Participant name: Paul Corbett

Participant organization: OSC, US Embassy Ghana

**How long have you been here? Are you new?**

* 7 weeks. I was in the Army Cyber Command before this.

**Can you give us your overview of the situation?**

* I don’t have much because I am currently doing an internal assessment. We are creating an inventory of what is working and what is not. It will be my focus for the next days – create a roadmap for the future, how we can apply U.S. funding effectively.
* Ghana is under the Brooke Amendment – if a partner owes a lot of money to the U.S., assistance is pulled.
* A lot of things the US has done here – equipment, training, SETAF. But it is not clearly defined. My job is to determine which direction to go to.
* I think the most useful thing to do would be to find an interesting path forward about misinformation and disinformation.
* In AFRICOM, we have a unit working on cyber and information [KH did not get the acronym -COIE?]. Their job is to identify misinformation, target it, and pluck it out. They don’t do security cooperation. They are not prohibited from doing that. Someone like me stationed in an African country is not convinced that Ghanaians, Ivorians, and Burkinabes can do it on their own. How can they do it if it requires millions of dollars of investments, shutting down social media?
* My job is to work with Ghanaians to find out what they see as the biggest problem. Then, we can leverage U.S. resources and resources of other countries like France, who have a lot of money available.
* I am going to start with getting the baseline for all the programs – what we as the U.S. are providing to the Ghanaian military and what works. We might not be interested in misinformation and disinformation. Maybe Ghanaians are not interested either.

**Q: We heard that the Ghanaian military and government have an appetite to improve efforts in the space, but they don’t know where to start.**

* Institute for Security Governance came to Ghana. They have done a lot of things within the MoD and the military. They don’t tackle cyber. I’d like to see if Ghana has a cyber strategy and media strategy.
* In some countries, the military is tasked with the overall approach to cyber. I don’t think they have their own networks. Even if they do, they are small.
* I am starting from the top, coming up with a strategy, multi-year plan. I want to find out what can be done and what is out of reach. Some things are too expensive.

**Q: Some things are, but other things can be surprisingly cost-effective**

* In cyber, I don’t know what the Ghanian starting point is. When we say cyber, we talk about very basic things here. They don’t talk about the manipulation of data. What to do – take an assessment of where they are now, make a multiyear plan, and identify resources like the Institute. Find where misinformation is and stamp it out.

**Q: What has already happened with our security cooperation that has influenced?**

* Not much. We provide a lot of material resources – building, shooting ranges, boats, a lot of assistance to their navy. Material resources + training to teach them how to use. A lot you can find on Google. Recently, we provided some armored personnel carriers. Our focus has been on the northern border and maritime security.
* So to everyone else like Chinese…Chinese got pirated in the ocean recently. A boat with a Ghanian flag snatched them. There are two theories. First, it was a piracy, which always gets good press. The second is that one group of Ghanaian had a legitimate concern with a group of Chinese and snatched them.
* Solutions to Ghanian and West African problems in cyber and misinformation and disinformation have to be less sophisticated than in the U.S. They don’t have a lot of cyber stuff they presented during panel 3 at the conference, like radars. They have only a few drones – it’s all a dream.
* They have a small homemade drone’s capability. They order parts from China and assemble them in Ghana. They can use them for themselves and sell them. It is out of character how the military operates here – to have such a home-grown solution. It is a small drone, but it does highlight that they have some creative solutions to their problems. But money is not there. There has to be an overall cultural change to highlight cyber security and cyber hygiene. They have to be like us – every kid under 15 has a smartphone. In Africa, if you are over 35, you don’t know how to use a smartphone. But kids do. Computer savvy-ness will come with generational change.
* I am their regional Africa guy. We don’t have many on the defense side. U.S. solution can interfere with local context. The most famous one is with the security cooperation – everyone uses their phone to transfer intelligence. There are ways to do that – become encrypted, use own services. From the U.S. perspective, what they are doing is bad. But when we provide them a high-tech solution – like an app on a smartphone or radio – they become solely reliant on that. And in this case, they will miss so much stuff. When you get a high-tech solution from us, you miss so much, as so few people are using it. How they get info – people call you. We can make it worse, so we have to be careful with what we provide. Do we want to disrupt the networks that have been building for 20-30 years? When we tell them to switch to our encrypted email and not their personal emails, they used to transfer information between countries. This looks good but doesn’t account for local context.
* Unsophisticated can also wreak havoc. A 22-year-old hacker in a coffee shop in Nigeria can spoof other accounts and scam people. Someone mentioned it. French actually look out for things like this.
* Not a lot is happening to track that. Someone will say – Did you see that General has 3 FB profiles. You’ll get two of down. I recently started to get LinkedIn profiles that look legitimate as Ghanaian military. But then it’s just someone trying to sell a car. But it looks legitimate with 20k followers.
* I have questions – is there a potential to do – there are some situations where overzealousness in Ghana, Cote D'Ivoire – monitoring of internet there can be negative effects – what is too much?
* *[Jackie engaging in a discussion]*
* If there is a coup forming right this second, do you want to curtain social media right away, or do you want to continue monitoring it? There are other countries where we’d be hesitant to use the tool allowing us to do that, like in like Burkina Faso. If they turn off their social media, somebody can come back and say – the U.S. provided the capacity to do it. We have to be careful.

**Are you working with communities?**

* We can get into communities. But I wonder how expensive it would be. But we can do some of it.
* There are AI solutions that can scan social media at all times for code words. It is probably done.
* People in this space – the cyber command element is in the space. It is an inextricable link – the team in Stuttgart has primacy in Africa and cyberspace. We tried to get them here to the conference. But they said no.

**Any other agents in the space?**

* I haven’t gotten my head around that yet. I will still look in Chinese influence. But I have a controversial opinion here: Is it necessarily a bad thing?
* 3 years. January.