Kremlin disinformation campaigns:

Recommendations to counter Russia computational propaganda in the UK

Kremlin disinformation campaigns:

Recommendations to counter Russia computational propaganda in the UK

Anne Applebaum, Edward Lucas, Ben Nimmo, Martin Innes, Keir Giles, Louis Brooke, Tanya Bogdanova, Rebecca Wiles and Peter Pomerantsev

Contents

Executive summary

Kremlin digital influence engineering involves the creation and dissemination of false narratives as well as technological manipulation such as the use of fake or automated social media accounts to distort public perceptions. The aim is to promote the Kremlin's foreign-policy agenda, boost its local proxies, erode trust in democratic institutions, increase polarisation and spread confusion during crises.

Examples in Britain include a campaign to cast doubt on the integrity of the vote count following the Scottish Independence Referendum in 2016; the amplification of ethnic and religious hatred following terrorist attacks in Britain in 2017; and the undermining of public confidence in the British government's explanation of the poisoning of Sergei Skripal in 2018.

Evidence-based analysis in this area this area is at an early stage. Challenges include identifying unattributed activity as emanating from or generated by Russia, as well as in measuring the scale and impact of activity. Measuring these key indicators would be significantly easier given more cooperation with the tech companies. Kremlin digital disinformation and computational propaganda has been enabled and facilitated, albeit unwittingly, by the nature and policies of social media platforms. These hinder analysis and countermeasures. Countering Russian digital influence engineering also requires dealing with urgent issues of privacy, online identity, data usage and wider digital rights. More broadly, digital disinformation and computational propaganda is just part of a much bigger "full-spectrum warfare" arsenal, which includes the use of money, cyber-attacks, military (kinetic) intimidation and abuse of the legal system. Though these tactics fall outside the scope of this paper, responding to them will require an unprecedented whole-of-government response.

Recommendations

1. Unite, Define and Expose Russian Disinformation

An Investigative Network:
Our approach is flawed and fractured. It lacks a common taxonomy, methodology and communications strategy. There is a lack of agreement over commonly used terms such as 'troll', 'bot' or 'fake news', and little public understanding of *dezinformatsiya* or the other distortions created by digital media. Many publicly funded, non-profit and private organisations across Europe and North America conduct important but uncoordinated analysis, duplicating effort. Government, media, think-tanks and academics should define terms of reference, pool results, share techniques and create a joint threat picture.

Measuring the Problem:
A key first step towards meeting the challenge of Russian disinformation is better diagnostics: he bits of the adversary's activity that we can see (bot activity for example) are not necessarily the ones that matter most; expert trolls may be more effective but less visible. Only when we know which tools and techniques are effective can we allocate the right resources to countering them. For instance, it is not always understood which tactics are deployed and why.[1] The Network described above would co-ordinating analysis and assessment of hostile campaigns in order to prioritise responses.

An Interagency Approach:
The FCO, DCMS, the Home Office and the MoD all have useful inputs on assessing and dealing with hostile influence operations. None of them is the right body to be in charge. A permanent interagency group based in the Cabinet Office, on the lines of the American Reagan-era Active Measures Working Group, is needed. It should analyse *dezinformatsiya*, share its findings with government and other recipients, and co-ordinate and commission counter-measures.[2]

OFCOM 2.0:
No regulator oversees digital news sources. Nor does any single public agency deal with online harm and harassment (which do not only result from the actions of malevolent state actors). Such a statutory, apolitical body, aiming to gain wide public trust, is needed.

1 For example, in the wake of the attempted murders of Sergei and Yulia Skripal in Salisbury, Russian-backed trolls appear to have been influential, but as the situation in Syria unfolded, a large number of bots were activated.

2 Regardless of Brexit, this group should work especially closely with the East Stratcom team at the EU's External Action Service, which is under-resourced and faces potentially crippling political pressure.

Recommendations

2. Reform the Digital Rules

Developments in technology have outpaced regulations and norms. Russian activity is just the tip of iceberg: there is nothing to stop other actors from using the same techniques. Social media and other tech companies need reform and, if necessary, regulation. Options include:

A Social Media Code of Conduct:
These companies are not publishers, who take responsibility for material that they circulate, but neither are they a utility, or a neutral public forum; their algorithms affect what people see and read; they curate content by recommendation and on occasion prohibition. The government should start consultations with the companies, the public and other interested parties to draw up a non-statutory but consensus-based Code of Conduct. The aim would be to mitigate social harm of all kinds and to offer redress to victims of abuse. A by-product of this would be to reduce the impact of *dezinformatsiya* and any other hostile state-sponsored information attacks.

An Algorithm Ombudsman:
The automated selection of material on social media platforms radically affects news consumption, and can therefore hamper or promote *dezinformatsiya*. These algorithms—in effect computer programs based on secret formulae—are accountable to no one. Publishing them would be counterproductive as it would allow malevolent actors to "game" the system, tweaking their content to evade prohibitions or increase impact. An ombudsman could allow companies to keep their technology confidential, while ensuring some external oversight over the way that algorithms are developed and applied.

Transparent Political Advertising Online:
All such material should bear an "imprint" analogous to the mandatory requirement on real-world election material. This would make clear the publisher or sponsor, detail any personal data employed to target particular users and also show the full range of advertisements used by any particular campaign. (Alternatively, the government might consider banning political advertising from social media altogether, just as political advertising is banned on British television.)

Anonymity and identity assurance:
Hostile information campaigns on the internet are typically enabled by the anonymity of social media accounts and by websites with scanty or non-existent real-world credentials. Nonetheless, the right to pseudonymous and unidentifiable behaviour on the internet is precious and should be defended. It is particularly important for internet users in authoritarian countries.

But we currently lack other rights: to prove who we are, and to check who we are dealing with. The "blue tick" on Twitter helps users on that platform distinguish between degrees of realness (Facebook

Recommendations

has a similar scheme). But a more sophisticated system is needed, in which authentication is a right, not a privilege. The UK and other governments should encourage tech companies to develop robust, opt-in identity assurance schemes to promote trustful online interaction. It should also encourage browser developers to include plug-ins and extensions that help users navigate the internet with greater confidence.

Protect and Sanction:
Tech companies need to take more responsibility for helping victims of harassment and deterring malefactors of all kinds, while at the same time protecting honest criticism and robust speech. Dilemmas and trade-offs are inescapable here. But the first step is for social media platforms to accept their quasi-judicial role in curating speech and policing behaviour. These rules need to be publicly debated, transparently formulated and independently administered, while taking account of the internet's borderless nature. Creating this new branch of what is in effect a new branch of international private law will be a long process. The UK government can take the lead in starting it.

Cooperation with the analytical community:
Social media companies need to provide data to outsiders in order to measure the nature and extent of *dezinformatsiya*. Facebook has initiated such a development; Twitter already provides material to researchers through its API. But more work is needed.

Recommendations

3. The Response

Which Counter-measures Work?
Understanding of the the effectiveness of digital *dezinformatsiya* is limited. So too is evidence about counter-measures. Experiments include fact-checking, counter-narratives and investigative journalism. A concerted effort is needed to support long-term analysis, testing different approaches together with media and other communicators. A model for this could be the UK government's existing "What Works Network".[3]

Media Literacy:
This needs updating for the digital age, not only in the education system but for wider society, on the lines of public messaging about cyber-security.

Not Just (Dis)information:
The Kremlin's digital *dezinformatsiya* cannot be considered in isolation from its other subversive activities: cyber-attacks, corruption, covert funding for political parties and extremist organisations, the creation of economic and financial bridgeheads, subversion, the use of organised crime, physical intimidation, military sabre-rattling and so forth. Investigations and counter-measures will contribute to the needed full-spectrum, "whole of government" approach. Finland and the Czech Republic have outward-facing government bodies with specific responsibility for hybrid threats (Finland also hosts a separate, international Centre of Excellence on the same subject). Britain's experience in counter-terrorism and in cyber-security has provided useful precedents for new efforts dealing with hostile state activity. The government should consider declassifying some elements of this activity and encouraging co-operation with civil society, academic and other partners

3 https://www.gov.uk/guidance/what-works-network