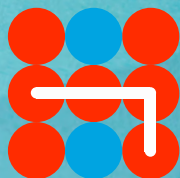


Hybrid CoE Paper 5

FEBRUARY 2021

Improving cooperation with social media companies to counter electoral interference

LINA ROSENSTEDT



Hybrid CoE

Hybrid CoE Paper 5

**Improving cooperation
with social media
companies to counter
electoral interference**

LINA ROSENSTEDT

February 2021

Hybrid CoE Papers include inspiration papers, conception papers, and the finalized outcomes of our seminars, workshops, exercises or other activities. In general, they reflect understandings of current unfolding events and trends, or personal views relating to the realm of hybrid threats.

The Hybrid Influence COI looks at how state and non-state actors conduct influence activities targeted at member states and institutions, as part of a hybrid campaign. The COI looks at how hostile state actors use their influence tools in manners that attempt to sow instability or curtail the sovereignty of other nations and independence of institutions. The focus is on both the behaviours, activities, and tools that a hostile actor use, rather than focusing exclusively on one actor at the expense of others. The goal of the community is to equip its practitioners with the tools they need to respond to and deter hybrid threats. The COI is led by the UK.

The European Centre of Excellence for Countering Hybrid Threats, tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-68-7
ISSN 2670-2053

February 2021

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

The responsibility for the views expressed rests ultimately with the authors.

CONTENT:

Introduction	5
Situational awareness	6
Increasing understanding	8
Engagement	9
Conclusion	10
References	12

Introduction

Hybrid threats are malign actions conducted by a state or non-state actor with the intention of influencing the target country's decision-making process. They are conducted using a wide range of means and are designed to remain below the threshold of both detection and attribution. Hybrid threats often exploit interfaces, such as the one between the public and private sector. This makes detection and an effective response difficult, increasing the need for cross-sectoral cooperation. Electoral interference, which is one such hybrid threat, exploits this interface between the public and private sector.¹

One way in which malign actors interfere in elections is through influence operations, defined by the Carnegie Endowment for International Peace as "coordinated efforts to influence a target audience using a range of illegitimate and deceptive means, in support of the objectives of an adversary". Influence operations use a wide range of means, which can include the use of mis- and disinformation but can also use truthful information, such as releasing material from an opportunistically timed hack and leak.²

Russian interference in the 2016 US presidential election highlighted the role of social media platforms in spreading influence operations.³ Consequently, effective cooperation between social media companies and governments is paramount in countering influence operations and electoral interference.

Many key actors have taken steps to counter the spread of influence operations on social media platforms. The EU's Democracy Action Plan, released in December 2020, sets out measures to counter disinformation by introducing a co-regulatory framework for online platforms. The Democracy Action Plan, in line with the EU's Digital Services Act, will be fully implemented by 2023.⁴ Introducing such a regulatory framework is an important action that will increase the accountability of online platforms. However, while initiatives such as the Democracy Action Plan will address existing challenges through regulation, the responsibility for resolving operational-level challenges associated with detecting influence op-

erations will continue to lie with individual states. To this end, governments need to continue to take action at the operational level to enable better cooperation with social media platforms.

Focusing on enabling better cooperation between governments and social media companies is important for several reasons. Firstly, the spread of influence operations can be challenging for governments to monitor as they combine a range of tactics to disguise their true intent, and occur on social media platforms into which governments have limited insight. Secondly, while social media companies improved their policies and practices to better tackle disinformation after the 2016 US election⁵, cooperation and information-sharing can still be improved. Developing new means of cooperation and improving the basic understanding of each other's processes will be mutually beneficial for both governments and social media companies. This paper focuses on practical measures that government practitioners can take to smooth cooperation with social media companies and duly counter the spread of influence operations on social media platforms

Over the past two years, Hybrid CoE has worked with both governments and social media platforms to define and develop best practices for cooperation between them. The actions listed below are drawn from this programme of work, comprising a summary of best practices that have been presented, discussed and refined in a series of events run by Hybrid CoE.

The report is divided into three time periods. First, 'over the horizon' actions that can be considered more than a year before an election. Second, medium-term actions that can be taken approximately one year beforehand. Third, actions that can be taken in the final stages of preparation, from about six months beforehand to election day itself and, where relevant, during the process of government formation.

This timeline reflects the different stages of preparing for elections, but as countries differ (for example in size of government, level of preparedness and resources available), the timings should be considered indicative rather than prescriptive.



Situational awareness

Establishing good situational awareness within government can enable easier collaboration with the private sector. Actions taken ahead of elections to baseline 'normal' activity are key in deciding when to contact social media companies with requests

+1 year before an election

1. Establishing a baseline of activity provides a strong basis for decision-making when encountering influence operations on social media. Setting a baseline for what constitutes a 'normal' day-to-day quantity of influence operations occurring on social media is a challenging task. Influence operations have become endemic, and not all operations can be prevented. Consequently, there will be some level of activity on social media regardless of the proximity of the election.

Setting a baseline means one has to monitor the information environment over a longer period of time to create a sense of what is a 'normal' degree of influence operations. Monitoring the information environment should be considered an everyday activity in government, and baselining should be conducted a long time in advance of the election to ensure that one has gained an accurate picture of the information environment.

Creating a baseline will help determine whether there has been an increase in influence operations on social media. It will assist in determining when to act and when to contact social media platforms to request the removal of content related to information operations. Further, when working with the social media platforms, it is important to include as much relevant evidence as possible, such as data showing rapid changes in the level of activity. Baselining is crucial in this respect as it provides a point of comparison.

While establishing a baseline is a difficult task, it cannot be neglected as it serves an important func-

tion in alerting government practitioners to unusual levels of activity. Establishing clear government points of contact, such as a government fusion cell working on elections, can greatly simplify and streamline communications between government and social media companies.

tion in alerting government practitioners to unusual levels of activity. The RESIST counter-disinformation toolkit, developed by the UK government communication service, offers practical guidance to support baselining.⁶

2. Creating good open source intelligence (OSINT) capabilities within government can improve information-sharing both within government and with social media companies.

Depending on platform restrictions, good open source intelligence capabilities can help reduce governments' dependency on information from social media companies, enabling them to respond faster to a developing information operation. Further, sharing confidential intelligence horizontally within government can be difficult. Open source material is easier to share both within government and with private sector representatives.

One should consider whether practitioners who do not normally work with OSINT analysis can be trained in basic-level OSINT tradecraft to enable independent further analysis when encountering a possible influence operation. This reduces the dependency and the demands on a separate OSINT team. There is a wide range of OSINT tools available.⁷ Speaking to a peer nation can be beneficial for gaining an understanding of which OSINT tools peers have found useful. When planning for the use of OSINT material, one should be aware of the fact that many countries have laws restricting the government's use of open source intelligence.

1 year before an election

3. Creating a 'fusion cell' or 'task force' can support the sharing of information within government. The team should focus primarily on monitoring the social media environment ahead of and during the election. One should think laterally about fusion cell membership and consider including practitioners that don't come from typical security ministries and that can put forward a variety of views within the team. Typically, fusion cells consist of members of the country's computer emergency response (CERT) team, strategic communicators, OSINT analysts, members of the intelligence community, foreign ministry personnel, and staff drawn from the authority in charge of holding the election.

6 months and closer to election day

4. Connecting with government colleagues monitoring different parts of social media can provide new insights. Non-security-related ministries like the Ministry of Education might monitor social media on a daily basis. These ministries may be well-rounded in working with social media, the social media companies, or have new insights into the topic. One should consider educating colleagues on influence operations, creating joint warning mechanisms, as well as appointing points of contact to be used in case colleagues from non-security-related ministries encounter behaviour that seems suspicious.



Increasing understanding

Influence operations on social media platforms are a difficult and technical topic. Conducting exercises with the private sector, gaining an understanding of the policies guiding social media

platforms⁸, and familiarizing decision-makers with the threat and the role of social media companies will prepare a government to respond more efficiently.

+ 1 year before an election

5. Conducting exercises with the private sector can serve as an opportunity to practise responses.

Exercises in which the private sector is present as a player have proved to be valuable opportunities to practise responding to an information operation. Many exercises in which the private sector participates are hosted by international actors such as Hybrid CoE. The exercises present an opportunity to familiarize oneself with the way in which other organizations, such as social media platforms, work and also provide a useful forum for asking questions and engaging with the private sector.

6. Mapping themes dividing the electorate is best performed by connecting with colleagues in and outside of government.

For government practitioners, staying informed about and aware of the main adversaries that may try to interfere in an election is key. Societally divisive themes have previously been used in influence operations⁹ because themes such as immigration, for example, tend to create aggression and heated debates. Divisive themes vary from country to country. Consulting other practitioners, peer nations, researchers and members of civil society about actors and themes that may be of relevance in the upcoming election can be beneficial. Seeking a variety of views can help to ensure that relevant actors and themes are monitored.

1 year before an election

7. Studying the thresholds and definitions that social media companies are using enables 'gaps' to be identified and monitored.

Social media companies use a range of definitions to characterize the threat related to influence operations. Many companies share these characterizations online. It is beneficial to read them and educate oneself on how the companies decide what to remove from their platforms. It is probable that the characterization of what is acceptable will differ to a greater or lesser extent from the characterization used by government. One should consider whether this causes 'gaps' between the two characterizations that should be monitored.

8. Sensitizing decision-makers, journalists, political candidates and parties to the risks that influence operations pose can make the escalation process easier.

Influence operations conducted using social media platforms can be a technical topic that is challenging to fully comprehend. Training key stakeholders on the threat, as well as the tools and strategies to counter it, makes addressing an influence operation in a timely fashion easier.



Engagement

Building relationships ahead of an election enables a better understanding of the current trends and tactics in influence operations. Building mutual trust among stakeholders is an important aspect of engagement as it lays the foundation for further cooperation.

Many countries are part of a range of initiatives aimed at countering the threat of influence

operations. Ahead of an election, it is helpful to utilize these partnerships to learn from and engage with both the private sector and peer nations. Six months before an election, it is worth conducting a final check, ensuring that all relevant stakeholders have the necessary contact details.

1 year before an election

9. Mapping multilateral cooperation mechanisms can provide links to relevant colleagues and useful insights into best practices.

Many countries are a part of various multilateral cooperation mechanisms aimed at countering the threat of election interference, disinformation and/or influence operations. Some cooperation mechanisms study the latest trends related to electoral interference, while others, such as the EU's rapid alert system (RAS)¹⁰ established in March 2019, focus on enabling joint situational awareness and facilitating a joint response.

Often, the mechanisms have links to the private sector and may serve as useful routes to reach the social media platforms. Many countries take part in numerous different initiatives, and engagement is often led by the Ministry for Foreign Affairs (or equivalent). A possible mapping of cooperation mechanisms should preferably take place prior to the most intense time related to elections.

10. Gathering best practices from peer states can support understanding of the latest trends in influence operations.

Peer states that have recently held elections can have valuable experiences and best practices to share. It is possible that peer states will have witnessed new trends or tactics worth being aware of when preparing for elections.

6 months and closer to election day

11. Being aware of various escalation channels can facilitate communications.

Ahead of an election, some multilateral organizations have created centralized escalation channels through which social media companies can be contacted. These serve as a channel for all support requests sent by countries to social media platforms so they can take down disinformation or influence operations that are interlinked, and prioritize requests.

Government practitioners have not always been aware of these escalation channels, which consequently risk remaining unused elections. Checking which escalation channels a particular country has access to and educating colleagues within government on these may prove useful. In many governments, foreign ministries will serve as points of contact for the escalation channels that are in place in multilateral organizations.

12. Ensuring that colleagues have the right contact details ahead of an election can prove to be important if an influence operation is detected.

Verifying that contact details for relevant government departments and teams are readily available for the private sector is important. If companies trying to get in touch with a government are redirected within the government system, it will take valuable time away from dealing with the crisis and may prevent a timely response.

Conclusion

Social media companies have become a permanent part of the information environment, and governments should consider taking measures to further improve cooperation with them, particularly to counter electoral interference.

Enhancing **situational awareness** within government by creating clear government structures enables both a faster response and an improved exchange of information. **Increasing understanding within** key stakeholders within government on the threat of influence operations on social media platforms, as well as enhancing broader awareness in government, enables both early detection and a rapid response. **Engaging** with the private sector is important both for understanding their work and for connecting with relevant counterparts.




The actions listed in this report will enable swifter detection of information operations and a more comprehensive response by improving both the exchange of information and the cooperation with the private sector.

Hybrid CoE's work to safeguard democratic processes

During the course of 2019 and 2020, the Community of Interest on Hybrid Influencing (COI HI) ran a project focused on countering electoral interference¹ in Hybrid CoE Participating States. During this work, COI HI hosted meetings, conferences and exercises with participants from Participating State governments, private sector companies and academia. The work focused on finding practical solutions to safeguard democratic processes in Hybrid CoE Participating States. In these events and meetings, new solutions, ideas and creative ways of approaching the problem of electoral interference were presented by the social media companies themselves, by Hybrid CoE Participating State practitioners, and by researchers working on the topic. This paper is a synthesis of the key points that emerged from this substantial body of work.

Hybrid CoE's safeguarding democratic processes project will continue in 2021 and further work will be published at www.hybridcoe.fi.

¹ A significant part of this work has been funded by the US Department of State's Global Engagement Center (GEC) through a grant of 500,000 USD received by Hybrid CoE in 2018. The grant was used to cover the United States Hybrid CoE participation fee for 2018 and 2019.

	1+	1 year ahead of elections	6 months and closer
Situational awareness 	<ul style="list-style-type: none"> Establishing a baseline of activity Creating OSINT-capabilities within government 	<ul style="list-style-type: none"> Creating a 'fusion-cell' or 'task force' within government 	<ul style="list-style-type: none"> Connecting with government colleagues
Increasing understanding 	<ul style="list-style-type: none"> Conducting exercises with private sector Mapping divisive themes 	<ul style="list-style-type: none"> Studying thresholds and definitions Sensitizing stakeholders to the risks that influence operations pose 	
Engagement 		<ul style="list-style-type: none"> Mapping multilateral cooperation mechanisms Gathering best practices from peer states 	<ul style="list-style-type: none"> Being aware of various escalation channels Ensuring that colleagues have the right contact details

References

¹ The European Centre of Excellence for Countering Hybrid Threats, 'Hybrid Threats as a Concept', <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.

² Carnegie Endowment for International Peace, 'The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework', James Pamment, 24 September, 2020, <https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720>.

³ Select Committee on Intelligence, United States Senate, 'Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views', https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling online disinformation: a European Approach', 26 April, 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN>.

⁴ European Commission, 'European Democracy Action Plan: making EU democracies stronger', 3 December, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250.

⁵ OSCE, 'International Election Observation Mission United States of America – General Elections, 3 November, 2020, Statement of Preliminary Findings and Conclusions', 4 November, 2020, <https://www.osce.org/files/f/documents/9/6/469437.pdf>.

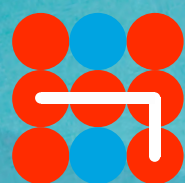
⁶ Government Communication Service, 'RESIST. Counter-disinformation toolkit', 10 November, 2020, <https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/>.

⁷ Information on various OSINT tools is available online. Bellingcat, among others, posts detailed descriptions of tools and methods on its website. They can be found at: <https://www.bellingcat.com/>.

⁸ The policies of some of the largest social media platforms can be found at: YouTube, 'Community Guidelines', <https://www.youtube.com/howyoutubeworks/policies/community-guidelines/>; Twitter, 'Platform Manipulation and Spam Policy', September 2020, <https://help.twitter.com/en/rules-and-policies/platform-manipulation>; Facebook, 'Community Standards', https://www.facebook.com/communitystandards/inauthentic_behavior.

⁹ Select Committee on Intelligence, United States Senate, 'Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views' https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

¹⁰ European Parliament, 'Foreign interference in democracies. Understanding the threat, and evolving responses', Naja Bentzen, September 2020, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652082/EPRS_BRI\(2020\)652082_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652082/EPRS_BRI(2020)652082_EN.pdf).



Hybrid CoE