LeeCTA Done

Fri, Feb 10, 2023 7:20AM • 39:24

SUMMARY KEYWORDS
cybercrime, zoom, bombing, people, crime, cyberspace, cyber, cyber crime, online, cases, spaces, cybersecurity, terms, targeted, computer, early, called, reported, internet, victimization

SPEAKERS
Claire Lee, Jenn Tostlebe, Jose Sanchez

Jenn Tostlebe 00:14
Hi everyone. Welcome to The Criminology Academy podcast where we are criminally academic. My name is Jenn Tostlebe

Jose Sanchez 00:22
And my name is Jose Sanchez.

Jenn Tostlebe 00:24
And today on the podcast we have Professor Claire S. Lee, who is speaking with us about cybercrime and cybersecurity with a more focused attention specifically towards cyber hate and zoom bombing.

Jose Sanchez 00:36
Claire Lee's an Assistant Professor at the School of Criminology and Justice Studies at the University of Massachusetts Lowell, where she is a member of the Center for Internet Security and Forensics education and research. She's also the UMass Lowell Donahue Humanities Ethics Fellow for 2021 through 2023. Dr. Lee's research interests include cybercrime, cyber security, and cyber terrorism issues. She has considerable experience in social big data and online data collection, big data analytics and database creation. She has worked in the educational media and legal sectors in Hong Kong, Shanghai, Taipei and Seoul. She currently serves as an editor of the International Journal of cybersecurity intelligence and cybercrime, and academic editor of PLOS ONE, and she is an editorial board member of the Sociological Review. It's great to have you on the podcast. Claire, thank you so much for joining us today.

Claire Lee 01:32
Thank you for having me.

Jenn Tostlebe 01:34
All right. So in today's episode, we're going to start off by talking, having kind of a general conversation about what is cybercrime and what is cyber security? Then we'll move into one of Claire's papers on

Zoom bombing, and then we'll wrap up by asking clear about some of her more recent projects on cybercrime. So Jose, why don't you get us started?

Jose Sanchez 01:58
So, in true Criminology Academy fashion, we're going to start with a broad question. So with the exception of a small section devoted to the internet in one of our episodes with Joan Reid, you really are our first guest that is going to talk to us about cybercrime and cybersecurity. And so we want to set the stage for this discussion with so asking you can if you can provide us with a definition as to what is cybercrime and what is cybersecurity? Because when I hear cybersecurity, I just think of like my anti-virus that I buy from Amazon every year, but I'm guessing it goes a little beyond that.

Claire Lee 02:40
Yeah, the anti virus software is a big thing. And it's a very important one. So you have a point there. So thank you, and I'm very honored to be one of the first callers who does cyber crime research to be on this podcast. So yeah, like some other types of crime, cyber Crime has many definition, [inaudible] define cybercrime as any type of crime that involves computers, networks, including crime's that do not really rely on computers. But I'm going to introduce my favorite definition and types of cybercrime, which are computer assisted cyber crime, computer facilitated crime, or computer focused crime. So the first one the person category I just mentioned is computer assisted crimes or computer facilitated crimes. This refers to crime that occurred offline, but computers internet technology facilitate certain types of crime. Like identity fraud, identity theft can be happening our layer live as an offline, but it also can be transformed into online setting. The so called online identity fraud can be existent due to computers and the Internet. In addition, examples of computer assisted crimes include but are not limited to digital piracy, online internet, online interests or property, online identity fraud, cyber bullying, and cyber stalking and so on and so forth. Another type that I'd like to highlight here is computer focused crimes. This type of crime is perhaps more straightforward than the previous one. And when people think about cyber crimes, people usually think about computer codes on hackers computer screens like in a movie like in a TV series and all that. So hacking and computer viruses worms are exam first off computer focused crimes. These types of crime occurs because the computer the internet and technology, in other words, it is about crime that occurred due to the existence or presence of computer in on adding technology, which are very much important to our society.

Jenn Tostlebe 05:05
So know, kind of putting this into perspective. You know, clearly, technology has expanded and changed a lot over the last few decades, which in turn, I imagine has had some pretty major impacts on how we think about crime and the environment where crime takes place. So, really, we're interested in when did cyber crimes start becoming something that has been in discussion and kind of given attention? And how as crime and online spaces changed over time?

Claire Lee 05:39
Yeah, this is a very good question and big question. I'm gonna probably answer some parts of the question on the on the to the time constraint. So as early as the late 1990s, some people started to discuss sort of cybercrime in the literature, especially from the UK, and Australia and moving towards the United States, later on. We're talking about cybercrime adding more digital crime, or online crime or

virtual crime. So the time has been changing. Around that time, they were mostly focusing on hacking computer crime, and also like digital piracy, on intellectual property, friends, and all that one very important research conducted into Sutherland was by an Australian professor, Peter Grabowski. He published a lot on cybercrime later on, but this article into sSutherland entitled virtual criminality, old wine in new virus, so he discussed in his paper virtual crimes in he was arguing that like cybercrime, or virtual crime, were not new at that time, but the element of nobility comes in the great capacity, great capability of technology to facilitate acting on these motivations. So that was one of the early on important paper that published around the concept of cybercrime. As I briefly mentioned, the area of cybercrime has been growing so much, not adding types, not only adding types, but also adding capacity of the crime can do, one can do that. And also like, amount of victimization, that victimized money and all that. So it's been a slightly like, it's going to be a goldmine for some scholars, that has to be somehow [inaudible] and about it. Yeah, absolutely.

Jenn Tostlebe 07:47
You started to kind of mentioned this how like the number of cybercrime has been growing over time. But I imagine this is something that's difficult to estimate. But are there any estimates for how many cyber crimes occur each year? Whether that's like, how many crimes are actually caught? Reported by victims or some other kind of measure?

Claire Lee 08:09
Yeah, that's another very good question. But it's very hard to answer. Okay. Especially in the world of cybercrime. We don't know how many victimization or incidents cases are actually happen, or that like, for instance, if I got hacked, like my social media account got hacked, I don't necessarily want to, or think about report this case to police, the police department, even if I did, police department might not take it very seriously, because there are other like crimes like gang related stuff, or homicide and all that. So people kind of discouraged to report a crime. Therefore, it is one of the underreported crimes as rare, arguably, right. But in the US the app for Internet Crime Complaint Center, which we call the IC3 publishes reports annually on internet crime complaints. So we only know about complaints like those who were reporting to FBI, but it's kind of a good sense for us to know how the size and amount of the victimization and victimization, victimized money could look like. So over the last five years, like sudden 17 221, the IC3 had received at least an average of 552,000 complaints per year. So these complaints address a wide range of internet scams affecting victims across the globe. So IC3 reports category of internet or cybercrime have changed quite a lot over the past 20 years because it was started in May 2000. I think I remember. So earlier on some of the types of Internet Crime Complaint they got earlier on my inadequacies right now, like ransomware. With the currency, those that are quite new, they appeared recently as part of their complaint.

Jenn Tostlebe 10:25
Yeah, I imagine that number, just in the abstract seems kind of small. So I can see what you mean that it's likely a very underreported, not to mention all the people that maybe don't even know that they were a victim of cyber crime. So, yeah, but it's good to at least put some kind of number to this and know what we're talking about.

Jose Sanchez 10:49

So just how difficult is it to police cyberspace for crime that's occurring on the internet or have occurred?

Claire Lee 10:57
Yeah, I would like to paint a rosy picture to say that policing cyberspace is already implemented, we don't have to worry about it and all that. But as you might guess, in reality, that's the case. So as early as 2004 argue that policing cyberspace space is a very scarce because the sophistication and computer and cyber criminals were rapidly increasing. And it becomes a real threat to our lives and all that, even almost after 20 years. Holistic cyberspace is inherently the precursor, and inherently complex due to the nature of cyber spaces. You know, cyber spaces are, tend to be like free, often not geographically bounded, and also highly unorganized. So we could see a lot of example, like online hate speech, or some other cyber crime that happens due to the anomie. And also, in terms of investigating cybercrime, in this like cooperation from one agency to another agency, or one country to another country, but these kinds of interagency international cooperation are highly challenging, especially we don't have a jurisdiction over some other country or VPN, or IP addresses and all that. So that comes with some costs. At the same time, cyber criminals are smart enough, intelligent, then more intelligent than us to try to maneuver how can they not caught by any law enforcement agency and all that so they could hide their location very easily, hide their identity, or use other people's identity over their own identity and all that. So, insurance policing cyber space for cyber crimes are started to implement it later by later, but there is a long way to go. And it's always difficult for law enforcement agency, and other organization to keep up with the speed or the development of the technology and new types of cyber crimes and all that.

Jose Sanchez 13:30
Alright, so let's start to transition into the paper that we're gonna be discussing today. And so, earlier, we talked about some of the crimes that fall under the Cybercrime umbrella. But we want to focus more on a particular type of crime. That's this episode, which is a hate crime in the digital space. And so we know that a hate crime is motivated by bias against protected groups such as race, color, religion, national origin, sexual orientation, disabilities, but what does this actually look like in online spaces?

Claire Lee 14:07
Yeah, hate crime in online spaces are not much different from what you just mentioned, in terms of offline hate crime, but the space has been transported to cyberspace and online spaces. So we often call this as cyber hate, online hate, or online racism, cyber racism in some cases or online hate speech. So as you can see that certain kind of hatred towards particular group whether it was from race, gender, ethnicity, religion, or disability or some other kind of condition the person or the global people might have, they are experiencing those things online. So people would receive hate messages like via Twitter, or some people posts something online, which is not true to their own identity or all that or they would [inaudible] or nasty emails based on the other person's, I mean, the receivers gender, race, sex early and or other kinds of elements of their social demographic factors, they could be cases of online hate, and hate crime in cyberspace is.

Jenn Tostlebe 15:28

Perfect. So I think we're at a good place to start to transition into the paper we're talking about today. It was authored by our guest, Claire, and it's titled "Analyzing zoom bombing as a new communication tool of cyber hate in the COVID-19 era." It was published in Online Information Review in 2022. And so just to give a little introduction, borrowing some of your own words, Claire. In this article, you explore the rise of cyber hate crimes on the Zoom video conferencing platform at the outset of COVID-19 pandemic. More specifically, you examine victimization cases of zoom bombing, where Zoom is used as a cyber hate tool. To do so you conducted a news media content analysis of 449 Google News articles and 79 tweets. And overall, the aims of the study were really twofold. First off to assess the current state and prevalence of zoom bombing victimization in relation to cyber hate in the midst of the COVID 19 pandemic. And two to examine the role of cyberspace as an effective atmosphere and zoom bombing as a tool for performing cyber hate. So our first question for you regarding the article then, is just can you tell us what the motivation was for writing the paper? Or what the gap in the literature was that you were filling?

Claire Lee 16:52
Yeah, I'd like to answer for the motivation first. So I started hear news about bombing when we had to stay at home, do you remember that time and the did not know about COVID-19 in terms of how it could spread out and whether we can be going out and all that, right? So around the time, we used zoom for pretty much for almost everything, from our social life to work and all that. So at the beginning of the COVID-19 pandemic, around March 2020, I read upon a couple of newspaper articles on Zoom bombing cases, especially one of the University in New York, which is a Jewish space university, and they had some kind of events, and some person who wasn't invited for the event, appeared and made a very nasty comments about the people who were participating in the event. And then later on, I also followed a few different cases, it seems such cases of Zoom bombing, were targeted at a particular group of people, not just like, randomly happened, and these to me are around the time that I was trying to get into this space. So I felt the urgency and responsibility to research this topic as a cybercrime cybersecurity researcher. And then I'm kind of going to the second question that you mentioned in terms of gap in the literature. What I found, I started for some information, some more information about what zoom bombing is, Am I overreacting into this situation? Because I'm, like, more empathetic to some group of people or not. Or I was trying to understand what's the sense of the situation. And then I could only found a couple of articles that was from purely computer science engineering, cybersecurity papers on Zoom bombing, about security breach and some other problems that the software might have had. As a social scientist, I've heard that, yeah, security breach or kind of thing might be there. But I felt that's more than that. So I tried to look out for more information and how should I want to engage with this topic? And there was almost no article in terms of social science and humanities literature talking about this. Of course, it was very new. In terms of the phenomena. It was very new. Given that the infancy of the topic, the gap in the literature was understandable. And what was really more outstanding to me was that like even before we are using Zoom, we also use sort of similar kinds of telecommunication to like Skype, or some other things, right. But there were not many papers on those telecommunication tourists and this kind of thing happened. So it was quite a wake up call for me to figure out, what is this, and it's continue. And if we are going to use Zoom for more than a year, more than two years, whatever, then what we need to do, and as a researcher, how can I try to educate other people or try to understand the situation better even for myself?

Jose Sanchez 20:46
So I think people can have, started to kind of get an idea of what we're talking about when we say like, Zoom bombing, and I think people, like professors, students, or professionals may have some probably know what zoom bombing is. But for those of those that don't know exactly what zoom bombing is, can you give us like a definition of what exactly we're talking about?

21:08
Yeah, sure. Zoom bombing has two words, Zoom, and bombing. Probably never the aggressive term that was targeted use in the community. I'm gonna go into that a little bit later. But turn bombing is the practice of disrupting virtual meetings with graphic explicit, threatening messages or emails and that opening called hate speech and online hate speech. Right. So the first zoom bombing recorded zoom bombing incident was reported in mid March 2020. And then the same month, the Federal Bureau of Investigation FBI, announced that there is an emerging video teleconferencing hijacking scheme, called Zoom bombing happens in the US probably later on in the world. So and I find it quite interesting that FBI was concerned and they were they putting out the information about Zoom bombing very early on, they were trying to engage what this would entail and all that. So yep, that's a quick answer to your question.

Jose Sanchez 22:18
Right. And so the focus of this paper specifically wasn't necessarily on, like the security or underpinnings of zoom, exactly. But do you have any idea of how exactly people were being able to do zoom bombings, how they were kind of taking over zoom meetings?

Claire Lee 22:37
Yeah. So it happened in a couple of different ways. Like from cybersecurity perspective, it happens if there was a glitch in the system, some people might go in. But what I found an issue by researching my cases, it wasn't like that it was more like intended or accidents kinds of stuff like, so people who wanted to go to different zoom meetings. But those people were not invited to go there. So called Zoom bombers, they searched public events that didn't need any reservation, or when registration or restriction to get a zoom link. So they intended to go there. And they start for a certain information, either meeting link, or meeting ID where passwords sometimes people were posted, like online, or site, or Twitter and Facebook and Instagram. So they went there to get those information. So as you can see, from these examples, it wasn't very highly technical, but it was more like the information was out there. So therefore, I can get it to school and get it. So earlier on, people were not realize anyone can do so called bad stuff. And you can go to anyone who would be interested in going to other people's meetings, but in reality some people have their agenda and their motivation, to particular, where will people end when they're to go to zoom cases? And I also found some cases like some people, especially like teenager, they don't have a lot of sense of so called awareness or cybersecurity and all that. So they just pass it around, like, you know, I'm very bored in this class, do you want to come over like, do you want to just show up? They found this other fun. But, you know, as the other side, if you are teaching to the, you know, if you to teach some classes, and some people just show up and then say something unnecessary than it's very shamed and disruptive to not only the latter also to the entire audience of the zoom classes. So yeah, that's how you've happened mostly.

Jenn Tostlebe 25:03
Yeah, I feel like I remember early on in the pandemic, like on Twitter, it was like everyone was posting the zoom links with the passwords, or no passwords. And now, for those meetings that are posted or discussed on Twitter, you know, they're like, please don't like, we're not sharing the password, you need to email so and so or just like this is happening. So I think people have noticed that and adjusted kind of how they post these more public events to try and prevent things like this from happening. So when I was reading your paper, I was like, Oh, this kind of ties into what I've been seeing that it's not super technical, they're not hacking into these, they're just kind of finding the information and going into the call. So I thought that was really interesting, that kind of what I've been seeing, you know, in my own personal experiences are matching what you were finding in the research.

Claire Lee 25:58
Yeah, that's great. Thanks for sharing. And we often try to do like cybersecurity awareness campaign or live training. I'm sure your university does that my university does for new employees and students, were some of the training that are implemented do not necessarily work very well. But this time, somehow people got to know about the risks and potential implication. And they started to do this kind of so called good baby behavior by themselves. So it's, uh, you know, the, that's zoom bombing started to happen, there wasn't happy. But in the end, there is a nice, people get out of it, peptide, I'm happy about it.

Jose Sanchez 26:42
So in your paper, you use this term cyber racism, which was surprisingly, actually coined back in 2002. I know for a lot of our students now that may seem like forever ago, and they might even wonder if the internet existed in 2002, but we promise you it very much did. And so building off someone else's work, you state that scholars have, quote, criticize the way the digital realm has empowered expression of racism. So can you tell us a little bit more about cyber racism and sort of how online spaces have worked to empower expressions of racism?

Claire Lee 27:19
Yeah, that ties into the way the cybercrime is structured, perhaps, because it is, ultimately a free and anonymized pace, to some extent compared to our offline life. What I mean by that is, in order to create my Twitter account, I can use any twitter handle that I would like to use unless it wasn't taken by other people, right. Or if I want to use my, if I want to create a Instagram account, or add in like hacker 123, then people would think that I'm hackers, or something like that. So that kind of practice opens up avenue for some people with quite a bad intention and some motive to harm people to do whatever they want to do. And one thing that I'd like to note is that in the US, because the First Amendment and free speech is current, very different from other countries. So people who often have more freedom feel like they have more freedom to speak about what they want to do, especially in online lives, they are not surveyed, or they are not governed by any authorities or any companies and all that. So that kind of practice opened up a lot of spaces for people who have either have a motivation for racism and some other things, or this used [inaudible] the internet to be an idea what they could do and what they couldn't do online.

Jenn Tostlebe 29:01

Okay. So you use content analysis to analyze your data. And if you want to speak a little bit about that, please do but we want to start to move into your results. And so based off of the content analysis that you did, how many incidents of zoom bombing were you able to identify between March 10, 2020 and April 10, 2020.

Claire Lee 29:26
Yeah, I used that timeframe because there was almost the forest to embalming is then there was reported, like in newspaper articles and all that. So I wanted to follow up the forest change of the zoom bombing instances. So around the first month, or the one the single month that I studied, I found 469 newspaper articles cases. One thing that I have to note here is that we don't actually know how many cases are happening. You know, like I mentioned, cybercrime is one of the most underreported crimes expecially online hate speech and all that you don't necessarily look for these kinds of cases to other people and agencies. So with that, it likely happened more than 469 cases. But at least that's what I saw in terms of my data.

Jenn Tostlebe 30:20
Seems like a lot for even a one month time span, let alone if you say it's underreported likely.

Claire Lee 30:26
Yeah.

Jose Sanchez 30:28
Yeah. Okay, so you split the remainder of your results into three sub sections. And so we'll talk about the first one, which was identity at the core of cyber hate, racial, religious and sexual minorities, indicating that certain identities were more at risk for zoom bombing. Can you tell us more about this finding?

Claire Lee 30:50
Yeah, I found a few different types of zoom bombing, as you mentioned. So one of the most significant cases that I could see from my data and analysis from my data was an anti-semitic, zoom bombing towards either Jewish descendants or religiously Jewish people. So and in March and April, there is and this one too, is holidays, Passover. So some zoom bmbardings were targeted at particular events like that. And also like funeral what's happened, dinner was happen before June because the older restriction that we control, so which is very secure, private, sacred place to mourn the people who passed away to give some empathy towards the family about the zoom bombers didn't really take, you know, take that perspective towards that. So that's one of the cases that I was in. And then yeah, that was about like, more than 70% of the cases that in my data, in some other data that I had, in terms of finding was education or settings, like, adds dimensions, some classes might experience some of the zoom bombing cases, that in my data, I found applications in California, unfortunately. So the zoom information was posted freely on the internet and the highs occur or two bomber try to get into that setting to do something for other people, too. So that's what the other cases happen, both at higher education and also K-12 education level. And I got also zoom bombing cases towards minorities, either sexual minority or ethnic and racial minorities. So they were targeted because of their minority status.

So they were doing bombers were saying some nasty stuff towards them on the Zoom events that were public enough. So these are some of the cases that I been analyzing my data.

Jose Sanchez 33:10
So one of your subsections ant the one that Jenn is probably most familiar with is like the hijacking or Zoom bombing of educational environments. Can you tell us more about how common it was for classrooms to be zoom bombed?

Claire Lee 33:24
Yeah, at least in my data, that was probably the second most, that, you know, if I remember correctly, I have to check. So runs the time that I studied zoom bombing we use or I also taught classes over zoom, so many of us were kind of locked into them every single day, you know, so, and some attackers might come in to the classroom to save them to better but the teacher, director, and professor and or that were, they appeared with a strange costume with their camera on and saying something, and went away and all that. So those things were happen. And in some cases, inappropriate photos from text messages, or chat messages were thrown out during the classes. I'm just imagining if those classes and what happened in my classes and would be quite awkward. So yeah, I feel very bad for you know, those who have actually experienced this during that time.

Jenn Tostlebe 34:35
Yeah, I know, I saw people posting things on Twitter, and I was like, I can't even imagine that happening in my classroom. So I feel ya. Alright, so the final section, then that we want to talk about was regarding anti-semitic zoom bombing. And so how many cases of zoom bombing were anti semitic in nature, and were they targeted in any way?

Claire Lee 35:00
But I think I kind of answered that earlier. Should I do it again? Or do you want me to answer a little more detailed?

Jenn Tostlebe 35:08
Yeah, maybe just a little bit more detail. Okay. Just so kind of, yeah, break it down.

Claire Lee 35:13
Right. So like more than 70% of the reported Zoom bombing cases were understand it. So the Zoom bombers were either infamous extremists or unknown perpetrator. So in terms of the impairments extremely, like, there was quite something to the research community around that time that like we can outdoor be targeted, you win on cyberspace like this in better public spaces. So it also zoom bombings happens on that was Jewish holidays, or the Friday sabbath events very regularly happening on every Friday to Saturday. So the perpetrator actually knew the content of the particular event, but they are going into, and they actually had an agenda to go there to do something. So there were probably arguably far lights people who have an intention to psychologically or culturally harm the targets.

Jenn Tostlebe 36:19

Okay, so then our final question for you about your paper is, given these findings, what are some of the implications that we can take away for this study for research as well as policy and practice?

Claire Lee 36:34
Yeah, first of all, I think it's important for us to note that cyber security awareness is very important, like we already talked about how important putting, not putting your own information on not put your zoom information public, and all that right, it is better to be more vigilant and aware of what you want to do. And what you want don't want to do in terms of sharing your class information, sharing your events' information on the public can not always be a good thing. So through this study that I conducted, I could see some implication towards how we can better govern and regulate digital platforms and cyber spaces, protecting a particular group of people that have been as diverse as a common target of cyber hate, online hate speech. And we might want to provide certain kinds of resources and training towards those people. And we also want to educate our younger generation who have a slightly, probably slightly different idea of cyberspace and how their behavior would be. So we might want to try to engage with them to make safer internet space. Awesome. All right, whether it makes sense.

Jenn Tostlebe 38:00
Yeah, it does. Alright, so that is all that we have time for today. We just want to say thank you once more for taking the time to chat with us is our where can people find you if they want to reach out and ask you more questions, whether it's about zoom bombing or other issues related to cybercrime and cybersecurity.

Claire Lee 38:22
Yeah, you can find me via email claire_lee@uml.edu. Yeah. Are we happy to be connected with any of you and thank you very much.

Jenn Tostlebe 38:33
Awesome. Well, thank you once again, and we look forward to chatting with you in the future.

Jose Sanchez 38:38
Thank you. Thank you.

Jenn Tostlebe 38:40
Hey, thanks for listening.

Jose Sanchez 38:42
Don't forget to leave us a review on Apple podcasts or iTunes. Or let us know what you think of the episode by leaving us a comment on our website, thecriminologyacademy.com.

Jenn Tostlebe 38:51
You can also follow us on Twitter, Instagram and Facebook atthecrimacademy.

Jose Sanchez 38:58
Or email us at thecrimacademy@gmail.com See you next time.