Working Group on Fighting Transborder Corruption

Journalistic investigations into cases of transborder corruption

Collection of case studies

2018
This collection of articles covers several types of anticorruption journalistic investigation. Each of the authors – journalists, experts and public activists – analyzes their preferred type of investigation.

The collection includes the descriptions of the following methods: data based investigation (big data journalism, state and commercial registers, open source research), undercover investigation, interview based investigation, search in DarkWeb. The goal of the publication is to show different methods of doing transborder corruption investigations. It is designed for a wide range of readers – novice authors, researchers, civil society activists, journalists interested in cooperation in international anti-corruption investigations, etc.
Table of contents:

Foreword 4

Part one. Investigations based on data analysis

Using real estate registers and databases: The case of Karlovy Vary 8
Mikhail Maglov

Working with Big Data: The Investigative Dashboard – A Swiss Knife for Global Reporting on Corruption and Organized Crime 14
Atanas Tchobanov

“Bringing together new investigative tools and traditional journalistic work”
Working with open sources.
Interview with Aric Toler 18

Part two. Other types of investigation

From Russia with Cash: An Experience of Undercover Investigation 23
Roman Borisovich

Interview based investigations. “Confessions”. 33
Anastasia Kirilenko

Look under the iceberg: hidden opportunities on the Internet for investigative journalists 43
Maksim Ishmatov

Conclusion. Fighting Transborder Corruption: 51
Building Capacity for EU and Russian Civil Investigators
Pavel Antonov
In 2010–2011, in Russia, a series of journalistic investigations brought into the spotlight the scandalous story of the *Federatsia* charity foundation. Back then, no one could have foreseen that this investigation would unearth a massive quantity of information on the origins, connections and networks of present-day Russian leaders that had previously been inaccessible for both journalists and the public. The foundation, which was barely known in Russia at the time, had organized a series of charity concerts, with the participation of global film and pop stars, to raise money for sick children. The concerts were held on a large scale, guarded by the Federal Guard Service and attended by government ministers. One of the concerts was even attended by Vladimir Putin, who was Prime Minister at the time.

After one such concert, the mother of one of the sick children told the press that her child had never received the promised financial aid.

Anastasia Kirilenko, one of our authors, who was then a reporter for RFE/RL, decided to find out what stood behind the arrangement. However, it was hard to sneak in: all the events held by the *Federatsia* foundation were invitation-only, and all information was closed off to journalists. Finally, she managed to land a job as interpreter for one of the foreign singers. This was not easy to do: all interpreters underwent a security check and had to sign a non-disclosure agreement pledging not to disclose information about the concert for five years and to cut short any attempts by journalists to obtain such information.

However, the ‘interpreter’ made it through to work at one of the strictly invitation-only events. She was able to collect the anonymous testimonies of several concert participants, to obtain the
invitation list, and to reveal the name of the main sponsor. This was a person who had twice been prosecuted on criminal charges.

She found out that the aim of this event was not to help sick children but to organize entertainment and business events for ‘the elite’ in order to launder money: this was a way for public companies to spend their charity funds.

To achieve this, Anastasia had to use various methods of investigation: undercover investigation, interviews with sources, and document analysis.

A journalistic investigation involves the research, analysis and publication of not publicly available but exclusive information that had been concealed from the general public. This is why conducting such investigations is impossible without a creative approach. Each story or case is unique, and one needs the ability to think freely in order to dig out the truth.

This is why, at first, the idea of writing a guide to anti-corruption journalistic investigations seemed strange or even counter-intuitive. It is hard to imagine a universal manual for scientists on how to make scientific discoveries; there are only general guidelines based on examples. The same applies to journalistic investigations.

Hence the main recommendation to those who want to engage in digging up information: think outside the box, keep coming up with unconventional ways of finding data, do not follow the journalism textbooks.

There are two major ways for the journalist to obtain information: studying documents (commercial and real estate registers, leaked databases, etc.), and conducting interviews (oral or written, on- or off-the-record).

A further method, undercover investigation, has been exemplified above. It has been in use for sometime, but it is applicable only when the first two methods do not produce the desired results.

A case of undercover investigation is described in the article by Roman Borisovich, an anti-corruption activist and organizer of the popular London Kleptocracy tours. The article tells the story shown in the acclaimed documentary, “From Russia with Cash”, in which Borisovich played the main part. Disguised as the Russian Minister of Healthcare purchasing an apartment in London, he examined the private life of high-end real estate agencies. He was able to capture on hidden camera and expose the details of the way in which those agencies helped overseas officials to buy
expensive apartments while turning a blind eye to the obviously corruption-based origin of their money.

Searching through foreign databases (such as commercial and public registers of real estate and companies) for the hidden assets of physical persons is also described in this book. Mikhail Maglov, the founder of the investigative website *The Municipal Scanner*, gives an account of such an investigation. Together with the author, you can take a walk along the streets of the Czech resort town of Karlovy Vary and look closely at the house numbers and company names. It is possible that, if you look in Czech open state registers, you will find a modest penthouse belonging to a certain official you might know.

Information leaks. Many journalists believe that information leaks are a godsend and can be used to publish sensational exposés. However, they must remember that information from leaks is not always ‘usable’. Confidential pieces of information which accidentally or intentionally become known to the journalists and have public significance might for example contain evidence of the rent-seeking behavior of a certain official, that can potentially be corroborated from other sources of information. It is not uncommon tough that information is ‘leaked’ on purpose by government to sustain reporting that discredits government opponents. Uncritical use of such information is journalistically not acceptable. Russian pro-government mass media regularly does this to destroy the reputation of journalists or opposition members. For instance, in 2011, the Russian state-backed channel Lifenews.ru published the hacked telephone conversations of the opposition leader, Boris Nemtsov, which had been leaked by the Federal Security Service.

There is one more type of leak: data of which the state authorities or other entities (such as banks) have unexpectedly, or possibly intentionally, lost control. This can be statistical data, copies of documents, correspondence between state agencies, court case materials, and so forth. Often, large and notorious leaks have public significance, because they reveal mass human rights violations or transborder corruption. They became possible due to a heroic work of whistleblowers who sometimes act on their own risk to life or freedom.

Recently there appeared so much information obtained through leaks that large investigative projects like WikiLeaks, OCCRP or ICIJ started creating databases to classify and process it. A Bulgarian colleague of ours, Atanas Tchobanov, editor-in-chief of the investigative group *bivol.bg*, has written a short review of the content and structure of those databases.

However, one can do without bulk data created by other people. They say that running is the easiest and cheapest sport, which needs no special equipment: you just get up and run. The same can be said about investigators who do not spend money on expensive databases but achieve
impressive results by using absolutely open and accessible sources. All that is required is the ability to search, identify and correctly use the information hidden in such sources. The interview with Arik Toler, one of the leading investigators and the coach of the international Bellingcat group, gives an insight into what can be achieved by digging in only open sources.

Some time ago, people who appreciated truly free and uncensored information created a dark, or anonymous, internet, which is hidden from the view of average internet users. Gradually, investigators are beginning to harness the potential of this DarkNet. Digging into and operating within deeply buried networks presents not only new opportunities but also new risks and enhanced responsibility on the part of the investigator. Access to these networks can be gained through an "onion" and "three pipes". What are these? Russian journalist Maxim Ishmatov, a "miner" of these concealed networks, explains in his article.

While using various investigation methods, the journalist must follow general journalistic principles. The main principle is "First, do no harm", which means that no person involved in your investigation should be harmed by your actions, except for the criminals. Specifically, it is necessary to verify all data, to analyze the public significance of the information to be published, and to try to foresee the results/consequences of this publication. The principles of journalistic investigation are covered in detail in the conclusion article written by Pavel Antonov, a Bulgarian expert and editor of the Foundation BlueLink.

***

The authors of this book — reporters, activists and experts — work together but live in different countries of the world: in Russia, Europe, the USA and beyond. While corruption is becoming global, spreading across national borders and hiding in remote and obscure places of the world, international anti-corruption cooperation is gaining paramount importance. Not only law enforcement agencies of our countries but also journalists and civil society groups should work collaboratively. International exchange of data, information and experience will help us, if not defeat, at least hold corruption in check. Public disclosure is the worst nightmare of criminal and greedy officials.

We hope that the experiences related in this book will inspire you towards new exciting investigations.
Part one. Investigations based on data analysis

Using real estate registers and databases: The case of Karlovy Vary

By Mikhail Maglov

Before 2016, the Municipal Scanner Project had been investigating cases of corruption, and violations of the laws of the Russian Federation, using the methodology of individual searches. That is, we were looking for information about particular officials who were deemed suspicious. However, given the openness of registers in the Czech Republic, we decided to use the territory search method, with the aim of finding certain persons there.

Since the first half of the 1990s, the citizens of the former Soviet Union, both businessmen and officials, have found it prestigious to buy properties in the Czech resort town of Karlovy Vary. By the mid-2000s, there was a big Russian-speaking community there. In general, it was believed that 90% of the real estate in the Czech Republic was owned by the citizens of the former USSR. The team from the Municipal Scanner Project decided to test this assertion, as well as to identify the politically exposed people who owned real estate in the town. This is how The Karlovy Vary Guide was created.

According to statistical data, there are about 50,000 people living in Karlovy Vary. We were unable to find a complete list of addresses of the real estate objects, so we decided to use the base from OpenStreetMap (a not-for-profit online mapping project created by internet users. Using the QGIS application, we managed to compile a table with 11,000 addresses in Karlovy Vary which were known to OpenStreetMap (with street names and house numbers).

The second step was to collect information about the properties’ owners.
The Cadastral Register of the Czech Republic provides up-to-date information on owners, based on the locality and residential address. However, there are two security features: CAPTCHA and blocking of the IP address for 24 hours after 15–20 queries. Our list was not too long and we had no resources to find a solution to bypass the CAPTCHA, so we decided to collect data from the Cadastral Register “by hand”. In order to bypass IP blocking, we used VPN services. Below are the types of data that we got from the Cadastral Register.

An example of real estate owner’s data in Karlovy Vary in the Cadastral Register of the Czech Republic.

Municipal Scanner

Real estate is owned by either legal entities or individuals. Foreign individuals’ residence addresses may be specified either in the Czech Republic or in their country of origin.

The next step was to identify the final owners of the companies to which the properties belonged.

The Commercial Register of the Czech Republic is helpful in that it provides information on companies’ owners, together with their addresses and dates of birth, as well as all the related documents. During this investigation, the search in the register revealed even powers of attorney notarized in Russia, complete with full personal data.
An example of real estate owner’s data in Karlovy Vary in the Cadastral Register of the Czech Republic. 

Municipal Scanner

In the end, we got a list of property owners in Karlovy Vary, from which we selected those coming from former USSR countries.

The last step was to determine whether our owners were politically exposed persons. In order to identify such persons, we used the following sources:

- searching the Internet by name and date of birth;
- searching the Single State Register of Legal Entities;
- checking the Russian addresses in the Russian registering authority, Rosregister, database;
- additional searching of the Commercial Register of the Czech Republic in order to find other companies belonging to a certain person, as well as to check the related data and documents.

While studying the individual cases in the Commercial Register, we found additional addresses of properties owned in the Czech Republic (outside of Karlovy Vary).
The Karlovy Vary Guide has 238 real estate objects together with personal profiles of their owners. This includes Russian officials and their immediate family members; businessmen engaged in the state purchase system; Ukrainian officials and MPs, including those related to Viktor Yanukovych; Azerbaijani MPs and immediate family members of President Ilham Aliyev; relatives of the President of Kazakhstan, Nursultan Nazarbayev. Due to this work, the Municipal Scanner Project managed to identify several undeclared properties, as well as cases of Russian officials illegally owning Czech businesses.

For example, in Karlovy Vary, we discovered two apartments belonging to Aleksandr Fendrikov and his wife. Fendrikov was a Member of the Legislative Assembly of Krasnodar Region from the pro-Kremlin United Russia party. For more than four years, he has not included information about those apartments in his anti-corruption declaration. After we sent a complaint to the regional Prosecutor’s Office, and it confirmed our data, Fendrikov waived his mandate.

Since 2007, the former Member of the Verkhovna Rada of Ukraine, Volodymyr Oliynyk, has owned four apartments in the center of Karlovy Vary through the Czech KROKUS Company. Oliynyk was the initiator of the so-called “dictatorial laws” adopted during the Maidan’s civil revolution 2013-2014. Now, he is on the Interpol's wanted list.

To further explore the real estate owners in the Czech Republic, one can also consult the website Cadaster 2.0, which allows one to view the cadastral boundaries on satellite photos and provides
links to the profiles of owners in the State Cadastral Register. Thanks to this website, we managed to identify a house in Prague that belonged to a Cypriot company and drew our attention.

Due to this incidental finding, the Municipal Scanner was able to reveal the scheme that enabled Arkady Rotenberg, a Russian oligarch and one of Vladimir Putin’s close friends, to regain access to financial instruments and purchase assets in Europe, bypassing the EU and US sanctions. This house belongs to Dmitry Kalantyrsky, ex-Chairman of SMP Bank and Arkady Rotenberg’s confidant. Mr Kalantyrsky moved to the Czech Republic after his boss was subjected to personal sanctions. In this country he began to register companies and purchase hotels in Austria, which Mr Rotenberg could not do himself due to the sanctions. Later the chain that had started from one suspicious house led us to another assistant of the oligarch, Denis Pospelov. The latter had settled in Latvia, where he started to register companies to his name, thus providing access to Western banks for Mr Rotenberg.

This investigation helped us to find out the actual information on the percentage of real estate in Karlovy Vary owned by former USSR nationals. At the beginning of the article we quoted a popular Czech belief this number reaches almost 100% of all apartments and houses in this town. It turned out that actually it is 50 to 60 per cent, which is also a vast number.

The Czech Commercial Register is an example of ideal disclosure, which is rarely seen in the European Union. In most EU countries, information about companies’ owners is only available on a fee-paying basis (e.g. Lithuania, Latvia, Estonia, Germany, Cyprus and others). In some countries, even the paid-for information does not allow 100% identification of the owner, because documents
are not published and even the date of birth and residence address are not disclosed (e.g. France, Spain). Nevertheless, it is necessary to work with the registers of those countries and to search for Russian kleptocrats there.

About the author:
Mikhail Maglov is a representative of the investigative website Municipal Scanner.
Working with Big Data: The Investigative Dashboard - A Swiss Knife for Global Reporting on Corruption and Organized Crime

By Atanas Tchobanov

A journalistic investigation now starts by digging through online databases. It ends the same way, during the fact-checking process. Linking individuals to businesses, assets and real estate is inconceivable without exploring commercial and real estate registries. To reveal cases of corruption and abuse of public funds in a globalized world, journalists have to track the data about “their” politically exposed persons (PEPs) from the country of origin through different countries, where such public databases are available.

The same demand for tracking the businesses and assets of PEP exists for private purposes. Individuals’ and businesses’ need for due diligence inquiries is served by a flourishing market of information systems. These harvest information from thousands of sources, many of them not public.

Very few investigative reporters, and certainly not those working for small media outlets, can afford the subscription plans of Lexis Nexis, Mint Global, and other big commercial databases. So at least three journalistic organisations have invested time and money in tools that aim to match those needs, and which, unlike commercial databases, are open to the public, or give access on the basis of free-of-charge partnership.

The International Consortium of Investigative Journalists (ICIJ) is maintaining a search facility for the database of their big leaks: Offshore Leaks, Panama Papers, Bahamas Leaks and Paradise Papers. The search engine gives information for more than 520,000 entities. The output is focused on the easy visualisation of the connections between entities.

Wikileaks has its own search engine to extract relevant information from all the leaks it has exposed over the years. You can search with keywords and filter the results by the date of the document. The search output can limit the results to those found in one or more leaks.

The Investigative Dashboard (ID) (https://investigativedashboard.org), maintained by the Organized Crime and Corruption Reporting Project (OCCRP), takes a different, scalable approach to the information queries a journalist, or a team of journalists, would run during an investigation. ID originates from the ideas of the OCCRP co-founder Paul Radu and Justin Arenstein from the African Network of Centers for Investigative Reporting (ANCIR). They implemented the first version in 2010 while they were both in residence as John S. Knight Journalism Fellows at Stanford
University. Over the years, since 2010, ID has evolved into a complex framework of tools, facilitating and bootstrapping the research process for reporting: from initial data findings, to visualisation of the final story.

ID offers a “self-service” repository of links to more than 750 online databases in 120 jurisdictions. This collection of the most useful public data sources for investigative reporting is compiled by the OCCRP researchers and covers more than 450 business registries, more than 150 intellectual property registries, as well as many court, land, and public procurement databases. They are conveniently organized by countries of origin, world regions, and there is a special tab for offshores.

Then there is a freely accessible search engine (at https://data.occrp.org) with more than 97 million leads from different sources, including some of the publicly available registries and databases, scraped by the OCCRP specialists, leaks, gazettes, articles, international institutions reports, etc.

If you register with the OCCRP website, following the “Search for leads” link on the ID homepage (https://investigativedashboard.org), you will see still more possibilities. You can upload your own documents, which will become searchable.

Create a personal or shared collection in the ID and upload documents. Atanas Tchobanov

This magic is possible because of the Aleph search engine, developed by the OCCRP tech team. Aleph is more than an indexer, as it handles both structured data (databases and sheets) and unstructured data (Word and PDF documents), runs OCR, extracts entities, like names of individuals, countries, and companies, and enters them into the database.
Within Aleph it is possible to create your own collections. This is a simple project-management facility, tailored to investigative reporting. For example, you can combine results from a search engine with your own uploaded data in one collection. Or create a watchlist of names, for example “persons of interest” or PEPs, and be alerted when new information occurs. Conveniently, these collections can be shared with other users, or assigned to a group of users working on a particular project.

**Example:** While working on the [Laundromat project](https://vis.occrp.org), a criminal financial vehicle to move more than 20 billion USD from Russia to banks around the world, journalists from OCCRP harvested and shared a collection with more than 700 entries: about 200 documents and 500 names of companies and individuals. Investigative reporters from 32 countries used the collection for research and supporting evidence.

If you cannot find relevant information through the search engine or by exploring public registries, you can address OCCRP’s team of experts. The process is quite simple: the journalist fills in a form explaining what he is searching for and why. There are two main tasks: identifying what a person owns, and determining company ownership. Free-text questions can also be posed to the researchers. The request is assigned as a task to one of the experts from the OCCRP research team. They run searches against the databases, including some expensive commercial resources, then communicate the results to the journalist, who can ask to refine the search. It is a mutually beneficial process: the journalists gain access to paid databases they cannot afford, and the findings enrich the entities database of OCCRP.

Finally, the Visual Investigative Scenarios platform (VIS) is a very useful visual tool to plot an investigation scenario (available at [https://vis.occrp.org](https://vis.occrp.org)). With VIS, a journalist can create a comprehensive map of the links between individuals, businesses, offshore companies, banks, criminal organisations, etc, thus visualising the core and the purpose of their investigation. Once the map is finished, the journalist can share it in the VIS public gallery, or keep it private and just export a picture of the map to be included in an investigative paper.

**Example:** A complex system of intertwined companies, offshore entities and proxies was used by the owners of the Bulgarian FIBANK to obfuscate a massive connected lending scheme. More than 600 million euros of depositors’ money (out of a total of 3.5 billion) went to companies linked to the main bank shareholders. Investigative reporters from Bivol.bg used VIS to [plot the connections](https://vis.occrp.org) between the offshores and the proxies.
An example of the map for visualization of links between entities created with VIS.

Atanas Tchobanov
Aric Toler: “Bringing together new investigative tools and traditional journalistic work”. Working with open sources

Interview with Aric Toler (Bellingcat) on using open-source methods for revealing corruption

By Andrey Kalikh

Q: Aric, what is an open-source investigation?

A: Open-source investigation is any kind of research that uses materials that are accessible and verifiable for the audience.

Of course, there are a lot of ways to do a really good investigation with non-open sources. For example, if you are looking into government ministers, you can search databases, commercial registers, but also look for new sources of information by filing requests for documents.

However, the way that we use open-source investigation provides much more transparency between a real viewer or listener and us, because if we write up a piece of information about a person, and the information that we write up is not correct or readers do not trust us, they have equal access to the materials that we use and they can check it. If someone claims that the information that we reveal is not trustworthy, we can say that all our investigations and reports are done with materials that are open to everybody.

These materials are most commonly accessible through these sources: social media — Facebook, Twitter, VKontakte, Instagram — videos on sites like YouTube, and satellite images. Sometimes we pay for satellite images, but usually we use free versions — Google Earth, Yandex Karty. There are also mass media reports: everything that has been reported or published on TV, radio, or digitally is open and accessible to others.

By conducting an open source investigation, for example, if journalists research a person, they try to use all accessible sources that relate to this person. If they are trying to investigate into the vacation of a Russian Duma deputy, they can look into the social media profiles of the deputy’s wife or children or close friends who may have accompanied them on a vacation and find out what this MP and their family members were doing there, in what hotel they stayed, at what restaurants
they had dinner together and how much the things — resort, hotel rooms, restaurants — cost at this particular location.

**Q: How do you think it is possible to use open sources for investigating corruption?**

**A:** While investigating corruption, open-source is usually not going to be your primary method of investigation. It has to be complemented with stronger investigations like database searches, interviews, undercover investigation, etc.

There are not so many cases where we have used open-source for an anti-corruption investigation but there is certainly an important one: our work on the Scottish Limited Partnerships, SLPs, in Scotland, which are often used for tax evasion and money laundering. Pretty much all information about these entities has to be publicly available due to a recent law passed in the UK requiring beneficiary owners to give information to the [Companies House website](https://companieshouse.gov.uk), which is now free of charge.

*(Companies House is an agency of the UK government. Its website is a part of the UK government's website).*

![Companies House website](https://companieshouse.gov.uk)

The Companies House website is a UK register for entities. *Screenshot*

The Companies House website is an open source because it is publicly accessible. If people need information, they can find publicly declared addresses, phone numbers and names of companies...
here. There are similar databases in other countries, for example, in Luxemburg, because if you are registering an offshore company you are required to declare information, but the requirements differ depending on the country.

Another important point is that, while doing open-source research, you are almost always relying on the person whom you are investigating to mess up, and you are looking for their mistakes. You are relying on accidentally taken photos on Instagram, posts on VKontakte, and videos that must be verified and geolocated. For example, we did an investigation into the assets of the family of Oleksandr Bondarenko, former prosecutor at the General Prosecutor’s Office of Ukraine. By analyzing the social media photos taken by his wife, Karina Bondarenko, we established and geolocated his family’s expensive vacation to a resort in the Maldives.

Open sources cannot definitively prove that this is all certainly corruption, and using only open sources is not as reliable as using other investigative methods, but it can certainly complement other methods of investigation. And this is something that we do to exploit mistakes that people make.

Screenshot of a picture by Karina Bondarenko of a resort in the Maldives on her Odnoklassniki account. Beilingcat
Q: *In recent years, the belief has arisen among civil researchers that, in the 21st century, you can investigate everything without getting up from your chair. Do you agree?*

A: Yes and no. First, I think it is rather an misconception. Open-source could be, at most, a part of an investigation, because, for the best investigation, you still have to be on the ground and do real journalism. So, you cannot do everything from your chair.

However, obviously, what we, at Bellingcat, do, we do from our chairs. The reason for that is that we know exactly what is possible and what is impossible to research, and we know what our limitations are. That is why our most impressive projects have been done when we collaborated with other journalists on the ground, because they can do what we obviously cannot do. They know people on the spot, they can knock on doors and make phone calls.

From the other side, we use methods “from our chair” that are not available or obvious to the journalists on the ground, for instance, finding and analyzing satellite images, videos, photos, and so forth. You can do a lot of investigation only from the digital aspect but you are under certain limitations.
There are some subjects that you can research pretty well that way. For example, access to a battlefield in Syria is limited, because it is dangerous, but you can still sometimes receive sufficient information and work with it, because people record videos and take photos from these places and post them on their social media profiles. So, I think there are some genres of investigation that you can conduct when the majority of your investigation comprises digital research, but the best investigations are done through a combination of methods. Therefore, the idea behind our workshops and trainings, which we provide to investigative journalists, is to bring together the techniques of both open-source investigation and traditional journalistic work.

Q: Is special knowledge needed to conduct an open-source investigation?

A: Again, yes and no. I provide special training for journalists all the time. The most basic and obvious prerequisite needed: you have to be pretty good with computers and the internet. You have to know how to work with Google Maps, satellite images, the keywords to use for effective research, how to proceed with results, how to navigate social networks. You must have a really keen eye for details. Thus, how you look for details in photos, videos and social networks, is the most important aspect in your work, in order to bring things together.

Most of the journalists, especially young ones, can do all of it to some extent, because we grew up with all these things: this is a language that we natively know. People already have these skills, for example, how to use social networks. The hardest thing is to know how to direct these skills and knowledge. This is what we try to give the people in training. We have a special chapter on our website, called “Guides”, where we publish new articles and reviews of new open-source investigative instruments. Or, for example, we bring together other experienced journalists who do teaching, for example, by organizing daily quizzes to train readers’ verification skills.

Aric Toler is a researcher at Bellingcat
Part two. Other types of investigation

From Russia with Cash: An Experience of Undercover Investigation

By Roman Borisovich

“The funniest anti-corruption film ever made”
John Sweeney, British investigative journalist

Opening scene From Russia With Cash. Copyright Amos Pictures

From Russia With Cash aired on 8th July 2015 on Channel 4 in the UK. The uproar it created was such that on 28th July – less than three weeks from its premiere – the then Prime Minister David Cameron in an anti-corruption speech promised to stop dirty money being laundered through UK real estate. Less than two years later, on 27th April 2017, the UK Parliament passed the Criminal Finances Bill; earlier in the same month the Department of Business had completed the second and final round of consultations on the register of Ultimate Beneficial Owners (UBOs) of offshore companies holding UK property titles. Below is my account of how a hidden-camera documentary changed national legislation.

***
One afternoon in March 2014, I sat down in a South Kensington hotel with Ben Judah, author of *Fragile Empire* and *This is London*, and documentary producer Tom Costello, to discuss what would eventually become *From Russia with Cash*. Back then all we had was an idea – not even that – just two words: “hidden camera”. But those two words would have an enormous impact – what better way is there to show how illicit cash comes into a country than documenting an insider view in a secret video recording? Initially, our idea was to create a fake oligarch with an absolutely macabre history that would be easily googleable – we were thinking he would have committed some despicable corporate crime, like causing an ecological catastrophe or mining accident due to embezzlement, before fleeing to England. He would go around London meeting lawyers, bankers and estate agents, arranging for the proceeds of his crime to be whitewashed in the UK laundromat. In our minds, this would have made for an amazing exposé.

That was before we went to see Dan Reed of Amos Pictures, who at that time was the most decorated documentary maker in the UK, with six BAFTA awards. Dan was fascinated by our two-word concept, but he viewed it from a very different angle. He saw the technical challenge, and immediately decided to shoot the best hidden-camera documentary ever made. He trashed our oligarch concept for a number of reasons. Firstly, however immoral or even criminal an oligarch may be, if he is not in jail it cannot be assumed that all his money is dirty. In the documentary the money under investigation needed to be linked to a specific crime, identifiable and illegal according to the laws of both the UK and the country of origin. Viewers should be presented with a horrid criminal walking free on the streets of London arranging for the proceeds of his criminal activity to enter the UK. This would keep them glued to the screen and cause a wave of indignation afterwards. Secondly, exposing bankers would have been both difficult and overly technical. Even if we succeeded in recording an incriminating conversation, as a financial transaction it would be full of terms which would need to be explained to viewers for their meaning and importance to become clear. The explanation would take longer than the recorded dialogue, and before it was over the viewers would lose interest and change the channel.

This is how Boris was born. Boris was supposedly a high-ranking bureaucrat in the Russian Healthcare Ministry, in charge of the national AIDS programme. Instead of expensive retroviral drugs Boris had sold aspirin or some other cheap pills to his Ministry, making millions of dollars from this illegal activity. This money was sitting somewhere in Cyprus. We thought it was hard to imagine a more appalling criminal – his money and anyone co-operating with him were worthy targets of national outrage.

We decided that Boris should try to purchase a luxury property with his criminal cash. We would take the scenario all the way to the point of exchange, when the buyer makes a 10% deposit and the seller commits to the sale. Dan – a lover of Russian literature – had a motionless Gogolian
scene in mind for the grand finale: lawyers and the seller gather for the signing, awaiting Boris who is supposed to arrive with the cash. A phone rings: “Boris has been arrested on money-laundering charges”.

Dan brought another major change into our concept – he told us that no actor could perform this role, because it required knowledge of anti-money-laundering rules and laws in order to expose the “enablers” in real time. If we were to continue with this project I would have to stop being just the technical expert and become the leading actor – play Boris myself. I cannot say that I was thrilled to play such a disgraceful role, but I could see Dan’s point. It would be next to impossible to quickly educate an actor to perform such a role. However, before I even got to these thoughts my co-authors Ben and Tom had already agreed on me playing Boris!

Dan had the hidden cameras made specially for the film. These were extra-light, credit-card-sized panels with a shirt button sticking out of their centre. This button would go through both sides of a shirt – and that was all there was to its fixing. One of the holes in the button had a fish-eye lens providing 180-degree wide-angle video in HD quality. The filming of *From Russia with Cash* was the first use of such hidden cameras in the history of cinematography. They allowed me and Andrew Shuran to have tête-à-tête conversations with the subjects while recording every detail of their facial expressions in HD.

Now we had equipment, actors and plot, the programme idea was ready for commissioning. This proved not to be as easy as we thought. Most TV channels turned us down due to the high legal risks. The chances of being sued by estate agents and lawyers were high, and few commissioning editors would entertain the idea. We were almost desperate when the Channel 4 legal team agreed to sign off on the film with their heaviest modifications. Boris had to lose his HIV programme and any mention of his fraudulent trading, there would be no transaction – just viewings of properties (an owner of a property could have sued Channel 4 for the loss of opportunity to sell), and no lawyers – only agents. Moreover, Boris had to make it crystal clear in each instance that a) his salary was insufficient to purchase the property and that he had other means of income; b) that the other income was bribes and kick-backs from his ministerial job; and c) that therefore the money for the property had been stolen from the Russian government. These seemingly excessive demands were totally justified – the brave Channel 4 lawyers assumed *a priori* that they would be sued by the estate agents, but if we followed all their demands they would have a very good legal position for their defence in court.

With the commission agreed, we started setting up the meetings. Preparation for this had begun almost a year before when Tom Costello registered a London concierge website. Under the assumed name Tom Ward he had been calling the best estate agencies in London, telling them he
was acting on behalf of wealthy Russian clients. He viewed some properties himself and sent Russian friends to view others, which, together with his website, posh accent and manners, convinced the estate agents that he was a real concierge. Now it was time for Tom Ward to make his ultimate calls – asking for an estate agency Director to attend a confidential viewing by his client. “It will be Boris – he is my client. That’s all you need to know” – this recorded phone conversation between Tom Ward and an estate agent opens *From Russia with Cash.*

In the film, Boris, his mistress, assistant and bodyguard view five properties ranging from 3.5 to 15 million pounds. Five high-ranking agents show the properties and have a confidential chat with Boris, who tells them exactly what the Channel 4 lawyers wanted to hear: “Needless to say, the money for this property comes straight out of the Russian government budget.” Boris is not bragging – he is telling his story so the agents will help him: with his dirty money, he needs to buy secretly, so that neither the UK nor Russian governments can discover the identity of the buyer. Five agents one after another agree to cooperate and advise Boris to buy through an offshore company so that nobody will know who the buyer is and how he made his money. Two go further, and in the follow-up meetings offer legal and fiduciary services.

The result of the filming was overwhelming even for us. Not only did all the agents agree to help Boris with his proceeds of crime, they offered exactly the advice we had hoped for: using an anonymous offshore company to hide the identity of the owner.
Throughout the film three QCs comment on Boris’s every move, explaining to the viewers how the law is being breached. Not reporting money laundering is a criminal offence in the UK, and the lawyers explain to the viewers that the agents have more than enough evidence provided by the perpetrator of the crime himself to file a suspicious activity report with the National Crime Agency (NCA), something that they are obliged to do under the Proceeds of Crime Act (POCA 2002).

According to the POCA specialist QC, the three agents who agreed to proceed with the transaction without reporting it are looking at a potential five-year jail sentence, and the two who offered further assistance are collaborating with a criminal and therefore can be jailed for up to 14 years.

Two more talking heads comment on the situation. One is a bank economist, who presents his published research on the UK balance of payments. According to him, one billion pounds of dirty cash has been coming to the UK from Russia every month for the last decade, and most of it goes into the real estate. The other commentator, NCA Economic Crime Commander Donald Toon, makes equally astonishing statements: “Hundreds of billions of pounds are laundered in UK properties each year[…] Real estate prices in London are skewed by the foreign criminals’ desire to sequester their assets in the UK.”

All of this made the film a national blockbuster. Nearly one million viewers watched the premiere, despite the fact that it was aired at the same time as the 10 o’clock news on the day when the UK budget had been presented. Millions watched it on All4 after the premiere. In the next two weeks, every UK national newspaper and major TV channel reported on the film, with Donald Toon giving an exclusive interview to The Times confirming and expanding the statements he made in the documentary. When the top economic policeman in the country made a public announcement of this sort, the government had to react, and the then Prime Minister David Cameron, speaking on anti-corruption matters in Singapore made a promise to stop money laundering in UK properties.

The government proposed creating a public register of the UBOs of offshore companies that own properties or do other business in the UK, and enabling law enforcement to freeze assets, including properties, when the financial sources of their UBOs are deemed suspicious.

The seemingly spontaneous public outcry and the government reaction were the starting point of a well-orchestrated political campaign, which some UK politicians have called the most effective in recent history. While we were busy secretly filming our culprits, two major anti-corruption NGOs, Transparency International and Global Witness, were laying the foundations of the future campaign. TI issued their report on offshore ownership of UK properties, ‘Corruption on Your Doorstep’, which painted a sad macro-picture of the problem in London. It was their report and its updates in 2016 and 2017 that discovered now well-known facts, such as that 100,000 offshore
companies own properties in the UK (with over 40,000 in London), and that 10% of properties in Westminster are owned by anonymous offshore buyers, etc. At the same time Global Witness was working on their report, ‘Mystery on Baker Street’, which uncovered multiple commercial and residential properties on Baker Street (including the assumed Sherlock Holmes house) that were owned by secretive offshore companies. GW linked these companies to Rakhat Aliyev, an ex-chief of the Kazakhstan KGB, who allegedly extorted billions from his fellow countrymen, and ended his days in an Austrian jail before he could stand trial for his crimes.

These two reports made a solid foundation for a political campaign – but they lacked mass appeal. On their own, the two institutions reached out to a very narrow segment of professionals interested in anti-corruption activities. By the time From Russia with Cash came out, only three thousand people had signed TI’s petition for transparency in property ownership. On the other hand, our documentary, which was based on five interactions with London estate agents, lacked broader factual support – exactly what was contributed by TI and GW, whose representatives appear in the film. They made Boris even more believable – TI by offering a detailed statistical account of how widespread the problem of money-laundering in the UK is, and GW by presenting a real-life “Boris”, albeit from Kazakhstan rather than Russia.

Shortly before the premiere I founded an NGO dedicated to political advocacy for offshore transparency: ClampK, the Committee for Legislation Against Money laundering in Properties by Kleptocrats. Together with TI and GW, ClampK started the official campaign the day after From Russia with Cash aired, by submitting an Early Day Motion – a form of appeal used in the UK Parliament – that quickly gained cross-bench support. The EDM in Parliament and the outcry in the media strengthened our campaign, which was soon joined by 16 prominent NGOs, including ONE, Christian Aid, Open Corporates, and Save the Children. Together we formed a coalition that coordinated the public campaign and interaction with the government, jointly participated in the Department of Business, Energy and Industrial Strategy consultations, etc.

Notwithstanding its immediate success in securing a prompt reaction from the Prime Minister, the campaign came to a halt a few months later, when, despite all our efforts, the matter was still not being addressed by the government. Our discussions with the then Anti-Corruption Minister Sir Eric Pickles and other government members were not getting results, despite David Cameron’s promise. In a ClampK discussion one of my colleagues joked that he wished he could take Pickles, Cameron and the Cabinet onto the streets of Westminster to show them the properties acquired by foreign kleptocrats right under their noses. In that moment the Kleptocracy Tours were born. The simple idea of driving a busload of politicians, NGO representatives and journalists around Central London to highlight the problem gained the immediate support of my anti-corruption journalist friends, who volunteered to speak at the event. This turned the bus tour into a press-
conference on wheels, and the inaugural Tour on 4th February 2016 was hugely oversubscribed. 49 seats were taken by MPs and Lords, London Assembly Members, TV and newspaper journalists. Our guides included famous journalists and writers: Mark Hollingsworth (*Londongrad*), Luke Harding (*Mafia State* and *A Very Expensive Poison*), Oliver Bullough (*The Last Man in Russia*), Peter Pomerantsev (*Nothing Is True and Everything Is Possible*), Ben Judah, and others. The tours immediately became a hit. ClampK even registered the name Kleptocracy Tours as a trademark to prevent copycats from using the name for commercial purposes. Soon enough the concept crystalized: invitation-only events, each with a different route and theme, with a core group of guides and guest speakers. That concept was fully realized at the time of the Global Anti-Corruption Summit in May 2016 in London. Mired in Brexit matters, the government did not have any media plan for the duration of the summit, so we quickly filled the gap by running tours every day of the summit. Kleptocracy Tours replaced the press pack of the summit, and at the end of the week Kleptocracy Tours featured in over 150 dedicated publications in 47 countries. The culmination of the media coverage was Roberto Saviano, the celebrated author of *Gomorrah*, labelling London “the corrupt capital of the world”, which quickly became a definition in the world media.

Media coverage of Kleptocracy Tours not only caused public indignation in and outside the UK, it also provoked a very different reaction: attempts by the kleptocrats featured in the Tours to silence the media. Lawyers representing these rich individuals repeatedly attempted to stop or retract publications in *The Guardian*, *The Times*, *Le Monde*, *Der Spiegel*, and other news media. In all but one case the journalists and lawyers representing their outlets made the decision to go ahead with the publication or TV programme, or not to retract them. Contrary to reports in the Russian media, these legal threats stopped neither Kleptocracy Tours and other ClampK activities nor media publications about the Tours and their subjects.

We carried on with our work with double enthusiasm because it was clearly having an effect, and because we were certain we used only reliable information for our Tours. These kleptocrats and their lawyers were merely trying to intimidate and frighten the media, knowing too well that they will not allow any of these cases ever to reach a court of law. The worst thing for someone like Vladimir Yakunin of Russian Railways would be to have a UK judge ask him or his son if they are not the ultimate beneficial owners of the lavish properties featured in the Tours. Even worse – given the fresh memory of the scandalous Berezovsky vs Abramovich hearing – would be to be forced to prove under oath how the money for these properties were made and deny any relationship between their offshore earnings and Russian Railways. Clearly their lawyers would never advise them to pursue the matter in court and, as we discovered, all these intimidation attempts were empty threats.
One case when a newspaper was bullied into retraction is worth looking into, primarily because it unveiled another very unpleasant type of service that enablers provide to international kleptocrats. Three employees of GPW, a political risk and business intelligence consultancy, were present at our first Kleptocracy Tour. Within four hours after the end of the Tour several newspapers and TV channels received letters from Mishcon de Reya, the law firm representing the Yakunins, threatening libel suits if any information from the Tour about their clients was published. The Guardian and other newspapers, having examined these letters with their lawyers, put them exactly where they belonged – into the waste paper basket – and carried on with their publications.

However, ClampK and the first Tour co-organisers spent weeks trying to find out where the leak was, until an ex-GPW insider told us that the firm had been hired by the Yakunins to help them better hide their assets and the true sources of their wealth. Moreover, having failed to suppress the publications, the furious Yakunin demanded personal data about the journalists who had written the articles; GPW eagerly complied. As reflected in the recent Quartz investigation, this is the first time such astonishingly unethical and unprofessional behaviour has been displayed by political risk firms – companies that are supposed to help fight corruption, not defend it.

The only newspaper in the history of Kleptocracy Tours that bowed to pressure from kleptocrats was the small London borough publication Hampstead and Highgate. Inexperienced in kleptocracy matters, having no budget for defence lawyers, and facing legal costs that would easily put it in receivership, Ham & High retracted their publication, apologised to the Yakunins, and covered their legal costs. The attack on Ham & High was shameful; however, the paper showed a certain degree of inexperience (bordering on incompetence): the publication was clearly not suitable for the paper's level of expertise and ability to defend itself. Other journalists from similar media outlets who participated in our Tours and realised that some information was unsuitable for their publishers toned down their articles to reflect the overall spirit of our campaign and not individuals highlighted in it.

Nevertheless, our campaign has made significant achievements, the most important of which was not labelling London the corrupt capital, but forcing the government to act on their promises. Soon after the first Tour and its coverage in the UK, the Department of Business announced the first round of consultations on the offshore UBOs register. ClampK and other members of the coalition came to the consultation table with very specific demands: the register should be open to the general public and should include not only property purchases going forward, but all existing holdings. This demand was voiced in Parliament by ClampK Advisory Council Chairwoman Margaret Hodge, a prominent Labor MP, and ex-head of the Public Accounts Committee. We also recommended that the administration of the register should be given to Companies House rather than the Land Registry. Similarly to the existing administration of People with Significant Control
At the same time, the Home Office started work on the Criminal Finances Bill, which included the key element proposed by ClampK in our discussions with Sir Eric Pickles – Unexplained Wealth Orders. These court orders would be issued to owners of assets in the UK, which, according to law enforcement bodies, cannot be explained by the officially declared income of these individuals.

Property and other assets will be frozen until the UBO presents a satisfactory explanation of the origin of his or her wealth. When this draft law was debated in Parliament, Margaret Hodge MP introduced the so-called Magnitsky amendment, which allows prosecution and asset confiscation of foreign human-rights abusers, similarly to the US Magnitsky Act. The law, which we heavily advocated for, was passed on 27th April 2017, at a time when ClampK was conducting its thirteenth Kleptocracy Tour, one dedicated to the Criminal Finances Bill and Unexplained Wealth Orders.

In the same month, the Department of Business conducted the second and final round of consultations on the offshore UBOs register. ClampK and other coalition members were pleased to see all our initial demands included in the draft proposal: the register will include all properties regardless of the time of purchase, the Land Registry will not register a title to a property without due information about the UBO being disclosed to Companies House, the register will be open to
the public and free. The second round focused on technical details and enforcement issues, and after completing these discussions we feel that the government has everything it needs for putting together comprehensive legislation introducing such a register. We hope to see the draft bill by the end of the year, passed by Parliament next year, and effective from January 2020.

Possibly, after what we at ClampK call the Transparency Act is passed by Parliament, the UK will have the most robust anti-corruption legislation in the world, and we will cheer the successes of the remarkable campaign started by “the funniest anti-corruption film ever made”.

About the author:

Roman Borisovich is a political activist and anti-corruption campaigner. After starring in From Russia with Cash (Amos Pictures, 2015) he founded ClampK.org, the NGO which leads the campaign for offshore transparency in Britain.
Interview-Based Investigations. “Confessions”

By Anastasia Kirilenko

‘Investigation’ usually means an inquiry that is made by digging into open, semi-closed or closed sources (subscription-based professional registries), that aims to disclose the corrupt ties of officials and their affiliated persons and to find their hidden businesses or real estate.

But what is the starting point of such an investigation?

1. Ideal situation: interview supported by documentary evidence

Very few people are aware that many of the notorious corruption cases in Russia started from either an interview with a knowledgeable source, an open letter, or a public figure’s slip of tongue, accidental or deliberate. The cases of Sergey Magnitsky, Gennady Timchenko (a Politically Exposed Person who has become a billionaire), and the case of businessman Konstantin Malofeyev’s allegedly corruption-related accumulation of wealth are among these cases. In response, the USA has introduced the Magnitsky Law, which warrants sanctions against corrupt officials across the world, while Gennady Timchenko and Konstantin Malofeyev have been subject to sanctions in connection with Russia’s annexation of the Crimea.

What does this mean in practice? Sergey Magnitsky, a lawyer with Firestone Duncan, was a famous whistleblower. For this, he was put in prison on a bogus charge and died tragically in November of 2009. In November of the previous year, 2008, had spoken to Bloomberg Businessweek’s Jason Bush, who later published an article entitled “Suspect Lawsuits Target Russian Financial Firms”. In the article, Bush observed, ‘The lawsuits appear to be an attempt to claim millions of dollars in taxes paid by companies linked to Hermitage Capital and Renaissance Capital’. In 2012, the journalist confirmed that his investigation had been based on information provided by Sergey Magnitsky, who had asked for his name not to be mentioned. This story has risen to international fame and is of pivotal importance for understanding the mechanisms of the transborder corruption that steals Russian public funds. It began with one journalist's confidence in the knowledge shared by a source.
The inquiry into the business empire belonging to Vladimir Putin’s old friend, Gennady Timchenko, conducted by some of the world’s leading investigative journalists, started after a statement made by Ivan Rybkin, MP.

Gennady Timchenko. ITAR-TASS

On 2 February, 2004, during the presidential election campaign, Ivan Rybkin, ex-Speaker of the State Duma, ex-Secretary of the Security Council and one of the presidential candidates, published a sponsored article in Kommersant entitled “Putin has no Right to Power in Russia”. In this article, he claimed that ‘I, and not just I, have a lot of concrete evidence that Putin is involved in business. The notorious Abramovich, Timchenko and the Kovalchuk brothers lurking in the background are responsible for Putin’s business.” It was then that Timchenko’s name was publicly pronounced for the first time. Investigative journalists lost no time in discovering the oil trading company that was registered in Gennady Timchenko’s name in 1997.

On September 26, 2010, the former CEO of Svyazinvest, Evgeny Yurchenko, sent an open letter to the then Minister of Communication Igor Shchegolev. In the letter, Yevgeny Yurchenko wrote, ‘I have decided that I will not work in a strategic field that has been turned into a plundering ground, a gold mine for Mr Malofeyev & Co and other cronies… Your colleagues from Marshall Capital have spelled out that no real understanding is necessary, all you need is a scheme to siphon off money’.
Following this statement, on October 15, 2010, Ilya Ponomaryov, Deputy of the State Duma, sent letters demanding an inquiry into Yurchenko’s statement, to: the Prosecutor General, Yury Chaika; Head of the Investigative Committee, Alexander Bastrykin; and Head of the Auditing Chamber, Sergei Stepashin. The now-deceased MP Viktor Ilyukhin sent a similar query to the Prosecutor General. The term ‘plundering ground’ (vorovaika) became widely known, and the responses to those queries became the starting point of further journalistic investigations.

Thus, as this case shows, it is necessary to closely follow open letters and other public expressions of public persons. They can, accidentally or intentionally, disclose important information (even though it may look like score-settling), that can serve as the starting point of an investigation.

People that may serve as useful sources for journalistic investigations, whether on- or off-the-record, are: law enforcement officers entitled to conduct investigative procedures, deputies (including members of city councils), members of the Auditing Chamber, and other persons entitled to request information from law enforcement agencies. Other sources may include social activists who send queries to Deputies and law enforcement agencies, and ordinary citizens. These may include lawyers and staff members who have witnessed acts of wrongdoing.

A whistleblower may have to pay heavily for a public statement, whether they are a state official or a private person. There is a sad saying in Russian: ‘everything is secret and nothing is a mystery’. This means that, officially, corruption does not exist, apart from a few publicly showcased lawsuits. However, there are numerous witnesses who are willing to share their perspective on the actual situation, provided their identity is kept secret.

One source, a witness, on condition of anonymity, once told me about the business interests of Sergey Vasiliev in the port of Ust-Luga on the Baltic Shore. Vasiliev is a businessman who has close contacts with organized crime. In Russia, businessman Valery Izrailit is being sued for the theft of funds at the Ust-Luga port. Members of both the Bundestag and European Parliament had addressed Vladimir Putin and Angela Merkel to express their concern about the breach of environmental standards during the construction of the port. Following up on the information from this source, I found in the list of persons affiliated with the port, not only Russian tycoons, but also a Liechtenstein attorney earlier affiliated with Vasiliev. The attorney was also a nominee in other controversial projects connected with road construction and oil trade.
In another example, a source with information says, ‘Do you know that the hotel we are sitting in right now belongs to AA, son of Minister BB?’ Is there any way to prove or disprove this information? The first thing to do in this case is to find out the name of the legal entity to which the hotel is registered. If there is no way to do this, for instance, if this information cannot be found on the hotel website, you can go to the hotel’s café, order a cup of tea, and keep the receipt. By law, all receipts must contain detailed information on the legal entity, including its unique number in the Register of Companies. The name of the legal entity may be different from the hotel trademark. By following this sort of method, one can try to find some documentary support for the source’s story. It is good if such a link can be established: the source’s words may be omitted in publication if there is documentary evidence.

2. Cases when an insider interview is the only evidence of crime

Finding concrete evidence for a crime is not always possible. For example, in Chechnya, according to its residents, all business belongs to the Head of the Government and to law enforcement officers. For example, a local taxi company, as rumour has it, belongs to one of the bodyguards of the Chechnya’s Head, and there is a portrait of this person in each car. However, this company does not give receipts to passengers, so it is difficult to even find out which legal entity is behind this taxi company. A journalist will thus find it hard to come by a piece of documentary evidence for this hypothesis, and will have an equally hard time trying to convincingly disprove it. In another example, small businesses in Chechnya complain that they have to make regular ‘charity’
payments to the Akhmat Kadyrov Foundation. However, this foundation will not show its books even in response to a journalistic request, and it reports losses to the SPARK (Russian company register). As a result, many corruption fighters leave Chechnya out of their investigations, despite the numerous reports of assets and wealth belonging to officials in this region.

Even without such exotic cases on the fringes of the law, searching for the actual owners of businesses and real estate in databases may be obstructed by obscure offshore locations, like the British Virgin Islands and Liechtenstein. These countries are notorious for their non-transparency: deep searching in these offshore centres reveals only nominal business owners, who officially have no ties whatsoever with the end beneficiary and allegedly corrupt official. In this case, an insider interview (with a friend, relative, colleague or subordinate of the supposed corruptionist) could provide enough evidence. But this is not enough: one would need at least some indirect documentary evidence to make such insider information suitable for publication. This is why most insider leaks cannot be published or are waiting in the wings.

One should not think, however, that an eyewitness’s testimony cannot stand as primary evidence of corruption. A judge may even rule that a witness is to be trusted if they believe that there are reasonable grounds for this. In court cases, including those on transborder corruption, they hear the witness’s statement, and the judge decides whether this witness can be trusted, based on factors like the way they bear themselves and the way they answer skeptical questions. An example of this occurred when Jalol Khaidarov accused a number of Russian oligarchs of corruption in the Regional Court in Stuttgart in 2010: the judge took his evidence seriously, as the defense lawyer had asked the witness threatening questions during questioning.

While preparing an interview for publication, it is necessary to establish which of the two sides is telling the truth and to find out their motives. There is no need to delve too deeply into physiognomy, but it is possible to get an idea of whether or not the interviewee is lying, by analyzing a video recording of the interview. As an example, a member of the city council who grins unblushingly into the camera saying, ‘I have given all my businesses to my wife’ will hardly convince viewers that he is honest. Often, officials or businessmen react to claims of corruption by avoiding communication with journalists, speaking evasively, or even threatening or insulting their opponents. This leaves an adverse impression on the viewers or readers.

Cross-checking is important: if several people give similar accounts of a certain situation, this raises the credibility of the story. If a witness tells the same story several times in a lively manner, each time remembering some new details but sticking to the same line, their credibility will also increase. If, on the other hand, the story sounds as if it was memorized, the journalist should grow suspicious.
Before publishing a story based on the words of an insider, a journalist should remember that the opposing side has the right to response or refutation. As a rule, if the journalist has evaluated all the circumstances and their information has a high degree of credibility, they will not be sued.

3. The right of the official to respond and to file a lawsuit

Although few accusations are followed by a lawsuit, investigative journalists are often accused of lying, both in Russia and in Western Europe. I am aware of some cases where the owners of certain French and German magazines were pressured over the telephone when their journalists investigated the suspicious, loss-bringing investments of high-ranking Russians in Europe. This concerned one of the *Les échos* correspondents in particular, as well as some publications in *Fokus* about Russian investors. In another case, in response to the demand of a Russian billionaire (which was not filed as a lawsuit), a Swiss newspaper issued a correction of an article that had already been published. Similar pressure has been put on British newspapers: an example of this is described in the article, “*From Russia with Cash*”, by Roman Borisovich, which is published in this book.

One might think that, if no lawsuit is filed, it means that there is no refutation. However, the press is sensitive to telephone calls and threats, which, in turn, creates the ground for self-censorship. Sometimes an article about corruption is ‘simplified’ by the editor, or is given a screaming headline to attract readers. This makes it an easy target for libel claims. One must bear this in mind while choosing the headline for an investigative article.

Russian officials have come up with an effective strategy to control public perception: they hold a press conference before an expected article is even published. This occurred as I was about to publish my investigation based on an interview with businessman, Maxim Freidzon. The interview was about how he and his partner allegedly gave a bribe to Vladimir Putin in the 1990s, and registered some of their businesses in the name of his nominees. No libel claims were filed. However, just before the publication of this investigation, Putin’s press secretary Dmitry Peskov held a briefing where he made a statement about ‘an attack against the President’, pointing out that no lawsuits would follow. A *Novaya Gazeta* journalist and an OCCRP expert, Roman Shleinov, followed up on my interview with Maksim Freidzon (although the latter had provided just a few documents, his interview laid the basis for my publication) and conducted his own investigation to find additional evidence supporting Mr Freidzon’s testimony.
A similar preemptive response came before the publication of the investigation conducted by Novaya Gazeta and OCCRP concerning the $2.2 billion that went through the offshore accounts of companies associated with Sergey Roldugin, a musician and personal friend of Vladimir Putin. The pre-emptive response in this case was a claim of an ‘attack’ after receiving a journalist’s inquiry but before publication. As in the previous case, no lawsuits were filed.

Andrei Zykov, a former senior investigator for especially important cases at the St Petersburg Main Investigations Directorate, is famous for his investigation of a corruption case in the St Petersburg City Administration (the so called “criminal case of Putin”). When money that was allegedly stolen from the city budget had gone to bank accounts in Spain and other countries, Zykov suggested that it was possible to file a case ex adverso in order to obtain some indirect documentary evidence for the stories under investigation. In 2011, Zykov made this suggestion in response to a press interview given by businessman, Sergei Kolesnikov. Kolesnikov said in a press interview that his former business partner, Nikolai Shamalov, had claimed that a Liechtenstein company issuing bearer shares was 96% the property of Vladimir Putin. No libel suit was filed after the interview was published. Andrey Zykov responded, ‘I believe that Sergei Kolesnikov can now file a suit against Nikolai Shamalov accusing him of belying the President. In this case, there would be a formal inquiry, which may well look into the actual owners of the company, and this would give us further clues’.

Zykov also wondered, ‘What documentary evidence may prove an act of bribery? In most cases, there can be only indirect evidence’. In fact, quite a few people are willing to talk about bribing officials, but only on condition of anonymity. For example, on one occasion, three different
businessmen conveyed to me circumstances under which they had all bribed one and the same official.

4. “Confessions”

One new way of working with sources of information is providing a voice for those who wish to speak out: the Russian investigative website, The Insider, has launched a new section entitled “Confessions”. Here, doctors, journalists of state TV channels, oil traders, and so forth can tell their stories of the corruption practices in their fields. Some of these contributors agree to publish their names, while others agree to speak on condition of anonymity.

According to Roman Dobrokhotov, the website’s editor-in-chief, Confessions have some restrictions: ‘We accept personal accounts of the situation inside some closed community, be it a ministry, an organized crime group or an ordinary school, when a teacher talks about budget embezzlement. The editorial staff is responsible for the choice of speakers: we must be sure they do have insider information and that they do know what they are talking about. We discard some of the incoming stories. For example, a person from a northern city tells us that their region is ridden with rent-seeking behaviour and dumps its waste into the river. However, this speaker is neither an environmentalist nor a corruption fighter. They are simply retelling what they have heard from someone else, and we are not interested.’

“Confessions” do not require documentary evidence, unlike that of the insider interview.
There is no special search for those who want to “confess”. Dobrokhotov notes, ‘We just bear it in mind that we have this section, and when, in the course of our regular journalistic work, we encounter a person who is willing to “confess”, we record a talk with them.’

However, Dobrokhotov says that fact-checking is required: ‘If the speaker says, “Russia has the highest suicide rate in the world”, we must check that, because that is not their personal experience but an objective statement. But if they say, “Half of my acquaintances in such-and-such village have committed suicide”, we leave it as it is, as it is their testimony.’

According to Dobrokhotov, “Confessions” appeared while the freedom of the press is dwindling in Russia, when, in many spheres, people have no opportunity to discuss the problems that they want to see discussed in the public domain: ‘We have been able to talk to rather high-ranking officials in the Ministry of Finance, in the Investigative Committee, with a police officer, with an environmentalist from a closed city where everyone has to sign a pledge of secrecy, a long-haul tracker who told us how ammunitions were delivered to Donbass [zone of the armed conflict in Eastern Ukraine]. It is obvious that our speakers would not have agreed to talk to us on any terms other than anonymity,’ says Dobrokhotov.

‘Old school mass media do not use this format, but if the new media take it up, it will be good for the openness of society,’ he believes.

In conclusion, very few journalistic investigations can be completed using just one method. Most of them use a number of methods, such as collecting documentary evidence, interviewing sources of information, or, in the minority of cases, working undercover in a situation that may yield evidence of corruption.

Technically, the newspaper article does not necessarily require an interview. This enables some journalists to investigate using only their computer, without going anywhere, and they may deliberately decline to use non-objective data, such as the account of a witness. For TV or radio programmes, however, it is necessary to use interviews to appear convincing to viewers. It often happens that well-recorded audio and video testimonies, conducted by an experienced, well-prepared interviewer, are more successful in convincing the viewer than a newspaper story containing information on the content of certain databases. However, when a newspaper journalist is asked to record an interview for a website, and a TV reporter has to write a text for the channel, the investigative journalist will need to work with all types of evidence.
About the author:

Anastasia Kirilenko, an independent journalist, works with Theins.ru and mediapart.fr. She investigates for the CBC’s *The Fifth Estate*, the BBC’s *Panorama*, France2’s *Envoyé spécial*, and France2. From 2009 to 2014, she was a staff reporter for the Moscow Office of RFE/RL. She has been based in Paris since 2014.
Look under the iceberg: hidden opportunities on the Internet for investigative journalists

Maxim Ishmatov

Threats to the confidential exchange of information emanate from both hackers and states. Authorities are adopting restrictive laws and trying to follow the correspondence of internet users and hackers. Such correspondence can be followed as it is spread from servers in the form of open access information.

Despite technological security features, personal messages or files from social networks, instant messengers, email and virtual hard disks often end up in the wrong hands. Many journalists have managed to make names for themselves from leaks in high-profile investigations based on, for example, the Panama Papers or WikiLeaks. For the data leakage investigator, this provides both new opportunities for work and new threats.

According to the Breach Level Index, a global database of data breaches run by security firm Gemalto, states and companies have lost more than 9 billion records of confidential data since 2013. This number reflects official information only: the Breach Level Index contains information only about publicly disclosed data breaches. Although we have to admit that users themselves are often guilty of leaks through computer networks, no one is immune from their mail provider server being hacked. Nor are they immune from the "wiretapping" of their Local Area Network (LAN) at work, or from a virus on their home laptop.

One of the possible ways out is to work in DarkNet services, rather than public networks. However, this requires even more caution.

DarkNet services can hinder the leakage of confidential information, but do not completely eliminate it. In the open Internet, however, the situation is even worse. Under these circumstances, reporters are finding it increasingly difficult to maintain anonymity for themselves and their sources. Protecting sources, at least in Russia, is required by law.

Anonymity, however, even in the Dark Web, is more myth than reality. Servers are hacked even in these hidden networks, and then the users' data can be published. For example, in February 2017, hackers shut down the infrastructure of Dark Web hosting provider Freedom Hosting II. Following
this, the hackers publicly posted torrent files from over 10 thousand sites, and included sensitive information.

It has also been reported that law enforcement bodies, including the Russian ones, have already learned to shut down resources in the DarkNet.

Despite the security risks of the Dark Web, journalists using tools such as Tor do have some advantages. If you want to see what can be learned about you without anonymity services, the Me and My Shadow project offers a number of useful tools for self-tracking.

Designers love to portray the Internet as the planet, shrouded in bonds. However, a more accurate image might be an iceberg in water. This image of the Internet as an iceberg can help us to better understand the relationship between what the average user sees and the wider and deeper structures of the Internet, including the Dark Web.

While search engines such as Google, Yahoo, Yandex, and Mail.ru index millions of pages, they are only aware of the existence of a fraction of all the websites in the world. In other words, They see only the surface of a large ocean of internet content, while the rest is hidden, like an iceberg, under water. Not all website administrators want to get into the top ten on the first page of Search Engine Results Pages (SERPs). These administrators prohibit robots from indexing their content and/or protect access to their content with a password. There are many reasons an administrator might make this decision, for example when they are out of fear of hackers attacking the server, which could be a working computer.

Sites accessible through Tor have a “.onion” domain name suffix instead of the more commonly seen “.ru”, “.com”, and “.net” suffixes of the wider Internet. An ordinary browser will not allow access to a “.onion” domain name address, even with a VPN service. Therefore, an ordinary search engine will not show results with links to Dark Web resources.

The Internet as a whole can be divided into approximately three levels: public (Clearnet), deep (Deep) and quite dark (Dark).

To go from the Clearnet to a lower level, you need the Tor Browser Bundle, or individual packages for other hidden networks, such as freenet and i2p. These technologies aren’t to be confused with private virtual networks (VPNs), as these work differently.
A VPN allows you to transmit information via an encrypted channel between the client and the server. You can imagine this as akin to sending something through a tube: it is visible to participants on either end of the tube, but the surrounding people do not see what you have sent. When using a VPN, the transmitted information is also available only to participants on either side.

Tor technology uses several of these VPN “tubes”. In the first, information is encrypted and transmitted through three Web-connected users, where the first does not know the last. Only after this will a .onion site open. If the page uses HTTPS (indicated by the 🗝️ icon in a browser), then in theory, no one can know what data you have received. If a site does not contain encryption (HTTP without the letter S), then the third web-connected user becomes vulnerable. Through it you can find the content, but it’s hard to say exactly who requested the data.
But these are technical aspects. Much more complicated than these technical aspects of Tor is finding useful information using this technology. Basic reference resources, forums, and directories accessed through Tor look like they are from the dawn of the Internet. In addition to this, many links may be old and not work.
There are, of course, Google search counterparts internal to the deep Internet. However, even these are difficult for an average user: a simple query could return to many results leading to one website.

The most interesting information on Tor-based websites is often open only for registered website users. To get into one of these communities, you often must either pay or receive an invitation from existing members.

Websites on Tor are unattractive in terms of design, but its users are active members that feel secure and ready to spread the sensitive information needed by reporters.

While conducting investigation, do not forget about security. Some files contained in the deep Internet carry information which may be protected by law: commercial or banking secrecy, correspondence or personal data. Files may also be blank or contain viruses.

While investigating opportunities for journalists in closed forums, I came across references to databases with the following names: "Thailand Immigration Database"; "Spanish database"; "1.4 Billion Clear Text Credentials Discovered in a Single Database"; "Database I collected from clearnet" [sic]; "Pennsylvania Voter Dump".

It was not easy to find journalists in Russia who use Tor to conduct their investigations. However, their overseas counterparts are already actively using these technologies.

Atanas Tchobanov, Chief Editor of the Bulgarian investigative publication bivol.bg, told me that as early as 2010, he installed, and has since then administered, the platform Balkanleaks.eu, where he "managed to get a lot of very important "leaks"."

The site Balkanleaks.eu is an openly available platform that is indexed by conventional search engines. On this site, you can find versions of a "black box" in the DarkNet through which informants can share sensitive information with reporters without risk to themselves.

![Screenshot of the Balkanleaks website](image-url)
The Dark Web service for sending hidden letters that Balkanleaks uses was developed by the non-profit organization **Hermes Center for Transparency and Digital Human Rights**. Their project, called **GlobalLeaks**, is open source. This means that any editorial office can use technology for free. This platform is also used by journalists from the Organised Crime and Corruption Reporting Project (OCCRP). This is what their Dark Web site looks like:

![OCCRP page for informants in Tor](image)

The sender, after pressing the big blue button "Blow the whistle", lands on a page with a form, in which he can send a message and attach files.

Atanas Tchobanov noted that he uses the instant **Ricochet** messenger for communication with colleagues and sources and **Onion Share service** to transfer files. Both programs can be installed on your computer, and the messages will be sent through Tor’s anonymizing technology. This allows for greater privacy.

Russian investigator Ruslan Leviev, the head of **the Conflict Intelligence Team**, explained in an interview with me that his team works closely with open sources on the ClearNet. Leviev noted that they have enough work without using Tor, but that he and his team did occasionally use Tor as ordinary users, to go to sites that are blocked in Russia.

Leviev highlighted one of the main tools in his team’s investigative work: the **archive.is** service. “It allows us to promptly preserve evidence, including war crimes evidence," he said. “For example, we save profiles of Russian soldiers while investigating Russia’s involvement in the armed conflicts in Syria and in Donbass (Eastern Ukraine), which soldiers usually delete shortly after a media
publication. This service is blocked in Russia by Roscomnadzor (the state media control authority), so we sometimes have to use Tor to access it.”

**Note:** A Russian Federal Law issued on 29.07.2017, # 276-FZ: *On amendments to the Federal law On information, information technology and protection of information* obliges the owners of VPN and Tor services, to block access to sites from Roskomnadzor’s uniform register of banned websites and webpages from November 1, 2017 onwards. To accomplish this, the agency must notify the organization and give them 30 days to customize their programs. However, this law will not affect all.

The Tor browser has added several useful security enhancements:

- **NoScript** blocks the invisible parts of pages that use scripts (i.e., Flash, Java). Despite the fact that many sites on the Internet use scripts, in the DarkNet they are most dangerous, and can cause issues for visitors. Allowing use of scripts is generally not recommended. If you want to allow them, allow their use only on verified pages.

- **HTTPS Everywhere** ensures that a site is automatically opened with encryption protection if the creators of the resource support encrypted protocol.

**When working in the Dark Web, avoid:**

- Registering for services using an email address that contains part of real name, such as `vaskin_93@mail.ru`.
- Using anonymous networks as an administrator of the operating system.
- Working in parallel using both Tor traffic and conventional one.
- Visiting everyday sites that require a login and password. For example, it is not advisable to log into your personal Facebook account via Tor. When you log into your social network, your anonymity will disappear.
- Logging into internet banking. The server may find your foreign IP address suspicious and your account may be blocked.
- Downloading torrents through Tor. This delivers your real location. Opening downloaded files from the Dark Web while connected to the Internet is also dangerous.

As many websites in the Clearnet record not only the IP address, but also information on the state of the computer (its operating system, the screen width — generally innocuous settings), it’s worth opening everyday sites in a normal browser and using Tor only for the “.onion” domains.
It is safest to work in Dark Web networks like Tor through a virtual machine, rather than using an everyday operating system. One popular program, VirtualBox, will create this workspace environment. There is also a special distribution for Tor, called Whonix, that isolates the user workspace from the Tor gateway. Using this approach, your Windows system files, Linux or MacOS will not be compromised in the case of a network attack.

Whonix also allows you to separate normal internet traffic from Tor

You now have a basic understanding of how the Internet iceberg looks under the water. It's time to begin to research — to open the deep mysteries of the DarkNet.

About the author:

Maxim Ishmatov – a Russian journalist. Author of investigations for the local media in Perm, Russia. Explores data journalism.
Conclusion

Fighting Transborder Corruption: Building Capacity for EU and Russian Civil Investigators

Guidelines for quality reporting on trans-border corruption

By Pavel P Antonov

The following guidelines are based upon the good practice standards at the BlueLink virtual newsroom and the recommendations for quality feature story writing of the BlueLink Foundation and the Climate News Network, UK.

Setting the ground

1. **Keep an open mind**: Investigators should come to a story with an idea of what the issues are, but it is vital that they let the evidence speak for itself. Your job is to gather all the relevant facts you can and present them clearly. **Be prepared to change your mind about the story, and don’t make assumptions about ‘the good guys and the bad guys’ before you’ve completed your research.**

2. **Build your credibility**: Investigators work in the public's interest. They may be campaigners or have strong personal views on the issues they probe, but for the purpose of their investigative work need to demonstrate impeccable transparent and unbiased approach to facts and information. **Build trust in your personal and professional integrity and demonstrate that you are well-intentioned, fair and professional in your approach even to the worst criminals of corruption perpetrators.**

Working with sources
3. **Use all available resources:** Investigators draw primarily on documents, but need to access information from all possible sources, such as: the web, archives, linked stories published by other media, as well as spoken or written communication with individuals and organisations. Gathering data on related or similar cases from other country or region is recommended. **It is essential that the investigator should scrutinize every source and apply her/his best judgment as to whether the source can be trusted.**

4. **Obtaining documents.** Access to official or other documents is the greatest resource for successful investigations. Some documents are public and can be found in institutions’ archives, obtained through Access to Public Information requests, or found online. Many institutions are obliged to publish information online, but do it in a way that is hard to find. Company registers might be available only for paid subscribers, lawyers or civil servants – work around finding access to it. Sometimes documents can be found through a search engine but not on a website. An insider, whistle-blower or a concerned citizen could be an invaluable source of confidential or hidden documents.

5. **Avoid being used as someone’s ‘post-box’**. Beware that some sources may have clandestine interest, seek to remove a competitor, revenge, or even try to mislead and compromise your investigation. Always question the motives of your document suppliers and double check the information received. **You cannot quote or refer to a source that is anonymous or whose validity you did not double-check.**

6. **Verify facts and information.** The investigator should be completely convinced in the credibility of every fact, number, and statement – and of every word used in her/his report. S/he has to crosscheck every document, and indeed - every bit of information with as many additional sources as needed in order to be convinced that it is trustworthy and can be published. You can only state things as fact when you are confident of your sources and have a good background in the story. **If there are any doubts in your mind check the facts again, or leave it out.**

7. **Diversify sources.** Identify and interview various experts/sources on the story. Even if you know you have one good source, don’t stop at that. Do your sources originate from an official institution or organization, hold relevant qualification or expertise, witness a crime, or why else is the information they offer credible? **You need to establish the legitimacy and authority of your source and demonstrate it to your readers.**
8. **Collect all viewpoints.** It is essential that you gather and present all the legitimate viewpoints to a case, or demonstrate that you did your best to obtain them. **If you have only talked to and represented one side, it is not an investigation.** Be objective and well intentioned to all sides, even if you are already convinced who are the ‘bad guys’. Drop them an email or call them, indicating what facts you have obtained. Represent their versions accurately, but indicate if you found they are not telling the (entire) truth. Provide the facts and statements, and help the readers make up their minds.

9. **Cultivate your sources.** In any case, remember that having one source is very rarely enough to build a case, so your success depends on identifying, knowing and successfully obtaining information from various sources. Your phone book is your greatest treasure. Knowing sources for a long time and knowing how much you can rely on them and for what is essential. You need to demonstrate the credibility of your sources, but also keep them safe. Negotiate carefully with your source what would be the best way to refer to him in your publication. Keep sources happy and willing to talk to you again. **Do not burn bridges, even to proven bad guys.**

**In the field**

10. **Keep safe.** Do not take risks, and do not put risks on others! Provide maximum transparency of your sources but be ready to protect their identity and safety. A journalist has the right to protect the identity of a source, as long as s/he has verified and trusts who the source is. Many investigators are taken to court, harassed, sometimes even shot at. Seek advice or legal support whenever you feel that your safety might be at risk. Inform the team and remember that you might be held responsible for the findings you publish and their consequences. **No investigation is worth imprisonment, taking or ruining a human life!**

11. **Be kind but persistent.** You may have to be persistent to a degree that might be considered rude, but sometimes that is your job. But at all times stay polite and calm and above all don’t argue! Some sources may be difficult to find and contact, or be reluctant to talk to you. Use lots of initiative and don’t take no for an answer. If people seem to be avoiding you don’t give up – go and see them at their office. It is much more difficult to refuse you there. Avoid confrontation, unless absolutely necessary to obtain information – your job is to investigate, not to accuse, sentence or re-educate people. If someone refuses to talk to you despite giving them lots of chances, mention that in your story. **Never be aggressive or violent and avoid abusing people’s privacy.**
12. **Keep questions short and simple.** Ask just one simple question at a time. If you ask three questions in one the respondent will only answer the easiest. At press conferences team up with other journalists to get the needed answers – repeat your colleague’s important question if it did not get answered properly. Ask as many questions as needed to make sure you understand everything.

13. **Establish the facts first.** Ask lots of factual questions first. **Don’t be afraid to ask what seem to be stupid questions – you must be sure to understand everything.** Use informative questions to establish facts, and ‘Yes-No’ questions to confirm them. Confront the source if needed at the end – that might deliver the quote, detail or lead you need. Do not argue, nor impress with how much you know: focus on obtaining the information you need.

14. **Get quotes and explanations.** Once you feel you’ve got your facts move on to gather opinion / useful quotes. An interview may be the only chance to connect or confirm the facts or understand the background of a case. Remember that you are asking questions for the public – in a way you represent them, so you have a right to ask both simple and ‘uncomfortable’ questions. Be friendly and curious. If your sources feel comfortable and enjoy the interviews, you are likely to get better material out of them than if you argue, judge, accuse or confront them unnecessarily.

**Compose the story**

15. Let facts, quotes and evidence tell the story. Build your story carefully, brick by brick. The bricks you should use are: facts, quotes from sources and other persons, statistical information, evidence, or eye-witness testimonies. Base every statement, fact, accusation, and conclusion, literally every sentence of your story, on the sources that you work with, and demonstrate this clearly in the text. Avoid speculative conclusions that are not based on evidence, even if someone else is making them on the record. Do not guess. Do not rely on ‘well known facts’ that you did not confirm personally. Use solid logic as ‘cement’ that connects the bricks, but make sure that every word you use could be defended against the toughest and most hostile prosecutor or court. Your personal opinion, interpretation, commentary, is not important, what is important is what your sources say or demonstrate. **Whenever you are drawing a conclusion, revealing a wrong-doing or crime, let this be articulated by the words of others – this may save your life or freedom one day!**

16. **Look out for the story ‘hook’.** There might be lots of complexity to a story, and lots of interesting material – but what makes it worth telling? A hard news, unexpected discovery, hidden connection, breath-taking personal story, action or inaction that affects the health, wellbeing or lives of many, might be revealed in the last minutes of a long interview, or at
the bottom of a stack of unimportant documents. Stay sharp through every minute of your investigation and look for that essential detail that will ‘hook’ people to your story. Then use the ‘hook’ to begin your report and get readers willing to follow you further along the story-path you are taking them along.

17. **Talk to your editor.** From the first idea of a new report, through the investigation, all the way until the final strokes of the pen, make sure you discuss with your editor. S/he bears equal, and in some cases greater responsibility for the quality of the report and its impact. **An experienced supportive editor could make a great difference for the quality of a report.**

18. **Make the story rich.** Many environment stories are complex – but they are often also photogenic, or can be illustrated with engaging human stories. Think about headlines, photos, graphs, maps, sidebars (separate boxes of information or colourful human stories). Even if the editor decides on headlines for your story it can help to focus your writing if you have a possible headline in your head before you start writing. Be ready to draw on additional resources, e.g. maps, graphs, photos from NGOs etc. to illustrate it. Use all of the resources available to bring the story to life.

19. Remember that you work for your readers/ viewers/ listeners – keep them interested, inform them, entertain them. Do all this and you'll have grateful readers/viewers/ listeners that will keep coming back. You'll sell more papers / have better viewing figures, and you will have a very happy editor, keep your job, and fulfil the central job of the journalist: to get more stories in the paper / win more airtime.

**In principle**

20. **You can change the world.** We live in strange times: corruption – both local and transborder – is a serious burden for society and ever more urgent to reveal. But it fails to get into the mainstream news often enough, and isn’t well understood by the public. The public often does not understand the grave consequences from corruption onto their lives. They do not always know (and do not necessarily want to know) how their own choices and actions can contribute to corruption. Investigators are in a position to change these. But they need to use all their creativity, skills, intuition, and stay safe at the same time. An investigator may be a campaigner, but her/his primary responsibility is finding out the facts and revealing them to the public. The world’s top investigative journalists have proven that you can make the news, and you can engage and motivate the public. **In other words – investigators can change the world for the better.**
About the author:

Pavel Antonov is the Executive Editor and co-founder of BlueLink.net – the civic action network in Bulgaria, and its virtual magazine for journalism in public interest Evromegdan.bg.