

Het verborgen gevaar achter COVID-19

(Rechts)extremisme, potentiële inmenging en een aantasting van
het wetenschappelijk en economisch potentieel

We zagen het fenomeen al eerder opduiken tijdens verkiezingscampagnes voornamelijk in het buitenland: groeperingen, al dan niet aangestuurd door buitenlandse trollenlegers, die gebruik maken van desinformatiecampagnes om hun invloed uit te breiden. Met de uitbraak van het coronavirus doet zich een gelijkaardig verschijnsel voor: via de sociale media wordt zoveel mogelijk desinformatie rond COVID-19 uitgestuurd met het doel om be-

volkingsgroepen tegen elkaar op te zetten.

Om de risico's in dit verband zo efficiënt mogelijk te beheren, hebben de twee inlichtingendiensten, de VSSE en haar militaire tegenhanger, de ADIV, een taakverdeling en een permanent overleg opgezet op basis van hun ervaring tijdens de jongste federale verkiezingen en hun toenevende samenwerking.

Ideologisch extremisme

RECHTSEXTREMISME

Zo konden beide inlichtingendiensten de jongste weken vaststellen, dat verschillende extreemrechtse individuen en groeperingen via de sociale media complottheorieën verspreiden en de COVID-19-crisis gebruiken om bevolkingsgroepen tegen elkaar op te zetten of met als doel het gezag van de Belgische overheid en de medische wereld onderuit te halen.

Onder andere de *Knights of Flanders*, een nieuwe extreemrechtse tempeliersgroepering, verspreidt de theorie dat de oorsprong van het coronavirus te situeren zou zijn in het griepvaccin.

Andere extreemrechtse groeperingen doen aan haatzaaijerij tegen moslims. Zo verspreidde de Franstalige splinterpartij Nation op een bepaald moment het bericht dat een zogenaamde fatwa besmette moslims 'opriep om te hoesten in het gezicht van ongelovigen'.

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

17 Mar 2020 A ne
pas manquer, Conflit de civilisation, Djihad



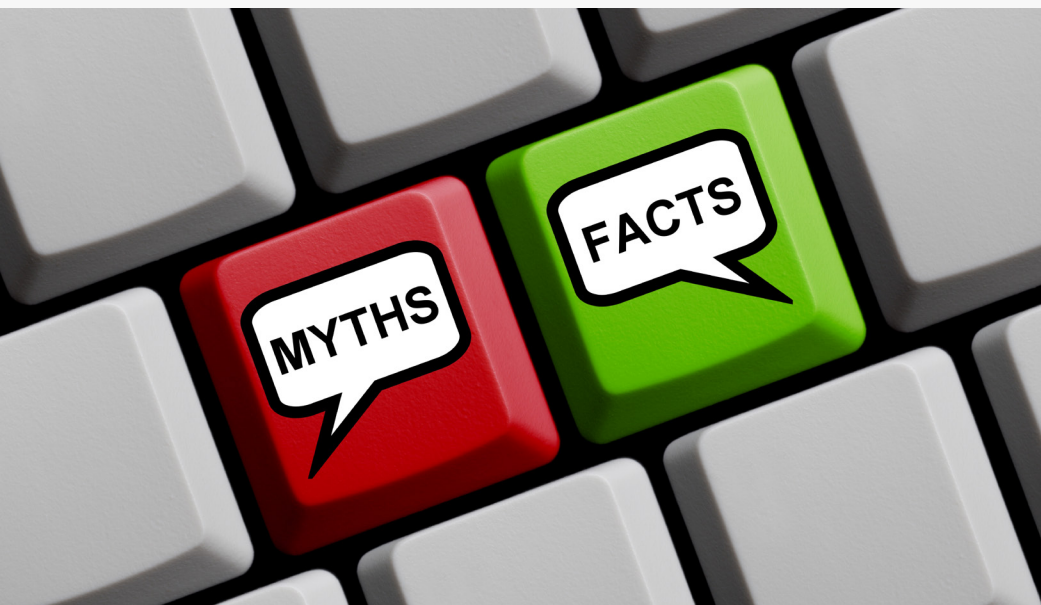
Ideologisch extremisme

RECHTSEXTREMISME

De VSSE/ADIV constateerden ook dat extreemrechts hamert op een verband dat volgens hen bestaat tussen de uitbraak van het coronavirus COVID-19 en immigratie. Een cocktail van feiten, fake news en extreemrechtse framing moet de boodschap duidelijk maken. Het is het toonaangevend discours

van extreemrechts op de sociale media met als gemene deler: migratie maakt de uitbraak van het coronavirus erger.

Er zijn tal van voorbeelden. De Franstalige extreemrechtse partij Parti National Européen (PNE) bijvoorbeeld, een afscheuring van het Franstalige Nation, omschrijft een asielcentrum in Moeskroen als een besmettingshaard voor de omgeving. De PNE eist zelfs de sluiting van het centrum omwille van het coronavirus en voegt eraan toe: 'ze (de asielzoekers) zouden allemaal in het parlement gehuisvest moeten worden: dat gebouw heeft anders toch geen zinvolle invulling'.



Ideologisch extremisme

PRO-RUSSISCHE BERICHTGEVING



De VSSE stelt ook vast dat bepaalde extreemrechtse groeperingen en organisaties in de context van de coronacrisis een pro-Russisch discours hanteren en Russische propaganda verspreiden in ons land, zoals het recent opgerichte **Squadra Europa**. Het gaat om een zeer recente pan-Europese, extreemrechtse beweging die actief is op Twitter en andere sociale media en een vertakking heeft in België.

De beweging post berichten tegen immigratie, de gepercipieerde islamisering van Europa en globalisering. Deze fenomenen worden ook in verband gebracht met de uitbraak van het coronavirus. Daarnaast is het opvallend dat Squadra Europa ook een anti-EU en pro-Russisch discours hanteert, zoals blijkt uit de hiernaast gepubliceerde post van 23 maart 2020.

Ideologisch extremisme

PRO-RUSSISCHE BERICHTGEVING



Andere posts van individuele profielen grijpen de uitbraak van de corona-epidemie aan om Russische propaganda daaromtrent te verspreiden. Maar de reële invloed ervan op de extreemrechtse scène **in ons land** is zeer beperkt. De verspreiders van dergelijke berichtgeving worden veeleer als “nuttige idioot” en spreekbuis voor de kar van de Russische belangen gespannen.

Ideologisch extremisme **EXTREEMLINKS**

Ook de Brusselse anarchistische scène laat van zich horen tijdens de coronacrisis. Op 8 april 2020 lanceerde de linkse anarchistische website Indymedia Brussel de oproep om van de uitbraak van COVID-19 gebruik te maken om **geweld te plegen tegen politie, penitentiare beampten en tegen de telecominfrastructuur** om de maatschappij maximale schade toe te

brengen. De uitbraak van het coronavirus is daarbij volgens Indymedia het ideale moment om tot de actie over te gaan: de ordediensten zijn geconcentreerd op andere zaken.

Andere organisaties, zoals het extreem-linkse Secours Rouge, blijven ook actief tijdens de coronacrisis



The screenshot shows the Indymedia Brussel website. At the top, there is a logo with the text "DON'T HATE THE MEDIA BE THE MEDIA" and "INDYMEDIA BRUXSEL". Below the logo, the article title "En mai, fais ce qu'il te plaît : un appel au conflit" is displayed. The article is dated "posté le 08/04/20" and has the keyword "Mots-clés art". The article 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."

Desinformatie door buitenlandse mogendheden



In de context van de coronacrisis onderzoekt de VSSE ook propaganda door buitenlandse mogendheden aan de hand van *Social Media Intelligence* (SOCMINT) en door een analyse van specifieke buitenlandse media naar narratieven over ons land en COVID-19 die een rol kunnen spelen in de beïnvloeding van de Belgische publieke opinie. De desinformatiecampagnes kaderen in een hybride strategie om het westen te verzwakken.

De propaganda die wordt verspreid is **voornamelijk afkomstig vanuit Russische hoek.**

Desinformatie door buitenlandse mogendheden

De Russische desinformatie past in de Kremlinstrategie om in het westen verdeeldheid en wantrouwen ten aanzien van nationale en Europese overheden aan te wakkeren. Het doel: de maatschappelijke cohesie ondergra-



ven. De desinformatie is deels ook gericht op de eigen Russische publieke opinie. Ze moet hen overtuigen van de zogenaamd juiste en efficiënte Russi-

sche aanpak van de crisis. Er is dus overduidelijk een propaganda-aspect verbonden met deze desinformatie-campagnes.

De meest verspreide theorieën die er de ronde doen, gaan over het virus als een door laboratoria gecreëerd biologisch wapen en de verspreiding ervan door migranten. Berichten bestemd voor Italianen en Spanjaarden focussen dan weer op hoe hun respectievelijke autoriteiten de crisis niet onder controle zouden krijgen, de onmacht van Europa en hoe in contrast Rusland goed met de uitbraak van het virus omgaat.

Het Kremlin ontkent alle beschuldigingen.

Bescherming van het wetenschappelijk en economisch potentieel

In de context van de coronacrisis wil de VSSE ook benadrukken dat we waakzaam moeten blijven voor buitenlandse mogendheden die azen op strategische overnames van bedrijven in nood ten gevolge van de coronacrisis. Het gaat hoofdzakelijk om buitenkansjes in de sector van de hightech waarmee een land zijn strategische positie kan verstevigen en voet aan de grond kan krijgen op de Europese markt.

De VSSE wil ook wijzen op het risico dat buitenlandse mogendheden hun geleverde humanitaire hulpacties mogelijk

aanwenden om aan inmenging te doen in beslissingsprocessen. Deze 'coronadiplomatie' is niet noodzakelijk in het belang van ons land.



Videoconferenties

De VSSE is zich ook bewust van de risico's die genomen worden door overleg en vergaderingen te houden via videoconferenties, nu een groot deel van de

werkende bevolking van thuis uit werkt. Buitenlandse inlichtingendiensten kunnen immers handig gebruik maken van de zwaktes van het systeem voor technische spionage.



Het is dan ook van belang om de meest veilige platformen te gebruiken en ze te gebruiken op een zo veilig mogelijke manier door volgende zaken in acht te nemen:

- > Zorg ervoor dat zowel het besturingssysteem van uw smartphone, desktop, laptop, tablet alsook de software voor de videoconferentie volledig up-to-date zijn.
- > Gebruik alleen videoconferentie-software die toelaat om op een adequate manier de vergadering te beheren (bijvoorbeeld een systeem om de deelnemers te beheren) en laat uw informaticaspecialisten de software correct instellen voor het gewenste beveiligingsniveau.
- > Voor een veilige videoconferentie moet ook uw lokaal netwerk afdoende beveiligd zijn. Op de website van het Centrum voor Cybersecurity België (ccb.belgium.be) kan u richtlijnen

Videoconferenties

vinden voor een veilig internet thuis, op het werk, op school en in de vitale sectoren.

> Voor het organiseren van een veilige videoconferentie kan u rekening houden met de volgende tips:

- Bepaal expliciet wie aan de videoconferentie mag deelnemen en laat alleen die personen toe.
- Gebruik een paswoord om de toegang tot de videoconferentie te beveiligen.
- Verifieer dat de deelnemers aan uw videoconferentie wel degelijk de verwachte personen zijn, bijvoorbeeld door ze herkenbaar in beeld te laten komen.
- Let op bij het klikken op 'meeting links' (uitnodigingen). Doe dat

alleen als de afzender gekend en betrouwbaar is. Het is aangewezen om de videoconferentie-software te gebruiken voor het versturen van de uitnodigingen. Doe dit zeker niet via de sociale media.

- Wees voorzichtig met de keuze van de plaats waar u vergadert.
- Zorg dat u in het oog kan houden wat er achter u zichtbaar is voor de camera (en dus voor de andere deelnemers). Gebruik eventueel een virtuele achtergrond.
- Andere apparaten in het lokaal (smartphones, computers, tablets, ...) kunnen de confidentialiteit van de videoconferentie aantasten. Het is dus aangewezen om tijdens een vertrouwelijke bespreking die toestellen buiten het lokaal te houden.

Videoconferenties

- > Ook na het afsluiten van de videoconferentie kan er nog informatie lekken. Het is immers mogelijk voor de deelnemers om de videoconferentie op te nemen (met de videoconferentie-software zelf of met andere tools). Indien er onzorgvuldig (of kwaadwillig) met die opname wordt omgegaan kan informatie ook op die manier nog openbaar worden.
- > Tot slot moet u er nog rekening mee houden dat uw videoconferentie over een infrastructuur loopt die zich niet noodzakelijk in België bevindt. Afhankelijk van de lokalisatie van de dienstverlener en diens infrastructuur kan het zijn dat buitenlandse compliance regels van toepassing zijn. Zeker buiten de Europese Unie is het mogelijk dat de regels over de

bescherming van de privacy en de vertrouwelijkheid van de communicatie verschillen van wat u gewoon bent in België.

