ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE INFORMATION DOMAIN

Issue 05/24 (May)

Information Laundering

INTRODUCTION

1. Information laundering refers to false or deceitful information that are surfaced from unverified sources through more reliable and credible outlets until it becomes mainstream. Through information laundering, such false information loses their “illegitimate origins” and become very difficult to attribute or trace its original source.

INTENTS AND MOTIVATIONS

2. Information laundering almost always starts from malicious actors, conspiracy theorists or as part of information operations. Such information also incubate within closed or niche communities over a given period of time. Eventually, these narratives surface through moderate social networks, political commentators and internet algorithms, where they then inter-mix with mainstream narratives and gain traction in traditional media sources.

3. Unlike disinformation, laundered information generally has a greater degree of traction before it is identified by the authorities, and often remains rooted within its support base long after the debunking efforts have taken place. An example was how the far-right conspiracy group QAnon[1] hijacked “Save the Children” rallies. QAnon attempted to use the non-government organisation’s work with at-risk children to gain traction in conspiracy theories of elite-funded child sex trafficking rings. This came in the form of right-wing extremists joining “Save the Children” rallies and using their social media to spread these stories.

HOW INFORMATION IS LAUNDERED

Use of Closed Groups as a Start Point

4. Information laundering efforts generally start from isolated, closed groups, which are difficult for authorities to access and monitor. These groups provide a conducive environment for the formation of "echo chambers" where such news is repeated and used to achieve a certain desired narrative or consensus by its members. This is especially the case for false documents and other materials, as these are rarely fact-checked before they are widely circulated. Hostile Information Campaign (HIC) perpetrators, foreign or domestic, can make use of these groups to disseminate false narratives.

5. For example, a press release by the Luhansk People's Republic in July 2020 falsely asserted that a US COVID-19 vaccine trial had killed five out of fifteen Ukrainian volunteers. The Australian Strategic Policy Institute (ASPI) tracked how these reports were laundered through Russian-language media and English-language conspiracy social media platforms. Traction for this report was high and reached as far as Australia, Canada, Germany, Italy and the Philippines before Facebook began removing these posts. Figure 1 provides

a selection of posts on how the story originated from Russian-language media to conspiracy groups on Facebook and finally to mainstream twitter.

Figure 1. Spread of Luhansk false news release across different information spaces

Source: ASPI International Cyber Policy Centre: COVID-19 Disinformation and Social Media Manipulation

Use of Misappropriation/Misleading Language

6. Instead of outright falsehood, information launderers typically use, or put emphasis on factual data, contexts or incorporate unrelated information to mislead audiences. They post summaries/comments of articles from mainstream media with misleading and disingenuous language, in order to provide credibility to the laundered content. In Germany, pro-Russian and Russian official media repeatedly amplified messaging from German opposition figures, using them to provide credibility to laundered content. This was likely done to promote policies friendly to Russia, as well as to support political groups within Europe which had pro-Russian

sympathies. For example, Russian-backed sources began pushing narratives around the lifting of EU sanctions arising from Russia's annexation of the Crimea in 2014. As part of this, pro-Kremlin media outlet *Izvestia* misappropriated several opposition politicians' speeches supporting the lift and portrayed it as a German policy. Over the next few days, articles from similar Russian and Russia-linked outlets[2] repeated, summarised or reposted the same article from *Izvestia* and each other.

Coordination Across a Network of Actors

7. Information laundering efforts are often coordinated across several accounts and platforms to quickly reinforce key narratives, using similar language and phrases. This coordinated effort makes it difficult to push out a quick response. On 13 June 2022, *Bloomberg* released an article on the Ukrainian bid for European Union membership titled "Europe is a vast idea. How does Ukraine fit in?". Within a day, a network of thirteen Russian and Baltic online sites propagated links to the article, claiming that it prophesised "collapse" of the EU if Ukraine were to join the EU. This was in line with previous Russian attempts to drive a wedge between European populations and Ukraine. In the example in Figure 2, *Baltnews* (Russian-language Baltic alternative

media) captioned it with “If Ukraine, Georgia and Albania are accepted into the EU, the organisation will collapse”.

Figure 2. Example of misuse of Bloomberg Article in Baltnews Telegram Group

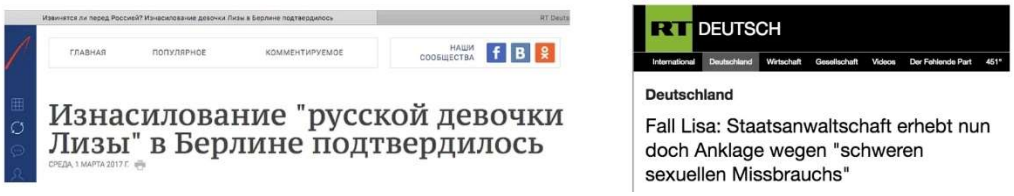
Source: NATO Strategic Communications Centre of Excellence “Information Laundering in the Nordic-Baltic Region”

IMPACT

8. Information laundering can erode the public’s confidence and trust in governments, influence public opinions and political decisions. The cover of reliability afforded by laundered information may cause individuals to be taken in by such disinformation. In 2016, a Russian-German girl was reportedly kidnapped and raped in Berlin by people of foreign “Arab” origin. This story was propagated in mainstream media and by Russian officials, resulting in ethnic Russians in Berlin and German anti-migrant crisis activists being unwitting crisis actors and organising protests in Berlin.

9. However, this story was false, and had only achieved legitimacy by being laundered through Russian officials and media. These officials and news sites then used it to accuse the German government of tolerating migrant crimes and child abuse, playing on and exacerbating existing European internal tensions during the ongoing migrant crisis. Some examples of these activities are captured at Figure 3.

Figure 3. Examples of Laundering of the Lisa case in Russian-backed media



Source: Screencaps of Russian-linked media taken from StopFake.org Article "Lisa 2.0: How pro-Kremlin media in Germany have been using a new fake to justify an old one" Left from Politonline.ru: "Will they apologise to Russia? The rape of the Russian girl Lisa in Berlin has been confirmed". Right from RT Deutsch: "Lisa Case: State Prosecutor launches accusation of serious sexual abuse after all"

FIGHTING INFORMATION LAUNDERING

10. The nature of information laundering means that malicious actors often use reporting by media outlets and other sources to build credibility and respectability. In response, authorities could consider releasing guidance on handling information to media outlets and government agencies, such as advising against the use of certain language and reports that could be

misappropriated, or to refrain from reporting specific stories during sensitive periods to quell the spread. This was practiced during the tail end of the campaigning of the 2017 French elections, where alternative news and internet media sites dumped what became known as the "Macron Leaks" - a group of fake and irrelevant stories on French President Emmanuel Macron. The French electoral commission immediately published a statement urging all media outlets to not comment on the "Macron Leaks" before election day and to respect the campaign blackout period. As most outlets heeded the call, the spread of leaks was contained.

11. Information laundering preys on the self-reinforcing nature of echo chambers online. An effective counter measure is to address its effects upstream. This may involve inoculating the population against its methodology via pre-bunking and raising digital literacy. In addition, counter-disinformation efforts could focus on questioning the credibility of the alternative media or dump outlets pre-emptively, by exposing the connections and destroying their myth of objectivity. This would require the authorities to closely monitor these websites and carry out such countermeasures before an incident occurs, which can be difficult to anticipate.

CONCLUSION

12. It is important to recognise that information laundering remains a difficult threat to identify, as provides options for malicious actors to surreptitiously spread unfriendly narratives. At the same time, identifying information laundering requires a different approach from general disinformation campaigns, and is most effectively countered before the start of any incident. By identifying coordination patterns and releasing targeted policy guidance, one will be better able to recognise when adversaries are seeking to push a narrative using laundered information, and react accordingly. Finally, enhancing information sharing and building digital literacy are also important to prevent laundered information from taking root within our societies.

---

[1] QAnon is a far-right American political conspiracy theory and political movement that originated in 2017. The movement developed in online communities and its narratives have been promoted by US right-wing media outlets and Republican politicians. QAnon played a notable role in the 2020 US presidential election by supporting then-US President Donald Trump, including efforts to overturn the elections, such as when associates of Trump promoted QAnon-derived conspiracy theories.

[2] These included *Lenta, M24, Wi-Fi.ru, Sputnik Georgia, Rossiyskaya Gazeta* and *Business-gazeta.ru*

References:

1. Online Information Laundering: The Role of Social Media [Link: https://securingdemocracy.gmfus.org/online-information-laundering-the-role-of-social-media/]

2. Pro-Russian vaccine politics drives new disinformation narratives [Link: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-08/Pro%20Russian%20vaccine%20politics.pdf?vMuk2m7DlWP_GG25A86MqWZ_bg_jxlXL=]

3. Information Laundering in Germany [Link: https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_information_laundering_in_germany_final_web.pdf]

4. Information Laundering in the Nordic-Baltic Region [Link: https://stratcomcoe.org/publications/information-laundering-in-the-nordic-baltic-region/26]

5. Lisa 2.0: How pro-Kremlin media in Germany have been using a new fake to justify an old one [Link: https://www.stopfake.org/en/lisa-2-0-how-pro-kremlin-media-in-germany-have-been-using-a-new-fake-to-justify-an-old-one/]

6. How Germany is Tackling Hate Speech [Link: https://www.foreignaffairs.com/articles/germany/2017-05-16/how-germany-tackling-hate-speech]

7. Exploring the Information Laundering Ecosystem: The Russian Case [Link: https://www.csis.org/analysis/exploring-information-laundering-ecosystem-russian-case]

8. The Macron Leaks: The Defeat of Information Warfare [Link: https://www.csis.org/analysis/macron-leaks-defeat-informational-warfare]