COMBATTING RUSSIAN DISINFORMATION

LAUNCHING AN ONLINE COMMUNICATIONS CAMPAIGN TO INFORM, DEBUNK, AND COMBAT STATE-SPONSORED PROPAGANDA

Comprehensive action proposal

Strictly confidential

INITIAL STATEMENT

Disinformation – false and twisted information which is intended to mislead – was a constant of Soviet propaganda policy during the Cold War. But in recent years, the means in which it can be employed have shifted dramatically, with significant implications for its scale and influence. Today, the Internet allows "fake news" and "alternative facts" to spread like wildfire, via multiple unsecured points of influence. This means that purveyors of disinformation, notably state propaganda outfits like RT and Sputnik, now have the capacity to influence audiences around the world, notably via social networks like Facebook and Twitter. The overarching objective of these campaigns is the same: to weaken Western democracies by aggravating societal divisions, damaging trust in institutions, and causing the public to question its "liberal" model.

In response to this threat, government, media, and civil society actors in the US and Europe have taken a number of first steps: NATO's StratCom Center is engaged in investigating Russia's disinformation campaigns, US government-funded, independent news sites such as RFE/RL offer new fact-checking resources such as Polygraph.info, and individual governments like France have taken steps to curb fake news during elections. Tech companies like Facebook, Twitter, and Google have also introduced new measures to ensure their services are not subverted by foreign interests, such as de-ranking or de-listing websites that are known purveyors of fake news. Civil society organizations like StopFake and media outlets such as Snopes have also taken action to expose Russian disinformation efforts, raise awareness of their tactics, and try to set the record straight. Until now these actions mainly consist in identifying "fake news". But there has been no convincing solution to fight them, much less to contradict their narrative and organize a counter-attack.

Yet with hundreds of millions' worth of budget, thousands of content producers and trolls, and new allegations of Russian disinformation and cyber hacking coming out on a near-daily basis – amounting to a massive bombing campaign – the West's response thus far of think tank papers and local resistance efforts by civil society isn't nearly enough. It is clear that Western democracies will have to undertake far more intensive efforts to address this issue.

Our approach

As we see it, the main weakness in the Russians' disinformation campaign is their embrace of a quantity - over quality and credibility - strategy as shown by their lack of credible spokespeople, their publication of a high volume of "easily" identifiable propaganda and "fake news", and their heavy reliance on a few biased partisan sites, dubious social media pages and uninspired trolls. Their stories are hard to believe, their arguments are weak and the model they promote is not very attractive. This means that their content is not very convincing and relatively easy to debunk. Nevertheless, their messages fall on fertile ground, and some stories are successfully spread by their allies, bringing new ammo to their global narrative. And we can expect they will improve their tactics with time.

As open democracies cannot undertake massive propaganda efforts and we believe that this is in any case an inefficient way to promote ideas, the optimal counter-strategy should take a smarter approach: choosing credibility over dubiousness, accuracy over distortion, facts over falsehoods, subtlety over ham-handedness, independence over partiality, both for content and for the platforms on which this content should be published. Sniping and chirurgical strikes instead of carpet-bombing. This being said, this implementation of this sniping approach should be as systematic as the Russian one is.

This is where we come in: deploying a multi-pronged strategy to

- *investigate sources of disinformation, perform threat assessment, and identify opportunities to combat false narratives*
- *debunk fake news and black PR operations*
- *discredit and intimidate the platforms broadcasting fake news*
- *promote democratic principles and criticize the Russian illiberal model in the public debate, online*

This plan should be implemented in every targeted country and language, including Russian.

Objectives

1. **Intelligence**: gather information on the Russian propaganda operations
2. **Defensive**: debunk Russian propaganda operations, educate the population, weaken their allies, and defend democratic models and values
3. **Offensive**: criticize the Russian authoritarian model, help our allies in Russia and other targeted countries where this model applies or is attractive to a majority

Targets

The battle of ideas and content online operates by language more than countries. So our targets are both strategic countries with specific languages and broader audiences (English, Russian, etc.)

- **Western countries** (primarily the US, UK, France, Germany, Italy, Spain, etc.)
- **Eastern and Balkan European countries**, especially where Russia is popular and active (Hungary, Bulgaria, Greece, Serbia, Montenegro, etc.)
- **Russia and Russian-speaking audiences** (Baltic states, Ukraine, etc.)

Strategy

I. INTELLIGENCE: MONITOR, INVESTIGATE, AND ANALYZE RUSSIAN DISINFORMATION

The first step will involve monitoring and performing open-source intelligence investigations (OSINT) into sources of disinformation:

- **Monitoring** of online media sites, social media, clear and dark web forums in multiple languages.
- **OSINT** into suspect campaigns, media sites, and profiles
- **Identification and analysis** of fake news and black PR operations, and emerging threats

We will engage the services of our subsidiary firm, Lexfo, one of France's top 5 **cybersecurity** firms (certified by the French Network and Information Security Agency (ANSSI)). Lexfo is specialized in offensive cybersecurity (penetration tests, response to incidents, investigations, etc.).

II. ADVOCACY: PUBLISH CONTENT ON ONLINE MEDIA

An indirect, untraceable, and expansive approach

To serve our defensive and offensive objectives, we will publish a steady stream of content in multiple languages across several hundred existing and credible news media sites. This will allow us to directly counter Russian disinformation by occupying the informational terrain, debunking false narratives, naming and shaming their allies and promoting the importance of safeguarding liberal democracies against the Russian authoritarian model.

At a macro level:
We recommend amplifying the existing but irregular coverage about the Russians' use of disinformation across most mainstream Western media sites in order to create a drumbeat effect (communication as

repetition) across hundreds of independent media sites – not only concentrated on a handful of sites like Polygraph.info.

At a micro level:
We will also conduct targeted operations to publish content in order to counter specific fake news and black PR operations that will be identified.

Our unique added value

We operate as an international newsroom. **Last month alone, we published more than 1,000 articles,** briefs, or opinion pieces online. Since 2011, we have built a wide network of hundreds of third-party experts, and the capacity to publish on several hundred high-quality, independent news, opinion, and analysis websites, lending us the unique ability to make our clients' voice heard in English, French, and Spanish. We have the know-how to open new languages and countries, with the ability to operate at full speed within several months depending on the market. Most critically, our ability to publish articles across hundreds of credible media outlets means that any campaign we undertake will have far more sway than the content published only on state-sponsored outlets RT and Sputnik, and their local few allies.

Counter-information hubs

Where we lack platforms to publish our content (notably in certain local languages), we will create news media sites serving our objectives, inside a broader editorial spectrum. These media sites will be ostensibly independent to assure their credibility. They will be registered on Google news in order to improve significantly their visibility, credibility and reach.

Social media amplification

- To amplify our actions, we will also **launch social media campaigns on Twitter, Facebook, LinkedIn** and other local platforms to push our content
- We would search for **online influencers and encourage them become natural allies to engage in the conversation online** by combatting false narratives and fostering constructive discourse

Wikipedia editing and monitoring

- Since **Wikipedia is the de facto, go-to source of information** for decision-makers and the general public alike, we recommend creating new pages, such as lists of known Russia-backed propaganda sites, as well as **expanding and updating pages related to fake news** and other relevant subjects
- We also recommend **monitoring** relevant pages related to hot topics such as the Ukraine conflict, or Western allies (pro-Western local politicians, journalists, medias, businesspeople, companies, etc.) which may be particularly vulnerable to manipulation by Russia-backed trolls

We will prioritize:

- Engaging and mobilizing credible, independent authors and spokespeople
- Publishing high-quality, compelling opinion, analysis, and policy articles
- Publishing infographics, videos and stories appealing for a popular audience, with an emotional dimension, attractive titles and images able to generate clicks and shares on social networks
- Countries where elections are happening

III. ENGAGE IN COUNTER-ACTIVISM

Undertake operations intended to intimidate those relaying fake news.

- **Raising the "price to pay" for the influencers and media relaying Russian propaganda and fake news**

- "**Name and shame**" the media sites and influencers being caught promoting "fake news" (reputations damages)
- Engage **legal actions** against the media site, whenever possible, to remove controversial contents and encourage them to more cautious in their publication policy
- **Limit their visibility** online: systematically alert search engines and social networks against every fake news publication, in order to encourage them to take stronger actions against the media and influencer responsible
- **Reduce the revenues** of the medias and influencers we are targeting by encouraging advertising agencies not to work with them (in order to avoid any reputation and economic damages for themselves)
- Launch "**response to incident**" operations against cyber attacks and **hacking** operations, especially during elections, to limit the damages, learn, raise awareness and, eventually, conduct ethical "hack back" operations.

IV. OPTIONAL

- **Organize international conferences** and local trainings focused on disinformation aimed at Western policymakers, journalists, diplomats, online influencers, decision makers and other stakeholders
- **Commission a series of white papers**, written by credible analysts, which will be useful sources for our contents, trainings and events
- **Create an international think tank dedicated to modern infowars**

Our team

Our team is very diverse and composed of online campaigners, strategy and communication consultants, engineers, political studies alumni, former journalists, web marketing or competitive intelligence experts. Altogether, we count **75 staff of 16 different nationalities** who speak more than a dozen languages. Our consultants oversee a vast network of several hundred writers specialized in numerous sectors (business, economics, foreign affairs, public policy, etc.), publishing on several hundred online media sites in each of our main operative languages (English, French, Spanish and Chinese).

- **Matthieu Creux**, is an expert in online influence and mobilization, son of a general in the French Air Force. Matthieu has participated in every French general election since 2006, notably working as an advisor to the French Minister for Higher Education between 2007 and 2009, where he was in charge of online strategies. He has also worked for a number of foreign governments and large corporate groups on online activism and counter-activism issues.`
- **Arnaud Dassier**, former online campaign manager for Jacques Chirac in 2002 and for Nicolas Sarkozy in 2007. Arnaud has directed dozens of online political campaigns since 1997 across Eastern Europe, Asia, and Africa and was closely involved with the International Republican Institute's (IRI) work in Ukraine, where he led a study and keynote presentation on Russian propaganda in 2015.
- **Samuel Dralet**, president of Lexfo and former technical director of Atlab, purchased by French telecommunications giant Orange to establish Orange Cyberdéfense.
- **Jacques Lafitte**, former advisor in charge of creating the euro in the cabinet of EU Commissioner in charge of Economic and Financial Affairs from 1995-1999, and chief lobbyist for Microsoft across the EMEA region until 2002
- **Antoine Violet-Surcouf**, former director of the digital strategy department of Adit and President of AEGE, a network of economic intelligence experts.
- **François-Charles Timmerman** heads the business diplomacy unit of Avisa Partners. He was a member of the French secret services (DGSE), and the former international director of the strategy and risk-management consultancy CEIS.

The strategic committee of the group, includes, among others, **Lynton Crosby**, Boris Johnson and David Cameron's election strategist, **Joe Trippi**, a pioneering Democratic political strategist in the US and consultant in emerging technologies, **Jean-Louis Georgelin**, former Chief of Staff of the French Armed

Forces from 2006 to 2010 and grand Chancellor of the Legion of Honor, **Eric Besson**, former Minister of Industry, Energy and the Digital Economy, and **Gerard Askinazi**, former World Vice President of Publicis Events, President of Havas Euro-RSCG Worldwide Events, and former President of Agence Publics.

Modus operandi

Following a mutually acceptable timeframe (ideally, at a monthly rate), our team commits itself to sharing with you:

- **A weekly monitoring review from our cybersecurity and intelligence operations**
- **A monthly press review on content written and published** by our teams on all online media platforms, with the recognition that we are dependent on our pieces being accepted by the platforms that we solicit. We aim to publish between 5 to 15 articles a month in each language, depending on the news. While news media sites appreciate our contributions, we must avoid overwhelming them.
- Our team's achievements on **Wikipedia** charting the evolution of how sections/pages shift over time
- **A quantitative and qualitative impact analysis of each of our online news sites' evolution**, as well as a situational analysis of these sites' positions on Google when searching for strategic keywords; a detailed report on the growth of the sites' social community (number of *followers* on Twitter, *fans* on Facebook, subscribers to the newsletter…)

We are able to mobilize rapidly.

- From the moment we are briefed, we are able to publish our first articles within 1 to 5 working days, depending on the media reactivity.
- Our commitment is prepared for the high level of **reactivity** that is often necessary for this type of mission. We are able to adapt to any adjustments in messaging immediately and we ensure the **availability** of a high-functioning team at your side at all times.
- We guarantee the absolute confidentiality of our exchanges throughout the mission. Our publication processes are anonymous and protected against identification attempts or hacking by our cybersecurity team.

Budget estimations

We work with retainers on a "per language" or/and "per campaign" basis.

We imagine that such a vast and ambitious infowar campaign will be long term and built in a project-by-project and step-by-step approach.

We can only give you a budget estimation for the first steps that we could quickly start with our existing capacities in English, French and Spanish.

1. Defensive and offensive online influence campaigns

Monitoring of online media, first level investigatory services on open public data, publication of content on existing media sites, editing of one online news media site (if necessary) and Wikipedia editing

Monthly budget per language (retainer fee)

- Low intensity: roughly 20.000 € (excl. VAT)
- High intensity: roughly 40.000 € (excl. VAT)

The difference of intensity depends on the volume of content being monitored and published every month.

2. Counter activism

In-depth technical investigations, response to incidents, special operations (negative PR, legal actions, ethical hack back, etc.): TBD depending on number of hours worked. Knowing our average budgets for these types of mission, we believe that a 50.000 € (excl. VAT) monthly budget could be a good basis, for a start.