**Interview with M.D., Africa Center, February 7, 2025**

Your thoughts on USAID stop orders? (Non attribution)

I had quite a bit of interagency cooperation collaboration with aid colleagues on the work we are doing, how we approaching, seeing the threats similarly, they were filling me in on what they are doing and their projects, making sure we are in alignment on terminology and frameworks. Esp., West Africa, their country and regional teams acutely aware of this issue, its impact on US missions in the region, our soft power and relationships with these countries. The obj of FIMI is to displace Russian influence. Usaid may have talked about it different, developing human capacity, media capacity but these are things that we and others identifies as things that are critical to address resilience to info campaigns. They had digital lit in Cot d’Ivoire, they were funding some of the monitoring of these spaces trying to detect these campaigns. Just yesterday I was speaking to a group doing a study on behalf of DITRA, they are concerned about FIMI around bio weapons that Russia is putting out in Africa around these claims that the US is moving biolabs from Ukraine to Africa, running experiments on Africans. Part of what they were asking, is this type of disinfo going to affect the willingness of partner nations to want to work with us on our public awareness initiatives. We did that ourselves being in the process of withdrawing…. This was defn an issue where there was active 3d participation and collaboration but it.

**What are your initiatives?**

I can walk through what we are doing.

Been with Africa Center since 2019, when our ears picked up this was a problem. Russian operatives popping up in Mozambique, Madagascar, Sudan, Libya, Mali, these the first wave of campaigns, 2018/2019. It was unclear what their objectives were. They were backing two candidates in the elections, in retrospect they were experimenting and probing. Seeing where vulnerabilities are, where some of these narratives would stick, what tactics would work. We started to document in written publications, interviews, analyses. Esp as they seemed to double down on the Sahel. They touched a nerve with these anti French conspiracies and campaigns that there was a receptivity to. A wave of coups. Russia FIMI was cheerleading that. Saw deals struck between them and Wagner. And around that time when these dominoes falling and Russia running these campaigns almost unopposed and overwhelming opposition to them or counter narratives. Russia didn’t have these countries interests at heart. We tried to be more involved to lets host some events and do some engagements. Did a lot of case studies from eastern Europe and Taiwan and decided the African center would run academic programs with security professionals. A lot of our academic programs means uniformed military officers but as regional center we have authorities to work with civilians. For this issue… the non-gov groups whether fact checkers or investigating journalists the analysts and researchers the democracy NGOs already concerned about this, setting up projects and programs to do something about this disinformation problem.

So 2022, Dec, we brought together 30 expert practitioners, brought to Nairobi and had an initial round table, sharing perspectives, sharing projects we working on, what and who they were seeing as bad actors, what they needed more support for… out of that came a clear signal that there needed more capacity on detection and analysis side. Unfortunately, we get a lot of second hand info, ppl doing anecdotal studies trying to figure out what is going on. Need for ppl with digital forensics, osint, technical analytic skills to detect, expose, track online manipulative campaigns.

So our second workshop in Senegal, it was Nov 2023, we had interpreters, French and English speakers and it was a technical training. We brought in a **Lithuanian NGO called debunk** which pioneered a lot of these strategies for analyzing and then doing something about disinformation. Trying to work with ministry of defense and their parliament. They did a threat hunt, looking for these types of online campaigns, esp from Russia and participants really liked that. A hard school they could use in writing reports, share with funders, collaboration and… we started developing this network of practitioners. From that we did more theoretical work, flushing out what this model looks like, starting with the phrase “you need good info to fight disinformation”. You need expert practitioners who can be the sentinals and eyes and ears on the ground.

From the Africa center and research, we did in between the first two workshops and then next s… **two mapping disinformation projects where we try to aggregate all publicly detected campaigns researchers are aware of and take stock of who are the sponsors, what are the obj, narratives, tactics, impact and this gave us a baseline from 2022 to 2024 looks like the problem is getting worse, it is expanding and accelerating.**

The last workshops, last summer, between July and sept we were in Abidjan, Accra, Lagos, those were each a weeklong workshops. The Cot’d Ivoire was interesting bc it is the only one where it was a civ-mil subject matter exchange; partially funded by Africom j39 so half military officers, some from cyber, public affairs or communications and then civil society journalists. A few orgs in Cot d’Ivoire specifically focused on disinformation. We brought them together to help them think about this as a multistakeholders problem and different roles and different lanes but it takes societal collaboration. Helping the military understand why journalists are key to a healthy information space. Helping them understand case studies from eastern Europe how there can be better relationships and info sharing between media and security sector. If disinformation was spreading, the military does not need to announce it or do awareness campaign but can leverage relationships to bring (civil society) media in. The ministry of communication was involved, they were motivated to do something, they see a threat from the Sahel, they see Russia trying to ramp up pro coup and authoritarian anti democratic information. This is when the global engagement center existed, they signed memorandum with Cot d’Ivoire aid was running digital literacy campaigns. They were I believe, the global engagement center working with another group, DFR labs, they were going to do more follow on training a lot of movement in Cot d’Ivoire.

Nyt article came out on public health disinfo, esp. in Burkina Faso, if go back to that there are quotes from Ivorian ministry of communication saying how much the US is helping them, how motivated we are to help them. Those quotes read differently now.

The GEC ppl working Africa are now in the Africa bureau. I don’t know if they will continue doing FIMI work.

I felt a lot more of a network before.

**IMPACT OF TRAININGS**

**Can you describe the impact of this?** The most promising ones were the ones in Ghana and Nigeria. Those had a number of repeat participants, they were the mentors to the newcomers and we were building out the network. From Nairobi to Ghana and Nigeria it was night and day how much the field had advanced. Ppl understood the terminology, what we needed to do, value of a shared professional language professionalizing the field. We are working teams like FIMI, Disarm, ppl know what that means. When you uncover a campaign on line and start to write a report you write it as a researcher in Nigeria but somebody in South Africa and DC can understand the incident, who the threat actor was, the behaviors, what the TTPs were, what their content they were trying to spread. A lot of this comes from cyber security. Basically this format of report writing is adapted from cyber security. That is where we were sensing where this was going and needed to do go. Bring that from Brussels, get buy in, get their inputs, they were buying in, still bought in … this is more than fact checking; this is analysis to understand where info space is being attacked and manipulated. There is a whole bunch. These are now five day trainings we do where we talk about writing these reports, the osint skills, we talk about the platform called Open CTI, which is developed for cyber security, now reworked and open source but for FIMI researchers so they can build a database tracking these campaigns so when an incident happens it is all driving for faster response times so that when something happens, the kill chain, which is referenced in the the Phoenix Challenge conference. You are trying to detect through constant analysis cycles of info space when there is an attack on it and be able to intercept it and do the pre-bunking, debunking, go after with legal means, it is developing an entire strategy on how to respond. And out of that through our trainings there are now a number of professionals who credit us who have introduced them to this, helping them understand on the technical side the problem, orient them to design responses, how to work collaboratively with other analysts and we see a number of pubs come out that have the finger prints of that. We saw one after the Nigeria event where, last summer, the Nigerian cost of living protests in which some waved Russian flags. This researchers at our event, he afterwords, did interviews and made the link, he exposed that it was the Africa initiative, Wagner successor, that was recruiting and paying these Nigerian influencers and exposed that. Which is a lot better coming out of Nigerian center than our center. Why it is so important to build that capacity on the ground.

**Was usaid funding these orgs?** I don’t know the whole picture of their funding, I know they are particularly funded by the social media platforms.

**Will meta get rid of them?** We had a virtual reunion last week and that was the first discussion topic. Meta said it was only closing the US fact checking so for now it does not apply internationally so nothing imminent.

**Recommendations?**

Two months ago our plan was lets continue to build momentum, see how we can scale up. I was doing calls and having conversations with aid colleagues, GEC, state, European colleagues. Lets make sure we are moving in the same direction. And deconflicting, mapping what we are working on. For us our narrow is in building up this technical capacity of the analyst, so we want to scale that up. Defender community, these are defenders of the info space. **We have 140 alumni of workshops we are trying to keep engaged through virtual follow on events with key note speaker and time for discussion. Lets try to get to a point where there are 500 or 700 trained professionals all speaking the same language, understand the field, equipped with these tools and these processes.** We had some goals in mind, we wanted to do more virtual trainings. Our partner from debunk Lithuania is developing an online course, in English and French. We could ask African participants to take before coming to workshops. We are still talking to Africom bc Africom funded the Ghana and Nigeria events. They were pleased with the outcome so talking about doing two more, one in Tanzania more focused on China that would bring more practitioners and west Africa possibly Cot d’Ivoire because such receptivity there. And other org from francophone countries, Senegal, Benin. Expand this network with these professional skills. That is tbd. Even before the change of administration been focused on this as a FIMI issue. Yes there is domestic disinformation. The most malign corrosive, sophisticated campaigns are these foreign sponsored. Then it becomes a sovereignty issue where other countries meddle inside…. That can be communicated and framed as strategic competition issue that is still should be a priority if we are concerned about countering Russia and China in Africa.

**Is there a risk that the work could be politicized?** Our selection process for who comes in. The participants we invited understood the threat from Russia and China in the information space. … elections and campaigns, so we are communicating that the graver threat is the foreign actors but if they want to take what they are learning and use for domestic disinformation, that is up to them. We can use this for all the work we are doing. Not FIMI but IMI (without the F for foreign).

Part of it is choosing partners wisely and working in countries where less of a risk to be used politicized. Cot d’Ivoire, there is an interest in countering FIMI. .. tread carefully in Nigeria bc it is more fractured country, less democratic. Kenya, Ghana, Senegal, Tanzania maybe.

**Can these skills be used for counter terrorism?** Some analysts who attend workshops are tracking the militant groups, one individual for who that is his thing. There is a lot of info manipulation and taking advantage of lack of platform oversight doing in local African languages. So it is definitely party of it. It is the same skillset, you want to have visibility of what these groups doing online and so the FIMI framework applies.

Your training is focused on Civil society vs. gov? it has all been civil society except for Cot d’Ivoire where half of participants were military or gov.

**Value in building government capacity or should the focus be on civil society?** This is one of the earlier lessons we embraced from Baltic countries and Lithuanian colleagues. Governments and political parties come and go and yes you want some gov institutions with longevity and continuity but the torch the needs to be held by civil society and the media and these civic organizations… so not concentrating too much capacity in the hands (of government).

**Role for gov?** if there is a gov that wants to approach this thoughtfully and carefully there is a role. Whether supporting civil society initiatives, leveraging gov capacity to pressure the social media companies, whether its, imposing costs on the sponsor of these campaigns, if carefully written policies and laws criminalizing some of these behaviors…. In Lithuania, there was no law on the books outlawing bot farms, … someone’s barn where running computers, the ngos were the ones that detected the bot network, tracked ip address, went to the police and the police said no jurisdiction so then they went to work with parliament to create legislation.

At the multi-lateral level, ECOWAS, they are working to do this, they want to have sophisticated early warning system, … having a finger on the pulse for how healthy their countries are in terms of information. USAID was working with…. More like, they felt like military coups caught countries off guard so early warning system could have given them a better beat.

**Training Military?** The militaries need to understand this domain, understand delicacy and have situational awareness. Military should be investing more in MISO and monitoring social media. Before going on patrol near Burkina Faso, they should understand what is the info env there is like. This is a huge issue for peacekeeping forces where they are targeted and attacked. Their sentiment inflamed. Really worked up in DRC, we know these intentional disinfo campaigns.

**How can information operations support?** I always say, it can be counter productive to dabble in the dark arts to defeat the dark arts. The French still paying the price in central African republic. They set up fake facebook profiles to fight Russia profiles and to this day certain African audiences cite this to say the French are the same as the Russians so created false equivalency issue that Russia exploits. So it was a self-inflicted wound what the French did. Being aware of those costs and risks and how trust is paramount and valuable. There is a lot to be learned from the military just good strategic communication principles and incredible, timely, accurate consistent comm and use that as a counter, which is the opposite of discredit, distort, deny.

Lithuanian.

Dr. Joe Segal, he is the Russia expert, follows these issues.