Interview: Lorenzo Franceschi-Bicchierai

Journalist **Lorenzo Franceschi-Bicchierai** talks with *Limn* about the details of the DNC hacks, making sense of leaks, and being a journalist working on hackers today.

Gabriella Coleman: As you know well, the DNC [Democratic National Committee] hack and leak were quite controversial, with a batch of commentators and journalists debating whether the contents of the email were newsworthy, and another batch of commentators assessing their geopolitical significance. Our Limn issue features pieces that in fact assess the importance of the DNC hack in quite distinct ways: one author taking the position [that] the emails lacked consequential news, while another author forwards a public interest defense of their release. As someone who has covered these sorts of hacks and leaks, how important was the DNC-Podesta hack? And in what way? Does it represent a new political or technical threshold?

Lorenzo Franceschi-Bicchierai: They were definitely relevant from a geopolitical standpoint, if you will. All signs point to Russia. So, this was a nation-state hacking a legitimate target from the point of view of their interests, and from the intelligence point of view, these were legitimate targets. So, that's not too crazy, and this is something that would get a lot of people on Twitter saying, "Well, spies are gonna spy." But I think it was interesting because, of course, it did cross a threshold or line, if you will. Because this wasn't just hacking and spying on them, it was putting everything in the open. They published the stolen data through WikiLeaks, they published through their own leaking platforms, they had this website called DC Leaks, and they had the famous Guccifer 2.0. They had all kinds of channels and they were actually very good at using multiple channels just to get as much attention as possible, even if the content wasn't actually that compelling.

GC: What you're suggesting is that the trade craft of state spying has always worked on these discretionary channels, that is, back channels that only the intelligence world has access to. And all of a sudden here's this moment where they decide to move everything from the back stage to the front stage.

LFB: Yes that's definitely a good way to put it. Spies, by definition, work in the shadows. We know about intelligence operations when they leak or when someone talks, and sometimes it's years later. At that point it's not even that newsy. But in this case, it all unfolded in real time, which was very interesting. The big question in the DNC-Podesta hack that we'll probably never know the answer to—if the DNC and Crowdstrike didn't come out with the attribution, if they didn't come out saying this is Russian intelligence—is: would the hackers and the Russian government have responded in the way that they have? By systematically leaking documents and slowly dripping information? I don't know. Maybe they would, maybe they wouldn't....

GC: Ah, that's a good point. Did Crowdstrike call out Russia before the material was leaked?

LFB: Yes, CrowdStrike attributed the attack to Russia on June 14, and Guccifer 2.0 came out on June 15. But it's important to note that there was another website, also linked to Russia, that started leaking stuff before that. The site was called DCLeaks and it started publishing stolen documents just a few days before CrowdStrike went public, but it's almost like no one noticed it right away. DCLeaks published hacked emails from Hillary's [Clinton] staff on

June 8, according to the Internet Archive. This means that perhaps Russia was already going to leak documents, and CrowdStrike's accusation only accelerated the plan. Perhaps they were planning to release the more interesting stuff closer to the election, but they felt like they somehow had to respond to the public accusation. Who knows!

GC: Your point is an important one because it suggests that perhaps the execution of this hack and leak was experimental and it also seemed quite sloppy as well.

LFB: Maybe it was the plan all along. Even if it wasn't, it definitely didn't look very well planned at times. I think the best example is this Guccifer 2.0 persona. He—let's say "he," just because they claim to be male—he showed up a day after the CrowdStrike and Washington Post reports and it definitely seemed like the character was a little bit thrown together. He claimed to be a hacktivist trying to take the credit he deserved, which would have made sense if he really wasn't a Russian spy or someone working for Russian spies. But then he chooses the name of another famous hacker as his own, simply adding the 2 in front of it and—you know this better than me—some hackers can have a big ego; why not just come up with a different name?

GC: True, they want recognition for their work.

LFB: Just like writers. You know, it's like, "I wanna have people know that I did something that I think [is] awesome and worthy of recognition" thing. We all have our egos. And using the same name as another famous hacker from years ago just sounds very strange. I don't think I've ever seen that before.

GC: It's funny to imagine the meeting where this happened in some nondescript Russian intelligence office where someone's like, "All right, we are looking for a volunteer to play the role of the hacker...." And whoever got nominated or volunteered didn't do a very good job. Which is a little bit weird because Russia does seem to obviously have a lot of talent in this area.

LFB: Yeah, they seem to be very good with these information campaigns and deception campaigns, and stuff like that. It's always possible that they contracted this out to someone. **Maybe they thought this would be an easy job, but somehow it snowballed.**

GC: Let's turn to the next question, which is related to the first one. Many of these recent leaks, from Cablegate to the DNC leaks, are massive, and the journalistic field mandates quick turnaround so that you have to report on this material very quickly, right? What interpretive or other challenges have you faced when reporting on these hacks and leaks?

LFB: Yes, there's many. You definitely nailed one of the biggest ones: the quickness and fast-paced environment. And I think that sources are catching up to it, or sources of leaks and publishers of leaks, I guess. There are still large data dumps that just drop out of the blue. And everyone scrambles to search through them. But, for example, WikiLeaks have become very good at staging leaks in phases. They slowly put out stuff because they know very well that they're going to extend the time that they cover [an issue], that they will get attention. With the Podesta leaks, it was almost every day that there was something new.

GC: Right, that was very well imed and orchestrated.

LFB: And it wouldn't have worked if they had just dumped everything the first day. Because we're humans too and we get overwhelmed. And everyone gets—readers get overwhelmed too. And if you dump 3,000 emails, you're just going to get a certain level of attention. If you do it in segments, and in phases, then you get more attention. I think sources are catching up to that.

But the other challenge is that sometimes you get things wrong, or you just assume that the documents are correct, and you publish the story based on the documents, saying, "Oh, this happened." And maybe you haven't had time to verify. There's also competition. You always want to be the first. The ideal scenario is always getting something exclusively so you have the time to go through it. The advantage, though, of having stuff in the public is the crowdsourcing aspect. So, for example, when The Shadow Brokers data came out, pretty much everyone in the infosec world spent the entire day, all their free time, looking through what had come out. And they published their thoughts and their findings in real time on Twitter.

For example, one of these people was Mustafa Al-Bassam. So that's something that maybe you can't get if you have information exclusively. And then getting something exclusively obviously has its advantages, but that's one of the drawbacks. You don't get the instant feedback from a large community.

GC: And that seems to have happened with the recent CIA-WikiLeaks leak as well.

LFB: And it happened with the Hacking Team leak. It was very useful for me and others to keep an eye on Twitter and see what people found because there was just so much data... That's also exactly what happened when the Shadow Brokers dumped hacking tools stolen from the NSA [National Security Agency]. These weren't just emails or documents that a lot of people could look at and understand or try to verify. These were sophisticated pieces of code that needed people with a lot of technical skills to understand and figure out what they were used for and whether they worked. Luckily there's a lot of very good infosec people on Twitter and just following their analysis on the social network was really useful for us journalists.

GC: Based on what you've seen and reported, do you think that we—not just lay people, but experts on the subject—are thinking clearly on vulnerability? Is there a focus in the right place on threat awareness, technical fixes, bug bounties, vulnerability disclosure, or do you think people are missing something or are misrepresenting the problem?

LFB: In the infosec world there's sort of a fetish for technical achievements. And it's understandable, it's not the only field. But sometimes this fetish for the latest, amazing zero-day, or the new proof-of-concept way to put ransomware on a thermostat—which, you know, is tough, I wrote a story about

it—but sometimes it makes us forget that these are still kind of esoteric threats, maybe, and also unrealistic threats. In the real world, what happens usually is phishing, or your angry partner or ex-partner still knows your password to your email and after you break up they get into your email... stuff like that. Some cybersecurity expert might scoff at this and say, "That's not hacking," but that's what hurts the most, though.

And I think that, for example, Citizen Lab has done a great job of highlighting some real-world cases of abuse, of hacking tools used against regular people, but also dissidents and human rights defenders. And in many of those cases, there was no fancy exploit, there was no amazing feat of coding or anything involved. It was just maybe a phishing email or phishing SMS [text message]. So I think that we could all—both journalists and the industry—do a better job of explaining the real risks to an average person and telling them what to do, because just scaring them is not going to help.

GC: Yeah, this is a great point and reminds me of considering public health–type campaigns: in this case, a concerted security hygiene program to teach everyday people the basics of security. The history of biomedical public health campaigns are instructive here. When the germ theory of illness was gaining ground, it took enormous effort and labor to convince people to change their habits, like to wash their hands, to cover their mouths when they were sneezing. It took a few decades of public health campaigns both to convince people that there was something called bacteria that could make you sick, and that you had to change your behavior. So why wouldn't we need something similar for computer security? But that's obviously something that info security companies—rightfully so—are probably not going to invest in.

LFB: Yeah, there's not a lot of money in that. But I think that we could demand more and expect more from companies that are only maybe tangentially in the infosec industry—like Google, Facebook, these big giants—that everyone yuses, more or less. So they can really make a big difference. If Google made two-step verification mandatory, or if they just made it an option to choose when you create your account, that could make a huge difference in the adoption of these measures.

GC: That's an excellent point.

Let's turn to another final question: Can you tell us a little bit about challenges you face writing on hackers and security?

LFB: One of the challenges is cutting through the noise. Infosec and cybersecurity have become so popular now that there's so much noise. And it's very easy to get lost in the daily noise. And as an online journalist, the risk is double because that's kind of like my job: I have to be on everyday and see what happens everyday. Let me give you an example: yesterday there was some revelation about a vulnerability in the web versions of Telegram and WhatsApp. It made a lot of noise. It wasn't that big of a deal in the sense that we don't know many people are affected. Probably quite a few. But we don't know how many people use the web versions of these apps.

Another challenge here is that so many people are trying to position themselves as experts in this field. As a journalist, it's sometimes very hard to select your sources wisely because there are a lot of people that want to say something. They want to have their opinion broadcasted, they just want to join the fray and talk about the latest infosec news.

GC: How do you go about resolving that noise? Are there some experts that you rely on more than others? Do you talk with colleagues?

LFB: Yes, I think it's a combination of everything you said. Talking to colleagues helps. I work with a really great journalist, Joseph Cox, who you know as well. It helps sometimes to share.... We ask each other: who shall I talk to? That helps. It's also just a matter of time. When I started out, it was really hard to tell [who to talk to]. You would go on Twitter or just...everyone seemed like an expert. It's very easy to say "cybersecurity expert" or whatever, and make claims that sound more or less informed.

The PR and marketing machine behind the infosec world is also very strong. Every time there's a breaking story, we get dozens of emails trying to sell random people saying stuff that is not even that interesting. But there's a lot of money involved, and so marketing is very powerful in the present world. I think after a while you just become very cynical—in a good way. If you smell the marketing campaign, then you're like, okay, I should probably ignore this because it's just marketing.

GC: Right. Is there sometimes a situation where it is a marketing campaign, but it is also a really cool important technology that has the potential to change things, or already has?

LFB: Yeah, sometimes attention is warranted. I'm trying to think of an example. I mean, for example, [the cybersecurity company] Kaspersky has a really big marketing side, and they do push their research very strongly through their marketing and PR people. Most of the time, their research is actually very interesting, so it's not necessarily—like if you use marketing, it's not necessarily bad. There's just too much of it now. The problem with marketing is mostly when the sources or companies try to make their research look too good or make unfounded claims. Obviously I understand that they're trying to get attention. But I think that actually—they don't realize it—that that sometimes can backfire.

GC: Right, that's a good point. And you know, I'm always thinking of potential PhD topics for my students; it would be really interesting to study the domain of infosec company research and the processes of knowledge vetting. How is it similar or different to academic peer review? And as you say, there's a lot of very respected researchers and the material coming out of there is often very strong and important. But from my understanding...they will limit what they release too. Right?

LFB: As a company, yeah.

GC: Right, because you don't want people being able to take things from you. So there's this fine line between researching, getting the data out there, but maybe not always being able to reveal everything.

LFB: And that's why, for example, an average Citizen Lab report is more interesting than an average infosec

company X and Y report, because—and this is the point that Ron Deibert, the director of Citizen Lab, made when I spoke to him recently—you know, we don't have to hide anything. And they want to encourage other people to look at the data and look at it themselves.

Another big challenge is the anonymity and pseudonymity of sources. It's almost like a default...I don't have the numbers...but I think a big part of my sources and my colleague's sources are often anonymous or pseudonymous. They have a nickname, they have an alias. And the challenge sometimes is: Is this the same person I spoke to the other night? And the challenge there is not just verifying who they are, which is sometimes impossible, the challenge is sometimes keeping your head straight, and your sanity. Because the person sounds a little bit different. And "sounds" is probably the wrong word... because the tone is different...and you start thinking, is this a group? A friend of the guy or the lady that I spoke to the other day? But I think that when this happens, you have to focus on the content of the conversation, what they're talking about, what documents they might be providing. The story might be there, although...it's sometimes easy to forget, but what readers care the most about is people. So, the hacker, the hacktivist, is very often one of the most interesting parts of every story.

GC: Right, often there's a lot of mystique around them or hacker groups. And...I know this well from my research about how difficult it can be to always be dealing with pseudonymous people. I thought Jeremy Hammond was an agent provocateur by the way he acted. And I was completely wrong, you know. It can be very hard to suss out these things.

LFB: Definitely. I think that's one of the biggest challenges, for sure. But it's also interesting in a way. I don't fault them for trying to protect their identity. And that's just how it is. And that's not going to change anytime soon. Sometimes it is frustrating. Sometimes you wish you could have that certainty. In real life, you see a face, and that's the person. But in these cases, there's not really much to go on.

LORENZO FRANCESCHI–*Bicchierai is a a staff writer at* Motherboard, *where he covers hacking, information security, and digital rights.*

Interview conducted March 2017.