing “fact checks” targeting the government’s political opponents, as well as local and international media outlets for their critical coverage of the current administration. While the communications firm never disguised the fact that it ran the website, its use of fact-checking and disinformation-monitoring rhetorical tropes gives casual readers the impression that it is an independent news source.

Press Monitor told the DFRLab that it created the website as a means of gaining the favor of and receiving further commercial contracts from the Indian government.



Case Study – Malaysian Netizens Vs. Israel

From Disinformation to Hashtag Poisoning and Cyber Attacks

While the fighting between Gaza and Israel resumed on May 10, 2021, the anti-Israel and antisemitism discourse increased on social media. In the following days, false and unverified information about Israel’s intentions to target Hamas’ operatives in different countries around the world including Malaysia has been identified.

May 15th, 2021 – ‘Israel Sasar’ Malaysia

A pro-Palestine authentic FaceBook user posted a picture of an old front page of a Malaysian newspaper from July 2014 (mentioning a previous round of fighting in Gaza). The post went viral with around 7,000 shares, and was calling to prepare for the arrival of the “Zionist soldiers”.



On the same day, an unverified and suspicious website in Greek named Warnews 24/7, with social media accounts created only on November 2020, claimed that according to information broadcasted in the Israeli TV, the Israeli leadership has ordered the

country’s secret services to assassinate top Hamas officials inside and outside the country, mentioning Iran, Turkey, Qatar, and Malaysia.

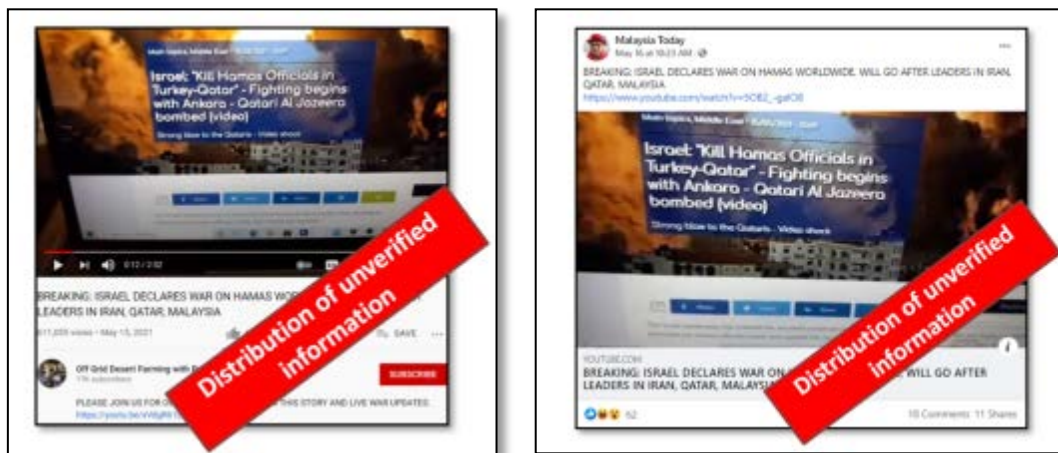
Later that day, Jonathan Schanzer from the FDD (The Foundation for Defense of Democracies) tweeted similar information to the fake article, also mentioning Malaysia. Following his tweet, Schanzer received anti-Israel and pro-Palestine replies from users, many of them from Malaysia.





May 16th, 2021 – the American YouTube channel

An American YouTube channel named “Off Grid Desert Farming with Paul & Adrienne” that usually publishes unreliable information regarding worldwide military conflicts, published a video in which the speaker is talking about the article from the Greek website. The video received a significant number of more than 600k views, and has been shared many times in different social media platforms, mainly on Malaysian accounts and pages, with “Malaysia Today” as one of the first pages to share it on Facebook. The post claims that Israel has announced an attack on Hamas-related targets around the world, mentioning Iran, Qatar, and Malaysia.



The Next Step – Hashtag Poisoning¹

About that time, when disinformation content about Israel was circulating in Malaysia, the social media hate speech towards Israel reached a peak in the country when hashtag poisoning was carried out alongside cyber-attacks on Israeli websites. The idea to poison the hashtag #VisitIsrael (mainly used by Israel’s ministry of tourism) was first posted on Facebook by an authentic Malaysian user with no significant reach. Nevertheless, the post went viral with 3,100 reactions, nearly 900 comments, and nearly 10,000 shares. The original post was written in Malay, shown below is a translation to English:

¹ Hashtag poisoning definition from Facebook’s February 2021 CBI report: “...‘hashtag poisoning’ and ‘location poisoning’... refers to posting large volumes of irrelevant or critical content with particular hashtags and location tags to drown out relevant information and redirect the conversation”.



2d · 🌐

Do you think you post about Israeli terrorism using the hashtag #israHell and #ihateisrael, Israeli and Israeli lovers will read the post? Big mistake

Among the good hashtags about Israel for you flood with Israeli terrorism related post is Israeli hashtag positivity related eg #iloveisrael #ImWithIsrael and #SupportIsrael. Who will read this hashtag? Israeli citizens and Israeli lovers. Use the hashtag #visitisrael or #israeltourism or #israeltrip for example can bring down the Israeli tourism industry because when people are interested in traveling there search " Visit Israel ", it is flooded with Israeli terrorism photos. Other hashtags that are suitable for example #israelfood, #israelfashion, #israeligirls, #israelnews etc. You need to be more creative in choosing hashtags and this needs some research. Find great hashtags popular regarding Israel to flood with their terrorism article. Use Twitter, FB, Instagram channels etc. **Imagine the hashtag #supportisrael trending on Twitter and when the people of the world click that link, the one exposed is Israeli terrorism. Message delivered to target audience.**

PS: You'll be cured by Israelis because this hashtag is so valuable to them, but the revenge experience is priceless.

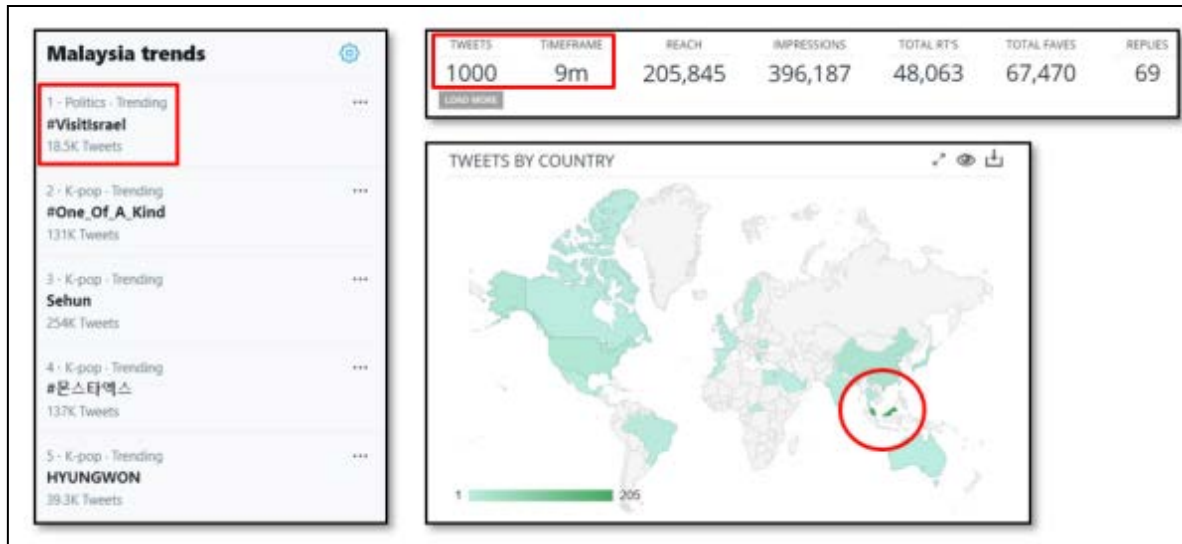
⚙️ · See original · Rate this translation

See below a comparison of 4 hashtags that have been in use in Malaysia against Israel on May 17th -18th. The significant increase in the number of #VisitIsrael mentions on May 18th can be seen clearly in the graph, with both authentic and inauthentic Malaysian users being almost exclusively responsible for its spread.

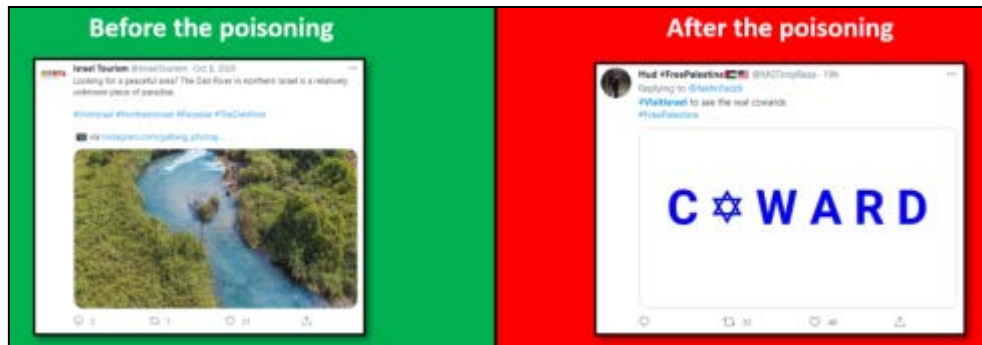




The hashtag trended to the extent of reaching 1st place in the list of “Malaysia trends”.






See the difference in the use of the hashtag before and after the poisoning:




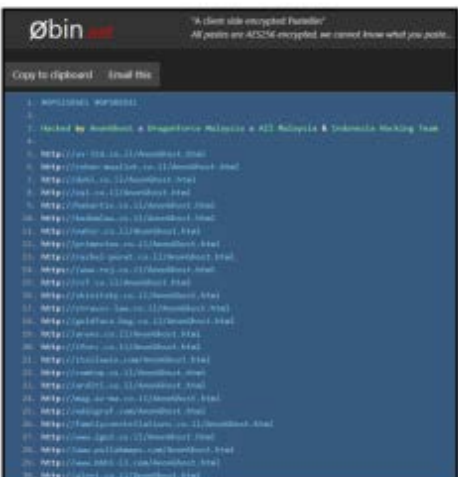


Additional campaign features were identified as well:

| Twitter | Facebook | Instagram |
|--|--|--|
| <p>Many Malaysian suspicious users using the phrase "Koyak Israel" (translates as "Israel is Lousy" or "torn off Israel") in their usernames</p>  | <p>Hashtags and new suspicious users</p>  | <p>Users creating templates which were spread on Facebook as well</p>  |

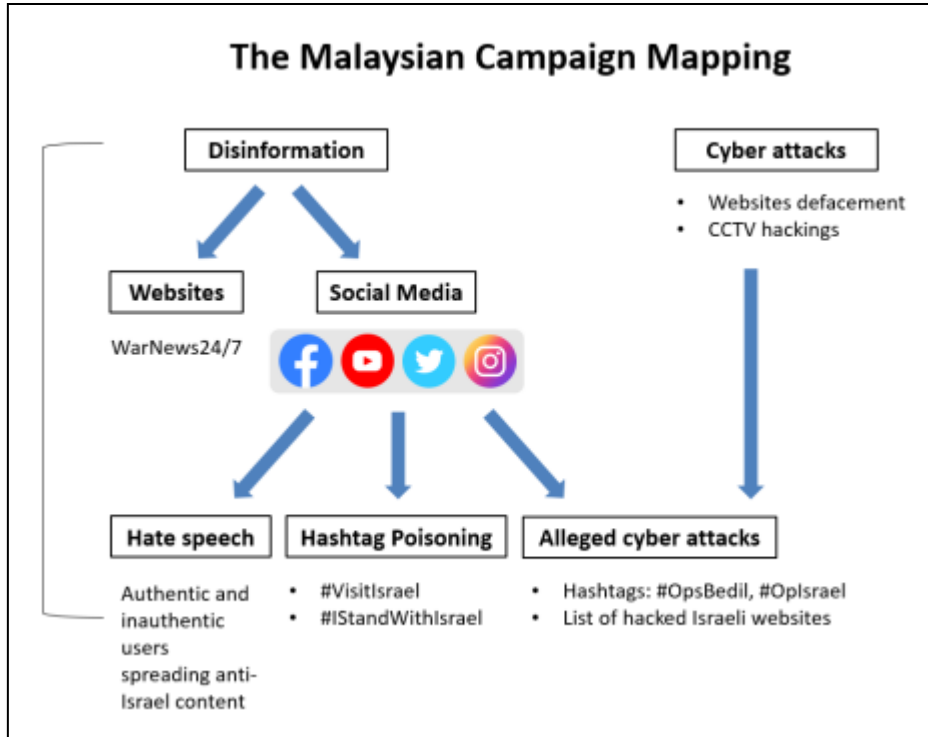
Cyber attacks

A cyber campaign (#OpsBedil), mainly driven by DragonForce Malaysia hacking group has been detected and was advertised on Twitter as well. In addition to #OpsBedil, there were multiple tweets about OpIsrael (#OpIsrael), which is an annual coordinated cyber-attack launched by Anonymous in 2013. The Malaysian hacking groups and users claimed to successfully operate cyber-attacks and CCTV hackings in Israel.

| | |
|---|--|
|  |  |
|---|--|



A summary of the Malaysian campaign against Israel:





Disclaimer and Limitation of Liability

Copyright and License of Product

This report (the "Product") is the property of Intercept 9500 Ltd. ("Intercept") and is protected by Israel and international copyright law and conventions. User acknowledges that access to the Product is limited to the License terms set forth herein and any expansion must be in writing. The granting of the License to access and use the Product is conditioned on User's agreement not to disclose, copy, disseminate, redistribute, or publish the Product, or any portion of or excerpts thereof to any other party.

User shall have the right to use the Product solely for its own internal information purposes. Reproduction of the Product in any form or by any means is forbidden without Intercept's written permission.

User agrees to maintain all copyright, trademark and other notices contained in the Product. User agrees that it shall not use Intercept's name or any excerpts from the Product in the promotion of its products or services.

Disclaimer of Warranties

Intercept does not make any warranties, express or implied, including, without limitation, those of merchantability and fitness for a particular purpose, with respect to the Product. Although Intercept takes reasonable steps to screen the Product for infection by viruses, worms, Trojan horses or other code manifesting contaminating or destructive properties before making the Product available, Intercept cannot guarantee that the Product will be free of infection. Intercept does not make any warranties, express or implied, of whatsoever nature with respect to the Product or to the accuracy of any conclusions set out in the Product.

Accuracy of Information

The information contained in the Product has been obtained from sources believed to be reliable and are provided by Intercept on an "as is" basis. To the full extent permissible by applicable law, Intercept disclaims all warranties, express or implied, of whatsoever nature including, but not limited to any warranties as to the accuracy, completeness, quality or adequacy of any such information, any conclusions set out in the Product and any translations in the Product. The reader assumes sole responsibility for the selection of the Product to achieve its intended results. The opinions expressed in the Product are subject to change at any time without notice.

Limitation of Liability

To the extent permitted under applicable law, in no event will Intercept be liable in any way for:

1. damages of any kind, including without limitation, direct, incidental punitive, special or consequential damages (including, but not limited to, damages for lost profits, business interruption and loss of programs or information) arising out of the use of or inability to use the Product, or any information provided in the Product, regardless of whether or not Intercept has been advised of the possibility of such damages;
2. Any claim attributable to errors, omissions or other inaccuracies in the Product or interpretations thereof;
3. actions taken or not taken by any person or entity as a result of the review by such person or entity of the Product or information contained therein or as a result of the interpretation of the Product or information contained therein by such person or entity.

Indemnification

User agrees to indemnify, defend and hold harmless Intercept, its affiliates, licensors, and their respective officers, directors, employees and agents from and against all losses, expenses, damages and costs, including reasonable attorneys' fees, arising out of the use of the Product by User or User's account.

Third Party Rights

The provisions regarding Disclaimer of Warranty, Limitation of Liability and Indemnification are for the benefit of Intercept, and its licensors, employees and agents. Each shall have the right to assert and enforce those provisions against a User.

General Provisions

Any provision in any memorandum received by Intercept in connection with the Product which is inconsistent with, or adds to, the provisions of this Agreement is void. Neither the parties' course of conduct or trade practice will modify the terms of this Agreement. If any provision of this Agreement is determined by a court of competent jurisdiction to be invalid, all other terms and conditions shall remain in full force and effect.

Governing Law

This Agreement and the resolution of any dispute arising hereunder shall all be governed and construed in accordance with the laws of the state of Israel, without regard to its conflicts of law principles. User consents to the jurisdiction of the courts of Tel-Aviv.

