Investigation Report:
The anti-URA cyber blockade, its breakthrough and perspectives.

Office of Exterior Intelligence
UNITED REPUBLICS OF ANTARCTICA
March 24, 2020

DECLASSIFIED AND PUBLICLY DISCLOSED

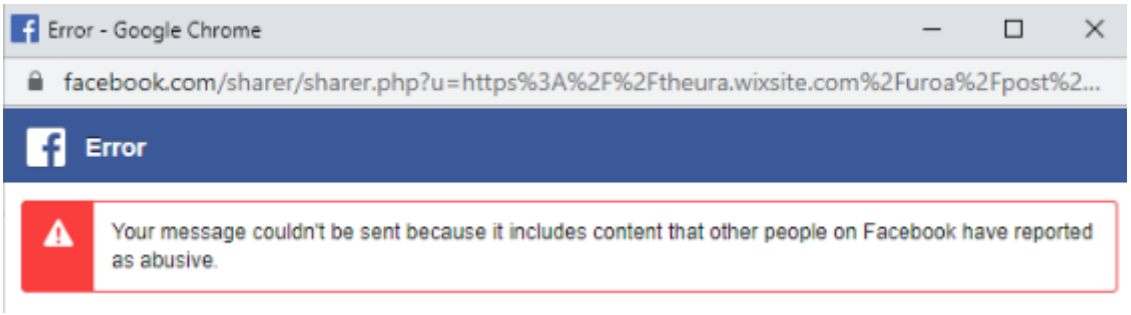
Addressed to the President of the URA and Transantarctic Supramicronational Alliance personnel with an A2 security clearance.

PREFACE

On March 22nd the Ministry of Information and Media of the United Republics of Antarctica experienced the impossibility of posting any content on the official URA (United Republics of Antarctica) Facebook page with links to the official URA website.

ANALYSIS

The website *theura.wixsite.com/uroa* turned out to be blocked as "not meeting" Facebook's Community Standards. The ban was in fact implemented as a result of multiple users firing complaints under certain URA Facebook posts as being "*abusive*":



These actions resulted in a ban with all URA Facebook posts containing links to the official website being deleted. The ban happened to be implemented right in the middle of the URA Diversity Program campaign, which was showing exceptional results through the third week of March 2020:

Since Facebook is one of the main traffic sources for the URA website – the ban has led to an estimated -x2.5 drop in the effectiveness of the Diversity Program campaign. The overall damage to URA's online presence and informational media outreach processes has been estimated as 42%.

INVESTIGATION RESULTS

The actions leading to an implementation of a Facebook ban described above were a thoroughly planned and carried out attack on the United Republics of Antarctica. The attack was carried out by a group of individuals/citizens of a micronation (or possibly micronations) hostile towards URA. Their actions fall under a Class C threat to the national security of URA ("*halting the processes of national digital resources and other activities resulting in a full or partial informational cyber blockade"*).

Though it is impossible to directly track down the individuals who carried out the attack due to Facebook privacy policy, we can surely state the following:

1. An internal diversion is ruled out.
2. Citizens of the following micronations are ruled out (having a high degree of non-hostility towards URA):
- Phoklandian Free State
- Republic of New Potato Land
- Flandrensis
- Westarctica
3. Micronations outside of Antarctica can be ruled out with a high degree of confidence.

Therefore, the attackers may potentially originate from the following micronations:

[redacted]

However, this is only an assumption which needs to be checked as soon as possible.

CONCLUSION

The aforementioned attack carried out by a group of individuals is a new form of *hidden* (directly non-trackable) micronational cyber warfare and can also be classified as a form of *micronational cyber terrorism*. The casualties of such an attack are extremely hard to make up for as the only workaround for a micronation to avoid Facebook banning its posts with links to a micronation's official website is changing its domain name.

The current attack has been successfully stopped by the IT unit of OEI, however the casualties of the cyber blockade have not been made up for. The micronation(s) from where the attackers originated should hold full responsibility for the hostile actions of their citizens towards URA.

Such actions of cyber warfare should be effectively addressed by the micronational community as whole including all micronational peace organizations (such as GUM and CUM) and proclaimed as a violation of microinternational law (or at least be regulated by it). Otherwise, there is no guarantee that the micronational community will not suffer from a series of such attacks in the nearest future.