Module 4 Video 2: Influence networks (A case study presentation) with Ben Strick

[00:00:00] Hello. My name is Ben Strick, and this is a case study on the influence operation in West Papua. This specific case study is about the successful identification analysis and attribution of that information operation by myself and Elise Thomas from the Australian Strategic Policy Institute.

[00:00:20] This whole investigation starts with this video that was uploaded on Twitter. Specifically, the video was about policy and budget to improve circumstances in West Papua. It's a very pro Indonesian government video. It's not necessarily disinformation. It's not wrong. However, there's an interesting way in which was uploaded. And that's where we're gonna start to look at the accounts that we're actually uploading this video.

[00:00:46] So one of the first accounts that we're looking at is marco267. Now, if we have a closer look at this account, we can see some interesting things. So, first of all, he's uploading this this video or re uploading from Papua West, which we can say down the bottom with the hashtags #westpapuagenocide #freewestpapua and #letwestpapuavote. The first sign of this being a information operation is the fact that we've got a multitude amount of accounts uploading the exact same text. And they're even making that exact same mistake with the West Papua hashtag that doesn't have hashtag and still has a space in it. And also organically sharing it from this single account, papa West.

[00:01:29] So now we need to start diving down into the accounts to get to the root of what's actually happening here. So, for instance, if we take a look at Marco, one of the first things we can do is have a look at the profile picture of the account to see whether he's real, whether he might be a real person or not. So a simple image versus search on Yandex image reverse search shows that his photo is widely used throughout the Internet on various scams, dating websites, and has even been reported on on a number of a number of different scams. So we can probably say for sure that that's a stolen profile.

[00:02:02] So we can go step further on that as well. And what we see here, we can actually try and scrape more data available from this. And we can do that with a simple Python code available on GitHub.

[00:02:14] This allows us to scrape information about an account and put it in an Excel spreadsheet. So what we can do now is we can open up that data into a spreadsheet. And I've got that for one of Marco's friends here, bellanow. And now having a look here at some of Marco's friends, we can see that some of these upload times are very similar. So we've got 32:56 for bellanow and we've got 32:54 for kevinma. That shows signs of automation, like there might be a script running that either retweets or uploads this content.

[00:02:43] We can also go a step further than that. And we can have a look at Marco in a network. Now, this is a visualization of what Marco's retweeting, liking, commenting and sharing network looks like on Twitter. Now, this entire network is scraped from the hashtags #freewestpapua and #westpapuagenocide. So these are all the accounts over a five day period that uploaded content to Twitter under those hashtags.

[00:03:08] Let's have a look at Marco's Network. But who are these other people in his network? Well, now we can start to dive down into that and see some patterns among all these accounts. And there's one specific account stands out and that's West Papua I.D.. So what we can do is we can go to that Web site. OK, so we have very similar pro-government content about West Papua. What else do we have? We have a Facebook page and Instagram account, a YouTube page and the Twitter account as well. So we can go into the Facebook page. Facebook has a little page transparency feature down there. It shows us advertising might show us who owns this page as well. So we can have a little look at that. We can see that this account has even been running ads through Facebook ad platform. We can also go a step further than that. And we can actually have a look at the registration details of the website. Usually they're blocked. But this one forgot. So we can see that we have a name there. We also have a phone number and an email address.

[00:04:09] Now, what can we do with that phone number? And most people have a profile picture with their WhatsApp number so we can use it in Yandex image reverse search. And this is what we got. And we could also take that name into LinkedIn and find fellow employees of that of that organization, Insight I.D..

[00:04:25] Now, if we go a step further than that, we can also have a look at the rest of the names associated with the email addresses that people own. After we reported these findings, the Web site since closed down. Facebook removed that content from its platform. Twitter also removed that content from its platform.

[00:04:43] Thank you very much. I'm Ben Strick and this was an investigation I did with Elise Thomas from ASPI. And thank you for watching.