A dive into the hacking sea (interview with Pr. Gabriella Coleman)

Gislene Feiten Haubrich[4]

Listening to Gabriella Coleman is inspiring! Not only is her research fascinating, but her willingness to share knowledge guides us in an expedition through the hacking world.

It was a summer day in July. Gabriella, among many commitments, devoted some time to talking with us. Throughout this conversation, we spoke of her first steps in research and her turn to hacking studies. She helped us to understand concepts such as hacker, black, white, and grey hats and the relationship between hackers and cybersecurity. She also introduced some historical events around the hacking world, and of course, we ended this conversation asking for advice for those who want to start studying this fascinating phenomenon.

Gabriella (Biella) Coleman is a full professor in the Department of Anthropology at Harvard University and a faculty associate at the Berkman Center for Internet and Society. Her scholarship covers the politics, cultures, and ethics of hacking. She is the founder and editor of Hack_Curio, a video portal into the cultures of hacking. She formerly held the Wolfe Chair in Scientific and Technological Literacy at McGill University and was an assistant professor in the Department of Media, Culture, and Communication at New York University.

We hope you'll enjoy reading this interview as much as we did while working on it!

Picture 1: Gabriella Coleman

"Often, when people think of hackers, they think: 'Oh, they have no ethics'. And it's the opposite"

Gislene: Thank you, Gabriela, for accepting our invitation. You were very kind since our very first mail exchanging. Thank you! I will start our conversation with a very preliminary question. Why did you decide to become an anthropologist, and when did you decide that this was what you're going to do for life?

Gabriella: In high school, our history teacher was an inspiration. We found out that she had majored in anthropology in college, and we asked her to teach us a class in anthropology. Then, I basically fell in love with it. I think, for me, the reason why I found it so powerful was that there were just certain aspects in growing up around certain norms and expectations that I just thought were given. And then the anthropology class kind of showed me that different societies treat all sorts of things, whether it's around relationships or norms, very differently. And I found it really eye opening and liberating. That was what drew me in. And then actually, a year later, I ended up living on a boat for a year, doing environmental research with people from very different parts of the world. And a lot of the misunderstandings happening there were not personal; they were cultural. So that experience kind of reinvigorated my commitment to anthropology. So, that's basically what put me on the path to studying anthropology.

Gislene: You've been studying hacking for a long time. Was hacking your first topic on anthropology? How did your research on hacking start?

Gabriella: It was not my first topic. I actually, in some ways, was doing pretty traditional anthropological work in graduate school, working on religious healing in Guyana, the Caribbean, South America. Whereas I did already have a side interest in free and open-source software, I'd never really expected to pursue that for my PhD. But then, I ended up getting quite sick for a year, and I was stuck at home, and I had fast internet connection. I read more and more about these hackers who were really committed to openness and had created these alternative licenses. The more I learned, I was just really struck by the way that engineers reworked the law. By the time I got better, I decided: 'this is really what I wanted to do'! There was no anthropologist really working in this area, I had learned a lot, I was intrigued, I was puzzled. And so that's when I made the turn to computer hackers.

Gislene: Very interesting. And we've been... I've been hearing about hacking all my life. However, based on the way people sometimes frame it, approach it, I think it is not clear what is hacking, after all. From all your research, and you are, I think, one of the best people to really explain to us what is hacking, and why is it important in our society?

[4] Researcher at CITCEM, board member and coordinator of RGCS.

Gabriella: So, hacking and hackers[5]. On the one hand, you use these terms, and everyone knows, at some level, what you're talking about, or a picture comes to mind. For a lot of people, it's a very narrow picture that often pertains to what sort of hacking is in the news. It might be around ransomware or nation-state hacking. Certainly, those aspects of the hacking matter, and they're sort of legit, bonafide hacking. But the domain of hacking is so much larger, so much more diverse, and so much more interesting. It tends to be technologists, although it doesn't necessarily have to always be tied to technology. But it's often tied to technology and computers. It's about individuals who have a sort of heightened commitment to either kind of computing or some aspects of computing in ways that often challenge normative treatments around knowledge and computing. That's a very broad sort of definition because, within that bucket, there are very different types of hackers. There are those that liberate information, those that secure systems, and those that use their skills for protests. So, there's nothing that kind of unites all hackers because there are different sets of practices and different sets of ethics. If there's something that unites all of them is a passion for computing. It is not of accepting the given ways that society treats computers and knowledge. And it is providing alternative paths around things like knowledge, security, and protest. Maybe one additional element is the idea that hackers are highly individualistic and loners. And for sure, some hackers are committed to notions of individualism, but it's a very collective practice as well. It's very, very collective. Whether it's the need to be collective to make things or the fact that hackers get together all the time, socially and professionally, to do their work, they also kind of get together to celebrate hacking as well.

Gislene: I will seize this comment you're sharing on how they have this 'will' to be together and socialize. One of the concepts that have been inspiring a lot of, for example, coworking spaces, at least that first generation, are the one of hackerspaces. What can you share with us about your experience in these spaces? How it was for you seeing hackers socialize in these spaces? Actually, how it was for you socializing with them?

Gabriella: I've been to a lot of hackerspaces, in different places, from San Francisco to Italy, to many other places. Hackerspaces are dedicated spaces, oftentimes in cities, where hackers come together to socialize but also to move projects forward. And this kind of face-to-face time is incredibly important for hackers. Hackerspaces are places where hackers get together routinely. There are very different types of hackerspaces. Some of them are very pragmatic, and it's all about the kind of technology and certainly creating a space where people can come together and learn from each other. And obviously, there's a politics to that. But other hackerspaces are very politically oriented. We have hackerspaces, for example, in Italy, that are kind of leftists and anarchists[6]. So, on top of the technological aspects, there's a real commitment to social change and social justice as well. I'll never forget this one time. I was in a meeting in Italy, in a big square, where they have a hackerspace. The meeting gathered a bunch of Italian hackers in Rome who were organizing a yearly meeting. They were going to hold the meeting at Hack lab that was a Makerspace, and it was called Fab Lab. And for, I think, two hours, it was just a big debate as to whether to call it a Makerspace or a Fab Lab, because that's what it was, but oftentimes makerspaces and fab labs don't have a very political orientation. But this group did. And so they were worried that by calling it a Makerspace or a Fab Lab, it wouldn't convey their strong politics. And so, for like, two hours, they were just debating what to call the space. So, this is a little story just to share that, along with creating spaces where people can come together to make, create, learn, and innovate, a lot of hackers also care about things like their ethics. Or the legal licenses or the terminology they use. Those social aspects that are non-technological are really important in hacking and partly bind people together as well.

Gislene: That's interesting. They choose to go to a hackerspace or create any other situation where they can gather and put forward some projects. So, that anonymity that sometimes might be related to hacking, maybe because one of the most famous hacking movements is 'Anonymous'[7], it's not a point for all possibilities of hacking.

Gabriella: Absolutely. And in fact, most hackers are not anonymous. Even though the kind of hacker hacktivist collective Anonymous is and was indeed anonymous. And historically, too, there were some hackers who were non-malicious 'Blackhat' hackers who broke into systems to learn about them and to protect themselves. Many of them were anonymous or pseudonymous. But the great majority of hackers are out in public. People know each other. And in some cases, identity and verification are really important. Certain hackerspaces are very open. Noisebridge, for example, had a very open-door policy, and it created some problems. So they had to put some limits on who could enter the spaces. People really get to know each other. In projects that are more virtual

[5] To go further, check the draft of Gabriella's book chapter on the definition of Hacker.

[6] To go further, consider Gabriella's text at The Atlantic: The Anthropology of Hackers - The Atlantic

[7] "Anonymous, part digital direct action, part human rights technology activism, and part performance spectacle, while quite organizationally flexible, is perhaps one of the most extensive movements to have arisen almost directly from certain quarters of the Internet". From *Coding Freedom* - Coleman (2013, p. 210)

projects, like free and open-source software projects, people work virtually, but they do get together face-to-face during conferences. In many of these projects, there are also procedures to verify your identity. For example, with Debian, which is one of the largest free software projects in the world, once you become an official member, you have to give your cryptographic keys to another member for them to verify and sign in person. It must be done in person. So yes, there are all these different elements of the hacker world that are face-to-face. But that's probably not something that most people think of when they think of hackers.

Gislene: Yeah, I think so. Because, well, you studied so much about Anonymous, but there is only one face that we generally see about it. We often see the only face of the movement available through television or social media. So, we don't really understand what is behind it. For most of the society, that's like: 'okay, they are doing some criminal things', because sometimes that's the way they are pictured. So, there are a lot of faces that we should shed some light on about hacking. And so, it's interesting what you're saying about how they have to show their identity; how they must prove who they are and what they do. And that's quite interesting and new, for people, I think.

Gabriella: Absolutely. And it's something that even as I think, more people understand that hacking isn't simply criminal. Nevertheless, that kind of stereotype of the loner hacker who, even if not malicious, is maybe a little bit, you know, crazy and not socially adjusted, is maladjusted. That's just so wrong, right? There are all sorts of people. And for sure, hacking is a great space for people with disabilities. For people who are not neurotypical, they're very safe spaces. But I would say that's the same for the Academy as well. The Academy and hackerspaces have a similar population. But the Academy is recognized and socially legitimated in a way that hacking is not.

Gislene: Could you explain some historical reasons why we don't socially recognize hackers? You do a lot of research in that sense. And recently, you and Mark Goertzen published a report about many aspects of hacking, including historical events. Can you share some of the ideas you discussed there?

Gabriella: I think one of the reasons why there are such strong misperceptions is the real lack of information and studies on the history of hacking. Apart from a handful of journalists who did some really interesting research and writing in the 70s and 80s, there's so little work done on hacking in the past or historically. The exceptions are Ron Rosenbaum, for Esquire magazine (Secrets of the Little Blue Box), or Steven Levy, who wrote a book on hackers (Hackers: Heroes of the Computer Revolution). However, that history is really interesting because it shows how social hackers were. For example, some of the first hacker communities were in universities like MIT[8] and Stanford and other European computer science departments. Hackers would get together in person and try to figure out ways to get more computing time because computers were not easily accessible. They had to use the labs at night to get access to computers. And the people that were really excited about computers, they were a small number, and they banded together and got to know each other pretty well. They became obsessed. Another important node of hacker history was the phone freaks. They were phone enthusiasts who learned how to make free phone calls. They were precursors to different types of hackers, and they would get together on party lines and conference calls. Again, it is a history we know very little about. It was only recently that a major book on phone freaks called 'Exploding the phone' (Phil Lapsley) was published. And then finally, another kind of important group that has also been very understudied was the small secret associations of hackers in the 1980s and 1990s. They banded together into small groups, and many of them broke into systems, largely because it was exciting. You could learn a lot about computers and security, and you couldn't learn this stuff at the university. So many of these hackers, and this is what I wrote about in this report with Matt Goerzen, many of these hackers eventually left the shadows and started to contribute to the security industry. But that pre-history, whether it's in the university, the phone freaks or the small kind of associations, there was very little work done on them at the time when they existed and even today. That kind of lack of knowledge about them is one reason why you have such persistent misrepresentations and stereotypes today.

Gislene: Yeah, this misperception is not out of the blue, but something that unfortunately, they have been on undeveloped...

Gabriella: exactly for a very, very long time.

Gislene: And about the report, the title is 'Wearing many hats', and earlier you talked about 'black hats'. I must admit, this is new vocabulary for me. What are these hats and why those colours? We can have an idea but if you can explain.

[8] Click here to read about the OWEE Expedition in MIT and Harvard University conducted by RGCS members. The expedition focused on understanding "how can elite institutions and an elite territory originate key collaborative practices and ideology such as hacking, open knowledge and open innovation?"

Gabriella: In the security world, hackers will often use the terminology of black hat, grey hat, and white hat. Nowadays, black hats usually mean sort of malicious hackers, while white hats are those that often work on behalf of security companies to fight the black hats. And then the grey hats. They are not morally ambiguous or dubious, but they historically or currently are willing to, perhaps, use methods like breaking into systems to understand security and improve security. Nevertheless, the terms also have a history, right? So, today they're used in a very straightforward way. But the terms themselves only came into being in the 1990s and really solidified in the 2000s. It was actually these non-malicious black hats, people who broke into systems, often for learning, pedagogy, and to connect with others. These non-malicious black hats were like: 'we have something to offer society and the security industry because we have the skills and the knowledge to actually stop malicious hackers'. But they faced a problem: they were breaking the law, at least some of them. They hadn't been legitimated by institutions. They didn't have credentials, like degrees or certificates. And certain individuals, we're saying 'don't trust these individuals, because they're like... if you hire them, it's like hiring an arsonist to put out a fire'. So, these hackers were like: 'no, we actually were breaking into systems, not to destroy them, but to learn about them. We're credible. We trustworthy'. And they had to spend a lot of time convincing the public, journalists, and other security professionals that they were to be trusted. And some of these hackers came up with the term grey hat to designate that they came from hacking subcultures. And they were still wanting to have a strong connection to those subcultures but also denote they were not black hats. They had the knowledge of black hats that could be put to good use. So, grey hat was a term that was invented to mediate that transition from the amateur, illegal scene into the kind of professionalized security world. And precisely, this history is interesting because, again, the terminology black, white, and grey is very common today. It has been used in a straightforward way. But on unearth that history? It took an enormous amount of work. And it was such an interesting history! It was such a perfect time to do that work because a lot of the hackers who had illegally broken into systems were willing to talk today because the statute of limitations had run out, so they couldn't get in trouble. And so they're willing to be public about their past in a way that 15 years ago, I don't think they would be willing to talk about it. It's also perfect because you could talk to individuals who were still very much alive. And then corroborate with archives as well. So it's, it's partially talking to people. And then it's digging into a lot of the material online as well, to unearth that history around the black, grey, and white hats.

Gislene: At the time, they weren't willing to talk about this because they could be persecuted. Were there some situations they went through? Was there a regulation that has changed that since then? Or now they feel secure just because a long time has passed?

Gabriella: Mostly because the time has passed. I mean, it is the case that, I think, this is quite recent. Even back in the 2000s and forward, when a lot of these former, again, non-malicious black hats were like: 'Hey, we have these skills. Let us advise you on security'. One thing they're doing is finding vulnerabilities and publishing details around them. And this was part of the full disclosure movement: 'let's disclose fully what the problems are'. Back then, and even today, you know, people can get into some trouble doing that. Even when it's done in the public interest. Over the years, certainly, norms have solidified that it has become accepted, as long as you're trying to fix problems in good faith. It's far more acceptable to release this stuff publicly. Although today, companies prefer what's called 'coordinated disclosure'. In this case, before releasing the vulnerability publicly, you'll go to the company and say: 'Hey, here's this problem, will you fix it?' And now companies will. Back in the late 90s and early 2000s, many wouldn't. They'd say: 'No, there's only a problem because you hacked it'. And the hackers would say: 'no, no, we were able to hack it because your security is bad'. So back then, it was quite risky. I think it continues to be risky, but nothing like it was in the past.

Gislene: What would be the highlights that you discuss in the report "Wearing Many Hats: The Rise of the Professional Security Hacker"?

Gabriella: The highlights. I think that the big one is there's a group of people today who are part of the security industry who are esteemed figures. And many of them are former black hats. The report details the cultural and ethical work they had to do to be seen as credible experts, given that they weren't credentialed and were breaking the law. We look very closely at that sort of labour that was necessary, so they'd be treated as credible experts. Another element has to do with the types of problems they focused on, which tended to be very narrow, technical problems. Today, with social media, you have problems which are not simply technical but are socio-technical, like harassment online. And it was one of the things we wanted to highlight: how, perhaps, the lack of diversity in the hacker world partly explains their technical, highly technical focus. Of course, that was what they were good at, and it's very valuable. Nevertheless, they tended not to be the figures who were being harassed or pushed offline, which was happening. And being aware of those issues and trying to mitigate those social vulnerabilities only came much later. In another point of the report, we wanted to highlight how the early origins of this community and their makeup also put them on a very technical path, something that led them to overlook socio-technical vulnerabilities that were always around but really came into full force with the rise of social media as well.

Gislene: Are there groups focusing on understanding these bubbles we have on social media and how this is making things more complicated than they already were? Or which kind of focus do they have?

Gabriella: Yeah, I mean, the hacker community still tends to focus on the technical side of things. However, the rise of misinformation and disinformation has spurred segments of the hacker community to think especially beyond the merely technical. Some solutions can be technical, but many solutions are about policy, law, and regulation. And there are lots of debates around what is an appropriate way forward. Given that, often, when you're dealing with things like disinformation or misinformation, you have to block information and block people. And it's something that, I think, again, the hacker community doesn't have some universal commitment to anything. But they do care about things like access and freedom of speech. And so many think very carefully about how to deal with these problems in a way that then doesn't introduce massive censorship, right? And there are no easy solutions often. But these are the sorts of issues and questions that many hackers that are a part of the security community do talk about and think about today in a way that they didn't do so much historically.

Gislene: Yeah, because nowadays, the problem is visible. We cannot deny it anymore.

Gabriella: You cannot ignore it. Again, always there to some degree, but it really just there was a tipping point, right? In the last five, seven years around this?

Gislene: Earlier, you talked about how good faith mobilises their action. Is this related to their ethics or not? What is the ethics of the hackers? I find it very fascinating, and I think we can learn a lot from them, in that sense, as a society.

Gabriella: I completely agree. Often, when people think of hackers, they think: 'Oh, they have no ethics'. And it's the opposite. Of course, there are some criminal hackers who are stealing things. And it's a very complicated domain. I mean, I'll never forget this one conference I went to with professional security researchers. And there was one person who talked about criminal hacking as like wealth redistribution because many of the criminal hackers came from, you know, places that yet don't have strong economies. So I was like: 'oh, that's definitely a way of looking at that'. But yeah, whether it's free software security, hacktivists, cryptographers, there's no universal ethic. Though, there are these tendencies to care about things like privacy, to care about free speech, to care about access. And what's remarkable is how ethnically dense the hacker world is. People will be writing manifestos or legal guidelines that instantiate ethical norms. There'll be big debates around these ethical questions. And to me, that's the most important part, not that there is some singular hacker ethic, although sometimes you'll hear that: 'oh, there's this hacker ethic'. And in part, that stems from this book by Steven Levy. It's a wonderful book. And he worked with these university hackers in places like MIT, and he saw that they were committed to access and computing. And they believed in meritocracy. And so he went and laid out the hacker ethic. And it's an interesting set of precepts that, again, a lot, but not all hackers adhere to. It's a general framework. But I think the more important point is that hackers care about ethics, that they're instantiating it, they're living it through their projects. It pertains to different things depending on the community. So the community that is building privacy tools, such as the hackers that are part of the Tor Project. They're devoted to creating systems where you can be anonymous and move through the internet privately. Other communities are about releasing source code and underlying directions of software. Other communities are about creating secure systems that help consumers. But again, the point about ethics is that they're talking about it, they care about it, and they instantiate it in their practices and their documents. And that's kind of what makes, I think, the hacker community a bit different from, let's just say, academic computer scientists. Some of them obviously do care about ethics and follow ethical guidelines. But as a community, they're not united by this sensibility, where the ethics of things like security, privacy, freedom and access to our front and centre.

Gislene: One reason I think we should and can learn a lot from them is that they know how to identify things. And we as a society, as regular people, often don't know how to do that. So, it's the knowledge that's quite precious. And that would be great to have access to and learn from it.

Gabriella: That's a great point. I mean, they're specialists, they're experts. And not all of us can become experts in different domains. And for sure, I think people can understand the general contours of the debates. Still, precisely, these hackers live and breathe the technology and the ethical questions. And in some ways, it is very interesting and important to turn to them for guidance around these issues. But again, there's a very technical component to them. And it's not something that every person can just fully understand off the bat.

Gislene: Yes, that's for sure. There are a lot of complicated terms, notions, and math behind it. But understanding them and their mindset, the way to question things; I think that's quite interesting and very inspiring. In that sense, I must ask you about Anonymous[9]. I've read your book, and it's fascinating. How was interacting with the group? What can you tell us about this experience?

Gabriella: So, Anonymous is a collective that, by 2010/11, became increasingly focused on protests and political activity. It was a kind of movement that I studied pretty intensely between 2011 and 2014. It started in 2008, but the height of their activities and popularity increased in 2011, 2012. They were highly anonymous. A lot of individuals, not all, but a small and very prolific group was breaking the law. They were hacking into systems or engaging in distributed denial of service attacks, which are also illegal. It was truly exciting but also a challenge to study them. I mean, they were open to me. I could be present in the chat rooms where many members were located and congregating to organize themselves. And so they enjoyed having a spotlight on them. I helped to facilitate relationships with journalists. I think they found me 'handy' to have around. In that sense, it wasn't too hard to, at least, get minimum access. But it definitely took time to gain the trust of individuals. I was never sure of what was true and what wasn't. I was very concerned about being included in illegal activity before it happened. I never wanted to know about things before they happened, and often, I had to remind people: "don't come to me with your hacking plans". I knew there was probably law enforcement, as well, on the channels or informants. It was a very challenging space. However, with time, I got to meet people, and those people could be forthcoming. So over time, in some ways, it got easier. But it really required a lot of time and presence to understand what was going on; to feel that some people gave me their trust. It is something that I don't think I could have cracked that sort of social puzzle without constant co-presence for many years.

Gislene: In that sense, considering this required virtual presence for you to get through this puzzle, you were also building methodological approaches to anthropological research. Can you tell us a bit about this process of creating methodological strategies to go through online data?

Gabriella: Yes, certainly. Unlike some of my other projects on hackers, this project was very virtual. There are different methodological aspects of doing research with hackers who are mostly online. One of the challenging aspects is the sheer quantity of information. For instance, there were multiple chat rooms and people chatting for hours, so it got very overwhelming. They were also doing many activities and were regularly in the news. One strategy I developed was writing a sort of 'daily log', something like a 'Captain's log', where you highlight the most important parts. I would also take a lot of the data and tag them to find them later in relation to the blog. But I only started to do that within a couple of months into the research, when it became clear that just writing my field notes every couple of days was not enough. That was just one aspect of the sheer abundance of information. I think that online ethnographers really confront that. There's just so much information, so much data. Of course, there are certain tools that can help you on managing it. However, sometimes, one of the best things you can do is have a team of people working on an area. For example, the Data and Society, which is a research institute in New York City. When they were researching the far right online, they had big teams working on it. It was ethnographic and anthropological, but they had teams. So, that's one aspect, which, again, is just the sheer gluts of information you encounter when you work online. And that certainly was one of the biggest challenges for me while I was doing my research on Anonymous.

Gislene: I can imagine because it's about dealing with the amount of data and with all the constraints around the situation. It's a lot of things to manage and to deal with. So, Gabriella, we're heading towards the end of our interview, and I must ask: what have you been working on and what are your plans?

Gabriella: So, the report you mentioned. It will probably be the basis for a book. It was a long report with 50,000 words. And we could have written more, but we were forced to cut it off. So we'll probably write the book. My co-author, Matt Goerzen, and I want to do a bit more research on European hackers. Even though we did interview quite a few European hackers, the story we told focused on a couple of big American groups. However, some of the most important hacker groups from whose members became key security professionals were in Europe. We interviewed some of them, but we want to tell that part of the story and centralise it. That's research that we still have to do. I'm also writing a book of essays that draws from former and new research. It's hard to describe the book in a sentence or two, although hopefully, I'll be able to, eventually. Briefly, the book juxtaposes different types of hackers, from those working

[9] You might also want to look at Gabriella's book based on this research on Anonymous. Click here to learn more.

for the State to those that fight the State. I also include hackers in different time periods and parts of the world. I'll gather the essays in one collection to remind people that hackers don't have one and only profile. We have hackers who are extremely antagonistic to the State, like Anonymous and other hackers who were part of this underground tradition and then became part of the security industry, whose work in part helps to fortify the State. The essays are story-driven, and the book is a collection of hacking takes on many different formats, depending on type, place, and group. The essays will show this diversity because they'll feature very different histories and projects in one collection.

Gislene: Oh, that's great! I'm already curious and willing to read it! Our final question is: for those researchers or these people who want to become an anthropologist and study Hacking, what are your recommendations?

Gabriella: Wow! There's so much to share! First, I hope people do it. The field has proliferated quite a bit. Nevertheless, especially ethnographically, there's very little research, and there's room for so much more. If you are interested and don't know too much about the world, you want to start by seeing what's out there. There is a website that a few other people and I created and currently curate. It's called 'Hack curio' and is a video museum of the cultures and politics of hacking. It gives a good picture of the different practices around hacking. Also, it spans blockchain to hacktivism to free and open-source software. I think it gives you a really good idea of what's out there. It gives you a good idea of what some of the work that people have done as well. But there's just so, so, so much to do, whether it's following really exciting projects in the world of blockchain or doing historical work. Also, the more work that can be done in the non-English speaking world, the better. There are really rich histories in places like Germany or, for example, Argentina, which has one of the biggest scenes for security and hacking. I don't think anyone has done anything about that. So, there are just these vast areas that are still untapped for research. It's a very exciting domain to enter if you're interested in technology and ethics. Also, if you want to enter in an area that has been understudied hacking is perfect.

Gislene: Very inspiring. I'm sure that people will come because the field is fascinating. The website is quite nice. I've been there and would really recommend to everyone to visit it! Gabriella, thank you very much. I learned a lot. It was great. Thank you for your time and for being so nice.

Gabriella: Thank you! And thanks for doing this as well and asking me to participate.