

INVESTIGATING AND UNCOVERING COORDINATED INAUTHENTIC BEHAVIOR

A practical toolkit



INVESTIGATING AND UNCOVERING COORDINATED INAUTHENTIC BEHAVIOR

A practical toolkit



INVESTIGATING AND UNCOVERING COORDINATED INAUTHENTIC BEHAVIOR

A practical toolkit

PUBLISHER:

Centre for Monitoring and Research (CeMI)

Bul. Sv. Petar Cetinjski 96

e-mail: info@cemi.org.me

www.cemi.org.me

EDITOR:

Teodora Gilic

AUTHOR:

Milica Zrnovic



This Toolkit was published as part of the Facebook Online Monitoring Follow-On Project implemented by the Centre for Monitoring and Research (CeMI), in collaboration with the International Foundation for Electoral Systems (IFES).

The content of the Toolkit is the sole responsibility of CeMI and should not in any way be interpreted as an official position of IFES.

CONTENT

INTRODUCTION	8
1. APPROACH TO INVESTIGATING COORDINATED INAUTHENTIC BEHAVIOR	11
1.1. MAPPING NETWORK	14
1.2. IDENTIFYING CONTENT	20
1.3. TRACKING BEHAVIOR	23
1.4. REPORTING	25
1.4.1. DATA VISUALIZATION	27
2. LIMITATIONS	30
3. NEW IDEAS AND APPROACHES	32
4. LESSONS LEARNED, TOOLS, AND TEMPLATES	34
TOOL 1	35
TOOL 2	37
TOOL 3	38
TOOL 4	39
TOOL 5	40

This toolkit introduces the Centre for Monitoring and Research's (CeMI) methodological approach to investigating online Coordinated Inauthentic Behavior (CIB) and provides instruction to emulate such an approach for prospective monitors and CSOs with low or no programming knowledge and access to CrowdTangle. Toolkit introduces valuable techniques for practitioners to leverage when investigating Coordinated Inauthentic Behavior specifically seeking to influence elections and the electoral process; though, such techniques may also be used when investigating CIB more broadly.

This toolkit has been developed as a continuation of CeMI's pilot investigation in 2021 in the lead up to the Montenegrin 2020 Parliamentary Elections. As part of this pilot initiative, CeMI developed the original methodology and leveraged this approach to identify potential Abuses of State Resources, Coordinated Inauthentic Behavior, and Campaign Violations during the electoral period. While the approach has considered social media monitoring from the standpoint of civil society organization, the insights are applicable to anyone who is monitoring social media and deceptive behaviors during elections and evaluating its effect on politics.

Monitors will learn how to set up a monitoring approach via the CrowdTangle platform, investigate suspicious content, collect, and analyze social media data, report research findings, and avoid common monitoring pitfalls relevant to investigating CIB. Toolkit also includes numerous tools, templates, methods, and other practical tips that may facilitate investigation efforts and identify key areas for possible further expansion of the monitoring methodology.



IN THIS TOOLKIT YOU WILL FIND:

- » Approach to investigate Coordinated Inauthentic Behavior on social media with detailed steps
 - » Possible limitations of the research
 - » New ideas and approaches
 - » Practical tools and templates that monitors may use
-

INTRODUCTION

Social media and online networks have become critical tools for organizing both online and offline social movements due to their capacity to rapidly disseminate information and facilitate collective action.¹ In recent years, however, social media has also played a crucial part in organizing online disinformation campaigns. Such campaigns have often sought to exploit existing societal divisions, influence elections, and, sow confusion on topics of high importance, including more recently regarding the Covid-19 pandemic.² It is obvious that, in the online environment, coordinated networks and behavior of social media activists can facilitate the pursuit of communication goals.³

Disinformation campaigns may be further classified by their authenticity. Some coordination on social media, even coordination of a disinformation campaign, is organized by networks of authentic actors, real users or pages organically sharing information. Thus, it is important to distinguish behaviors that occur organically in digital space from the coordinated types of behavior which are organized and manifested in a deceptive way.

Though both authentic and deceptively manufactured coordination have the possibility to cause harm, authenticity is a factor some social media companies use to regulate content. Recognizing the importance of social networks when it comes to communication and interaction, Meta (formerly Facebook) maintains a set of Community Standards that outline what is and is not allowed on their platforms, including Facebook and Instagram. This policy is intended to protect the security of user accounts and Meta services, and create a space where people can trust the people and communities they interact with.

In line with Meta's commitment to authenticity, users are recommended not to engage in or claim to engage in inauthentic behavior (IB), defined as the use of Facebook or Instagram assets (accounts, Pages, Groups, or Events), to mislead people or Facebook:

- » About the identity, purpose, or origin of the entity that they represent.
- » About the popularity of Facebook or Instagram content or assets.
- » About the purpose of an audience or community.
- » About the source or origin of content.
- » To evade enforcement under Community Standards.

Likewise, users are recommended not to engage in, or claim to engage in Coordinated Inauthentic Behavior.

¹ Earl, J., *The dynamics of protest-related diffusion on the web*, *Information, Communication & Society*, 13:2, 209–225, 2010, DOI: 10.1080/13691180902934170

² *Idem*

³ Giglietto, F., Righetti, N., Marino, G., *Understanding Coordinated and Inauthentic Link Sharing Behavior on Facebook in the Run-up to 2018 General Election and 2019 European Election in Italy*, LaRiCA - University of Urbino Carlo Bo, 2019



DEFINITION

Coordinated Inauthentic Behavior (CIB) is defined as the use of multiple Facebook or Instagram assets, working in concert to engage in Inauthentic Behavior, where the use of fake accounts is central to the operation.⁴

Besides the definition provided by the social media platforms, there is no authoritative definition of what CIB is, but what's clear is that, while social media companies improve user's protection policies, the people behind CIB — whether economically or politically motivated — change their tactics and improve, too.⁵ They are well-funded and have every incentive to continue their efforts, even if some of their actions have very little impact.⁶

Social media policies regarding coordinated and inauthentic behavior are generally flexibly interpreted and inconsistently enforced by the platforms themselves, and social media companies have their own internal mechanism to regulate this kind of behavior, while national legislation and regulation mechanisms in this field are lacking. Meta's enforcement record suggests that reported CIB networks may not cross the indistinct threshold that would qualify them as coordinated inauthentic behavior, and thus no corrective actions are taken.

When monitoring social media it is important to mention that inauthentic behavior and coordinated inauthentic behavior are interrelated concepts. Both terms refer to an effort to mislead people or Facebook and Instagram about the popularity of content, the purpose of a community (i.e. Groups, Pages, Events), or the identity of the people or organization behind it. Due to the misleading and inauthentic components of the behaviors, centered around amplifying and increasing the distribution of content, neither of them is allowed based on Community Standards.

When monitoring CIB, there are two tiers of activities to differentiate: 1) coordinated inauthentic behavior in the context of domestic, non-state campaigns (CIB); and 2) coordinated inauthentic behavior on behalf of a foreign or government actor (FGI).⁷ Foreign or Government Interference (FGI) includes two groups of behavior: 1) foreign-led efforts to manipulate public debate in another country; and 2) operations run by a government to target its own citizens. These can be particularly concerning when they combine deceptive techniques with the real-world power of a state.⁸

While CIB may include financially motivated activities, whether foreign or domestic, state or non-state, investigating and searching for evidence of CIB may reveal networks run for a variety of different reasons or motivations, which may not be distinguishable from the outside. In order to effectively distinguish other behaviors from CIB, in continuation, a quick explanation on what CIB is and is not is presented, through three main characteristics.

⁴ Meta Transparency Center, Facebook Community Standards, Inauthentic Behavior

⁵ Gleicher, N., Rodriguez, O., *Removing Additional Inauthentic Activity from Facebook*, Facebook, 2018

⁶ Gleicher, N., *Inside Feed Coordinated Inauthentic Behavior*, Facebook, 2018

⁷ *Idem*

⁸ How We Respond to Inauthentic Behavior on Our Platforms: Policy Update, Facebook, October 2019

COORDINATED INAUTHENTIC BEHAVIOR

IS		IS NOT	
Type of behavior	Description	Type of behavior	Description
Organized behavior	Actions <i>in coordination</i> with multiple entities, for example: a network of accounts that conceal their relationships with one another sharing similar, if not identical content, within short periods of time	Organic engagement	Random, uncoordinated post sharing by multiple different entities within a short period of time. Note: suspicious content may be shared organically, mere sharing of suspicious content does not always constitute CIB
Misleading/ Deceptive behavior	CIB entities usually share/create content with the aim of spreading misleading information, hate speech, disinformation campaigns, and influence operations. The purpose behind the manifested behavior is the key.	Sharing inauthentic content	Facebook entities may share content that is manipulated or misleading. This may happen when accounts share content while unaware that it is incorrect or otherwise problematic. The key to distinguish CIB from other online behavior is the purpose behind it.
Fake accounts	CIB network includes the presence of fake accounts. These types of accounts are identified by having generalized profile/cover picture, suspicious connections or likes, empty or suspicious "About" section, a suspicious external domain connected to the profile, etc.	Superficial online identity	Sometimes users are not willing to post their profile picture or share personal data on Facebook. This is not a reason to automatically conclude that the account is fake.



1. APPROACH TO INVESTIGATING COORDINATED INAUTHENTIC BEHAVIOR

The social media investigation methodology presented in this toolkit builds on methodology previously developed and implemented by the Centre for Monitoring and Research (CeMI), in collaboration with the International Foundation for Electoral Systems (IFES). This methodology presents one approach to monitoring CIB but can be augmented or adapted to align with complementary approaches.

The main tool that is used for the implementation of the methodology is CrowdTangle, a platform allowing researchers to access public data available on Facebook, Instagram and Reddit⁹. For the purposes of monitoring CIB during elections, CeMI used additional features, e.g. CrowdTangle Link Checker, Ad Library, and Page Transparency data. CT Link Checker is a simple browser plug-in for Google Chrome that can help monitors to see which social media accounts on Facebook, Twitter, Reddit, and Instagram are sharing a piece of content. Ad Library offers insights into a Page's paid advertisements, and Page Transparency data¹⁰ provides insights into the history and administrators of specific Pages and Groups.

Though these tools allow for access to data across various platforms, this approach to investigating CIB focuses on the behavior of actors on Facebook, and identifying violations of Facebook Community Standards where they take place.¹¹ This approach may also be applicable when monitoring behavior of other social media platforms available through CrowdTangle, specifically Instagram and Reddit.

Especially, this approach to investigating CIB focuses on monitoring the behavior of suspicious Facebook pages, accounts, and groups potentially engaged in deceptive and manipulative behavior, as well as their connection with the political parties, politicians, and media outlets during the electoral period.

The approach consists of four main phases: mapping network, identifying content, tracking behavior, and reporting.

When mapping network, the monitor focuses on understanding and identifying **who** are the actors engaging as part of the network as well as what is **the source** of the content shared. This phase consists of pinpointing the entities engaged in CIB through the analysis of established technical signatures unique to a network.

Identifying content implies the process of determining the type of content that is repeatedly shared in a predictable manner within the network. In other words, it focuses on ascertaining **what** type of **content** the network is amplifying and distributing, and whether it violates Community Standards (hate speech, incites violence, misleading information, etc.).

The third phase consists of tracing coordination in the behavior of the network or better tracking link-sharing **behavior** and connecting entities of the network through analyzing their activity on Facebook.

Last, but not least important phase is reporting which implies analyzing and presenting data and findings collected through monitoring period, as well as estimates of the impact the identified content and behavior could have on the overall electoral process and voters' rights.

Above mentioned phases are conducted iteratively as each later phase builds on the previous one and might reveal new actors whose behavior can then be investigated as well.

⁹ It is important to mention that CrowdTangle can be accessed only with a license provided by Facebook.

¹⁰ Page Transparency data is available either on the profile or through CrowdTangle.

¹¹ Researches show that in many countries, Facebook is the leading social network. See: <https://vincos.it/world-map-of-social-networks/>. Also, researches show that 76,47% of world population is using Facebook. See: <https://gs.statcounter.com/social-media-stats>.

Graph 1: Coordinated Inauthentic Behavior monitoring steps



01

Mapping Network



This phase consists of the initial discovery and identification of suspicious entities potentially engaged in a CIB network.

As an initial step in monitoring, different media content related to politics and elections should be investigated. If monitors come across a suspicious piece of content, for example an article from an online news source that appears to be false, misleading or incites hate, monitors may investigate which accounts are sharing that same piece of content by using CT Link Checker. Once monitors identify a piece of false content, it is important to investigate the following:

1. Who else shared it
2. Are they themselves suspicious
3. Start testing for authenticity

This can give monitors a sense of a network of actors that are working together to share problematic content and also identify other Pages, Groups or accounts that might be problematic or suspicious.

Next, monitors should assess the authenticity of identified Pages, Groups or the individual accounts that administer those Pages or Groups. This step is one of the most important when detecting CIB as the inauthenticity represents a constitutive pillar of the CIB policy.

In practice, this is done by finding technical signatures (signals) that, collectively, create a credible suspicion that the accounts are engaging in prohibited behavior. Taken alone, any of these signals are not in and of themselves sufficient to conclude that CIB is taking place. However, when multiple signals are present, researchers can increase their confidence that prohibited behavior is taking place.

Example Box

When cemi identified a page or group that wished to more actively monitor of further investigate, they would add it to a crowdtangle lists created based on page category. Tool 1 contains technical details and exact steps on how to create lists in the dashboard for the purposes of social media monitoring.

Suspicious signals:

Type of suspicious signal	How to search for it	Example
Suspicious spikes in follower counts	CrowdTangle Intelligence	Increase in number of page followers in the identified network may be a valid signal in particular if it occurs in the timeframe that coincides with the elections. For example, if the page was newly created and the number of followers increased drastically in a short period of time and disproportionately to the page activity, it raises concerns about authenticity of its audience and potential fake support to the page.
Similar account creation date	Page Transparency Data	If some of the identified suspicious pages have been created on the same date or during a short period of time, it represents a valid signal for suspicion. Additionally, it is relevant to note if creation of these pages preceded the electoral period or happened around some important politically motivated event.
Inauthentic name behavior	Page Transparency Data	In case pages within the identified network changed their name in a short period of time, in particular around some political events, this could be a relevant clue as well. A drastic change, such as a comedy account taking on a political nature would be a highly suspicious signal, however the change may not always be a drastic modification. The political and social context of the country where the network was identified may reveal that a name change from Latin to Cyrillic font, for example, is significant.
Inauthentic or similar profile and cover photos	Profile	<p>It may be useful for monitors to check profiles of members and followers that cross-post or comment frequently in the suspicious pages/groups. It does not include checking all of the members' profiles but only those that appear frequently. In this way monitors may investigate if fake profiles are amplifying certain type of content, e.g. politics related content.</p> <p>If the monitor notices lots of profiles with very similar profile or cover photos – like they all have flowers, or they all have a cartoon that looks like it was generated by the same website, it is important to keep track of that sort of coordination, e.g. "profile photo black and white cartoon" or "cover photo with political symbols" in form of an Excel file or Word table, as preferred, where this data will be stored.</p> <p>Monitors should be careful to not imply that just because a profile photo is an impersonal image that the account is fake. There are reasons why real people would want to not have their photo on social media.</p>
Page account category	Page Transparency Data	An important aspect of CIB is misleading behavior that can be manifested through page categorization. For example, if page categorized itself as "art", "fun", "satire", "entertainment", and then posts content only about politics or elections, this may be a valid signal for further investigation suggesting that these page are misleading users about who they are and what is the purpose of their activity.

Some accounts already appear in previous fact-checking archives	Fact-checking archives, Desk research, Search engines	<p>Although the investigation of CIB's is not focused on fact-checking, monitors should track discrediting and disinformation campaigns happening during elections. This is important in particular when names of certain individuals or pages engaged in the identified network may have appeared before, not only in fact-checking archives but also in other places. For example, during the monitoring CeMI found a research paper that lists pro-Russian media outlets that are source of disinformation. This helped the research as some of the media appeared engaged in the CIB network and lot of pages and groups were connected to them and shared their content.¹² Other sources of information such as different CSOs projects/researches may be quite interesting and useful for the investigation as monitors may come across some personalities/media which are already flagged.¹³</p> <p>Likewise, a person involved in deceptive behavior may have been legally sanctioned before for similar activity. This information may appear in the media. Monitors may not have access to the police files to know how exactly they were sanctioned, but may come across news and media articles stating that certain personalities were taken into custody and interrogated for spreading panic and disinformation online, in particular during electoral period.</p> <p>Also, a monitored page may be deleted from Facebook during the research and afterwards a new one may be created with the similar name, same profile, and cover picture. It is important to collect data regularly so that monitors, in case of deletion of some pages or other unexpected occurrences, have data to analyze and compare.</p>
Connections with suspicious external domains, already flagged domains or accounts	Page Profile	Some pages may be linked to external domains that have been flagged before as suspicious by other monitors, media outlets or researchers. Sometimes links may lead to domains that do not exist which raises concerns. This is a valid signal questioning the authenticity of these pages and accuracy of the content they share. For instance, monitors may find out that various pages are connected to the same external domain flagged as a fraud. Usually, different media outlets, investigative journalists or researchers may flag certain domains/web sites or address the exact issue that occur in their country. Thus, it is important for monitors to continue investigation after they find that some Facebook pages are linked to the external domains/websites that are not trustworthy.
Suspicious external domain registration data	External Domain	By using online tools that provide more details about internet domains, monitors may investigate further suspicious external domains through getting data about registration date, owner, location, etc. For example, monitors may find out that the owner of the various suspicious domains is the same. ¹⁴

¹² See example: <https://medium.com/dfrlab/pro-kremlin-media-spins-story-of-u-s-military-transporting-covid-19-test-swabs-from-italy-548b98c0435d>

¹³ See example: <https://dossier.center/>

¹⁴ For example, tools such as Whois History or ICANN Lookup.

Same group admins and members	Page Transparency Data	Another signal that can be useful in proving coordination are managers of the pages. Through their investigation, monitors may find out that various pages have the same admins. By going further in the research, checking out admins' profiles or going through public groups' discussions, monitors may note that same person is admin of more than one page/group. It is also important to note if admins are located in or outside of the country where the monitoring is conducted, which suggests and may give some clues of the existence of foreign influence operations.
Similar languages the content is spread in, region-specific phrases or colloquial language	Page Profile	It is important to note if identified pages use the same language, i.e. phrases, when posting content. This may be a relevant signal in particular in cases of hate speech and harassment manifested by using dehumanizing and discrediting words or names to refer to a certain person or group of persons.

For the network mapping process to be precise and clear, it is advisable to develop a set of criteria for attributing encountered entities to the CIB network. If an entity fulfills at least some of the criteria, it shall be attributed to the network. Monitors may decide to continue monitoring Pages and Groups that may be borderline by adding them to CrowdTangle list specifically for this purpose. The above table – list of signals – is not intended to be exhaustive. There are other criteria that may need to be considered depending on the type of research and methodology.

If initial signature discovery research provides sufficient starting points for further analysis, monitors can utilize other datasets to map external key actors associated with identified networks. For example, if identified accounts are connected to some external domain, its registration data and ownership may be useful for further investigation. This is important in case of influence operations, when a foreign government or a private firm is part of the CIB network, and they will need infrastructure that creates a footprint that can be used to not only identify a current CIB effort, but also identify future efforts or parallel, previously-unknown efforts.

When collecting data about inauthenticity of the network, it is necessary to look at profile and cover photos, "About" information provided, friends and followers, as well as linked pages or domains connected with. Monitors may use Tool 4 – case template when

Example Box

To identify if a page or group is linked to the external domain/website it is advisable to look at entity's profiles and "about" section.

When identified such pages, cemi used whois and icann lookup tools to check registration and ownership data. The icann registration data lookup tool gives monitors the ability to look up the current registration data while the whois history provides a domain names or a domain ownership history. It consists of the list of the domain's past owners, their address and contact information, and other registration details. With this data monitors may track is suspicious or even politicaly-related personalities are behind those domains.

identifying how many accounts of the CIB network are fake. Data about page activity may be used as inauthentic metrics, i.e. to assess further the level of inauthenticity of entities engaged. For instance, posts having more shares than views, accounts having too many or too few followers compared to their activities or nature, sudden spikes or drop of metrics, such as likes, followers, may be signals of inauthenticity.

To facilitate the process of mapping networks, as previously mentioned, an extension such as CrowdTangle Link Checker can be useful, only for pages and groups. After the identification of a few entities, it is advisable to create a list and add those Pages and Groups in the dashboard on CrowdTangle platform to continue investigation. Tool 1 contains technical details and exact steps on how to create lists in the dashboard for the purposes of monitoring.

Additional tools such as Ad Library features, and external domain websites, i.e. online tools that allow access and lookup to domain ownership history, can be used¹⁵. In the table below, datasets that can be extracted from each of these tools are presented.

Table: *Tools and datasets*

Crowd Tangle <ul style="list-style-type: none"> - Account activity - Number of followers / likes - Type of content - Interactions / reactions 	CT Link Checker <ul style="list-style-type: none"> - List of all entities that shared certain link URL - Access to those posts 	Page Transparency Data <ul style="list-style-type: none"> - Account transparency - Creation date - Name change date - Category - Number of admins - Admin location 	Domain <ul style="list-style-type: none"> - Domain creation data - Owner of domain - Owner location - Other domains connected
Ad Library <ul style="list-style-type: none"> - Any ads run by a specific Page - Basic information about those ads, including date that the ad run, and an estimate of how much was paid for the ad, how many impressions the content received, basic data on how the ad was targeted based on age, gender and geography. 			

¹⁵ Tool such as Whois History or ICANN Lookup

Practical tips

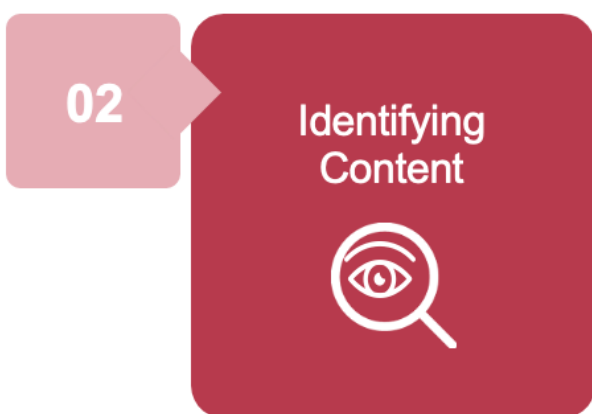
CeMI's first step in discovering and identifying suspicious networks was to monitor media articles related to the politics and elections. By using the **CrowdTangle Link Checker** monitors checked which social media accounts were sharing one specific article. Monitors paid attention to the media outlets already flagged as a source of fake news, disinformation propaganda, foreign influence operations or similar.

At this point, any article may be the initial one. The essence is to look up for pages/groups that repeatedly share politics related articles.

When checking entities that shared those articles, monitors further looked for users they interacted the most, other content they posted, in order to investigate if other entities are engaged as well. This was done by checking their profiles, news feed, etc. Reading comments and public discussions in the suspicious groups/pages is a must. Monitors identified several same profiles appearing, commenting, and cross-posting in different groups and pages.

To keep track of those profiles, monitors may create Excel document with few columns, e.g. profiles name, URL link, and suspicious page/group they appear within. Optionally, those few columns may be integrated to the abovementioned Excel file containing profile inauthenticity data (see the table of suspicious signals). In this way, it is easier to trace cross-posting and inauthenticity of the network.

After identifying a certain number of entities, CeMI monitors created lists on **CT platform** and continued the process of monitoring content and their behavior.



After the identification of the entities potentially engaged in the CIB network it is important to secure the continuous monitoring in order to determine the type of content that's being shared among the network. Identifying content implies the process of determining narratives and themes of the content used to communicate with the audience. This phase is important as CIB network is centered around amplifying and increasing the distribution of content. For example, by looking at the profiles of the identified entities from the previous phase, monitors may see what other problematic content is being shared by these accounts.

Creating list of entities (Phase 1) in itself is not enough to prove the CIB network. Monitors need to continue investigating, building the case by analyzing the content, and collecting evidences of different violations online (e.g. Facebook Community Standards, national legislation, etc.). This phase gives monitors space to gather data and prove violations over time.

Identifying content should include, but not be limited to monitoring:

- » How frequently entities are posting on social media?
- » What type of content do they usually use? Video, photo, live?
- » What type of content users interact most with?
- » Is the content violating Community Standards or national laws?

Monitors should assess which type of narrative identified entities are trying to push and promote. Monitors should assess the presence and spread of hate speech and incitement to violence, intolerant rhetoric (towards minorities, women in politics, LGBT, migrants, etc.), manipulative content, and political messages. It is important to continue monitoring for specific signals as mentioned in prior section.

Monitors should focus on reviewing paid ads that suspicious accounts may have on social media. It is relevant to assess whether an advertisement is related to politics or elections, and whether ad disclaimer is transparent in a way that it is easy to track who is behind it, i.e. who finances it. The focus is on determining whether non-political Facebook entities engaged in the CIB network are having paid ads about social issues, elections or politics, but are running without disclaimer. This represents not only the violation of Facebook advertisement policy, but open space for the national authorities to discuss

online campaign financing and how it could be monitored. In some cases, disclaimer may be on the name a certain private company that has political affiliation, which can also be useful evidence for monitors in their investigation.

Depending on the scope of the research that is being conducted, as well as the size of the identified network, when identifying patterns of CIB network, it is advisable to monitor lists of suspicious pages and groups, in parallel with the lists of media outlets, political parties, and politicians. The goal of monitoring parties and politicians is to investigate if non-political Facebook actors are sharing campaign materials or conducting political propaganda in favor of certain candidate/party, which may lead to discovering potential political motivation behind the CIB. Although users do have freedom of expression and freedom to show support to any political belief they stand for online, it is important to distinguish it from the organized influence operations aimed at impacting public opinion and voters rights.

It is advisable to monitor content on a regular basis. Depending on the scope and aim of the monitoring and the research that's being conducted, regularity can vary from daily to weekly basis. When collecting data about network's content, it is advisable that monitors to collect data in form of screenshots or to use Tool 2 for saving posts on CrowdTangle.

Practical tips

At this stage of monitoring, CeMI focused on discovering patterns of network's behavior and documenting cases of deceptive behavior. This process was realized by monitoring pages' post activity and regularly saving suspicious posts in CT platform or in a form of screenshots. Posts and screenshots were stored in folder and were inserted in the Final report, as well as in the report delivered to Facebook regarding the discovered CIB.

CeMI evaluated pages' behavior based on established **Facebook Community Standards**. Although there are 25 standards of behavior regarding what is and what is not allowed on Facebook, CeMI's emphasis was on spread of hate speech and incitement of violence, in accordance with its research.

In continuation, some examples of spread of misleading information, hate speech and cases of incitement of violence documented by CeMI are presented.



03

Tracking Behavior



Once the phases of mapping network and identifying content are concluded, the process of tracking coordination follows. This phase consists of tracing link-sharing behavior within the network. Link-sharing behavior may reveal actual density and extent of the network, thus it may show additional entities engaged that were not discovered in the previous phases. Tracking behavior in this sense means linking and connecting entities of the network through activity tracking.

With this regard, it is important to monitor time of posting content or copy-pasting the same content. Monitors should assess if identified accounts are posting the same content or messages at the same time or within a very short timeframe. The coordination in this sense refers to the organized activities planned in advance with the aim to manipulate and influence users.

Although this can be done manually by analyzing each post separately, monitors with technical skill can use the CooRnet, the R package developed by the University of Urbino, to detect coordinated link sharing behavior (CLSB).¹⁶ Alternatively, link-sharing data about the coordinated behavior can be extracted also from the CSV data available for download on the CrowdTangle platform. Tool 3 should be used for downloading CSV file. Section containing links of each post is useful for tracking link-sharing behavior suggesting coordination among entities.

It is important to mention here that entities engaged in the CIB do not always share identical posts but sometimes each entity creates its own content while the message they spread and promote is the same across all other entities. With this tactic, it is hard to track all the shared posts within the network, thus it is crucial for monitors to go through the CrowdTangle dashboard regularly and assess their tactics carefully.

During the behavior tracking, again depending on the scope of the research, size of the identified network, it is advisable that the CSV and other data is downloaded on a weekly basis. If the network is small and if the monitor prefers so, CSV data can be downloaded at the end of the monitoring period. However, it is important to mention that during elections many of Facebook account and pages engaged in some kind of deceptive behavior will be removed or deactivated, by Facebook, government, or the user itself. Relatedly, if data about their activity was collected and stored, monitors do not run into the risk of losing traces about behavior of the respective page/account, which will happen if a CSV file was downloaded after the monitored entity was deleted/deactivated.








¹⁶ Available at: <https://coornet.org/>

Practical tips

To track link-sharing behavior, one of the tools that CeMI used was CrowdTangle Search feature as well. While monitoring entities' behavior, CeMI monitors noticed spread of the same content through link-sharing behavior. In order to check who else shared that same link, and to determine the size of the network, CeMI monitors copied the link of the original post and pasted it into the search bar of the available feature.

The CT Search feature is different than CT Link Checker as it allows monitors to check who shared a Facebook post on Facebook (similar to the "Share" option of the post interaction, but it allows monitors to see all messages, dates, and interactions in one place which is not visible to users), while CT Link Checker allows to see who shared an external link, e.g. media article, on Facebook or other social media platforms.

Simple as that, CeMI had an overview of all entities that shared specific Facebook link on Facebook, that were public. Below is a screenshot of how data look in practice.

WHO SHARED THIS LINK?	MESSAGE	DATE	INTERACTIONS
 Vladislav Dajković 57,103 Page Likes	"Štajkujem gladu i žeđu dok ne pustite moju ženu na slobodu da bude kući sa našim sinom. Mene držite koliko hoćete u pritvoru." Zdravko Kasalica, uhapšeni oficir Vojске Crne Gore koji - zajedno sa svojom suprugom - trpi nesvrtaoši progon zato što se protivio odluci obojane naše Crkve. Muljavar.	JUL 5, 2020	8,153
 Подришка Митрополиту Црногорско... 31,177 Members		JUL 5, 2020	106
 SRDJAN NOGO ZA MINISTRA PRAVDE... 19,887 Members		JUL 5, 2020	78
 Радио Србона 9,925 Members		JUL 5, 2020	18
 Glas Slobodne Srbije- Sima Rad... 1,396 Members		JUL 5, 2020	10
 Србија Србија 600 Members		JUL 5, 2020	8
 КРУНА НЕМАЊИЋА СПАЈА УЈЕДИЊЕНО... 3,273 Members		JUL 5, 2020	6

Presented example is a post that was created by a politician, that was shared by some of the suspicious entities identified by CeMI. However, not all entities listed above are actually part of the CIB, as sometimes a page can share a post that is viral. In the next step, it is on the monitors to verify if additional pages found are potentially part of CIB by repeating phases 1 and 2. As mentioned in previous sections, creating an outline of the network is iterative process.

As monitoring during elections comprises a wider period of time, usually 6 months, depending of the size of the identified CIB network and its post activity, monitors sometimes may have hundreds and thousands of posts to analyze and check who else shared that exact post. To address this challenge CeMI used CSV data. Namely, column V of the Excel file contains URL link of each post shared by the entities in the network. By coping this column and running it through a link matching software, monitors may have accurate data in a short time.

Although this solution analyses and summarizes wider datasets, it requires technical expertise or hiring an IT company/expert to run it for you, which is what CeMI opted for.



Last, but not least, an important step of the social media monitoring approach focused on CIB is reporting, which implies analyzing and presenting data and findings collected through the monitoring period, as well as estimates of the impact it could have on the overall electoral process and voters' rights.¹⁷

Most of the time, one of the first purposes, if not the only purpose, of a CIB network is to increase amplification of content. So analyzing content distribution metrics is important at this stage. A useful practice is to investigate the metrics of the suspected network's posts, reach, engagement, and other similar indicators.

For example, statistical data about posts could determine the level of activity of a certain entity on social media, data about reactions and interactions could establish the topic users react most to, type of posts could determine the preferred tool for the communication, etc.

In the report, monitors should assess strategies of the identified network, whether it matches tactics of certain political entities, their involvement in disinformation and smear campaigns, and cross-platform presence. It is important to determine when certain accounts were created, at what point the number of followers of entities engaged in suspected CIB started to rise, and whether the rise of their activity coincides with the electoral periods.

Additionally, monitors should assess if CIB is likely to be domestically operated or if the collected data suggests involvement of foreign actors. Through their analysis, monitors can determine if administrators, moderators, or group members of the entities within the network expressed support for certain domestic or foreign political entities.

Paid ads should be reviewed and assessed. Monitors may explore whether CIB entities' paid ads are linked to political parties or their activists. However, third-party engagement in the electoral campaign and its finance tracking is challenging due to lack of transparency and non-disclosure of paid advertisements.

¹⁷ While this type of analysis is unlikely to influence a decision by Meta to remove a network from its platforms, it is useful for a monitoring organization's communication efforts to build public awareness about their work, or share findings with the media or other researchers interested in furthering or validating findings.

Gendered disinformation and online violence against women in politics

In monitoring of the online electoral campaign, monitors should focus on identifying gendered disinformation and cases of online violence against women in politics. Disinformation, malinformation, influence campaigns, trolling, doxxing, dissing, bullying and harassment, all represent different forms of discrimination and violence against women that are present online, in particular during elections.

Monitors should focus on assessing if the identified network is involved in coordinated behavior aimed at discrediting women in electoral campaigns.

Aim of coordinated online violence against women is to discredit women politicians, who are involved in the electoral campaign and to present them as unworthy and insufficiently skilled and capable for leadership positions. In these kinds of posts, women's traditional role as housewife and a mother is highlighted, who is not supposed to bring political decisions. Long-term goal of these activities is to discourage younger generations of women to take an active role in decision making and state management.

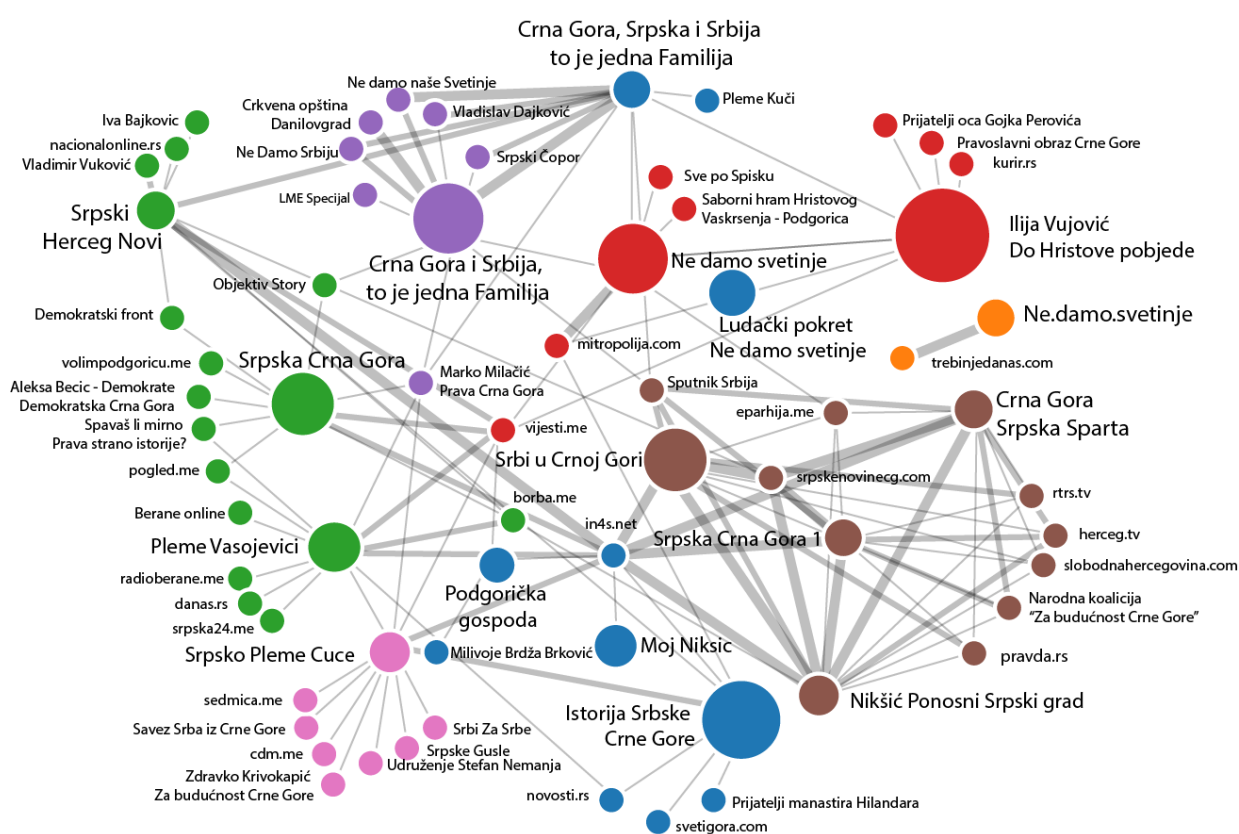
Besides women, other socially vulnerable groups, such as LGBT+ population, ethnic minorities, migrants, can be targeted. Monitors should focus on assessing whether rights and freedoms of these groups were violated in any way by the CIB network.

1.4.1. DATA VISUALIZATION

For data visualization a variety of free and paid easy-to-use web tools can be used in order to present findings in a clear and understandable manner. In the picture below, monitors can find an example of data visualization developed by using databasic.io tool.

The visual represents link sharing behavior among different Facebook entities that were part of the identified suspicious network. The graphic implies that Pages and Groups created a dense link-sharing network together with political parties, politicians, political organizations, media outlets, meme accounts, religion-related pages, that were involved in spreading of the same contents suggesting coordinated behavior.

Different colors represent different „communities“ created within the cluster. One color (community) is a group of entities in a cluster that have more connections to each other (link shares) than to other entities outside the community, but inside the cluster. The size of the circles depends on the post activity of the entity. The size of the connection lines depends on the number of same links shared between entities.



Practical tips

In its report, CeMI analyzed content distribution metrics such as reach, engagement, interactions, in order to assess the relation between number of followers (likes), interactions, and post activity of CIB network. The identified CIB network was composed of 51 entities in total, 17 of which are Pages, 8 Groups and 26 Meme accounts. Parliamentary Election were held in August 2020 and most of the entities in the network were created at the end of 2019 or the beginning of 2020, with 13 created during the period from January–February 2020. Additionally, most of the entities changed their name in the period from January – March 2020.

While reporting and analyzing data CeMI monitors determined that the network marked growth and notable spikes in number of likes in short period of time right before the elections. CeMI noted that number of CIB network followers is higher than the actual number of Facebook users in Montenegro, suggesting that some of the followers were likely the same person across multiple entities, as well as from outside of Montenegro. Namely, from March–August 2020, the network marked growth of +302.1K new page likes, with notable spikes in May and July, counting a total of 536.2K page likes, while there are 381.8K Facebook users in Montenegro.

By comparing number of shared posts and interactions, CeMI divided Facebook entities engaged in the suspected CIB network into three clusters based on their categorization as follows: Pages, Groups, and Meme accounts. In this way, CeMI monitors determined which cluster was the most and the least active one, whether the number of likes and interactions was proportionate to the number of followers and post activity, which type of content caused higher reaction and engagement of followers, etc. The cluster of Pages was the most active one and had the most followers. The identified cluster of Meme accounts had significant number of followers and was active, but it generated the least interactions in the network. The cluster of Groups was the least active and had less followers than other two clusters, however, it generated the most interactions which suggests that the members of the groups were the most engaged in the network. Additionally, during the Local Election in 2021 CeMI analyzed the percentage of politics-related content shared by non-political entities categorized as “fun”, “art”, “satire”, i.e. meme pages, and draw conclusions that it is high as 85%, suggesting that CIB network operated with the aim to influence political topics concerning elections.

CeMI also monitored and analyzed foreign influence operations during electoral period in Montenegro. Using Facebook Ad Library feature, CeMI collected data about the number and location of the account administrators. However, the administrator’s location is not necessarily an accurate representation of where the admins are located, as some of them might use VPN software to hide their computer IP address, which obfuscates their exact location.

Bearing in mind this limitation, as well as the fact that some pages did not provide the information on their admins, the public data that was available demonstrated that most admins are from Montenegro (69), Serbia (8), Germany (3) and USA (1).

However, CeMI further analyzed and identified that members of the groups/pages are in many cases located outside of Montenegro, with many fake profiles. CeMI determined this by analyzing profiles that were frequently posting and participating in the monitored groups'/pages' discussions. The analysis has shown that administrators, moderators, and group members of the entities within the network expressed support for and few are members of foreign political entities, which is an information that they shared on their public profiles in „About“ section. In addition, during 2021 Local Elections in Montenegro CeMI assessed influence operations conducted by foreign media outlets. See the link below for the detailed methodology and report.

CeMI monitored social media and behavior of political and non-political actors during elections in the digital space in 2020, and continued doing so in 2021. In this way, CeMI created a database of information which enables the conduct of a **comparative analysis**. By comparing activity metrics and other indicators in various periods of time monitors may conclude at what point activity of the network increased/decreased and whether it collides with the electoral period. Monitors may determine if the network has been growing (number of entities involved increased during the time), or if the online scene has changed in terms of tactics or new actors gaining support in digital space.

CeMI – IFES “Reshaping the Electoral Run through the usage of Social Media in Montenegro” 2020 Final Report:

<https://cemi.org.me/storage/uploads/7PcumL64x7X88mwwhAkk6N2DRIGtHH9zePYDXJA8.pdf>

CeMI Civic Monitoring of Local Elections 2021 Final Report:

<https://cemi.org.me/storage/uploads/SX38E5uX53vRXqXkL78afd pQ00e4JCod5As4un33.pdf>



2. LIMITATIONS

As previously mentioned, by using the Page Transparency feature – Tool 5, the data about the number and location of the account administrators could be collected. Page Transparency Data is one tool that can help make a judgement about how credible a Facebook entity is.

The information that can be found in the Page Transparency section includes:

- » The date the Page was created;
- » The primary country locations where the Page is managed. This applies to all Page roles.
- » The number of people who manage the Page in each country;
- » The Page's previous name changes;
- » Any Page merges that happen on or after September 6, 2018;
- » The confirmed business or organization that has claimed ownership of the Page;
- » Any confirmed businesses or organizations who have been granted access to help manage the Page;
- » If the Page belongs to a state-controlled media organization.;
- » If the Page is currently running and advertisements.

However, the data about the administrator's location, for example, is not necessarily an accurate representation of where the admins are located, as some of them might use VPN software to hide their computer IP address, which obfuscates their exact location.

Bearing in mind this limitation, as well as the fact that some pages/accounts do not provide the information on their admins, i.e. page managers, proving the coordination may be challenging.

Also, some of the researchers suggested using Ad Library to track when suspicious pages and other (fake) accounts are having paid ads during the electoral period and monitor whose name is written in disclaimer in order to potentially connect the work of those entities with the political parties, their activists and sympathizers, and campaign financing. The issue is that non-political entities of the CIB network usually run ads without disclaimer which makes it difficult to track and trace money circulation in the online space, in particular to prove it was financed by the political entity.



3. NEW IDEAS AND APPROACHES

The approach presented in this toolkit aims to deliver a set of tools that enable and trigger new research and new investigations, enabling the decentralization of research, and supporting democratization. Hopefully, this methodology will help researchers and CSOs to populate their investigations and reports with evidence of CIB.

A comparative analysis regarding how political and non-political actors are behaving on different online platforms during election period could be an interesting future approach to investigate. This could be relevant also from the point of view of electorate and targeted usage of different social media platforms to reach them through technology. Due to variation of popularity of different social media platforms in different countries, it would be interesting to investigate relationship between social media trending and online campaign tactics during elections. Market analysis show the rise of popularity of Reddit worldwide, where users can access different communities of their interests, hobbies and passions¹⁸. Platforms such as YouTube, TikTok or Snapchat are also increasingly used in online campaigns to reach young voters, while introducing a number of new tools and features. Taking into consideration different platforms and collecting data from the latter may provide evidence of new online campaigning tactics, which may include new forms of deceptive and inauthentic behavior, encompassing CIB.

With this regard, upgrading existing methodologies and establishing a common/ universal CIB detection approach among various CSOs and researchers would be useful. Furthermore, developing new tools that can be used to check on social media platforms will be useful and may lead to the identification of CIB campaigns, in particular during sensitive times, such as elections.

This could improve the communication channels between independent researchers and online platforms to provide a wider and more public knowledge of platform policies and takedowns around CIB and Influence Operations. Collaborative initiatives with private companies and social networks should be supported. For instance, initiatives can include: enforcing 'Community Standards'; working on introduction of additional privacy and security mechanisms; development of app or technology for reporting entities that are potentially engaged in CIB, and similar.

¹⁸ Marketing trends for Web Summit, Social Media, Web Summit, 2021

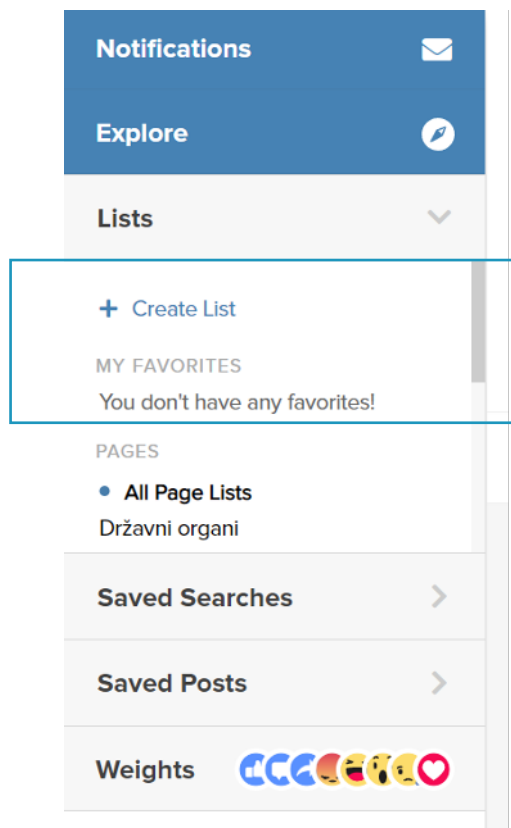


4. LESSONS LEARNED, TOOLS, AND TEMPLATES

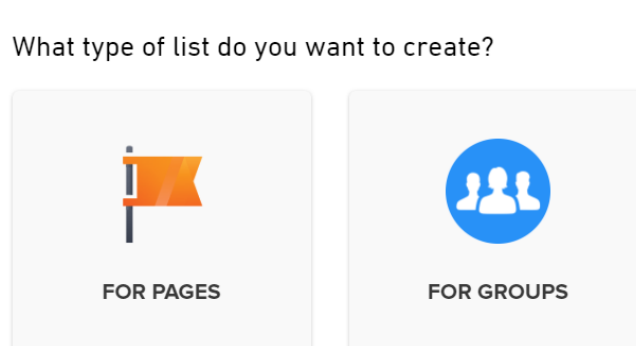
TOOL 1

CREATING LISTS

1. Open the dashboard created for the specific election monitoring.
2. From the left-side menu, select “Lists” option and then “+ Create List”.



3. Choose the type of list you want to create.



4. Name the list and Save Name.
5. Add accounts. Entities can be added by typing the name or copy/past Facebook account URL.

Save Name

Posts

Leaderboard

Notifications

Manage

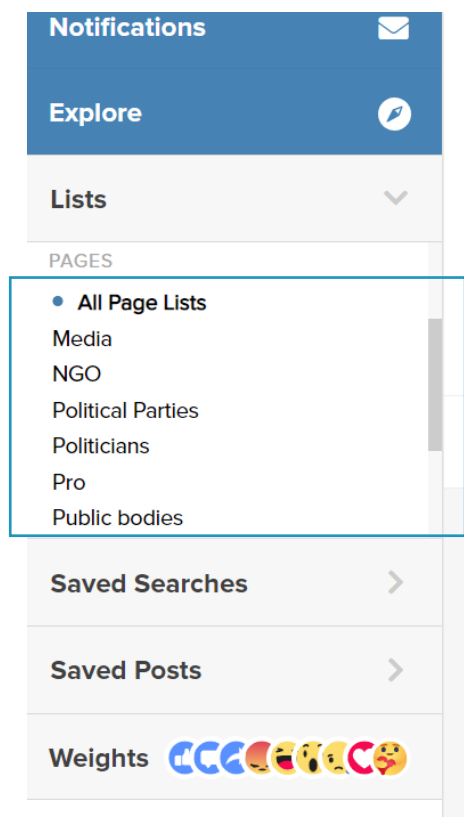
View Pages

Add Pages

Advanced Settings

✕ Delete List

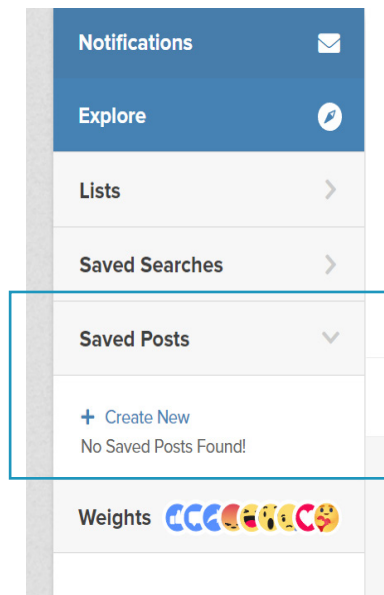
6. All created list will show up in the left-side menu.



TOOL 2

POST SAVING

1. In the left-side menu, go to the "Saved Posts" section.
2. Click "+ Create New" in order to make a new folder where saved posts will be stored, name it and click "Save Name".



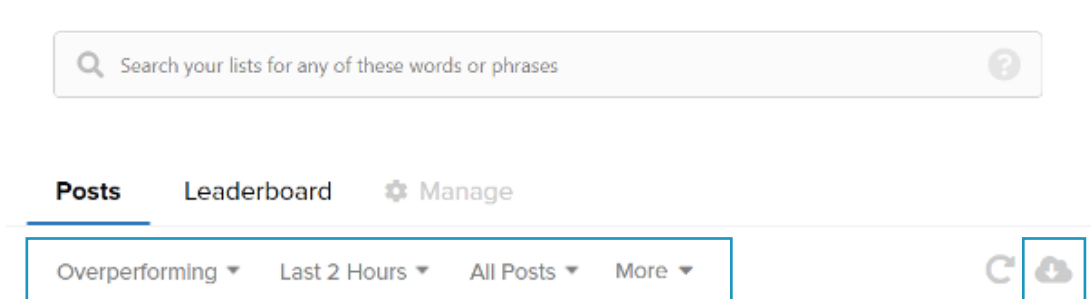
3. When scrolling down the newsfeeds, click on the drop down menu of the post you want to save, select "Save Post" and add post to the folder previously created.



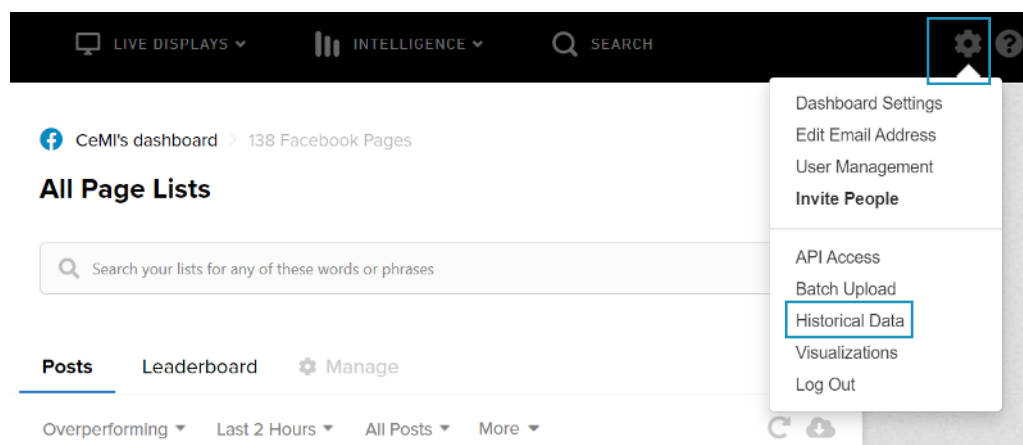
TOOL 3

CSV DOWNLOAD

1. CSV can be downloaded by clicking on a cloud icon in the filter menu of news feeds. Depending on the data that you need, you can apply different filters available in the filter menu. CSV is downloaded directly to your email.



2. If wide time period and huge amount of data is required, it can be downloaded by clicking on "Historical Data" option in the upper right corner of the Dashboard. It is important to note that Pages and Groups, for which historical data is needed, must be added to CrowdTangle. Note that this option is limited by platform, thus, historical data gives access to any posts from the CrowdTangle database and provides the data available in CrowdTangle system, it will not fetch posts from Facebook's API.



TOOL 4

CIB – CASE TEMPLATE

Summary	<i>Brief summary of the case</i>
Type of Pages and/or Groups in this network	<i>Brief description of the pages/groups engaged, their categorization</i>
Suspected motivation for network	<i>Brief description of the potential motivation behind the network operation</i>
Signals of Suspected Coordinated Inauthentic Behavior <i>Networks at high likelihood of engaging in violating behavior will demonstrate evidence of multiple signals. Networks displaying at least 4 of these signals would rise to a level of high suspicion. Include screenshots and URLs whenever possible.</i>	
Suspicious spikes in follower counts	<i>Data about number of followers and trend line can be accessed through the CrowdTangle Intelligence option. Drastic increase in number of page followers in the identified network may be a valid suspicious signal in particular if it occurs in the timeframe that coincides with the elections. Intelligence feature enables viewing the number of followers of all pages engaged in one single chart which facilitates comparative analysis and spike identification.¹⁹</i>
Similar/Identical creation dates of Pages and/or Groups	<i>Page creation data can be accessed through Page Transparency Data. If some of the identified suspicious pages have been created on the same date or during a short period of time, it represents a valid signal for suspicion.</i>
Recent substantive/suspicious name changes for a Page or Group	<i>Name change data can be accessed through Page Transparency Data. In case pages within the identified network changed their name in a short period of time, in particular around some political events, this could be relevant to include here.</i>
Page/Group “About” sections that are not filled out, or are suspicious	<i>Checking Page Profile is useful when investigating details about page authenticity. It is important to check the “About” section for suspicious signs such as invalid external domain links, or fraud related web-sites, or no data at all.</i>
Cross posting of verbatim posts	<i>This data can be looked out on different Pages’ Profiles. If same or similar posts with the same message are shared it should be included here.</i>
Suspicious post timing and frequency	<i>It is important to check page activity through the CrowdTangle Intelligence feature. For example, sharing a post in short period of time with the other pages and entities in the network or post frequency that increases during the electoral period, are all signal that may be considered as a suspicious.</i>
Page/Group Administrators located outside of the country	<i>Pages’ admins and managers might be located in other countries which is a relevant signal of CIB that should be pointed out. This data can be accessed by clicking on Page Transparency Data.</i>

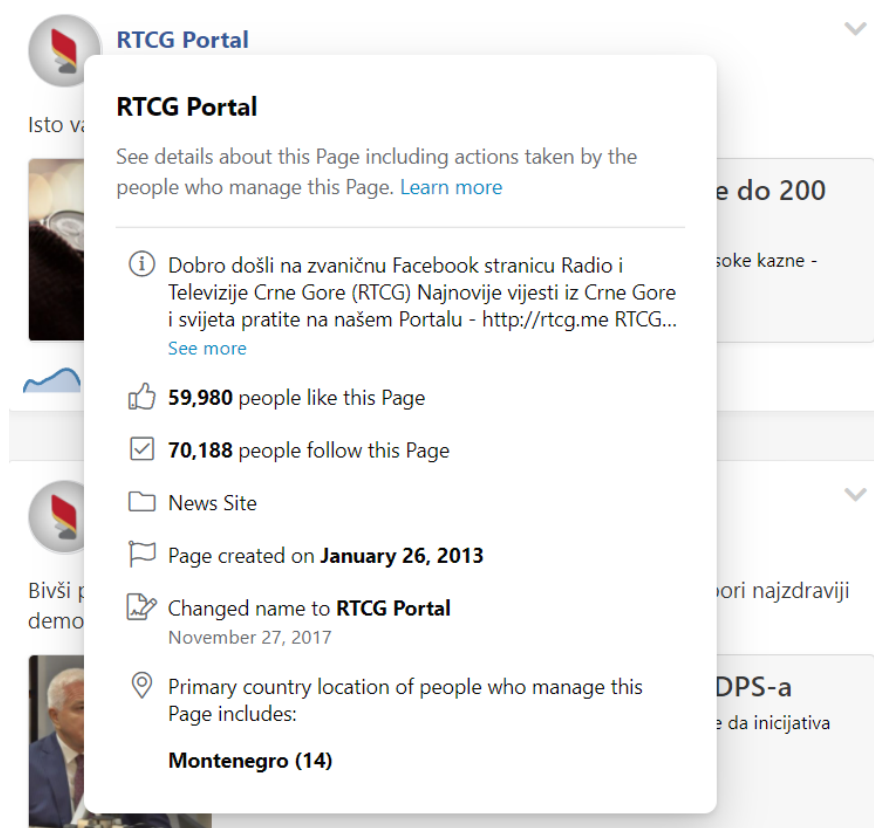
¹⁹ If a Page or Group was added to CrowdTangle relatively recently, the spike in followers might just reflect the date in which the Page or Group was added. Thus, it is important for the monitors to add Pages and Groups in the CrowdTangle system through Lists as soon as they identify them, for data to be collected.

The same Page/Group Administrators managing multiple accounts in the same network	<i>Page Transparency Data might show if the same person is managing multiple pages. This data is relevant to include in this template as it suggests that the network operates coordinately.</i>
Page/Group Administrators or Most Frequent Posters are (Suspected) False Accounts	<i>While checking members of groups, admins, public discussions on Pages'/Group Profile, it is important to track accounts that may be fake. In case some of the fake accounts have similar or same characteristics such as the same profile or cover picture, it is important to note it here.</i>
Content Shared by Network in Violation of Facebook Community Standards	
Hate Speech, Incitement to Violence	<i>Insert examples of hate speech, incitement to violence, or other violation of Facebook Community Standards</i>
Domains linked to/ creation data	<i>Insert domains linked and domain data details</i>

TOOL 5

PAGE TRANSPARENCY DATA

1. You can access Page Transparency Data through CrowdTangle with simple positioning of the mouse over the name of the entity. Data will be shown instantly.



- Also, you can find and access the Page Transparency Data of any Page in the left column.

The screenshot shows the Facebook profile of 'RTCG Portal', a news and media website. The left-hand navigation menu is expanded, highlighting the 'Page transparency' option. The main content area displays a post from the page, featuring a woman speaking at a podium with the Montenegrin flag. Below the post, the 'Page transparency' section is visible, explaining that Facebook provides information to help users understand the purpose of a page and the actions of its managers.

Page Transparency

Page Information for RTCG Portal



Page History

- Changed name to RTCG Portal
November 27, 2017
- Page created - Internet portal RTCG
January 26, 2013

People Who Manage This Page

- Primary country/region location for people who manage this Page includes:
Montenegro (14)

Ads From This Page

- This Page is not currently running ads.

[Go to Ad Library](#)

[Find support or report Page](#)

Close

For more information about Page Transparency: <https://www.facebook.com/help/323314944866264>

BIBLIOGRAPHY

CeMI – IFES, “Reshaping the Electoral Run through the usage of Social Media in Montenegro”, Final Report, 2020

CeMI, Civic Monitoring of Local Elections, Final Report, 2021

Earl, J., The dynamics of protest-related diffusion on the web, *Information, Communication & Society*, 13:2, 209–225, 2010, DOI: 10.1080/13691180902934170

Giglietto, F., Righetti, N., Marino, G., Understanding Coordinated and Inauthentic Link Sharing Behavior on Facebook in the Run-up to 2018 General Election and 2019 European Election in Italy, LaRiCA – University of Urbino Carlo Bo, 2019

Gleicher, N., Rodriguez, O., Removing Additional Inauthentic Activity from Facebook, Facebook, 2018

Gleicher, N., Inside Feed Coordinated Inauthentic Behavior, Facebook, 2018

How We Respond to Inauthentic Behavior on Our Platforms: Policy Update, Facebook, October 2019

Marketing trends for Web Summit, Social Media, Web Summit, 2021

Meta Transparency Center, Facebook Community Standards, Inauthentic Behavior

