

The hidden danger behind COVID-19

*Disinformation campaigns and the protection
of the scientific and economic potential*

In a note published earlier today, the State Security reports that an increasing number of individuals and groups are spreading fake news about the coronavirus COVID-19 with a view to polarize society. In addition, certain foreign powers hope to capitalize on the deep economic crisis in the aftermath of the coronavirus crisis and are looking to take over companies facing financial difficulties.

The hidden danger behind COVID-19

(Right-wing) extremism, potential interference and damage to the scientific and economic potential

In the past, we have seen the emergence of this phenomenon during election campaigns, mainly abroad: groups, in some cases driven by foreign troll armies, use disinformation campaigns to expand their influence. A similar phenomenon is occurring during the coronavirus outbreak: social media are flooded with disinformation about COVID-19 with a view to set population groups against each other.

In order to manage the related risks as efficiently as possible, the civil intelligence service VSSE and its military counterpart SGRS have set up a distribution of tasks and a permanent dialogue based on their experiences during the last federal elections and their increasing collaboration.

Ideological extremism

RIGHT-WING EXTREMISM

In recent weeks, both intelligence services have been able to establish that various right-wing extremist individuals and groups are spreading conspiracy theories via social media and are using the COVID-19 crisis to set population groups against each other or to undermine the authority of the Belgian government and the medical community.

One example is the theory that is being spread by the Knights of Flanders, a new group of far-right Templars, that the origin of the coronavirus is to be found in the flu vaccine.

Other far-right groups engage in hate speech against Muslims. For example, the French speaking splinter party Nation at one point published the message that there was a so-called fatwa calling infected Muslims to “cough in the faces of nonbelievers”.

Fatwa du cheikh
Abou Noomen :
les musulmans
infectés doivent
touser sur les
mécroyants pour
les contaminer

17 Mar 2020

A ne

pas manquer, Conflit de civilisation, Djihad



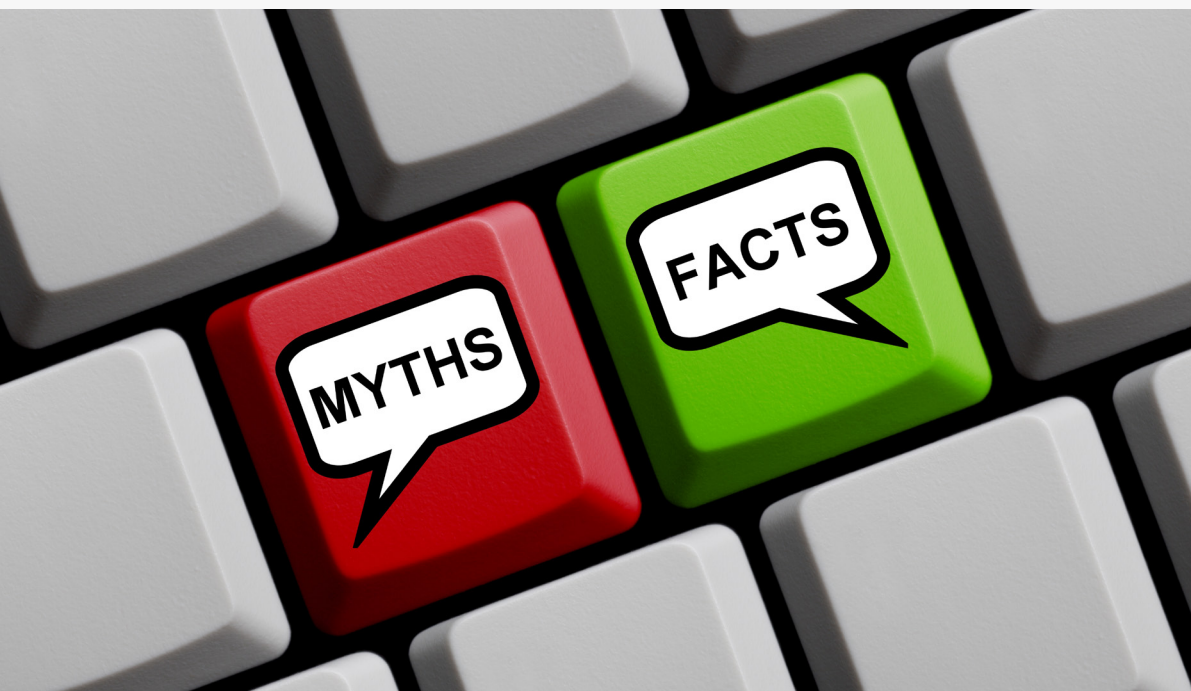
Ideological extremism

RIGHT-WING EXTREMISM

The VSSE/SGRS also observed that right-wing extremists claim that there is a link between the outbreak of the coronavirus and immigration. A mixture of facts, fake news and far-right framing is used to make their message clear. It is the leading discourse of far right on so-

cial media, with one common denominator: migration makes the outbreak of the coronavirus worse.

There are numerous examples. The French speaking far-right party Parti National Européen (PNE), a breakaway party of the French speaking Nation, describes an asylum centre in Mouscron as being a source of infection for the surrounding area. The PNE even demands that the centre should be closed because of the coronavirus and adds that: “they (the asylum seekers) should all be accommodated in Parliament: the building does not serve any meaningful purpose anyway”.



Ideological extremism

PRO-RUSSIAN REPORTING



The VSSE also perceives that certain far-right groups and organisations are using a pro-Russian discourse in the context of the corona crisis and are dispersing Russian propaganda in our country. One of those groups is the recently founded **Squadra Europa**. They are a very recent, pan-European, ultra-right movement, active on Twitter and other social media and with a division in Belgium.

The movement posts messages against immigration, the perceived islamization of Europe and globalisation. They also link these phenomena to the outbreak of the coronavirus. Furthermore, Squadra Europa clearly uses an anti-EU and pro-Russian discourse, as proven by the post below from 23 March 2020.

Ideological extremism

PRO-RUSSIAN REPORTING



In other posts from individual profiles the corona epidemic is used to disseminate Russian propaganda on the topic. But the real impact of these posts on the far-right community **in our country** is very limited. The distributors of such messages mostly serve as a “useful idiot” and mouthpiece to the benefit of Russian interests.

Ideological extremism

FAR LEFT

The anarchist community in Brussels also does not fail to make their voice heard during the corona crisis. On 8 April 2020, the leftist anarchistic website Indymedia Bruxsel launched a call to make use of the COVID-19 outbreak **to commit acts of violence against police and penitentiary staff and to damage telecom infrastructure** in order to inflict as much

damage as possible to our society. According to Indymedia, now is the ideal time to take action: because of the coronavirus outbreak, the attention of law enforcement is focused on other matters.

Other organisations, such as the ultra-left Secours Rouge, also remain active during the corona crisis.



The screenshot shows the homepage of the Indymedia Bruxsel website. At the top, there is a logo with a stylized 'i' and the text 'DON'T HATE THE MEDIA BE THE MEDIA' and 'INDYMEDIA BRUXSEL'. Below the logo, the main headline reads 'En mai, fais ce qu'il te plaît : un appel au conflit'. To the right of the headline, there are two buttons: 'Articles' and 'Local'. Below the headline, the text 'posté le 08/04/20' is visible. Further down, there is a section for 'Mots-clés' with the word 'art' highlighted. The main body of the text begins with 'Ici nous pouvons aisément réaliser que le gel hydroalcoolique sert aussi bien à se désinfecter les mains qu'à allumer des incendies.' and continues with 'En d'autres termes que nous n'avons pas besoin des directives de l'état pour prendre soin de nos proches, et, une fois réglée la question de la survie, nous n'avons rien de mieux à faire que de sortir traîner à l'affût d'un mauvais coup, nous avons plus que jamais besoin de vengeance et d'amitiés réellement vécues.'

Disinformation by foreign powers



In the context of the coronavirus crisis the VSSE also investigates propaganda disseminated by foreign powers, by means of Social Media Intelligence (SOCMINT) and by analysing narratives regarding our country and COVID-19 in specific foreign media that might have an impact on Belgian public opinion. The disinformation campaigns are part of a hybrid strategy to debilitate the West.

The propaganda that is being **spread mainly originates from Russia.**

Disinformation by foreign powers

The Russian disinformation is in line with the strategy of the Kremlin to sow discord and distrust in the West vis-à-vis national and European authorities. The goal is to undermine social cohesion. In part, the disinformation is also aimed at

Russian public opinion. The intention is to convince Russian nationals that the way their country is handling the crisis is correct and efficient. These disinformation campaigns possess a clear propagandistic aspect.



The most widespread of these theories claim that the virus is a biological weapon created by laboratories and spread by migrants. Reports targeted at Italian and Spanish civilians, on the other hand, focus on how their respective authorities fail to control the crisis, on how Russia, by contrast, is efficiently dealing with the outbreak of the virus and on the incapacity of Europe.

The Kremlin denies the accusations.

Protection of the scientific and economic potential

In the context of the coronavirus crisis, the VSSE wishes to stress that we must remain vigilant with regard to **foreign powers which are seeking strategic takeovers of companies that are struggling due to this crisis.**

Opportunities may arise predominantly in the high-tech industry allowing a nation to strengthen its strategic position and to establish itself in the European market. The VSSE would also like to draw attention to the risk of foreign powers exploiting their humanitarian aid operations to engage in interference in decision-mak-

ing processes. This 'corona diplomacy' is not necessarily in the interest of our country.



Video conferences

The VSSE is aware of the risks involved in the organisation of consultations and meetings through video conference, now

that a large part of the working population is working from home. Foreign intelligence services might exploit the vulnerabilities of these systems for technical espionage.



Therefore, it is important to look for **the most secure platforms** and to use them in **the safest way possible** by taking the following precautions:

- > Make sure that both the operating system of your smartphone, desktop, laptop or tablet and the video conferencing software are up to date.
- > Only use video conferencing software with features that allow you to adequately manage the meeting (e.g. management of the participants) and ask your IT specialist to adjust the software settings according to the desired level of protection.
- > A safe video conference requires a secure local network. Visit the website of *the Centre for Cyber Security Belgium (CCB)* to learn more about internet safety at home, at work, at school and in vital sectors.

Video conferences

> Follow these tips to organise a secure video conference:

- Explicitly determine who is allowed to participate in the video conference and only give access to those people.
- Use a password to limit the access to the video conference.
- Verify whether the participants of your video conference are indeed the people you wish to include, for instance by checking if they are recognizable.
- Only click on 'meeting links' (invitations to take part in a video conference) if the sender is

someone you know and trust. It is recommended to send the invitations through the video conferencing software. Avoid sending invitations via social media.

- Think carefully about the place where you choose to take part in the meeting.
- Make sure you can monitor what the other participants can see behind you. If possible, use a virtual background.
- Other devices in the room (smartphones, computers, tablets, ...) can compromise the confidentiality of the video conference. It is thus recommended to remove these devices

Video conferences

from the room before a confidential discussion.

- > Information may still leak after the video conference has ended, since it is possible for participants to record the video conference (via the video conferencing software itself or with other tools). If the recording is handled carelessly (or maliciously), information can still become public.
- > Finally, you should bear in mind that the infrastructure you use for the video conference might not be based in Belgium. Depending on the location of the service provider and its infrastructure, foreign compliance rules may apply. Especially outside the

European Union, the rules on the protection of privacy and the confidentiality of communication may differ from what you are used to in Belgium.

