CiFAR
CIVIL FORUM FOR ASSET RECOVERY

INVESTIGATE

THE MANUAL

CONTENTS

INTRODUCTION

1

ABOUT THIS MANUAL

This manual was designed in order to provide readers with an overview of state of the art practices in investigative journalism, with a focus on illicit financial flows and asset recovery. It has an introductory to intermediate level. It is the result of over three years of collaboration between CiFAR and civil society organizations specialized in various fields of expertise relevant to the practice of journalism, beginning with the launch of our first training and mentoring program Investigate the Meditarranean in 2017.

Our Introduction to Investigative Journalism manual aims to cover points that we have identified as being important for investigating grand corruption, financial crime and asset recovery, the main areas of investigative reporting useful for, namely: theoretical and research frameworks, investigative resources for deep web research, databases and access to information, as well as digital safety. Three supporting case-studies have been added as an illustration of the use of these tools and techniques, based on three investigative cross-border stories published by some of our trainees. This last part is designed to provide a "behind-the-scenes" overview of the investigative work of these three journalists that, we hope, will be useful for current and new early career investigative journalists.

This manual has been developed with the support of German Cooperation, implemented by the GIZ - the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, through their Global Program Combating Illicit Financial Flows.

Supported by the

Federal Ministry
for Economic Cooperation
and Development

Norwegian Ministry
of Foreign Affairs

Implemented by giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

1 INTRODUCTION

WHAT IS CIFAR?

CiFAR was founded in 2015 to support civil society to campaign across borders to prevent public asset theft and for accountable and transparent asset recovery. Our vision is a world where public officials are unable to steal public money and hide it overseas. Our mission is to end cross-border corruption and to ensure transparency and accountability in asset recovery.

CiFAR was founded after realising a gap existed in support for civil society – in a broad sense – to work on cases of cross-border corruption, both in terms of understanding how the process was supposed to operate and in making connections with civil society abroad. These issues were, and still are, particularly prominent in countries of origin, countries where the corruption originated, as the expose of large cases are often the first case local civil society has worked on.

The aim of CiFAR from the start was to address this gap and be both a capacity building and network-support organisation. In that line, since our founding we have worked to train civil society activists and journalists, networked together actors working on different parts of ongoing cases, developed tools and engaged policy makers on asset recovery reform.

While continuing in that role, we also have expanded our mandate as more and more actors have come onto the scene and as cases and returns became more varied.

CiFAR
CIVIL FORUM FOR ASSET RECOVERY

CIFAR AND INVESTIGATIVE JOURNALISM

At CiFAR, our goal is not only to support the civil society organisations to work better and more collaboratively across borders, but also to build broad-based coalitions of all members of civil society to fight against public asset theft and for the recovery of stolen assets.

Starting in April 2016 the Panama Papers have and are exposing how hundreds of politicians and other public figures are systematically using offshore companies to avoid paying taxes on their wealth. The same schemes are used by corrupt officials and private persons to channel and launder billions in assets stolen from public bank accounts or obtained through other criminal activities.

While this has been positive, the perspective of these stories has been northern and, except for a few examples, voices from elsewhere have been much less prominent. This risks not only losing the perspective of people from states losing assets, but also focuses attention primarily on the receiving states, reducing pressure for reform on those where public officials have or are stealing state assets.

Our work with investigative journalists focuses particularly on early-career journalists and aims to support them to develop their expertise in investigating and reporting on cases of grand corruption and the processes for returning that money. We further help them to develop stories and to pitch and publish these in leading news outlets.

ABOUT THE AUTHORS

Jean-Baptiste Renaud

Journalist, director of investigative documentaries for television, he has directed several films for the news agency Premières Lignes, including Chemical Weapons, a Western Poison (Canal +) selected at the Investigative Film Week in London 2015 and Drones, Obama's dirty war, co-directed with Benoit Bringer (Canal +). He has also worked with the main investigative French program "Cash Investigation" for France 2 for various investigative projects targeting the agro-food industry.

Albrecht Ude

Albrecht is the editor-in-chief of the Newsletter Netzwerk Recherche and contributor at Zeit among other media. His main areas of work includes structured internet research with analytical and forensic methods, source-checking, data and communication security. His preferred topics include research, communication security, civil rights in the digital age, as well as the erosion of the rule of law due to increasing digital surveillance. He has also worked on internet censorship and how to protect informants and users. He has been an investigative journalism trainer for the M100 Colloquium and N-Ost, among others.

Šarunas Černiauskas

Šarunas Černiauskas is a regional editor for OCCRP, based in Vilnius, Lithuania. He leads Siena.lt, the first Lithuanian non-profit organization entirely dedicated to investigative reporting. Černiauskas has contributed to numerous cross border investigations, including OCCRP's Troika Laundromat, ICIJ's Panama Papers and Paradise Papers. One of his stories exposing the misuse of EU funds by members of the European Parliament was shortlisted for the European Press Prize in 2017. Černiauskas has received several national awards and became the first laureate of the Investigative Journalism Prize established by the Vilnius University, awarded for reviving investigative journalism in Lithuania.

ABOUT THE AUTHORS

Tactical Tech - Exposing the Invisible

TACTICAL TECH EXPOSING THE INVISIBLE

Tactical Tech works with an international audience of engaged citizens and civil society actors to investigate and mitigate the evolving impact of technologies on society since 2013. One of their main audience groups is made up of civil society actors, such as journalists, other NGOs or human rights defenders, who they work with to create safer, more robust and more informed practices with regard to their use of digital technologies. Projects such as Exposing the Invisible help empower people to use digital investigations to uncover truth or corruption. Similarly their work on Data and Politics provides a unique contribution to understanding how the misuse of data is impacting negatively on democracies around the world.

Nataša Tomić

Nataša Tomić is a journalist based in Banja Luka, Bosnia and Herzegovina, currently working for online portal eTrafika.net and collaborating with some other media outlets in Bosnia. She focuses on human rights and marginalized groups, corruption and other national based topics. She participated in the CiFAR training and mentoring program “Investigate the Western Balkans” in 2020-2021.

Access Info Europe

access !Nfo

Access Info Europe is a human rights organisation established in Madrid in 2006 and dedicated to promoting and protecting the right of access to information. Access Info runs a range of projects designed to leverage the right to information in order to increase participation and accountability, to defend human rights, and to advance democracy. Activities include a mix of research and monitoring, standard-setting, law reform campaigns, and strategic litigation. Access Info also provides support and training for civil society and journalists. They have contributed to developing civil society activism on transparency in Europe, building a network of national organisations dedicated to securing increased transparency in practice.

ABOUT THE AUTHORS

Menna Ayman

Menna Ayman is a Cairo-based journalist with a particular interest in asset recovery and cultural topics. She has covered stories on Palestinian and Syrian refugees, expatriate communities in Egypt, and properties and asset theft during the Mubarak era. She developed a knack for journalism post the January 2011 Revolution. Menna is also a copywriting and translating enthusiast.

Arlis Alikaj

Arlis is an investigative journalist with critically acclaimed reporting on environmental and social issues in the Balkan region. During his Balkan Fellowship for Journalistic Excellence by the Balkan Investigative Reporting Network (BIRN), he wrote an investigative report on illegal logging in Albania's largest national park. He won the CEI SEEMO Award for Outstanding Merits in Investigative Journalism 2019 for this work. He joined CiFAR's second "investigate" training program the same year and published a cross-border story on illegal working permits in the UNESCO site of Lake Orhid, shared by Albania and North Macedonia.

THEORETICAL FRAMEWORK FOR INVESTIGATIONS

2

THEORETICAL FRAMEWORK FOR INVESTIGATIONS

Jean-Baptiste Renaud

It is often said that “investigative journalism” as a term shouldn’t exist because “investigative journalism” is a pleonasm. In this rather unrealistic conception of journalism, every reporter should always investigate, in every piece of journalism he/she produces, in other words, investigation would be inseparable from journalism.

In reality, and for various reasons, most media outlets do have investigative experts, reporters who only work in this field.

Also, numerous aspects of journalism usually don’t require any investigative element to serve its mission. We can think for instance about local newspapers, local radio or TV networks that are designed to produce news made to be used in the community’s daily life.

We can also think about sports journalism. Although sports is definitely a tremendous field of investigation, reporting about games results, leading scorers, injuries is by definition journalism made as a service for sports fans. Remember the famous EIC Football Leaks for instance.

So, in a general way, every piece of journalism produced with the intention of offering a service to your audience is not easily compatible with investigations.

In a broader perspective, some might even try to oppose investigation, which would consist in a harrowing quest leading to countless hours behind a desk looking for clues, and reporting, in its purest conception : going outside in the field and telling stories.

Portraying the investigative journalist as a copyist monk and the reporter as a fearless Indiana Jones is pretty reductive, and while it might be true to some extent, or has been true in the past, this opposition doesn’t stand today.

Indeed, we can’t oppose investigation with reporting since, as we will describe, reporting is an important phase of the investigative process.

In this first introduction, we offered a definition of investigative journalism by explaining what an investigation isn’t. Now, it’s time to wonder what an investigation is.

WHAT MAKES AN INVESTIGATION ?

Revelations, scandal, muckraking. These are some words often used either to praise or to discredit investigative journalism. But none of them are specific enough or thorough enough to describe an investigation. Here is an attempt to characterize it through several of its objectives or missions. An investigation should:

- **Highlight a dysfunction**. It could be corporate misbehavior, government malfunction, criminal activities.
- **Question the actions of big players** (corporates or states) or should have big implications on society.
- **Confront those big players with their actions**. Transparency and accountability from those organizations should be at the center of the process.
- **Uncover something hidden from the public**, whether it is new documents, new witnesses or simply a new way to present facts.

Many investigations stand at the crossroads of these notions. Some will check one or multiple items from this rough checklist. But not all of them are mandatory for a report to qualify as an investigation. In my own work, some of the investigative documentaries I have produced actually tick all the boxes, others don’t.

My latest one, “American crusade in Africa”, focused on investigating the actions of the US NGO Invisible Children in Central Africa, gathers pretty much all of those notions. In this piece, I clearly managed to establish a dysfunction : how a humanitarian effort actually turned into a shady NGO with unclear ulterior motives. It also questioned the actions of two States : the US, and particularly the US Army and the Ugandan regime. Both actors were confronted in the film, along with the NGO itself in a very revealing interview. Finally, it contained several new pieces of information made public: for instance the revelation that the NGO turned over one of its Ugandan employees to the Museveni regime leading him to be tortured. I had found this allegation in a diplomatic cable but no one had been able to find the victim and ask him to corroborate the information, and no one had ever asked the NGO Invisible Children to comment on this on camera.

One of the notions which is the most difficult to achieve is confrontation: because most of the institutions and persons at the center of your work are simply not willing to talk to you. This has happened to me a lot - for instance when the CEO of a French milk multinational refused to answer my question and I had to shout those questions through the window of his car - and, unfortunately, this will happen again in the future.

Nevertheless, this first classification of what an investigation is can be a benchmark for your ideas.

FINDING A LEAD TO INVESTIGATE

In every public screening of my documentaries, I always get the same question: how do you find ideas for your investigations? Of course, I always have in my web browser a file containing bookmarks labeled “ideas for later”, and add to it every time I read something I find promising. Whether you choose the same method or not, keep in mind that reading a lot and being curious of all trends emerging in society can only be helpful to your preliminary research.

The following is a list of some resources you can use to find ideas, keeping in mind that they can be combined:

- **Your own intuitions**: Any intuition can transform into a good investigation. Any observation in your daily life, any conversation with friends or family can start a good investigation. It is always helpful and rewarding to dig into the most underreported topics.
- **Following-up**: Think also about your previous work: are there any aspects of a story you have covered in the past that would need a longer investigation, some sources you met at the time you can reach out to? Or the other way around: crucial sources who didn’t talk to you back then and can now help ?
- **Open sources**: This is pretty counterintuitive with the idea that investigative reporting is about publishing confidential documents, state secrets, etc. but more and more investigations are based on the use of open source data. The brilliant success of OSINT (open source investigation) with some respected pure-players such as Bellingcat or Forensic Architecture as ambassadors.
- **Leaks**: Documents that were not supposed to be published are also obviously sources of inestimable value. In this case, access to those documents is not the climax of your investigation but the start. A huge amount of work is then necessary to build your investigation from that. Those documents are, most of the time extremely technical and require weeks or months of work to be used properly.
- **Freedom of information requests and equivalents**: This is time-consuming because you have to dodge administrative slowness and face the lack of transparency. Also, your request must be extremely precise otherwise it might be quickly overturned. Nevertheless, crucial documents can be made public using those requests.
- **NGO reports**: Those organizations conducting field work, sometimes in areas where they are the only organizations allowed, and can also provide the expertise of their staff for the preliminary research.
- **Political fact-checking**: Following up on the fact that two years ago, for example, this government promised that *this dysfunction* would have disappeared in a few years. A few years later, what actually happened ?
- **Through story-telling**: Choosing a story that is particularly relevant can produce an interesting storytelling based investigation. In that case, you choose to focus the start of an investigation with the intention of telling someone’s story because the story perfectly symbolizes the dysfunction highlighted by the investigation.

EXAMPLE #1: BUILDING A LEAD THROUGH NGO REPORTS

In 2015, I led an investigation on the carbon offsetting scheme created by the EU. At the very beginning of this work, I relied on the pre-existing work of several NGO that had established that this scheme originally designed to make the biggest CO2 polluters pay for their emissions actually benefited them by hundreds of millions of euros each year.

This major dysfunction was the main conclusion of several NGO reports, but it remained too vague to be fully understood by the public. I then decided to get all the CO2 emission data from every industrial site in all EU member states. From this open-source data, I was able to highlight the case of one particular company, the cement multinational Lafarge, based in France.

Based on the data, it became clear that this company actually earned more than 500 millions euros thanks to this flawed scheme when it was actually one of the most polluting companies in the continent.

This was achieved by combining NGO reports, open data and also field work. Indeed, I had noticed in the data set that a specific Lafarge cement factory in Burgundy was receiving half a million euros through the EU carbon emission scheme for a given year but with a “0” in the “CO2 emissions” column. This needed to be checked because it could have been a bug in the database. I travelled there and I managed to get inside the factory only to realize it was closed, with no one working there. Lafarge was cashing in EU money for zero emissions and this claim wouldn’t have been possible without field work.

EXAMPLE #2 : BUILDING A LEAD THROUGH A LEAKED DOCUMENT

In 2014, I started working on the French nuclear industry and its lack of transparency. Pretty quickly I decided to investigate a nuclear incident that took place in 1980 in the center of the country.

When researching, it appeared that this nuclear incident had always been underreported by the press and downplayed by the operator of the plant and the French government. Above all, there was a rumor that said during this incident, some plutonium had been released into the Loire river without anyone knowing, which would have been not only shocking if true, but also illegal and would question the transparency of the operator.

But at the beginning this claim only appeared on anti-nuclear publications and no document or testimony could corroborate it. Then, I found a reliable source. The source not only confirmed that she had knowledge of the plutonium story but that she also had documents that would prove it. I went quickly to meet the source and conducted an interview, blurring the face of the source during the filming. I went back home with the interview and a copy of the document confirming the operator had full knowledge of the radioactive contamination of the Loire river but had decided, with the consent of the French government, to keep it secret from the public.

Later, at the end of my investigation, I was able to confront the president of the operator of the power plant with this document for the first time in public. He basically said keeping the contamination and the document secret was deliberate and that making it public would only make the situation worse at the time.

EXAMPLE #3 : BUILDING A LEAD BY COMBINING FOLLOW-UP AND STORYTELLING

In 2018, I was commissioned by the Paris based production company Slugnews to follow-up on the work of another team of investigative reporters. Back in 2014, this team was filming in the Central African Republic to cover the civil war going on at the time. While reporting, they met with a very curious NGO: Invisible Children. It had offices in a remote part of the country where the NGO wanted to participate in the capture of the infamous warlord Joseph Kony, wanted by the International Criminal Court for war crimes and crimes against humanity.

Four years after their return, I watched every video from their filming, discussed it with them and it became clear that this NGO, who had produced the viral video KONY2012, should be at the center of a new investigation. Indeed, at the time, some of the segments filmed by the team had led them to think that this NGO wasn't following the usual guidelines that applied to other NGOs: they were blatantly serving as a proxy for the US Army based in the region.

This was the hypothesis of this new investigation. But then, I decided that this first investigation in 2014 would be useful in the storytelling of this new film. This is why I chose to open the 2018 documentary, African Crusade in Africa, by a scene showing myself taking the hard drive containing the 2014 filming and starting the investigation from it. As a consequence, this film is not only a film about a questionable NGO, this is also a film about an investigative reporter following the work of other investigative reporters.

FROM A LEAD TO A HYPOTHESIS

In the three previous examples, there was a general theme: CO2 emissions, nuclear energy, and a strong hypothesis to start. Whether it is that the EU scheme is flawed, that a serious nuclear incident has been kept secret or that a NGO is actually a proxy for an army.

So, in the first phase of the investigation, one of the priorities was to transform the idea into a hypothesis and then organize the work in order to confirm or deny this hypothesis.

In all cases, ideas became hypotheses only by researching. Researching is the key to the first phase of your investigation. This is where you read everything that has already been published on the issue, either by other journalists, by researchers, NGOs etc.

But the research phase also contains a good amount of outreach. Contacting the right people, taking the time to test your hypothesis on those first sources, reaching out again to them when necessary, everything must be put into verifying the hypothesis, building new ones or secondary ones, or in some cases dropping the initial hypothesis.

HOW TO ORGANIZE YOUR WORK

The three main phases of an investigation are: researching, reporting, confronting. Generally in that order but they can also be more overlapping. Make those three phases suitable for your deadline, the size of your team, and the budget available for this investigation.

Given the diversity of deadlines, resources and formats, it would be difficult to associate each phase with a theoretical duration. When I work on a year-long investigation in order to produce a documentary I can typically expect that the researching phases would take between 3 and 5 months, the reporting/filming around 2 to 3 months and the editing/confronting phase around 2 to 3 months.

So roughly, 50% of the time is dedicated to preliminary research, finding and testing hypotheses and contacting sources and around 20 to 30 % of the total time of investigation is dedicated to the two other phases. Once again, given the fact that all phases can overlap up to a certain point, this theoretical schedule can be adapted to suit your own resources and deadlines:

- **Find a strategy**: who should I call first, who should I call last, when do I have to call the person/institution/company at the center of my investigation? These are crucial questions because some hasty emails or phone calls can put your investigation in jeopardy. This could happen either with a source or with an institution. A source could be reluctant to talk to you at a particular point of your investigation but might feel different at another.
- **Know how to present your work**: depending on who you're talking to and at what point of your investigation, take the time to think about a good way to present your work. Some sources that might help you would need to know how comprehensive your work is; especially the persons or institutions at the center of your revelations. For instance, if you feel you need to get access to a particular location or site, make sure that the company or institution who can grant you that access will not deny it because of the way you present your work to them.
- **Make room for field reporting**: field reporting is crucial, every good investigation is embedded in reporting. It could be on the field or over the phone, based on your time and budget. Numerous investigations can be unlocked while reporting, just by asking the right questions at the right time.
- **Prepare every detail of the confrontation**: the climax of your investigation would very often be the confrontation with the person or institution incriminated by your work. Sometimes, they would agree to meet for an interview that you would prepare differently if it takes place via email, over the phone or in real life. Prepare also for the common case that your request is denied and you have no one to ask your questions to. What would you do? Go to meet them anyway, for instance in a public place where they attend a public event?
- **Save enough time to put your revelations on paper/screen**: never underestimate the time needed to write your paper, edit your audio or video segment. Writing/finalizing the investigation obviously comes at the end of the project but don't forget you will still need to research and investigate until the very last minute.

STRATEGY 1: THE IMPORTANCE OF FIELD REPORTING

In January 2019, I went to Libya in order to report for an investigative documentary about migration through the Mediterranean and detention camps in Libya. Before coming to Libya, we had a lot of research indicating that a particular detention camp near Tripoli - Zawiyah - was a perfect illustration of the atrocities migrants face in their journey: torture, beatings, killings, poor living conditions, sexual assault etc.

All of this was documented by NGO reports but we couldn't base our film only on those reports. We set this detention camp as our top priority and it was only through reporting, in the field, in Libya that we were able to confirm our hypothesis about this detention camp. Managing to get in and being able to escape the guards for a few minutes allowed us to gather some priceless testimonies on our own, only by field reporting.

STRATEGY 2: A WELL-PREPARED CONFRONTATION

After investigating for months into the US NGO Invisible Children, I worked on how to approach them, softly enough so they wouldn't be too suspicious about the tone of the interview, but convincingly enough for them to be interested in giving the interview.

Later, I had to face another dilemma: the NGO would only grant the interview if they had the questions listed in advance so, should I send the questions which I always refused to do for ethical reasons? If so, the risk for me would have been to have an overpepared interview on the NGO side with a limited flexibility on my side.

HOW TO HANDLE UNFORESEEN EVENTS

In such a versatile field as investigative journalism, unplanned events, even though they should be limited to the maximum by your research plan and strategy, will always happen. Here are a few tips on how to mitigate unforeseen events:

- **Don't be afraid of dead-ends**: Some leads will need to be investigated for days or weeks before you realize they are not usable in your investigation. This is a foreseeable outcome when you try to pursue every lead.

- **Always think against yourself**: Don't let your discoveries blur your common sense. This is a quite common risk in many investigations: getting so excited about the revelations you're about to publish that you discard every other hypothesis disproving your theories. In order to avoid that, communication with colleagues, members of the team is crucial.
- **Be creative when facing unforeseen events**: This is inevitable - everything will not come out as planned. The big confrontational interview has been cancelled and you only have a written statement from the PR to use? Find creative ways to counter that.
- **Make sure to have legal assistance**: In many cases the entities at the center of your revelations will threaten to sue you or your organization. In some of those cases, they will. This is a common but nevertheless scary threat, especially for a small organization. Legal assistance should be provided all throughout the investigation because of a whole range of situations that would require legal back-up: should I record this phone call? Can I publish it afterwards? Am I allowed to publish documents that have been stolen? Can I use a hidden camera? All these questions should be asked to a legal advisor first, keeping in mind the answers can vary from one country or another. Private lawyers are expensive, especially for small organizations, and your legal assistance could rely on another person in your organization, but legal protection is priceless with so many powerful players involved.

HOW I KEPT ON WITH MY INVESTIGATION DESPITE SOME SETBACKS

In 2013, I produced an investigation about chemical weapons and especially on who were the providers, the enablers for this industry. The confirmed first hypothesis of this investigation was that throughout history, western companies were the main providers of equipment to dictatorial regimes looking to obtain a chemical weapons stockpile.

I conducted one part of this investigation in Germany where there was some controversy about the revelation that the German government approved the export of chemical products and equipment to Syria, despite the fact its chemical weapons program was public at the time.

I had an hypothesis about France, suggesting that my own country could have allowed the same kind of exports to Syria in the recent years. Even if some sources were not very adamant about it, they suggested that this was plausible. But despite all my efforts and so many requests made to the French government, I couldn't go any further on this question, not because the hypothesis was false, but because I lacked resources to confirm it.

RESOURCES FOR INVESTIGATIVE JOURNALISTS

3

RESEARCHING THE DEEP WEB – A STRUCTURAL APPROACH

Albrecht Ude

The Internet is not an “infinite expanse”, because the amount of storage space on all computers on this earth is limited and will always remain so. Consequently, the internet is also finite and always will be. “Immeasurable” it is, however. How big it actually is, how many “documents” it comprises, nobody knows.

Many users believe that when they make a Google query, they are searching “the internet”. This is wrong on several counts. For one thing, Google is not the internet, but a database in which a small part of the World Wide Web is copied. The WWW, in turn, is a part of the internet, but is often confused with it. Google (and all other universal search engines) permanently search the “surface web”: that part of the WWW that can be reached by mouse clicks. They copy what they find there into their “index”, their database. Unstructured web pages thus become structured data sets that can be searched for keywords and with special operators. Every search engine is therefore (only) a copy of a part of the surface web. Everyone knows how much can be found there. Very few realise how much you will never find there: the World Wide Web is much bigger. It includes the “deep web”, the social networks and the “darknet” .

The **Deep Web** (also called the “hidden” web) includes all content on the WWW that cannot be accessed by simple mouse clicks. Figuratively speaking: as soon as you need a keyboard to reach something, this content belongs to the Deep Web. It is called the “Deep Web” precisely because normal search engines cannot search and index it. This content is spread across millions of databases, closed forums, websites behind paywalls or websites whose owners use robots.txt to prevent search engines from including them in their index. There is no central place to search this huge quarry.

THE ROBOTS EXCLUSION STANDARD
This allows website owners to prevent search engines from “spidering” the web pages they are targeting through appropriate meta tags in the HTML header of webpages. Learn more about them here.

Social networks are places of exchange and contact on the WWW. The software is always provided by the network operator, while the content (text, images, audio and video files) comes from the users: this is called UGC, “user generated content”. The business model of most social networks is to hide this content from search engines so that you can only use it with an account. Mind you, you need one for each social network you want to research. One for Facebook, one for Twitter, one for Instagram, hundreds and hundreds for the hundreds and hundreds.

What is called “**darknet**” in the reporting should correctly be called “darkweb”: it is part of the WWW (computer scientists understand “dark net” to mean something quite different, namely quasi “unused” parts of the internet address space). There are several of these darknets, not just one. What all these platforms have in common is that they anonymise their users and thus protect them. What is usually understood by “darknet” is primarily the Tor network and its hidden services.

SEARCH ENGINES
Besides Google, there is Bing from Microsoft. In Russia, Yandex is the market leader, in the People’s Republic of China it is Baidu. All these search engines work with user tracking, they spy on their users. Anonymising alternatives are DuckDuckGo and Qwant.

FINDING AND USING DATABASES

Databases belong to the “Deep Web”, the “hidden” part of the World Wide Web. Their contents are hidden from search engines. You need special strategies to find them.

In practice, the biggest problem for many users is to find a database in the first place. Search engines often deliver large numbers of hits, even with nonsensical queries, the examination of which then leads to a lot of wasted time. For example, a search for the e-mail address of a Hamburg architect named “Volker Hauth” returns many hits, but unfortunately no e-mail address. However, if you simply enter “Hauth” in the Hamburg Chamber of Architects’ member database, you will find the one correct answer immediately.

The problem is that successful searches begin in the mind, not in search engines. A database containing Volker Hauth’s data is of course not called a “Volker hauth database”. In concrete terms, then: when searching for the appropriate database, one has to abstract for a moment. As long as one searches for the database, one must not search for what one wants to search for in the database.

**Don‘t look for information on Volker Hauth.
Look for information on architects in Hamburg!**

In the result sets, one finds the start pages of databases, but not their contents. Unlike search engines, databases do not search the World-Wide Web. They do not get their data through unstructured searches, but by entering structured data. The research problem is therefore to find the relevant databases in the first place. There are a few strategies for this.

WHO OPERATES THE DATABASE?

Setting up and running a database (keeping the information it contains up to date) is work and costs money. Nobody does it for fun, those who do it have an interest. Often databases are found by simply asking who should actually have them. For example: a database on architects in Hamburg is run by the Hamburg Chamber of Architects. After all, they want to promote their members.

SEARCH ENGINE QUERIES FOR DATABASES

In queries to search engines (SEs), you can combine content-related and formal search words. So if you are looking for databases on architecture, you can query “architektur datenbank” (architecture database). Such queries should always be formulated in English as well as in your own language.
Suitable formal search words: database OR directory OR catalogue OR list

Important: With such combinations of search words, one should not search for the desired contents of the database (as mentioned, search engines do not find these), but for the topic of the database. For example, if you are looking for oranges from Spain as a commodity, you should look for a database for suppliers, and then in this database search for Spanish orange traders.

HARVESTING DATABASES FROM WIKIPEDIA

You can often find references to databases in the “weblinks” of Wikipedia’s thematic articles. As with search engines, you should always check the English version of Wikipedia and other relevant languages. Some categories (keywords) in Wikipedia lead to databases. Finally, Wikipedia contains lists of databases.

WIKIPEDIA DATABASE CATEGORIES

Also pay attention to the links to other language versions:

- https://en.wikipedia.org/wiki/Category:Databases
- https://en.wikipedia.org/wiki/Category:Digital_libraries
- https://en.wikipedia.org/wiki/Category:Scholarly_databases
- https://en.wikipedia.org/wiki/Category:Scholarly_search_services
- https://en.wikipedia.org/wiki/Category:Bibliographic_databases_and_indexes
- https://en.wikipedia.org/wiki/Category:Scientific_databases

DATABASE LISTS IN WIKIPEDIA

- https://en.wikipedia.org/wiki/List_of_academic_databases_and_search_engines
- https://en.wikipedia.org/wiki/List_of_online_database

DATABASES OF DATABASES

The Database Information System (DBIS) allows the use of 11,554 scientific databases (of which 4,754 are free on the internet). The databases which are subject to payment can be used in 307 academic libraries.

The databases are offered sorted by subject. In addition, there is also an advanced search, in which, among other things, a keyword search is possible or it is possible to search for databases with a geographical reference.

http://www.bibliothek.uni-regensburg.de/dbinfo/ .

LISTS OF DATABASES

To find lists of databases, look for “a * z database” in search engines. Many subversions have compiled long, comprehensive lists of databases, such as “A-Z databases” or “A 2 Z databases” etc.. This search phrase can, of course, be supplemented with content-related search words.

LIBRARY CATALOGUES

Library catalogues are a special type of database. They document which holdings can be found in one or more libraries. The system of different library catalogues works in a staggered manner. The basis are the catalogues of the individual libraries “on site”, which simply show which literature is available (and can be obtained most quickly) there. These catalogues are usually based on “autopsy”, i.e. the librarians have seen the listed books themselves.

Building on this, there are union catalogues, which make the holdings of several libraries (usually of a region or country) searchable. Finally, there are some specialised catalogues such as the national libraries, which list the entire literature production of a country, but not necessarily where to find it, or databases for journals, dissertations and the like.

LIBRARY CATALOGUES

- Library of Congress (LoC), USA
- British Library (BL)
- Deutsche Nationalbibliothek (DNB) / The German National Library
- KVK - Karlsruhe Virtual Catalogue
- The European Library
- Worldcat
- International Federation of Library Associations (IFLA): Library Map of the World
- Helpful lists in Wikipedia:
  - https://en.wikipedia.org/wiki/List_of_national_and_state_libraries
  - https://en.wikipedia.org/wiki/List_of_archives
  - https://en.wikipedia.org/wiki/List_of_repositories
  - https://en.wikipedia.org/wiki/Open-access_repository

Library catalogues normally only list “independent” literature, i.e. books, anthologies, journals, CD-ROMs, etc. Not listed are “dependent” works such as essays from anthologies or articles from journals. It is important to note that each library’s own catalogue is the most comprehensive and therefore the best. The digital catalogues allow searching according to certain criteria (such as author or person, title, keyword and others), and often also “browsing”, i.e. browsing through an index (a list).

The catalogues allow searching not only for literature, but also for persons (authors and editors), organisations and fields of interest. Thus, for each person who holds the doctoral title, one can look up the subject on which he or she did his or her doctorate and usually find even more data ad personam.

WEB ARCHIVES

Orderly archiving of WWW content does not yet exist. Currently, the most important freely accessible collection of old (changed and deleted) web content is the “WayBackMachine”, the web archive run by a private foundation.

Unfortunately, the archiving there is very incomplete. Archive.org has long respected the Robots-txt standard, large files such as images and videos are often not saved, the frequency of spidering is often very long. Therefore, with the **WayBackMachine** you can only verify, not falsify: if you find something there, you have proof. If you don’t find anything there, it doesn’t prove anything. Nevertheless, this archive is currently an indispensable research tool.

The International Internet Preservation Consortium (IIPC) mainly brings together national libraries. Their initiatives are still in their infancy. Further initiatives for worldwide digital archiving can be found in a list from Wikipedia and Unesco.

WEB ARCHIVES

- WayBackMachine
- International Internet Preservation Consortium
- List of web archiving initiatives
- UNESCO Information preservation

SCIENTIFIC SEARCH ENGINES

Normal search engines spider the surface web, they search for new and updated web pages and include them in their index after analysing the content. Scientific search engines work differently. Either they do “focussed crawling”, i.e. they only search specific servers in the WWW, or they are supplied with the data by the operators of these servers. The servers supplying the data are operated by scientific organisations and are not accessible to normal search engines. Thus, scientific search engines open up parts of the Deep Web.

In addition to the pure data (for example, the text of a scientific article), these search engines also receive the metadata, i.e. the names of the authors, the publication date, the source and keywords. This increases the search quality considerably. In addition, many scientific search engines publish their lists of sources, so that you know exactly which databases you have searched and which you have not - unthinkable with normal search engines.

The search engine **Wolframalpha** plays a special role. It works with “curated data’’ and does not deliver web documents as results, but data, graphics and images. These are obtained from (unfortunately unnamed) sources. Wolframalpha provides, among other things, weather information for places, including historical information. This possibility of data retrieval makes the search engine an important tool for fact checkers.

NOTABLE EXAMPLES OF ACADEMIC DATABASES

Bielefeld Academic Search Engine (BASE)

Operator: Library of Bielefeld University
Data sources: Metadata of academic documents according to the OAI Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH), partly web harvesting.
Results: Metadata, full texts, local document servers.
https://www.base-search.net/
https://www.base-search.net/Search/Advanced
List of sources: https://www.base-search.net/about/de/about_sources.php

Directory of Open Access Journals (DOAJ)

Operator: Infrastructure Services for Open Access (is4oa)
Directory of open access electronic journals
https://doaj.org/
List of sources: DOAJ: journals added and removed: https://docs.google.com/spreadsheets/d/183mRBRqs2jOyP0qZWXN8dUd02D4vL0Mov_kgYF8HORM/edit#gid=0

Google Scholar

Advanced search via menu (Javascript)
Operator: Google Inc.
https://scholar.google.com/
Data sources: Probably the largest search engine for freely accessible and paid scholarly documents. Indexing of full texts and some metadata (author, journal, period).
Source list: not published (just Google)

OAIster

Operator: University of Michigan / OCLC
https://www.oclc.org/en/oaister.html
https://oaister.worldcat.org/
https://oaister.worldcat.org/advancedsearch
Data Sources: Virtual Union Catalogue - Searches specific servers according to the OAI Protocol for Metadata Harvesting (OAI-PMH), i.e.: metadata only, no documents directly.
Source list: https://www.oclc.org/en/oaister/contributors.html

WolframAlpha

Semantic search engine that does not return web documents as results, but data, graphics and images. Operator: Wolfram Research on https://www.wolframalpha.com/
Data sources: unclear, structured and curated data.

WorldWideScience

Operator: Office of Scientific and Technical Information (OSTI) of the US Department of Energy
https://worldwidescience.org/
https://worldwidescience.org/wws/desktop/en/search.html
Data sources: international science portal, links approx. 100 databases from over 70 countries,
List of sources: under the Advanced Search mask.

FROM OPEN DATA TO FINANCIAL INVESTIGATIONS, TOOLS AND TECHNIQUES

Šarunas Černiauskas

I. DATABASES AND TOOLS FOR INVESTIGATIVE RESEARCH

Crime and corruption works across borders. In order to successfully expose these wrongdoings, journalists should also work across borders. However, sometimes finding a teammate is hard due to time restrictions, and some people just prefer working solo. Although having a local journalist with good knowledge of finding and accessing data is, in my personal opinion, always a better option, a set of tools can empower a solo journalist to dig up just enough for a great story.

I.A: FOREIGN REGISTRIES

Whenever there's business involved, there's always some paperwork that has the potential to move your story forward. However, it's not always the same and not always accessible.

In tax havens like Belize or the BVI, official registries or gazettes give you nothing more but the company's name and the date of its registration. The really valuable data sits with service providers like Mossack Fonseca. Other countries, especially in Europe, have made significant improvements in the availability and transparency of business ownership.

For decades, the UK has been known to be a magnet for shady foreign investment, and a push for transparency has resulted in major improvements. The UK's Companies House now provides a lot of information free of charge, including company ownership and data on their true beneficiaries. It is very user friendly, easy to search and with lots of open data available.

Another great example is the Czech Republic. Both the business registry and the land registry are available free of charge, searchable by company name, address of the real estate or name of the beneficiary. The websites are entirely in Czech, which makes it a bit challenging, but Google translates the websites well enough to make it easy to navigate for a non-Czech speaker.

Until the Maydan revolution, Ukraine was far from excellent in data availability. The revolution led to a surge in transparency, moving Ukraine to one of the biggest leaps in data transparency in the continent. Apart from official services, like the state business registry, several great tools were developed privately. My favorite one is YouControl, a relatively cheap resource that provides you with detailed information on Ukrainian entities and has a nice English interface for any foreign users.

Data availability differs across Europe. Russia has a lot of information on business ownership free of charge, which might be somewhat surprising given the country's political regime. The abundance of data has resulted in multiple private online tools that allow browsing company data by name, number or an individual. Zachestnyibiznes is my personal favorite, mainly because of the name (it stands for "in the name of honest business"). However, it is one of many similar resources available across Russia.

Apart from business and land registries, there are databases on public spending, collections of court records and loads of other data scattered across the internet and just waiting for you to come and go fishing. We could go on and on, country by country, but the tools for that have been developed years ago.

OCCRP's Investigative Dashboard gives probably the best collection of data resources (free and paid) across the globe. Under 'Find Online Resources', you get a collection of business and land registries, public and private databases, gazettes, court rulings and lots of other official documents in most of the countries in the world. Some links sometimes get broken due to changes in official websites, but they get fixed as soon as someone notifies the data team about the issue. OCCRP also provides their human resources – brilliant researchers capable of gathering intel and documents for the story. However, due to vast demand, these resources have been limited to OCCRP member centers (you can still give it a shot, however).

I. B: FISHING RODS

By my own rough estimate, at least 35% of my investigative stories have come from random fishing on the internet. A single name or a document found by simply browsing in one of many possible resources is often the starting point of a major story. Here are some tools that work as excellent fishing rods.

OCCRP's Aleph is, by far, my favorite, and it has nothing to do with my position at OCCRP. Aleph is simply the best resource there is. It gathers data from public registries, official gazettes, court records, public procurement and all kinds of other records available online, including some basic data from international leaks, like the WikiLeaks cables and others. It is a very wide resource – probably the biggest vault of official, semi-official and unofficial data adapted for the journalist mindset. In many cases, Aleph also gives you the scans of original documents and saves you loads of time. It is being updated constantly, so there's no point in saying that it has data on 215 million entities now – because this number will probably be bigger when you are reading this manual. Aleph is very concise; it saves hours and days of work by doing the data gathering and processing for you. It lets you do both narrow and superwide searches and modify the scope of your research at any moment. Of course, Aleph is not an official registry of any kind, and some data is being refreshed more often than others, so once you find something of interest, you must double check in the primary source.

When it comes to famous international leaks, the ICIJ put all of the key ownership data from the Panama Papers, Paradise Papers and other leaks into the OffshoreLeaks database. It's easy to search, very visual thanks to the Linkurious platform, and it's one of the few cases where light is being shed on offshore secrecy. The system also has its downsides. First and foremost, it is leak-based, so the information is not updated regularly, and data from, e.g. 2010 is still there, but isn't necessarily still valid today. One might get demotivated by the fact that the data has been browsed by millions of outsiders already. But there is still stuff nobody has discovered, and there's still lots of stories there.

OpenCorporates is one of the resources that have been there for ages. Easy to search, regularly updated with data from numerous registries – it is a very good tool to gather basic information on foreign companies or go fishing for persons of interest.

All of the above are great alternatives for expensive resources like Orbis or LexisNexis, but if your organization has the funds needed to use either or both, don't hesitate.

I. C: HARPOONS

A separate set of tools can be used to both fish randomly and do a precise hit, especially when it comes to tracking expensive assets like jets or ships, including yachts.

MarineTraffic is a live database for ships, browsable by name or the unique IMO number. The free service gives you the basic search options, including the vessel's former names, which makes tracking ships really user friendly. When it comes to tracking the vessel's movement, the free service is not that good and you need pay in order to get a detailed history of where a particular ship has been.

FlightRadar provides, basically, the same kind of service as MarineTraffic, but for planes. And, just like with MarineTraffic, you need to pay if you want details on where the vehicle of interest has been moving.

Other resources might give more data on movement, so it's recommended to use several tools for both flight and ship tracking. For example, Vesselfinder for ships and Planefinder for jets.

When it comes to defining ownership, quite a lot of information is available in the paid services of systems like MarineTraffic. There are, however, free resources that give you just that:

Equasis is my personal favorite when it comes to ship ownership. It's free, it's pretty simple and it has lots of data on vessels from around the globe, including superyachts. Equasis gives you the ship's management, ownership and flags, with historical records included. It is searchable by ship or by company. Also, Equasis often provides data about inspections carried out in particular cargo ships, and the data on those inspections can be extremely valuable.

For example, the Beirut explosion story was centered around a cargo ship, and our OCCRP investigation into it was largely based on the Equasis data. Personally, I recommend tracking vessels with their IMO numbers, findable easily on MarineTraffic, since vessels tend to change name after changes in ownership or being exposed in criminal activities. A vessel's name can change, but the IMO cannot – just like you can change your name and surname, but the ID number is forever.

Similarly to Equasis, AirFrames gives quite a lot of data on airplane ownership. Just punch in the tail number, and you have a good chance of learning a lot about the jet's owners. Also, do not disregard sites for enthusiasts like PlaneSpotters or SuperYachtFan, where people aren't usually investigating stuff, but tend to have detailed information about a plane or a yacht, just because they enjoy it.

When it comes to concise international trading statistics, UN Comtrade is probably the best available resource. It lets you analyze trading statistics of a particular country or between states, both in general figures and in specific commodities. Based on stats from official agencies across the globe, it is probably the best available set of trading statistics. It is a bit complex for a new user, since the stats are based on commodity codes, which are hard to figure out and distinguish. Also, the data is not necessarily accurate when it comes to mirror analysis in trading between particular countries. Inconsistencies in data are likely and primary sources need to be contacted to verify your findings, but playing around with Comtrade data can certainly lead to breakthroughs.

Last, but not least, Bellingcat has one of the most detailed journalist toolkits in the world. There, you will find most of the above resources and much more.

II. COMBINED USE OF LEAKS AND CORPORATE DOCUMENTS: A CASE STUDY

Combining the information from business registries, financial documents and other sources of information often leads to major breakthroughs in investigative stories. Here, I will present several tools and techniques of following the papertrail, along with some practical examples of how these tools and techniques lead to big stories.

To investigate an entity, one needs to know its essential facts:

- Who owns (or owned) it
- Where it is/was based
- What it does
- What assets it has
- How it makes money

Any of the essentials can be the story. A company owned by a decision maker or his/her relatives can lead to corruption. Several companies registered under the same address can indicate money laundering, fraud in public procurement and a variety of new leads. Business operations and assets can lead to a whole range of investigative scenarios. And the best way to gather the essential information is diving into the papers.

II. A: AN INTRODUCTION TO FINANCIAL READING

Every legal entity – for profit or nonprofit – follows the same structure of reporting its activities. Depending on jurisdiction and local legislation, these documents can be bought or accessed free of charge in many countries.

The **balance sheet** is all about figures. It reflects the basic information about the entity in numbers. How big is the value of its assets, divided into tangible and intangible assets, value of its capital, liabilities etc.

The **profit and loss account** is a reflection of the entity's operations, yet again, in digits-only. The table shows how big the entity's earnings were, its spending, and how profitable (or unprofitable) it is. Often enough, it also gives a glimpse at some of the taxes being paid. Or not being paid.

Worldwide accounting standards often make the balance sheets and the profit/loss accounts readable without speaking a word of the language. Most importantly, these documents reflect the state of the entity on a yearly basis. Therefore, combining several of these documents allows you to see how the entity operated in retrospective.

Personally, when starting to investigate any legal entity, I always begin with the balance sheets and profit/loss accounts. Looking at these figures almost instantly gives the general impression of what scope of activities I'm dealing with. In some cases, these documents alone contain the essential data that ends up being the story.

This is exactly what happened in the practical case. But before we go to practice, one more document needs to be introduced.

The **annual report**.This is a detailed reflection of the entity's operations during the financial year. In some cases, it fits into 3-5 pages. In big businesses, it can reach dozens or hundreds of pages. Good and detailed annual reports give a great understanding of the entity's operations. They explain changes in assets, profits and losses. These documents often include descriptions of major deals an entity made, relationships and business conducted with related entities, investments, and lawsuits etc.

The annual report might look scary when you first open one. Tens or dozens of pages seems overwhelming, and the financial language can sound like gibberish to an untrained eye. But when you learn to read it, it's no longer a nightmare. It can be your best friend.

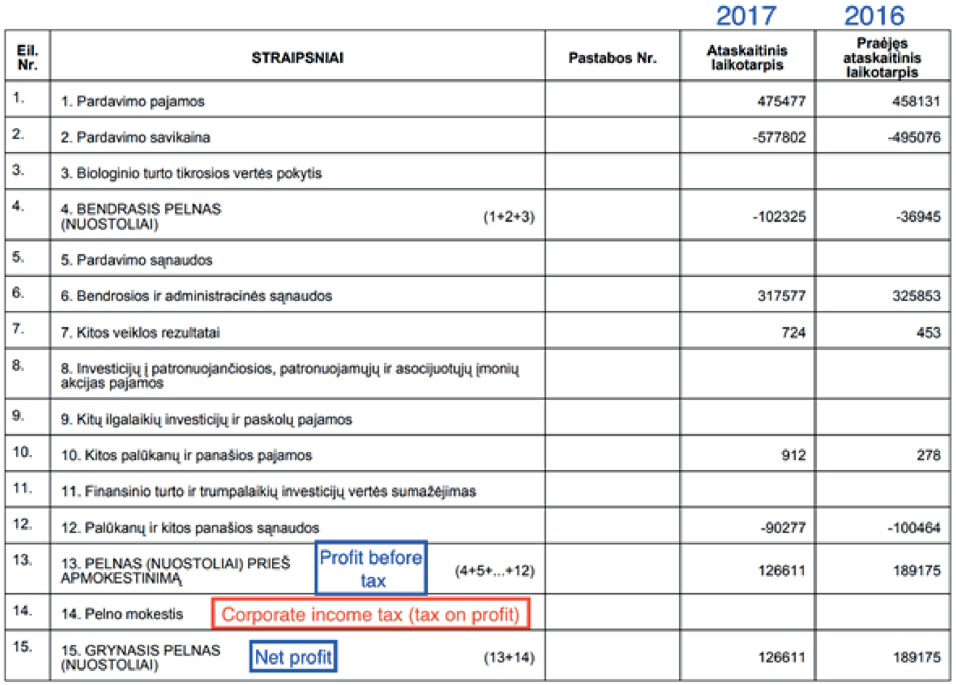
II. B: BONO'S SECRET LITHUANIAN VENTURE

The 2017 Paradise Papers 2017, an ICIJ global investigation based on several sets of leaked documents, offered another rare glimpse into the secretive offshore industry and exposed a variety of power players and celebrities involved in it. Among them, there was Paul David Hewson, better known as Bono – the lead singer of U2.

The Paradise Papers data showed that Bono was the co-owner of a shopping mall in Lithuania. To be precise, in Utena – a small town with a population of some 25,000. That's way below what U2 usually gathers when it throws a concert.

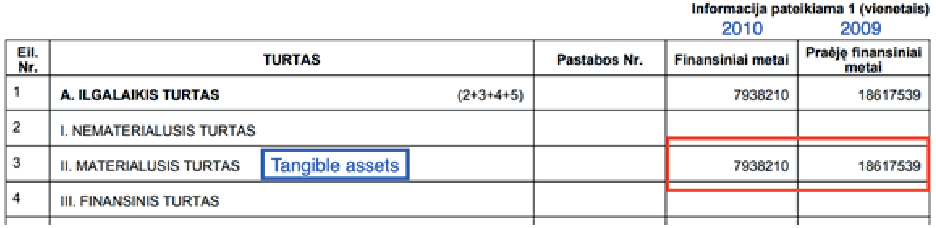
So, the story was there already. Bono secretly owning an average mall in a very average Lithuanian town – that's a national sensation by itself. But the story ended up being much more than that.

While looking into the Lithuanian company's most basic documents, I first noticed something in the profit/loss statement. More precisely, something was missing. The company was making profits on a yearly basis, but the field for corporate income tax was blank, repeatedly.



			2017	2016
Eil. Nr.	STRAIPSNIAI	Pastabos Nr.	Ataskaitinis laikotarpis	Praėjęs ataskaitinis laikotarpis
1.	1. Pardavimo pajamos		475477	458131
2.	2. Pardavimo savikaina		-577802	-495076
3.	3. Biologinio turto tikrosios vertės pokytis			
4.	4. BENDRASIS PELNAS (NUOSTOLIAI) (1+2+3)		-102325	-36945
5.	5. Pardavimo sąnaudos			
6.	6. Bendrosios ir administracinės sąnaudos		317577	325853
7.	7. Kitos veiklos rezultatai		724	453
8.	8. Investicijų į patronuojančiosios, patronuojamųjų ir asocijuotųjų įmonių akcijas pajamos			
9.	9. Kitų ilgalaikių investicijų ir paskolų pajamos			
10.	10. Kitos palūkanų ir panašios pajamos		912	278
11.	11. Finansinio turto ir trumpalaikių investicijų vertės sumažėjimas			
12.	12. Palūkanų ir kitos panašios sąnaudos		-90277	-100464
13.	13. PELNAS (NUOSTOLIAI) PRIEŠ APMOKESTINIMĄ Profit before tax (4+5+...+12)		126611	189175
14.	14. Pelno mokestis Corporate income tax (tax on profit)			
15.	15. GRYNASIS PELNAS (NUOSTOLIAI) Net profit (13+14)		126611	189175

Then, I followed the trail back in time in order to see if there were major fluctuations anywhere else. And indeed – there were. The next piece of evidence appeared while going through 7 years worth of balance sheets. The analysis showed that in 2010, the company's tangible assets shrank by some 57%.



Informacija pateikiama 1 (vienetais)

			2010	2009
Eil. Nr.	TURTAS	Pastabos Nr.	Finansiniai metai	Praėję finansiniai metai
1	A. ILGALAIKIS TURTAS (2+3+4+5)		7938210	18617539
2	I. NEMATERIALUSIS TURTAS			
3	II. MATERIALUSIS TURTAS Tangible assets		7938210	18617539
4	III. FINANSINIS TURTAS			

The next step was picking up the annual report for 2010, because that is when the major drop in tangible assets occurred. And there it was. The company reported a huge loss, but it was not the usual kind of loss, when you spend more than you earn. The loss was mostly generated by the revaluation of the company's principal asset – the shopping mall.

The company revalued the mall's market price due to the ongoing financial crisis. The new value of the venue was most probably true and accurate, but the company didn't suffer an actual financial loss. However, the drop in the mall's value was reported as a real multi-million loss, and that allowed the company to pay no corporate income tax for years to come.

After the story ran, the Lithuanian tax office started investigating Bono's shopping mall. As a result, the company agreed to willingly pay additional tax, and Bono announced he is pulling out from his Lithuanian venture.

The catch with these essential financial documents is pretty simple. First and foremost, you must look for big fluctuations in the entity's assets or money flows – these events tend to signal unusual activities that can end up in an investigative story. Also, anything unusual can be the story. As in the practical example – the initial lead was not something that was in the table. It was something that was missing – the empty line for corporate income tax.

When it comes to reading annual reports, the first few pages are usually standard and contain little or no information of value. Most of the interesting stuff tends to come later, when the reports explain the entity's activities, changes in assets and deals. However, that doesn't mean one should automatically disregard the introductory part of the annual report. In some cases, the first pages contain vital information about the entity's ownership, related entities and major events of the financial year.

Some essential tips on what can be found in annual reports:

- Changes in the entity's ownership;
- Transactions with related parties (subsidiaries, other entities owned by the same owners etc.);
- Sale and/or acquisition of assets;
- Lawsuits.

Any of the above can end up in an investigative story. A chain of related party transactions can lead to a tax evasion mechanism. Transactions involving assets can be the evidence for tax fraud or political corruption. Lawsuits can lead to court records that disclose unknown transactions of the entity, and those transactions can be the basis for the entire story with a multitude of possible scenarios.

If you can't decide if something in the balance, profit/loss account or the annual report is shady, there is nothing to worry about. You aren't a business manager or a stock trader trained to understand all of it. But you most probably know people who are. So, whenever you find something suspicious, consult an expert.

Practical tip: The expert can be a few footsteps away. If you're working within an organization that runs its own accounting, your accountant is very likely to be your first reliable option to verify if something in the financial documents is signaling wrongdoing. From my personal practice, accountants tend to be very helpful and enthusiastic about getting involved, because you give them the unusual opportunity to use their expertise for something really exciting.

FUNDAMENTAL APPROACHES TO DIGITAL SAFETY

Tactical Tech - Exposing the Invisible

Staying safe is an integral part of any investigation. Your safety, and that of your data, your human sources and your collaborators should always be a priority. It is important to recognize that safety is not just a matter of employing safe tools. Tools are only a part of your approach to security. Understanding the risks you face and the context you find yourself can help you with picking the right tools and digital security strategy.

Safety is about the function you perform and the context in which the function is performed. It cannot be neatly divided into digital and non-digital, so pay attention to how online and offline behaviors affect one another and your overall safety. You cannot approach safety in isolation from that of other people you work and communicate with. Think of it as a team sport rather than an individual practice.

It's therefore vital to think of the risks associated with the type of research or investigation activity you are undertaking in any context, in order to mitigate those risks. This is part of a process called **risk assessment.** Risk assessments are a common exercise in a number of disciplines involving online and offline / field activities including scientific research, journalistic investigations, information collection by NGOs, or law enforcement investigations.

Before starting your work, make sure you also have a **risk mitigation** or **risk reduction plan**. This involves coming up with ways you could prevent, respond to and resolve problems that might arise. This plan can help you navigate the potential issues highlighted in your risk assessment.

RISK ASSESSMENT

When conducting an investigation, the topic of your investigation or who you are investigating can greatly affect the risks involved. At the same time the findings of an investigation, even when conducted with digital safety precautions can cause an investigator to be targeted and challenged, rather than just the findings of the investigation. Therefore it is important to think of the risks associated with what you are trying to uncover and the risks that are associated with the personal safety of the investigators involved.

When thinking about risks, a good practice is to brainstorm all possible risks that you can think of. The process of writing them down helps with visibility of risks particularly if there is a team involved in the investigation. Since it is difficult to focus on all the possible risks, a good practice is to focus on those risks that are most likely and will have the most damaging impact in order to mitigate.

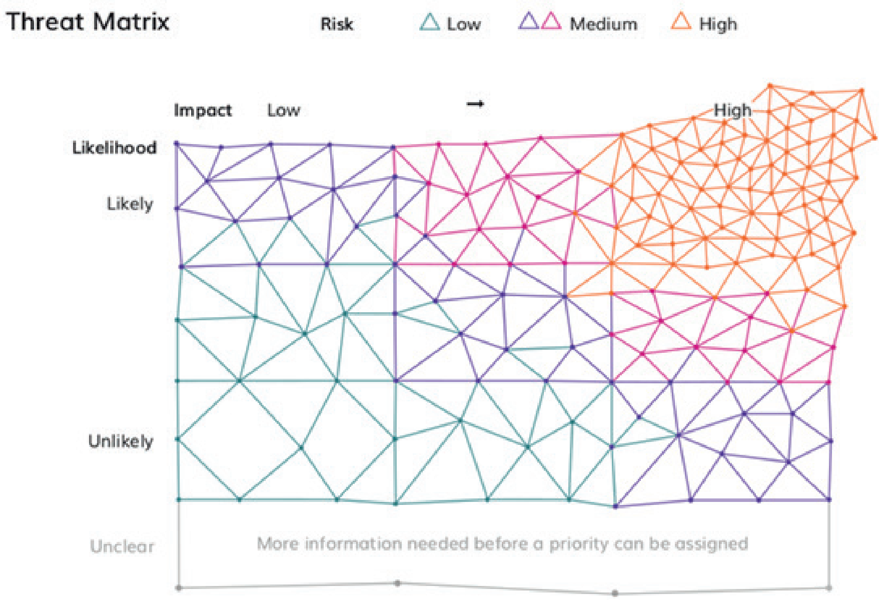


Image of threat matrix from Tactical Tech's Holistic Security manual, source: https://holistic-security.tacticaltech.org/chapters/explore/2-8-identifying-and-analysing-threats.html. The idea behind this matrix is that threats can be viewed and categorised in light of the following: 1. - the likelihood that the threat will take place, and 2. - the impact if and when it does take place. Likelihood and impact are concepts which help us determine risk: the higher the likelihood or impact of a threat, the higher the risk. If a threat is less likely or would have a lower impact, the risk is lower.

In order to identify the threats you may face, ask yourself what data do you want to keep safe or private. If you want to keep something safe, who are you protecting it from? This is important because the answer to this question gives you an insight into what technical capabilities you are up against. What would be the impact of failing to keep data safe? This can help determine how you compartmentalize your data and help with contingency planning.

There is no particular risk assessment and risk mitigation template that you should follow as a rule, you will need to adapt this process to your own research methods and your context as well as to the topics and subjects of your investigation. You would have different degrees and kinds of risk or threat if you search the internet for NGO reports about human rights abuses by corporations from your home, or if you conduct field research to observe facts and interview affected people. Similarly, you would have to plan for different kinds of risk if you take photos of the town hall building in the centre of a peaceful town than if you need to photograph an area where deforestation is on-going, in an isolated place at the edge of the same town.

RISK IS INHERITED

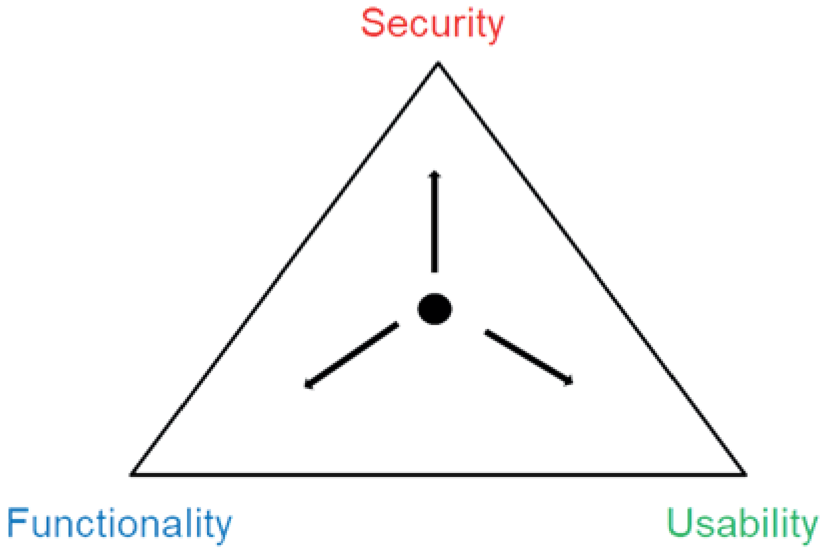
If you are someone with little to no risk (you may live and work in a safe area) but you are interviewing a person experiencing high risk (living in a dangerous area, being under pressure, working on controversial issues), you inherit that risk. Your risk level will be higher for a period of time before and after the interview. If you interview someone for a report or an article that will be published, be prepared for your risk to increase at the time of publication. When investigating individuals in positions of power and influence, be prepared for a prolonged higher risk (both digital and physical) if they become aware of your investigation.

THE SECURITY TRADE-OFF

When choosing tools, you often have a trade-off between what is useful, easy to use and secure.

While many tools have focused a lot more on security, you still have to weigh your security against functionality and usability. The key here is to understand the context you are in, and what you are gaining or giving up by using a particular tool. It is important to identify your weaknesses rather than reinforce your strengths. Usually your weakest points are those that are exploited, and for these weaknesses it makes sense to invest in security aspects over functionality or usability at times.

For example, a very secure tool might require entering a password every time you use it, while another is more easily usable by saving the password for you. The trade-off is between simply using the application, which takes less time, but making it susceptible to being accessed if your device is stolen.



SOME CRITERIA TO HELP YOU ASSESS A DIGITAL TOOL

A lot of times tools are recommended by security experts. These recommendations come from evaluating what the tools do, how they're written and what vulnerabilities they have and what they can expose. You do not need to be a digital security expert to understand the basic reasoning that makes tools secure. You can apply a set of questions to any new tool you may encounter to get a general idea as to how safe a tool is.

Always check if the tool:

Is Open source - Is the source code publicly available for you or others to see? Even if you cannot read or assess the code, being open source means it can be verified and audited by those with expertise.

Provides end-to-end encryption - This means that data is encrypted before sending to the receiving party, and only they can decrypt the data and not even the service provider providing the infrastructure, platform and applications to deliver the message.

Does not store data unnecessarily - Tools that keep track of more data than they need in order to perform their function risk exposing this data in the future.

Does not leak data - When performing functions with that tool, no unnecessary data is inadvertently exposed to the public or third parties.

Does not share data - Some tools or services share your data or sell them to third parties; you can often find out about this if you read a tool's (app, software, etc.) terms of use and/or data policy.

DIGITAL SAFETY TIPS

When thinking about keeping your data and information safe you may be thinking about two separate things:

1. The first is about safeguarding your data so that it cannot be used by a malicious actor to cause harm or does not constitute a breach of privacy.
2. The second is about keeping it safe so that you can recover it in case it is damaged or lost.

Digital safety is about safeguarding your data. This data can be your:

- contacts
- location
- passwords
- digital habits

This data can be available in your:

- devices
- communications
- online accounts
- internet traffic

But **remember that safety doesn't just mean tools**. Most of what compromises us is not the technical tools we choose but our behaviour. Humans are often the weakest link and even if you are using the most secure tools, you can still be breached.

Some things to keep in mind when thinking about safety:

- what you choose to share,
- how you communicate,
- what you click (phishing attacks),
- which services you choose,
- who you choose to share with.

SOME PRACTICES TO HELP KEEP YOUR CREDENTIALS AND DATA SAFE

- Use long passphrases,
- Use two factor authorization,
- Safeguard passwords using password managers,
- Ensure having recovery tools set up where possible, like adding a recovery email,
- Backup data,
- Encrypt data,

- End-to-end encryption helps guarantee that the service provider cannot access your content,
- Be aware of who has access to your data,
- Assess tools you use.

SECURING DATA AND DEVICES

When conducting investigations a lot of the data you gather will live on your devices. These devices can be your mobile phone, your tablet, laptop or your storage devices such as hard drives and flash disks. As mentioned earlier, it is important to safeguard your devices and data against malicious actors that may use the data to cause harm. At the same time you should safeguard your data from loss in case your device is lost or stolen.

Make sure that you have your data and devices secure, you can do so by ensuring that your devices are encrypted and that you have regular backups. Some recommended practices and tools are:

- Use Full Disk Encryption: use tools like Bitlocker (for Windows), FileVault (Mac), dm-crypt (Linux) to encrypt your disk and the files on your computer.
- Use VeraCrypt or Cryptomator file containers for data you store on your device.
- Backup your data on cloud and hard drives to secure it in case of loss of devices.

ONLINE SAFETY IS CONTEXT BASED

Searching and collecting evidence online - whether it's about social media data, online company records, domain ownership details, website history, image metadata, etc. - involves navigating a large number of platforms, tools and services.

Some of these work with the Tor Browser and that allows you to protect your privacy to a certain extent. Others not only do not work on Tor but they also require you to sign up with an email address, name and other personal details.

Depending on your investigation subject, your context and that of the people you work with, leaving digital traces while you investigate online might put you at higher risk.

Always remember that digital/online safety and physical safety are strongly interconnected and they should both be included in your risk assessment at all times. Digital vulnerabilities can lead to physical threats and vice-versa.

Consider these suggestions for digital safety techniques and tools that can help protect your digital privacy and enhance the security of your devices and data.

ACCOUNTS

Some online services require you to create an account, to choose a username, to provide payment information, to verify an email address or to sign up with your social media profile to gain access to their platforms.

- Try to limit your exposure by considering these options:
- Create a more secure, compartmentalised email account, which you can do easily with services like Tutanota (tutanota.de) or Protonmail (protonmail.com).
- The more complicated and risky your activity, the more comprehensive your risk assessment should be.
- The Tor Browser is a browser that keeps your online activities private. It disguises your identity and protects your web traffic from many forms of internet surveillance. It can also be used to bypass internet filters.
- Establish a separate set of social media accounts to use with services that require your data, in order to compartmentalise (separate) your investigative work from your personal online identity.
- Create a single use “identity” for a particular investigation, and dispose of it once research is done. This may be needed especially when doing sensitive work.

BROWSERS

As someone who is looking to uncover hidden truths, you probably already use the internet for personal communication and for some of your research. We recommend you choose a "privacy aware" browser for your research and avoid logging in to web-based email and social media on that browser. This will prevent a lot of your personal data from being sent to the websites you visit.

Before using any of the online tools we talk about here or in the online Kit, it's a good idea to download and install one of these browsers. Then, add an extra layer of certainty by testing the browser with a tool like Cover Your Tracks or Browser Leaks. The results of what you see when using a privacy aware browser should look different from when you visit Cover Your Tracks or Browser Leaks with a normal browser, which would usually reveal more weaknesses.

These are some examples of tools that can help protect your privacy while researching online, with pros and cons of using them:

Tor Browser (torproject.org)

- Pros: This is the best privacy aware browser. The code is published openly so anyone can see how it works. It has a built-in way of changing your IP address and encrypting your traffic.
- Cons: There are places in the world where Tor Browser usage is blocked or banned. While there are ways around these blocks, such as Tor Bridges (torproject.org/docs/bridges), using Tor may also flag your traffic as suspicious in such places.

Firefox (firefox.com)

- Pros: It blocks trackers and cookies with a setting called "Enhanced Tracking Protection", which is automatically turned on when you set "Content Blocking" to "strict".
- Cons: You need to turn on this option, it's off by default. When you use Firefox, it's important to remember that your IP address is still visible to the sites you visit.

Brave (brave.com)

- Pros: It tries to protect privacy without the need for turning options on or adding add-ons or extensions. Brave has a security setting to erase all Private Data when the browser is closed. It has a feature called 'Shields' where you can block ads and trackers. It also allows you to create a new "Private Tab with Tor", which uses the Tor network to protect your IP address (regular use doesn't protect it).
- Cons: The "payments" or "Brave payments" feature that allows donations should be kept off as it sends data that could be used to identify you. When using use Brave, you should use the 'Private Tab with Tor' feature to protect your IP address.

DuckDuckGo (duckduckgo.com)

- Pros: This is a privacy-aware search engine (not a browser) that claims not to collect any personal data about its users. You can use DuckDuckGo in combination with the Tor Browser to further preserve your privacy.
- Cons: DuckDuckGo does save your search queries but it doesn't collect data that can identify you personally

VIRTUAL PRIVATE NETWORKS (VPNS)

If you cannot use Tor, another option, though less effective in preserving your anonymity, is to use a VPN (Virtual Private Network). Visiting a website is like making a phone call. The website you are visiting can see your "number" - your IP address - which can be used to map where you are coming from.

Think of the VPN as a concrete tunnel between you and the site you want to visit. The VPN creates a tunnel around your traffic so it can't be observed from the outside, and routes it through an intermediary server owned by your VPN provider, so your traffic looks to any site you visit like it's coming from a different location than where you actually are.

Neither the web browser, your internet service provider nor the site you visit will see your IP or be able to identify you. Sites will only see that your traffic is coming from the IP address of your VPN provider.

There are many VPN options and it can be confusing when deciding which one to pick. To add to the confusion, most VPN reviews and listings are not independent, some are really biased. ThatOnePrivacySite (thatoneprivacysite.net) is a VPN review site we can endorse.

It is recommended you choose a VPN company that claims that they do not record logs of your traffic. While you should avoid most free VPNs because they are often funding their operation by selling their log data (records of what sites users visit via the VPN), there are some reputable ones we recommend:

- Bitmask,
- Riseup VPN,
- PsIPhon,
- Lantern.

COMMUNICATION

When picking a means of communication, there are many factors to consider. While the security of an application that you use is important, communication involves at least two parties and it is only as secure as the least secure party.

Whenever possible, use encrypted email (PGP - Pretty Good Privacy,) in communication with collaborators, sources and interviewees. For calls and messaging, there are different applications with enhanced levels of encryption and privacy such as Signal or Wire. These can be considered more secure than WhatsApp because they retain less metadata (information about the communication) though WhatsApp is of more common use and you may encounter people who are not easily accessible on any other apps.

Besides the security of the communication means of your choice, consider whether that choice leaves a digital footprint that can add to your risks instead of keep you safe. For example, if you're using a secure messaging app to communicate with someone in a country where that app has a poor reputation with that country's authorities, you may be placing the other party at risk of being unnecessarily targeted.

When you are forced to rely on conventional ways of communication[1] - non-encrypted phone calls, landlines, etc., - make sure that you provide only the minimum information and try to establish in advance what details are less risky to communicate with the person at the other end of the line, and how. When fearing threats and surveillance, use the above encrypted methods to get in touch with someone close to your sources who can help organise a meeting.

ONLINE COLLABORATION

When collaborating through document writing or sharing, data on the cloud must be secured. One alternative to Google Docs can be cryptpad.fr which allows for access without signing up and encrypts documents. Upon sign up you can also share files and password protect them. Secure collaboration can be very important as you work across different countries and with multiple people.

KEEPING YOUR LOCATION SAFE

A number of common apps, including Google Maps and WhatsApp, allow you to share your real-time location with specific people for a limited period of time. This feature could potentially be helpful when conducting field research because it can allow a trusted colleague to monitor where you are, as a safety measure. It is also an important element when documenting movements and storing geolocation of your evidence (such as photos, videos) to be used as proof later on.

On the other hand, sharing your location in real time can put you at risk if others who are interested in your whereabouts are able to access the data you share. When researching sensitive topics, or if you suspect that you might be under surveillance, you should avoid sharing or storing your location without using encryption.

Instead, consider finding alternative ways of tracking your daily movements while investigating, such as marking places and details manually, or using a printed map. In many cases, it is wiser to disable such location sharing features from your mobile phone and other devices with location tracking functions. Most smartphones allow you to do so under "Location Settings."

[1] For information about navigating communication: tools: https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools

ACCESS TO INFORMATION FOR JOURNALISTS

Access Info Europe

THE RIGHT TO KNOW AND ITS POTENTIAL FOR JOURNALISTS

Journalists play a central role in initiating and stimulating public debates, but face constant challenges in accessing information from public bodies, particularly when that information relates to sensitive issues such as corruption, organised crime, environmental contamination, or relationships with business and lobby groups. They can only achieve this role through the information they are able to obtain.

Similarly, in a democracy it is essential that people can access a wide range of information in order to participate in a real and effective way in the matters that affect them. Everyone's right to form an opinion and express that opinion depends on having access to information.

Many international human rights bodies have recognised that access to information is a fundamental right, and is an inherent part of freedom of expression, a right which is in turn enshrined in multiple international conventions:

- The United Nations Declaration of Human Rights, article 19
- The International Covenant on Civil and Political Rights, article 19
- The European Convention on Human Rights, article 10
- The Charter of Fundamental Rights of the European Union, article 11
- The African Charter on Human and Peoples' Rights, article 9
- The American Convention of Human Rights, article 13

Even where the language of these conventions does not explicitly mention "the right of access to information", that it forms part of the right to freedom of expression has been recognised by the UN Human Rights Committee, the European Court of Human Rights, and the Inter-American Court of Human Rights.

This right can be exercised using access to information laws, which 130 countries worldwide now have, including 46 laws in the wider European region. In addition, the EU and many inter-governmental organisations have rules for accessing their documents.

For journalists, access to information laws are a particularly useful tool in both everyday reporting and in more in-depth investigations, ensuring that journalists can exercise their role as public watchdogs. This guide gives you key tips on how to exercise this right and, specifically, how to use access to information laws.

THE TWO DIMENSIONS OF THE RIGHT TO INFORMATION

All governments have an obligation to ensure that they respect the right of access to information in order to ensure full respect for freedom of expression. The right has two dimensions:

- **Proactive:** There is a positive obligation on public bodies to provide, to publish, and to disseminate information about their main activities, budgets, policies and plans. This is essential so the public can know what they are doing, can participate in public matters and can control how public authorities are behaving.
- **Reactive:** Everyone has a right to ask public bodies for information they hold and the right to receive an answer. The majority of information held by public bodies should be available, but there are some cases where the information is withheld in order to protect legitimate interests such as privacy, national security or commercial secrets.

FIFTEEN TOP TIPS FOR JOURNALISTS

The following tips are designed to help journalists working in any media – newspapers, radio, and television – as well as bloggers and other information professionals to get access to information held by public bodies for their stories, in their own country or in another.

The tips are based on a comparative analysis of access to information laws globally. As not all countries have perfect access to information laws, there are small variances, which is why we suggest that you check the law that you are going to analyse. You can find the laws here: www.RTI-Rating.org.

1. PLAN AHEAD TO SAVE TIME

When submitting an access to information request, first consider how you can request from the institution or body you are seeking information from. For example, can you request via email (do you have the email address of the transparency office of the institution?) or do you need to submit an application form providing personal information (and where can you find the form?).

> **Check your national access to information law or the law of the country where you plan to submit the request. You can find more on all access to information laws at www.RTI-Rating.org**
>
> **At the EU level, requests can be sent via the AsktheEU.org platform www.asktheEU.org or again, can you request on a similar national platform.**

Second, it is wise to think about what kind of information can be requested, whether you can request any kind of information or just documents. Some rules, such as the EU's Regulation 1049/2001 require you to request "documents", although **in most countries you can ask for either information or documents.** We recommend **being very specific** about which documents you want to access.

Another important consideration is the **timing of your request**. It is recommended that you submit your request at the beginning of your research so that you allow for the time that it takes to get a response about your request. The time frame between your initial request and getting a response is usually 15-30 days but it may take more time depending on where you are requesting the information from. Acquaint yourself with the time frames in the law you will use before you submit the request.

2. START OUT WITH A SIMPLE REQUEST

The best way to submit a request is by keeping it simple. In all countries, it is best to start with a simple request for information and then to add more questions once you get the initial information. It is not necessary to state the reason why you are requesting, simply state, in clear and concise manner, the information that you wish to access. Starting out simple would limit the chance of delay for the public body to extend your request because it is not precise enough or is 'complex'. Once you have received an initial response with some information, then it is possible to make more specific or supplementary requests.

You also have the option to hide your "real" request in a more general one. For example, you are interested in a specific public procurement contract, but you could ask for all the contracts from that month. **Just note that you need to make your request broad enough so that it captures the information you want but not so broad as to be unclear or discourage a response**. If you realise that the information you are requesting is broad, try to select a range of time within which the documents were created or shared.

It is possible to submit multiple requests to different bodies. This is particularly useful if you are unsure about where to submit your request or if you want to request the same kind of information from two or three different bodies whilst allowing you to submit your requests all at the same time. The various responses you may get from the institutions or bodies may be extremely useful in helping you to get a full picture of the information available on the subject you are investigating.

3. CHECK THE RULES ABOUT FEES AND ASK FOR ELECTRONIC DOCUMENTS

It is a good idea to check before you make your request whether you can be charged a fee. You will find this information in the national law or any implementing regulations. This way, if a public official suddenly asks you for money, you will know what your rights are.

In some countries you can be charged for the copying and postage of documents. **To avoid these fees, you can request for documents to be provided electronically.**

If a large number of documents are involved and there is a risk of paying copying charges, you can also ask if it is possible to consult the originals on the premises, which should be free of charge. This may not be possible if exceptions apply to the documents.

4. SHOW THAT YOU KNOW YOUR RIGHTS!

It is not a requirement to cite an access to information law or freedom of information act in your request, however, **it is recommended that you do so,** as in that way you demonstrate that you are aware of your legal rights, which should encourage the correct processing of the request according to the law.

You can use the RTI Rating website to get more detailed information about national access to information laws, see www.rti-rating.org for more details.

It is always recommended that you use language and etiquette appropriate to any other professional communication in your country.

5. STATE HOW YOU WOULD LIKE TO RECEIVE THE INFORMATION

Be clear about the format in which you would like to receive your information once you are granted access. It is your right to request information according to your preference, which could be consulting the document at the premise, a copy by post, or digital copies by email.

The public institution or body should respect your preference, but remember in the case of producing and posting original documents you may be charged a fee, so it is often best to choose an electronic copy as your preference. We strongly recommend to include a sentence at the end of your request that states that you would like to receive the information in electronic and machine-readable format.

If you are looking for quantitative data, you could mention specifically that you would be happy to receive a spreadsheet or other machine-readable extract from a database.

6. NEVER SAY WHY, BUT YOU COULD CONSIDER SAYING YOU ARE A JOURNALIST

As the right of access to information is a fundamental right, you never need to justify the reason of your request nor what you plan to do with it. Most access to information laws are very clear about this – **the EU's rules make clear that the requester is "not obliged to state the reasons" (Regulation 1049/2001, Article 6).**

You might, however, want to signal that you are a journalist, especially if you think this will help you argue to get the information more rapidly. You could do this by getting your media outlet to make the request or by including the organisation's logo (if this is acceptable to the organisation). Another option is to mention in the letter or email that you are a journalist and/or who you work for.

Remember, however, that, just as it is not necessary to disclose the reason why you are requesting information, you never have to state that you are a journalist. If you plan to send an email from your work address, it will often be obvious that you are a journalist, e.g.: jsmith@dailytimes.com. **If you do not want to give the game away, it might be worth using a different address**, such as a Gmail/ Hotmail/Yahoo account.

7. KEEP A RECORD AND CHECK THE TIMELINES

Make sure to keep on track of the timelines, starting the moment you submit your request. Take note of the timelines set by the institution in which you are requesting the information from, considering that **the average time to expect a response is 15-30 days**. Be careful to check the law here, as these might be working or natural days, which makes a difference as to how long you might have to wait for an answer.

By paying close attention to the timelines **you can then submit an appeal if it appears that the institution did not respect the given timelines**, unless they notified you in advance that there will be a delay. Note that proper reasoning has to be given for any extensions to the time frame, and this is something you can challenge if you are not convinced by the reasons.

8. SPEED UP ANSWERS BY MAKING IT PUBLIC THAT YOU SUBMITTED A REQUEST

A way of speeding up a response to your request is by **writing a story about it and broadcasting it for the public** to read. The main reason for this is so that the public institution feels pressure from the attention surrounding the request and processes and responds to the request quicker. As your request is being processed or there is an official response, you can continually update your story.

If there is no response or if the institution does not respect the deadlines/ time limits, **you can also make this known to the public**. No matter what the eventual response is, there are great benefits in making your request known to the public, as it not only puts pressure on institutions but it can educate members of the public about the right of access to information and how it works in practice.

9. HOW TO CHALLENGE REFUSALS AND SILENCE: THE APPEAL PROCESS & OVERSIGHT BODIES

If your request is refused or if no response comes within the timeframe, it is likely that you will want to make an appeal. The law should make clear what the process is. Normally it's either an appeal to the same body or you can go straight to an oversight body such as an information commissioner or an ombudsman.

If you are not sure what to do for the first stage of appeal, **contact the office of your Information Commission/Commissioner or Ombudsman** and they will be able to help you. If you don't have such a body, try phoning the institution which issued the refusal and asking them. If you still are having problems, **then contact the Access Info team** about it and we will try to help you, for example, by giving you the contact of an NGO or lawyer in the country.

10, APPEAL BY CHALLENGING THE EXCEPTIONS: THE HARM AND PUBLIC INTEREST TESTS

If your request has been rejected due to an exception within the access to information law, check to see if the cited exception is subject to a harm and public interest test, and whether these tests have been properly applied.

> **Harm test:** If the exception is subject to a harm test, the public authority must show that disclosure of the information would cause real and non-hypothetical harm to a protected interest in order to justify withholding the information. If the body hasn't done so, you can argue that they have not sufficiently demonstrated that harm would be caused upon release of the requested information.
>
> **Public interest test:** If the exception is subject to a public interest test, the public authority must balance the harm that disclosure would cause against the public interest served by disclosure of the information. If the public body states that there is no public interest in the release of the information, you can argue why there is a public interest. One widely recognised public interest is that the information is needed for democratic purposes, such as transparency in spending of public funds or permitting public participation in decision-making. Another strong justification is that the information is needed for a journalist to play their watchdog role, investigating corruption and defending human rights.

Once you have drafted the first internal administrative appeal with references to the law and your rights, keep the letter in your computer and you'll find that you have a template for future appeals. That will save you time as it should only need a little bit of changing depending on the content of the other requests.

11. ASK FOR PARTIAL ACCESS

If you have been refused access to information because the information falls under one of the exceptions, **you can still ask for partial access**. This is especially relevant when the institution rejects your request based on the privacy exception. It is very rare that the whole document is 'private', so go ahead and ask the institution to redact sensitive information or personal data, and leave the rest, which could still allow you to gain access to the information that you need for your research.

12. INVOLVE YOUR COLLEAGUES IN USING ACCESS TO INFORMATION AND MENTION THE RIGHT IN YOUR STORIES

If your colleagues are sceptical about the value of access to information requests, one of the best ways to convince them is to write a story based on information you obtained using an access to information law. Mentioning in the final article or broadcast piece that you used the law is also recommended as a way of enforcing its value and raising public awareness of the right.

13. MAKE A STORY OUT OF REFUSALS

A way to use a refusal of your request to your advantage is by **making a story** out of it. Sharing your story and why your request was refused can be particularly useful, **especially if you feel that there was a strong overriding public interest.** Be creative and constructive with the fact that the information was refused, get examples from other countries, ask experts what they already know, discuss the public interest in the information. This can help to create awareness of the importance of the right to access information and the need to campaign for greater transparency.

14. SUBMIT REQUESTS AT EU LEVEL USING EU REGULATION 1049/2001

The first thing to acquaint yourself with when submitting a request at the EU level is the rights that you are entitled to under Regulation 1049/2001. Note that at the EU level you have to ask for documents, rather than for information.

You can submit a request in any of the EU's twenty-four official languages and you can choose the way in which you would like to receive your documents.

You can also use AsktheEU.org or as journalists you may prefer the service of the pro version, AsktheEU Pro. AsktheEU.org is run by two organisations, Access Info Europe and mySociety and allows you to send access to documents requests to any EU institution, agency and body. The website, AsktheEU.org, gives all the details and a step by step guide of how to submit a request using the platform. AsktheEU Pro is a toolkit specifically for journalists and researchers to help them submit their freedom of information requests. It is particularly helpful for those doing in depth investigations and it helps to solve problems for journalists and researchers who are managing multiple requests.

Sending a request to an EU institution, agency or body is easy. Look for the institution "access to documents team"'s email on their website or fill out the form in case the email address is not available. AsktheEU.org has collected all the emails addresses, so use the platform if you want to make your life easier. The only institutions which ask you to provide some kind of identification when submitting a request are the European Commission and the European Border and Coast Guard Agency (Frontex). The former will ask you for a postal address, and the latter for your ID.

After you submit your request, wait for 15 working days for the institution to reply. Note that they have the right to extend this period for another 15 days if your request concerns too many documents. If your request gets refused, you can submit an internal appeal. What the EU calls 'confirmatory application'. Regulation 1049/2001 has procedures in place to help you.

In your confirmatory, you can state the reasons as to why you think you should have access. You also have 15 working days of the receipt of refusal/partial refusal of your initial application to present your internal appeal. If your confirmatory application is refused again, or if you are simply not satisfied with what you have received, you have the right to either submit a complaint to the European Ombudsman or to bring your case to the Court of Justice of the European Union. Feel free to always contact the AsktheEU.org team if you need help!

15. SUBMIT INTERNATIONAL REQUESTS

Access to information requests can be submitted electronically, which means you can make a request no matter what country you are living in. Alternatively, if you do not live in the country where you want to submit the request and you are unsure where exactly to submit your request, you can sometimes send the request to the embassy and they should transfer it to the competent public body.

You will need to check with the relevant embassy first if they are ready to do this – sometimes the embassy staff will not have been trained in the right to information and if this seems to be the case, it's safer to submit the request directly to the relevant public body. Remember you can also use national platforms for access to information requests, the platform should be able to give you advice on how to submit your request and it may allow you to submit multiple requests to different public bodies.

KEY LEGAL TEXTS

As a journalist planning to use the right of access to information, it's always worth knowing a bit about what the international standards and the key legal texts are. Here we give a summary:

The **UN Human Rights Committee** concluded in General Comment No. 34 that Article 19 of the International Covenant on Civil and Political Rights protects the right of all persons of access to information: Article 19, paragraph 2 embraces a right of access to information held by public bodies. Such information includes records held by a public body, regardless of the form in which the information is stored, its source and the date of production.

The **African Commission on Human and Peoples' Rights** adopted the Declaration of Principles on Freedom of Expression in Africa, that not only further elaborates on the right to freedom of expression, but also includes a principle that sets out core elements of the right of access to information. In addition to this, the expansion of the mandate of the Special Rapporteur on Freedom of Expression to include access to Information in 2007, further cemented the recognition of access to information as a distinct right.
The Inter-American Court of Human Rights linked freedom of information to freedom of expression as protected by Article 13 of the American Convention on Human Rights, stating that: "by expressly stipulating the right to "seek" and "receive" "information," Article 13 of the Convention protects the right of all individuals to request access to State-held information, with the exceptions permitted by the restrictions established in the Convention. Consequently, this article protects the right of the individual to receive such information and the positive obligation of the State to provide it, so that the individual may have access to such information or receive an answer that includes a justification when, for any reason permitted by the Convention, the State is allowed to restrict access to the information in a specific case". (Claude Reyes et al. v. Chile 2006 para. 77)

The **European Court of Human Rights** has on more than one occasion confirmed that Article 10 of the European Convention of Human Rights embraces a right of access to information. Key jurisprudence includes the case Youth Initiative for Human Rights v. Serbia (June 2013), in which the Strasbourg Court referred to earlier jurisprudence: "the Court recalls that the notion of "freedom to receive information" embraces a right of access to information (see Társaság a Szabadságjogokért v. Hungary, no. 37374/05, § 35, 14 April 2009)." Importantly, in this case, the Court confirmed the existence of a right of access to information and cited General Comment No. 34 of the UN Human Rights Committee as well as declarations by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR (African Commission on Human and Peoples' Rights) Special Rapporteur on Freedom of Expression, which also confirm the existence and scope of the right of access to information.

The **Council of Europe Convention** on Access to Official Documents. Also known as the Tromsø Convention, this Convention entered into force on 1 December 2020. It is the first international treaty guaranteeing a general right on access to official documents held by public authorities, establishing minimum rules for the prompt and fair processing of requests for access to official documents, including review procedures when access is denied. It also includes a list of exceptions that may be used to limit access to official documents.

The **Aarhus Convention on Access to Information, Public Participation and Access to Justice in Environmental Matters**. The Aarhus Convention came into force on 30 October 2001. It grants the public rights and imposes on Parties and public authorities obligations regarding access to information, public participation and access to justice, in governmental decision-making processes on matters concerning the environment. Moreover, the Aarhus Convention is also forging a new process for public participation in the negotiation and implementation of international agreements.

CASE STUDIES

4

A WASTE FUEL LAUNDERING SCHEME FROM THE EU TO THE BALKANS

Nataša Tomić; Investigate the Western Balkans Programme

The story started in late 2018 when residents of a Skopje suburb started noticing clouds of foul black smoke pouring out of the local maternity hospital. Reporters who investigated discovered the smoke was caused by dirty waste oil that was being supplied as heating oil to public institutions and factories by a North Macedonian company called Evrotim. It turned out that what they were selling wasn't real heating oil at all, but waste oil that was being falsely marketed as suitable for heating. Sources said the scheme was masterminded by Koco Angjusev, a powerful Macedonian politician and businessman, who intervened to ensure the oil was not properly tested when it was imported. The waste was sold to North Macedonia by Bosnian company Hifa Oil, whose owner Izudin Ahmetlić is one of the richest people in Bosnia and an influential figure in the Bosnian political party SDA, which imported the oil from the Czech company Unipetrol. Our investigation found such cases are common across the Western Balkans, where poor enforcement of regulations governing hazardous waste allows companies to trade and burn dangerously polluting fuels with virtual impunity.

MAKING THE POWERFUL ACCOUNTABLE ON ENVIRONMENTAL WRONGDOING

I came up with my hypothesis together with one of the trainers at the previous CIFAR cross-border corruption training: Saska Cvetkovska from the OCCRP (Organized Crime and Corruption Reporting Project). Saska had some information about serious misuse of international laws and regulations in the trade and transport of oil and oil derivatives in North Macedonia and it turned out that one company from Bosnia, Hifa -oil was involved.

Here in the Western Balkans, environmental topics aren't that popular. Problems of the sort in the region are only starting to become a hot topic to the public and media. There are many environmental problems and problems of corruption in the environment that the media isn't covering at the moment. I believe all of that will come to the surface very soon, meaning that the media will be more interested to write about these topics.

That was one of the main reasons I decided to choose this topic. I really believe that people in my country should know what is happening and what the people in power are doing in front of their eyes, on account of all of us and of future generations.

A LARGE REMOTE TEAM FOR A WIDE CROSS-BORDER TOPIC

Since this was a cross-border story, many different team members from various countries were involved in our work process. There were journalists from North Macedonia, Bosnia and Herzegovina and the Czech Republic in the team, as well as members from OCCRP such as Will Jordan, Caroline Henshaw and Amra Džonlić. Our coordinator was Caroline, who was well informed about everything going on in the team but also in the development of the overall research. We had a team meeting every 15 days where we gave updates but also discussed next steps that should be taken. Tasks were divided by countries, meaning that me and my colleagues from Bosnia, for example, did the part of the story relating to Bosnia and Herzegovina, so did others in their own countries.

When it comes to remote work, it can get slightly unsettling - I still haven't met most of my colleagues that were working with me on the story. But team communication was very good and I could get every information or advice at any given time.

THE RESEARCH PLAN

First thing to be done is to develop a **detailed research into the main protagonists of a story**. We looked into pretty much every detail, it took us a long time to collect everything and we went in a really broad way. Me and my colleague for instance focused on Izudin Ahmetlić, owner of Hifa – oil and one of the richest people in Bosnia. I went through his political history, since he is one of the main people in the SDA - one of the ruling political parties - as well as through some political cases he had been involved in. My colleague went through public procurement relating to his company and through court cases he was charged in.

We then made a list of **people of interest** and we were looking for ways to approach them. We made a list of questions to ask them. After the interviews we did transcripts and we were discussing our findings at meetings and then made further plans. We made a script for our story and a script for a video that would go along with the article.

Techniques we used were pretty much standard. **We conducted interviews and talked to people of interest, actors, victims, and opposition**. This was supported by **desk research** - to find information about our people of interest (a lot of online research, looking at previous articles written about them, official websites etc.). Our Macedonian team also used video to film everything they came across, and it will be turned into a documentary for Macedonian audiences. I personally did a lot of online research to find out more about Izudin. This is the first step and where everybody starts: you continue further with other stuff when it is necessary.

When it comes to databases, I used the **national business register** from Bosnia and Herzegovina, as well as a **database of public procurement** in the country and **statistical data about the import** of oil and oil derivatives from the Czech Republic. My colleagues also had data from the Macedonian customs authorities, and Czech colleagues used their own company registries.

TOR, SIGNAL AND DISCRETION TO MITIGATE SECURITY RISKS

There was a risk that someone would discover us and interrupt our research, threat us and endanger us. This also involved potential threats towards our family and friends. There was also a risk that speaking with one interlocutor could endanger part of the team in Macedonia and their sources.

To mitigate this last I, personally, did not tell anyone about the story; only my boss and editor knew what I was working on, but I did not share any specific details with her and she knew only basic things. While we worked in the field, we tried to be as quiet as possible, keeping as many details as possible for ourselves, even though it is hard to balance that and decide whether to share something with the person or not during an interview.

Communication was done via Signal, which we considered the safest channel. We also did not communicate on other channels and everything concerning the story was kept amongst team members. On the side, my online searches were only going on through the Tor Network.

At the beginning, everything was stored at wiki, OCCRP's platform for stories they work on. Basically, it is a platform where you can store everything about the story you work on. We kept data there about the main protagonists, documents, files, laws and regulations and so on. The good thing was that everything was at one place, really well organized and secured. But some of us had problems accessing it so we had to contact IT support often. We also made a google drive file and we shared it among team members on signal. There we had mostly voice recordings, transcripts, story plots and scripts.

INVESTIGATION-RELATED CHALLENGES: FINDING PROPER SCIENTIFIC EXPERTISE

There were some difficulties that showed up during our research. First was the COVID-19 pandemic, which really slowed down the whole process of developing the story. Many people were quitting previously arranged meetings and interviews because they were infected, so it really made it harder for us to work. Of course, we journalists were also highly at risk of infection.

It was very hard to find experts in the area of oil and fuel. Not only are there few of them who are well knowledgeable on the topic, but the few that were showed little interest in speaking to the media - even though they could stay anonymous.

Laboratory testing also took a lot of research and requests with few positive answers. Only one laboratory in the Federation of Bosnia and Herzegovina responded. But in the end, I had to find a lab in the Republic of Srpska, since the previous one stopped communicating with me. There were lots of exchanges and meetings from my side with very little results, which really slowed down the whole process.

THE SHOCK OF VALIDATING YOUR OWN HYPOTHESIS AND THE HOPE FOR IMPACT

To me, the most shocking information, or better - reveal, happened during my interview with the guy that was working in the oil testing lab. When he confirmed to me that Hifa was exporting some trash that could hurt millions of people and cause great damage, I was really shocked. Even though I knew that our politicians and businessmen are all mostly corrupt, I was really shocked to find out how little they value our lives.

I really hope that the public will realize the importance of the topic and the results we will present. I hope the story will awaken the public and encourage them to react in every case of their human rights being violated. Also I hope they will become more aware of the importance of environment protection.

NATASA'S ADVICE TO FELLOW YOUNG INVESTIGATIVE JOURNALISTS

My first piece of advice is to be very patient and persistent. It will be hard sometimes to get the right information or find the right person to talk to, but in the end everything will turn out well. You also have to be patient and persistent because of the public. Remember that they deserve to know the truth! Also, be careful and take care of yourself and your colleagues. Double check every piece of information you get and be unbiased and don't let anyone fool you.

THE EU FREEZING ORDER BREACHES ON MUBARAK CLAN ASSETS

Menna Ayman; Investigate the Mediterranean Programme

Throughout his rule, former Egyptian president Hosni Mubarak concentrated within his very own control the judicial, legislative and executive powers. Along with his clique, such as businessmen Hussein Salem and Ahmed Ezz, or through his own family relatives, he is also alleged to have monopolised strategic commodities such as steel, iron, and oil as well as seizing public land to make lucrative businesses. Their influence is alleged to have extended to Cyprus, France, Spain and the United Kingdom and involve possession of several offshore companies, and a number of luxurious houses and cars spread out in the European Union, most of which fell under a EU asset freezing order in 2011, in order to support national jurisdictions in their corruption and money-laundering cases against the Mubarak clan.

Our investigation focused on uncovering, seven years later, what had happened to these so-called frozen assets - wherever and whenever we could find information. Not only was it a tedious task to get elements on the status of these assets, but we quickly understood that in the EU, little to no progress had been made on these national judicial cases. NGO's, prosecutors offices and ministries remained mostly silent to our requests for information.

We nevertheless managed, in the space of one year, to establish that several potential breaches had happened in the EU freezing order framework regarding the Mubarak assets. In the British Virgin Islands, a frozen company managed by Credit Suisse for the benefit of Alaa Mubarak had simply vanished without leaving any trace. While in France, a luxurious Parisian flat worth several million euros was still being used and inhabited, despite european and national prescriptions regarding the assets of the owner: Khadiga El Gammal, daughter-in-law of the former Egyptian president. In another article, our investigation revealed that his other daughter-in-law, Heidi Rasekh, had received funds from the French bank Audi France, this after the EU freeze, and from a Credit Suisse offshore company owned by her father Magdi Rasekh. This resulted in the publication of a 3-part investigation in Daraj (Pan-African), Middle East Monitor

(UK) and Jeune Afrique (France).

DEVELOPING A LEAD: FROM RUMORS TO EVIDENCE

The Arab Spring re-ignited our fight against deep-rooted corruption. The country was making history in every possible way. Everyone wanted to be an active participant in this phenomenal change. Growing up in Cairo in the '90s meant witnessing vivid political upheavals and financial burdens. Toppling Mubarak in 2011 paved the way for investigating asset theft and allowing sincere attempts to recover these lost and hidden sums.

When we started working on possible leads, Mubarak's clique was atop the list; especially the individuals subject to the EU freeze order. Upon initial research, I found one too many loose ends to prior attempts by Egyptian and international journalists, lawyers, and researchers. Rumors and evidence were widely abundant. Either scattered around random weblogs or leaked by national and global news outlets. It was solely a matter of knowing where to look after deciding to dig for EU freezing order breaches from the Mubarak clan.

We connected over a common interest in Egyptian politics around which we created a team of four; two Cairo-based journalists and two others based across Europe. The geographic location of our team was of great essence. It helped immensely in dividing up the tasks. We would utilize our proximity to local sources or possible site visits, while our teammates could examine and investigate the stolen properties scattered around Europe.

We were able to set our working dynamic long before we had a solid lead in play, thanks to CiFAR's mentoring program. It is then that we found out that a British Virgin Islands based company owned by the son of the former Egyptian President, Alaa Mubarak, had disappeared from the local business registry, while it should have remained frozen. We further identified another asset located in Paris: a luxurious apartment that seemed to be still in use by the Mubarak clan, while it should have remained unoccupied according to the EU freezing order.

A STRAIGHTFORWARD RESEARCH PLAN FOR TWO SIGNIFICANT LEADS

Having found two significant leads, we divided our plan into research, outreach to sources, points of contact with mentors in our program, then drafting the stories in Arabic, English, and French, and lastly, fishing for publications. We wanted to mimic the successful dynamic of the Panama Papers. One of our stories, tackling the updates on Mubarak's offshore company Pan World in the British Virgin Islands, was an extension to the significant revelations made by the cross-border network in 2016.

None of the teammates had experience in developing stories this important remotely. So, the key was to keep an open communication lane at all times, along with maintaining weekly or bi-weekly virtual meetings to exchange updates and data either via Signal or Slack.

The plan went as follows, setting a timeline for the research work, contacting relevant sources, drafting the investigations, and then allocating a buffering period for all adjustments.

Our research plan mainly entailed surfing a diverse array of databases including OpenSource, Offshore Leaks, Doctrine Veille, BVI database, French judicial Databases, and the Panama Papers database, enabling us to form an outline of the two stories and picturing their structures, before moving on to filling the gaps and obtaining any necessary extra insights.

The next phase was locating the sections that required further illustration; outtakes from financial and judicial experts, affiliate sources, responses from the story players. During our drafting process, we attempted to contact the French prosecution, the EU commission, Transparency International UK and France, the infamous Mossack Fonseca, the Mubaraks, local and international lawyers, Credit Suisse, as well as the leading law firm Bedell Cristin.

EGYPT REMAINS ONE OF THE MOST SENSITIVE COUNTRIES TO REPORT ON, AND FROM

We carried out our stories amid an extensive crackdown on journalists in Egypt, especially after Italian student Giulio Regeni was found dead with signs of torture in 2016. This case, as well as many others, caused quite a stir and revealed how unforeseen matters can escalate. I recall receiving phishing emails and electronic flies started following my personal social media accounts, especially on Twitter. During our initial brainstorming for leads, early on in 2017, I wanted to pursue a heavily close ally to the Mubaraks, however, I was advised to discard the story for security reasons. One of our sources was also temporarily arrested during the process of the investigation.

All fact-finding was completed by using secure browsing and communication tools such as Tor, Sandstorm, Signal Messenger, Google Hangouts, WeTransfer, and IP altering software. Even with using these tools, we were extremely cautious not to reveal or specify any contexts. While this was initially done for security reasons, we discovered along the way that many of the databases and websites were blocked in Egypt.

Back in 2017, I couldn't install Signal with my Egyptian phone number, so I had to use a British phone number instead. Simultaneously, I created a fake e-mail address to correspond from, along with new social media platforms, too. All the while browsing incognito and using IP altering programs. As a team, we agreed to not share any valuable documents online unless absolutely crucial. We relied on transcribing snippets from written, video, and audio documents. Fortunately, we got to exchange the basic data face-to-face upon meeting for our second training session in Tunis, Tunisia.

LACK OF SOURCES AS ONE OF THE CHALLENGES OF THIS INVESTIGATION

We constructed our stories over the time span of a little less than a year. Along the way, we stumbled across diverse challenges that halted or altered our project. Most notable was the scarcity of cooperating sources and organizations. At one point, we deeply thought that our stories, the Pan World Investments status, and the breached Parisian apartment, lacked sufficient legitimacy, which was devastating as we'd spared no efforts in identifying, contacting and following up with the affiliate personnel and institutions. Most of the sources we'd reached pled that they do not possess new information regarding the matter under investigation. So, as a result, we were in a standstill.

Moreover, having relied on the initial leaked documents, we needed back-up data that further supported our claims. We surfed the Internet as well as all relevant legal and judicial databases in an attempt to find definitive reports and information. However, the process was much harder in reality. We were sometimes bombarded with useless or scam documents. Thus, we had to browse and select carefully the documents we wanted to purchase, as to avoid any budget constraints.

From French and BVI authorities, to NGOs and entities involved in our stories, no one seemed to want to "dig back" into this story: probably everyone would have liked to keep it dormant. We didn't get a significant number of sources to support for this project.

THE ACHIEVEMENT OF A JOINT CROSS-BORDER PUBLICATION

We owe the discovery of the lead of our first investigation, the fate of Pan World Investments, to mere coincidence. As we were actively looking for fresh leads, we noticed suspicious activity and movements in the assets of PWI, while the offshore company should've been adhering to a freezing order.

Upon reaching solid leads, we confronted affiliate key players relating to our findings and presented potentially table-turning data that should push asset recovery forward. However, we were hit with neglect from multiple organizations and sources, as well as utter lack of support from EU prosecutions. It comes to my recollection that as our team was interviewing an employee in the French prosecution, he said that the paperwork and documents concerning Egypt's Mubarak's assets and violations had been sitting in the drawers for years.

I believe it is safe to assume that my team's biggest achievement was managing to bring two investigations of international importance to light. We wanted to mimic the media fracas created upon launching a series of leaks, such the Paradise Papers or the Panama Papers, thus, we drafted and published each investigation in three key languages: English, Arabic, and French.

INSUFFICIENT IMPACT AS A DOWNSIDE OF THE PROJECT

We had major aspirations that the two produced reports would cause a national and a regional stir. Besides, surfacing these new pieces of information to light could motivate individuals to come forward with any possible leads or data they have. Lastly, we were hoping for reactions from the BVI and France that might assist in identifying the stolen assets and recovering them. However, in reality, the two investigations had some regional coverage and recognition in news outlets, but no progress was made either from governments or through initiating new investigations.

MENNA'S ADVICE TO FELLOW YOUNG INVESTIGATIVE JOURNALISTS

As you phase into your project, organize your every move and plan for every possible scenario. Your outline should be dynamic. Leave room for further adjustments at all times.

Equip yourself with the convenient physical, cyber and legal security kits and measures and never take on a story if it can reflect on your personal safety and well-being.

Furthermore, be factual and data-driven. This is the sole direction to highlight your work and entice publications and news platforms to publish your investigations. Finally, when you feel stuck or hesitant, always seek help and advice. Reach out to references and senior specialists. If they cannot help you themselves, they will surely refer you to someone who can.

INFORMAL CONSTRUCTION ENDANGERING LAKE OHRID

Arlis Alikaj, Investigate the Western Balkans Programme

For several years, the non-governmental organizations that take care of the preservation of the Ohrid region have been sounding the alarm that buildings, hotels and cafes are being illegally built in the protected area around the lake. The permits without studies given from respective municipalities are threatening the heritage of Lake Ohrid.

Corruption and the arbitrary decisions of certain powerful local figures are taking place on both sides of Lake Ohrid. The city of Ohrid has only one construction inspector for the whole city, which is a very big problem to deal with all of the (400 as of 2021) illegal buildings around the lake. Last year, the Albanian side of the lake was declared a protected world heritage site for the first time, and the other part (Macedonian), which was protected as natural (1979) and cultural heritage (1980) was debated by UNESCO to be included in the list of endangered world heritage sites.

Local governments are turning a blind eye towards informal buildings, legalised in contravention of relevant laws and often connected to municipality councilors. Most interesting is that at the height of UNESCO's warning against demolishing illegal buildings, a municipal councilor built a pizzeria within the protected area, accompanied by the mayor of Struga (a city next to Ohrid).

FINDING A LEAD THROUGH YOUR AREA OF INTEREST: DEVELOP YOUR OWN FIELD OF EXPERTISE

My personal motivation for choosing this topic was my passion for environmental preservation. I always suggest that journalists write on issues where they feel confident and strong because this way their reports and investigations will be unique and their passion will help them find the path leading forward. For me, being part of civil society environmental organisations in Albania, being in touch with their newsletters everyday, and having connections within the area help me develop ideas and understand the problems.

As the team leader of this project, developed in cooperation with my colleague Ivana Nasteska, I came up with the basic idea, the lead. With the North Macedonian side of the Lake being a UNESCO site, but not the Albanian one, it seemed the latter had more issues to be addressed. So being non-developed was a good thing in a way, because I had a lot of things happening to write about, such as illegal constructions, the missing general action plan, illegal fishing in sensitive conservation areas, including areas with endangered species. People didn't know about these issues in Albania while in North Macedonia, for example, people were more aware of them.

My hypothesis was a prediction which involved more than a guess. It began with a question which was then explored through background research. When I went to Pogradec, a lake city, which is close to my hometown Librazhd, the buildings on the lake shore always grabbed my attention. While travelling I always told myself something was wrong there.

People need to see the lake while travelling there. But it's simply impossible to get a view of Lake Ohrid and enjoy its beauty, because of the unpleasant buildings (fancy hotels and restaurants) which reflected the sunlight and blinded me through the glass of the bus for a moment. While being in Pogradec, I got in touch with people. I always recommend talking to the local community when something seems wrong, always talking to random people and asking questions. Someone will bring you where you want.

During the research alongside Lake Ohrid in the Albania part, I noticed the chaotic situation. There are a lot of businesses such as restaurants and hotels which are not legalized. They tend to build as close as possible to the Lake. What is interesting here is that the damage to public infrastructure and lack of investment is especially highlighted in these private zones. Built in a disorganized way, there you can see urban waste, secretly dumping polluted waters, and no sidewalks for pedestrians. While having a closer look to ALUIZNI registry (State Agency for Legalization, Urbanization, and Integration of Illegal Property) 80% of the owners of these buildings in Pogradec city in Albania are connected to politics.

Some of them are former mayors, current municipal counselors or familiar with the Environment and Engineering department in respective municipalities according to the Albanian National Business Registry. I regard it as the best achievement talking to local people affected by this chaotic situation and having their quotes telling me the opposite of what was on papers and municipalities' reports.

THE RESEARCH PLAN

- Press reviews and visits to the field(reports on UNESCO, ground data, seeing what has been published on media before and finding our strong angle that has not been covered) (up to a week)
- Talking with citizens, sources, NGOs and addressing their concerns (2 weeks)
- Investigations into the respective municipalities (Pogradec, Albania and Ohrid, North
- North Macedonia (requests for information, collection of data from construction registries; investigating permits given to informal buildings, legalization databases) (1 month)
- Visualizations, Maps (we saw the hotel, restaurant and cafe locations and their populations). How many of them are built in the protected area? Who owns them? Where is their waste dumped, where is illegal fishing carried out and what other challenges does Lake Ohrid face today? (1 week)
- After the research and data collection, we contacted the members of the bilateral commission from Albania and North Macedonia (this commission was formed last year by UNESCO recommendation) (1 week)
- Talking with the mayors from Ohrid and Pogradec (1 week)
- General time needed for conducting the story: 3 months. We used the database of the Albanian State Agency for Legalization, Urbanization, and Integration of Illegal Property, ALUIZNI

COVID-19 RELATED CHALLENGES AND MITIGATING SECURITY RISKS

Working at a distance was a challenge, especially during the COVID-19 pandemic where everything was closed and hard to reach. So what did we do? We just adapted to the situation and stayed calm. We had an advantage since things were happening online, we were sending a lot of FOIA requests. One of the reasons I don't usually prefer remote work was my fear I will slack off without that physical, in-person oversight. But, in fact, the opposite tends to be the reality: remote work is more likely to speed up work. The other challenge was travelling. Public transportation was closed and sometimes the country was in total quarantine and I didn't have the same opportunity to travel to collect data or verify sources.

My hypothesis was impacted by these difficulties which were hard to prove at that time. I found a solution, postponed my research and used hired private cars to travel within villages. Some other challenges were: the public was not consulted for these cases and was strongly against the construction. Documentation could not be obtained by the community or lawyers and lots of information requests needed to be filed to obtain the information.

Because we were reporting sometimes close to these informal buildings the physical threats were the most visible dangers while we were taking photos and interviewing tourists, fishermen etc.. Fortunately nothing happened, even though intimidation and attacks on the protection of our sources were some potential risks because Albania is a small country and very conservative, so is North Macedonia. We also made sure to mitigate legal risks we could have eventually faced with very trackable, data-based and factual reporting.

OBJECTIVE: TO ALERT AND PROTECT A WORLD HERITAGE SITE
The countries involved in our story are Albania and North Macedonia. The story was expected to raise awareness of how important it is to preserve one of the oldest lakes in Europe, which it actually did. Lake Ohrid is a superlative natural phenomenon, providing refuge for numerous endemic and relict freshwater species of flora and fauna dating from the tertiary period. As a deep and ancient lake of tectonic origin, Lake Ohrid has existed continuously for approximately two to three million years.

In the last 15 years, no government in North Macedonia has been able to prevent the destruction of this world heritage site, and that happens in favour of the financial gain of a few powerful people. Both countries - Albania and North Macedonia - are candidates for entering the EU and they are opening negotiations about this. Environment and Heritage are very sensitive for the European Union so both countries need to be on the proper pedestal and ready to go with EU standards.

Our target audiences were: Ohrid citizens and farmers, Environmental NGOs and activists, the tourism sector, businesses which operate in the area, and local authorities in both countries.

After the article got published in two national media outlets in their respective countries, two regional environmental forums took place in Albania. In Pogradec (Albania) and Ohrid (North Macedonia) there was also a municipal council meeting which analysed the problems and organised a conference. Many local media outlets spread and republished the article. We had calls from NGOs and tourism businesses who thanked us for the article.

We had initially hoped for a reaction from UNESCO about this, which was not forthcoming, but we are happy that our reporting shone a light on the issue and encouraged better management.

ARLIS ADVICE TO FELLOW YOUNG INVESTIGATIVE JOURNALISTS:
To other young investigative journalists, I would advise them to start locally. Even if city councils departments are boring, they are the nuts and bolts of local politics. You will meet people who later will give you valuable scoops. After they trust you to get it right. Big stories take a lot of work and require time to develop and probably a team. Be a good team player. Try to minimize or avoid unnamed sources. You can do plenty with public records and people willing to go on record. Be curious about the world around you. Respect your sources and subjects and the most important thing is to believe in yourself: you can do it.

IMPRINT

Investigate: The Manual

Published by:

Civil Forum for Asset Recovery e.V.
Köpenicker Str. 147
10997 Berlin
Germany
cifar.eu

Supported by:

Federal Ministry
for Economic Cooperation
and Development

Norwegian Ministry
of Foreign Affairs

Implemented by giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

CiFAR and the individual authors have made reasonable steps to ensure that the content is accurate. The views, opinions and evidence presented in this paper are the sole responsibility of the authors and CiFAR and may not reflect the views of the supporters of this manual.

CiFAR

CIVIL FORUM FOR ASSET RECOVERY