

RESONANT

RESEARCH INSIGHTS

NO. 1



1/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

Konstantinos Margaros is based at the Center for Security Studies (Kentro Meleton Asfalieas, KEMEA) in Greece. He has been working in the law enforcement sector for more than 25 years and is one of our partners in the RESONANT consortium. Sandra Balbierz from the Center of Excellence for Police and Security Reserach (CEPOLIS, Germany) talked with Konstantinos about his research, the challenges he has faced, the collaboration with other EU-funded projects and what he would recommend to analysts when using OSINT tools.

SB: *Konstantinos, thank you for your time. You are based at the Center for Security Studies in Greece. Let us first talk about your work in RESONANT. What is your work about?*

KM: I am leading the tasks of KEMEA related to the assessment and the evaluation of tools that can be used for investigating real-life FIMI-cases. FIMI is the acronym for foreign information manipulation and interference.

SB: *What are the main objectives of this work?*

KM: There are two main objectives: First, to identify open-source tools that can be used in identifying tactics and techniques relating to foreign information manipulation and interference campaigns in the EU. We focus on forms of information suppression applied by actors in the EU and in the neighbouring countries targeting diaspora communities. And second, to utilise these tools to investigate cases of information suppression in diaspora communities in the EU. The results will be the foundation for analyzing behavioural aspects of these FIMI activities.

RESONANT

RESEARCH INSIGHTS

NO. 1



2/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

SB: *Research is very often not linear. In the beginning, there is an idea and the more it 'unfolds', the more complicated it gets. So, what kind of challenges have you faced during your work?*

KM: One of the main challenges that we faced was the sheer fragmentation of the available tools. As we pointed out from the very beginning, no single tool could adequately cover the broad spectrum of tactics, techniques and procedures associated with FIMI. We evaluated a wide variety of tools with different functionalities, different levels of maturity, which made the whole testing process quite complex. Now, we made the conscious decision to focus exclusively on open-source tools. This was based on two main reasons: First, open-source tools are freely accessible which ensures that our methodology and our results remain replicable by practitioners, researchers, and civil society actors, without having the constraints of licensing. A second reason, and perhaps the key one, having the law enforcement background that I mentioned, is that in law enforcement and the public sector in general, they typically don't adopt paid solutions, mainly due to procurement rules. In fact, we found that most rely heavily on open-source tools. So, we decided to focus on this kind of solution. We faced another challenge that is important for me to mention: developing realistic testing scenarios. That was challenging, and to be honest, we had a bit of a setback in the beginning, and we had to redesign three scenarios to be able to provide accurate results. But I think we managed it in the end.

SB: *Can you tell a bit more about this? So, why did you modify these scenarios?*

RESONANT

RESEARCH INSIGHTS

NO. 1



3/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

KM: Yes, well. I'll provide an example from the area of fact checking. We first tried to test full articles within the fact checking websites and see whether this article is accurate or not. This proved ineffective. So, we took a different approach, redesigned the scenario to extract individual claims and test them separately which better reflects how these tools operate in real investigations.

SB: ... because claims are smaller than articles. It's a smaller unit and as such, complicated enough.

KM: Yes, and in some cases, it was difficult for these tools to identify to what extent an article contained false or misleading content. It was not all fake. Sometimes there were one or more fake claims, but the article also contained actual and correct information.

SB: So, one part of this approach are these scenarios...

KM: Yes. We followed a five-step process inspired by the waterfall model. We began, of course, by reviewing the existing frameworks such as DISARM and the Coordinated Inauthentic Behaviour concept and conducted desk research to identify and group tools into functional categories. We had several discussions and feedback loops with practitioners throughout the project to validate our actions and to make sure that we're on the right path. Therefore, we collaborated with the law enforcement agencies within the consortium, and during a dedicated CEPOL onsite training activity we organised. *(next page)*

RESONANT

RESEARCH INSIGHTS

NO. 1



4/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

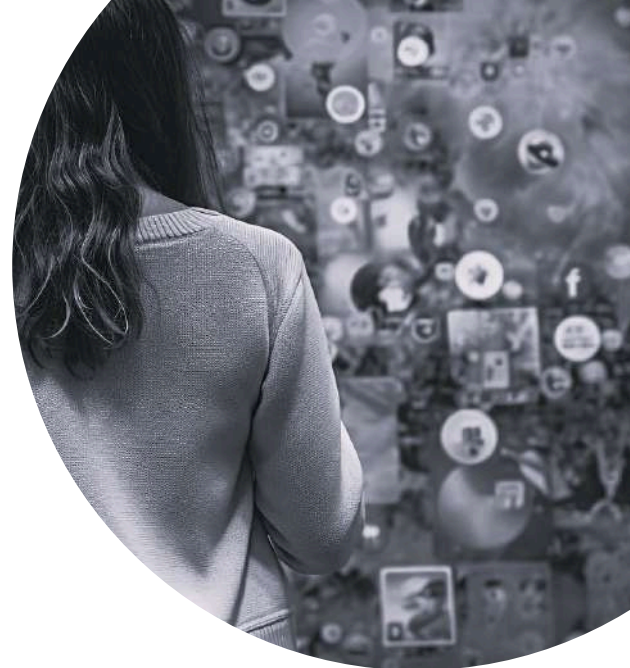
For this training activity, we had OSINT experts on board giving us the opportunity to discuss the tools with them, the categories that they use in their daily work and to make sure that we're on the right path. Beyond that, we created a controlled testing environment, synthetic datasets, sets of criteria and metrics to be able to test the functions that we highlighted. These functions were mapped to the detection of tactics, techniques, and procedures. Each tool was evaluated using a common set of parameters, including usability, detection capability, and relevance to the defined TTPs (tactics, techniques and procedures). We also included some multi-tool workflow scenarios, which represented typical steps in FIMI investigation activities. We asked our cyber expert teams to use the tools performing several different functions, like image search, validation of facts, etc. to mirror how they would proceed in real investigation. The key innovation here was not just to propose a list of "top tools", but instead we developed a methodological framework that others can use to test new tools under the same structured conditions and compare their effectiveness across different scenario types.

SB: *Now the big question: Do these tools do what you expect them to do? So, can the law enforcement agencies work with them? What are the main findings of your research?*

RESONANT

RESEARCH INSIGHTS

NO. 1



5/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

KM: Yes, they do perform, and law enforcement officers use them every day, perhaps for different activities. But what I need to mention is that these tools were not created specifically for investigating FIMI activities. They were created for other purposes. What we tried to examine is *whether* they can function and *how effectively* they can function under this specific investigative framework. So, the main findings are, and I'll begin with operational insights: We confirmed that no single tool can address the full spectrum of FIMI detection needs and that experts need to take this multi-tool approach in conducting their investigation. Now, our work has led to the development of the RESONANT Suite of Tools, which is a curated selection of open-source tools that showed the highest performance in specific function areas like fact-checking, image verification, image search, detection, etc. The second finding is, we found that practitioner workflows are very tool-dependent, but also very context sensitive. Even highly functional tools may underperform if used outside the proper context or without sufficient understanding of their limitation. This underlines the need for this methodological framework to guide tool selection and application. And that required going beyond just listing some recommendations on how to use tools but providing the framework to test their effectiveness that I mentioned earlier. And the third finding that complements the other two is the value of the simulated and controlled environment. It allows for the replication of the experiment with other tools, using the datasets that we have created that go along with each scenario. *(next page)*

RESONANT

RESEARCH INSIGHTS

NO. 1



6/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

Well, in summary, I think that one of the two key outputs of this work package is a tested transferable methodology that can support ongoing tool evaluation and training in terms of using the tools in a proper sequence or using the tools for the functionalities that perform better for this specific task at hand: the identification of tactics, techniques and procedures of FIMI investigations. And that can take place even beyond the RESONANT project cycle.

SB: So, you're coming from the law enforcement perspective, but you also mentioned that these tools were not tailored to a specific target group. What about journalists? Can they also use these tools and the methodological frameworks?

KM: These tools are not tailored to a specific target group in the sense that they cannot be used by other target groups. We adapted the framework for law enforcement officers as they need to be sure to receive process information that is valid for criminal investigations. Other groups may use them, but perhaps journalists or civil society experts may not be interested in the methodological framework as such. They would be more interested in the final product: the RESONANT Suite of Tools.

SB: You're also collaborating with colleagues from other EU-funded projects. Can you tell me a bit more about these collaborations. What are you doing there?

RESONANT

RESEARCH INSIGHTS

NO. 1



7/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

KM: I participated in the VIGILANT project's general assembly. The VIGILANT project works a lot with tools, and we had discussions on their methodological approach, the tools they tested, and possible synergies. We had a very useful discussion, especially on the selection of tools, on the categories that we and they use. We also collaborated with the ATHENA project within our FIMI cluster. We streamlined our reporting templates for the real-world case analysis we conducted, and we also aimed to have a consistent approach on how to classify, document, and analyze incidents throughout the projects of our cluster. So, we had long discussions and exchanged templates to see how to provide a result that would be more useful for the European Commission and the rest of the recipients of the project results.

SB: *Was there anything surprising during this research process?*

KM: In the beginning of June 2025, I had the opportunity to gather OSINT experts once again for another CEPOL training event, and that confirmed an initial surprise for me, namely the high degree of dependence on manual investigation and human interpretation even when using advanced OSINT tools. I mean, one would expect that solutions exist where you can just insert a claim and then you've got the full analysis of a case with actors and all. That doesn't happen. *The role of the investigator is very important. His or her interpretation is key to this effort, and that, in my view, reinforces the idea that tools are always complementary to the analyst's expertise. They don't substitute the analyst. (next page)*

RESONANT

RESEARCH INSIGHTS

NO. 1



8/8

Tools are always complementary to the analyst's expertise

An Interview with Konstantinos Margaros from KEMEA

The second surprising thing is that apparently, even though the FIMI campaigns have already been observed and documented for quite some time, there are no tools, at least to my knowledge, that were originally designed for FIMI detection. We tested several tools that were not developed with FIMI in mind but performed well in relevant functions, such as narrative mapping or metadata extraction. But there were other tools - we call them general purpose tools. There are tools like, for example, the Wayback Machine. The Wayback Machine is an archive that takes screenshots of websites at certain points of time. They're very useful in OSINT investigations, apparently. I see that OSINT investigations repurpose these tools for their activities. That adaptability was surprising and shows that creativity in how tools are often used matter more than the tools themselves.

SB: *Do you have any recommendations for analysts on how to tackle FIMI?*

KM: Trust your expertise and use the tools to complement your work, not replace it. The second one would be, I think most of them do it, but I'll mention anyway, they need to attend forums, OSINT forums, and always check for new tools or for new workflows that can really support their work. FIMI evolves quickly, so staying connected to the OSINT community is key to staying effective.

SB: *Thank you for your insights, Konstantinos!*