[Intro music.]

Welcome to Off Mute, a podcast about women in cyber security.

We're Sophie, Isabella, and Sam, three Cyber Fast Streamers just beginning our careers in the government security profession.

Join us as we hear from women across government about their careers so far, the challenges they've faced, and the great achievements they've made.

[Intro music.]

Umaira: Hi, I'm Umaira, an exercise lead in the Government Security Red Team.

Isabella: Can you maybe start by telling us about your current role?

Umaira: Sure, so, I work in the Government Security Group Red Team, as an exercise lead on personnel security. We're based in Government Security Group in Cabinet Office in 70 Whitehall in London. There's a team of five of us, so we've got two people who lead on cyber, one, I lead on insider, and I have another colleague that leads on physical, and then we've got a head of the Red Team, so there's only five. Quite a small team. There's loads of different ways to explain what red teaming is, sometimes it's called wargaming, and we can probably spend like an hour talking about what red teaming is and what it means to different people. But what we do is security red teaming, which is basically where you step into the shoes of the adversaries and you role play as the bad guys and understand how they think and how they might approach a situation or an attack and try and learn from how they might try and do it and identify those vulnerabilities in government. And then learn from it and then help actually input, those remediations and mitigations of the vulnerabilities that we found. It's quite fun, I didn't think this is what I'd be doing when I joined government, but it's really, really interesting, and I really enjoy it.

Isabella: That's good to hear. I think in terms of context, we originally saw you at a government security conference. And when we first heard about red teaming, we were like, wow, what, what is this? It's not really a facet of security that I think people talk about as much. I mean, you said you're quite a small team as well.

Umaira: Yeah.

Isabella: Um, so maybe we'll start off by getting a bit of previous background experience and then how you found yourself getting into something that, you know, not everyone might know about.

Umaira: So this is actually my first role in government, um, straight after university. I had a few internships though that I think definitely helped me find my way

here. I don't know if people have heard of Spring Weeks, it's something that I've only found out about in like the second year of university, where people who work in banking or finance get an internship at banks, to learn about, I don't know, economics and finance.

And I obviously had no interest in finance, but it was a good thing to get experience in your CV, so I thought I'd apply. And I got a place at a bank in the IT security team. And I learned everything about hacking, and pen testing, and cloud-based systems, and all of these things I was, I didn't really know much about before, but found really interesting, especially the pen testing area. So I got to be involved in some of the pen testing and understand how that works, why we do it, and even though I came out of it really interested in that area, but knowing I didn't want to go down finance, it was still like a really valuable experience.

So when I saw the job advert online on Civil Service Jobs, for a red team advisor, I immediately knew I wanted to apply. And I actually had help, so during my masters at university we had a career panel, and someone that I knew from my masters alumni who worked in GSG, I reached out to them and asked them if they could be like a mentor. And they helped me understand the recruitment process, what behaviours to focus on. And we did mock interviews and she really helped me understand the Civil Service. Thankfully I got the job, and very happy and grateful for that help. And now I try and replicate that as much as I can and help other people from the inside to understand what it's like to actually apply for a job in the Civil Service.

Isabella: Yeah, what did you do your Masters in, if you don't mind me asking?

Umaira: It was Applied Security Strategy. And it was after a degree in history and politics, but I was always really interested in like international relations, diplomacy, conflict management, all that stuff. So it was like the perfect, degree for that sort of stuff.

So I started in this role in November 2020, so literally a couple months after I finished my Masters. So I've been here just under three years now, and so much has changed from the team itself to the fact that when I joined there wasn't even a cyber directorate, and I've definitely seen a bigger appreciation for red teaming and exercising as a whole in government. I think when I started, it was still a bit of a selling game to get departments onboarded. Maybe because, like, the team was quite new then, only a couple years old when I joined. And it can be quite daunting for departments to let a third party in and, you know, break all their stuff and tell them where they're going wrong. But we try and really hone in on that relationship of we're here to help. It's here to help you to help all of us. And I think that has really helped us maintain that relationship across government and that's built and built and built over time. And now it's not that much of a selling game I think. We get departments coming to us to say, Can we get tested? Can we get tested

again and again? Which is so nice to hear because we're such advocates of red teaming and exercising across government and it's nice to think that we don't have to push it so hard anymore. It's actually something that people are coming to us for.

Isabella: Yeah, I mean hopefully as well for listeners out there, maybe they can like get inspired by red teaming as well and either reach out to you or or partake in some of their own too.

Is there such a thing as a typical day in your role with red teaming? And if so, what does that look like?

Umaira: So it's gonna be one of those really annoying answers where I say it depends at what point in the year you drop in on us. But I would say if we're at one point in the year where we're not testing, we're getting ready or gearing up to be testing, it'll be a lot of conversations with. with the policy teams, with the assurance teams, the engagement teams, to be picking the right departments to be tested, um, and having those discussions with them and planning the scope. So it's a real, it's a really big conversation, with as many people as we can bring into a room to make sure that we're targeting the right departments and hitting the right points. When we do, when we're live testing, the day might be, having daily conversations with contractors, um, who are doing the operations. If a contractor..., found something particularly interesting, like passwords. Then the next day we went like, should we use those passwords and see where, where we could go from that? And having those daily calls to be like, how is this exercise going to pan out and make those go, no go calls? And also just generally making sure that the exercise is going okay and just those check-in calls.

And then after we've kind of finished the exercising month, you'd see a lot of debrief calls. So for the more technical teams to understand what happened, and then the senior teams to kind of get the key takeaways out of the findings. And then there's more ad hoc stuff. We get quite a few requests to do the weird and wonderful things, like tabletop exercises on anything that you can think of, as well as more corporate stuff, across Civil Service. So, like when we met at the panel, doing talks like that, um, because we've got such interesting exercises and case studies, people really like to hear what we do. So we attend all these conferences. We have this Let's Attack workshop where we actually get people to..., be honorary members of the red team for an hour and a half and they actually get to, do some red teaming and get into the shoes of our adversaries and we give them a target to attack and it's, it's really fun. So hosting those sort of, workshops as well. So it can be quite busy throughout the year.

Isabella: It's good to be kept on your toes, I guess. So moving into the sort of meaty part of red teaming, how does red teaming in cyber security specifically fit into the wider government security profession?

Umaira: I think that's such an important question. And of course our team sits in the cyber directorate and a lot of our work, and the oldest kind of area of our work is It's the cyber, testing. It's the first thing that we did. We're all advocates for, making sure that all areas of government security are implemented in our exercising. So we have this thing called the government security ecosystem. And cyber obviously sits quite high up there. And then there's physical and there's personnel. But then there's all these other areas of security like procedural and technical and information security that we just don't talk about enough but are vital to help make our cyber security strong. So we try and really push to the forefront of all of our exercises that you need to have an appreciation for all of those areas and not just cyber. To make all of them work, there needs to be a level of harmony there. It would be quite impractical to invest equally against all of them. You just can't do that. But to have an appreciation for all of them at some point is really important.

It's all great having the best cyber security around, spending millions on it. But if your physical security is so bad that someone can just walk in and enter a server room, there's not much point. So it needs to work together, it needs to be a lot more holistic, even though everyone uses the word holistic all the time, but it does. Because if we're not integrated in our security, we can be sure our enemies are, so we need to be prepared for that.

Isabella: So what role does red teaming play in terms of national security? How does it help to build resilience?

Umaira: So I think red teaming is essential for preparedness, for avoiding groupthink, and for ensuring that we know what we're up against. We use this quote by Sun Tzu quite pretentiously all the time, but I think it perfectly encompasses what we do. And the quote is, If you know the enemy and you know yourself, you need not fear the result of a hundred battles. And that's exactly what we're about. We're here to prepare ourselves to find the weaknesses and exercise and exercise and exercise.

And whether it's, you know, exercising a ransomware attack at a local council, or a hostile state actor attack at an embassy, or even just crisis management for flooding. Red teaming and exercising helps us prepare and build our resilience and it just makes us stronger. Even though we say like, please do not do red teaming at your home department tomorrow because you think you can do it, we use people who are experienced from years and years of doing this and from law enforcement and security consultancies. But the mindset of being, you know, red teaming, and tactics that you can use can be adopted by anyone like role playing or post mortems or team A and B exercises or what if analyses. All of these are things that anyone can use in any aspect of life, not

just national security. You know, Red Team is something that is a tool that's available to everyone and should be used by everyone. I feel like everyone actually does do Red Teaming a lot. Like I said, it's an umbrella term. But even if, you know, when you've had to have a difficult conversation with someone, and you're like, what are they going to say, what if they say this, and then I can reply this, and you, you, like, pre empt what they're going to say and almost, like, practice the conversation in your head, I feel like that's almost like a what if analysis of, like, preparing for every outcome possible.

Isabella: Yeah, for sure. And just as you were speaking there, I think we've realised a lot of listeners that we have, who we work with are probably aware that they've been involved in, like, crisis simulations or tabletop exercises and have maybe participated more in red teaming than they might have initially thought.

Umaira: Yeah, definitely.

Isabella: We've discussed how exciting the role is. Can you maybe share any interesting stories from your time in the role?

Umaira: Yeah, I do have to caveat here a little bit and say... A lot of the exercises aren't always conducted by us, and not always at government departments. I'm going to talk about a lot of broad security principles, that anyone can explore at any point in any department or any place. But, a lot of the examples aren't technically us and not technically in government.

When we're doing exercises, we have loads of different ways to do it. So there's social engineering, we have an OSINT phase and a threat intelligence phase, and then obviously there's physical and personnel. Physical would be getting into the buildings, so kind of bypassing guards and receptions and all those controls. And then personnel would be putting insiders in teams to see if people behave differently, and if we're noticing any insider behaviour as well. So social engineering is a big one, I think usually the one where the weird and wonderful stuff happens.

Social engineering is generally using human behaviour and human biases against people. We have a lot of good examples of when we use social engineering in our exercises.

Other things like quick, quick wins. You know a hard hat and a clipboard can get you anywhere. Tailgating is a big thing. People are just polite and we're British and we like to be polite. So holding doors open, is a, is a good way to kind of... Get into buildings, something we see, we see quite often.

Some really good ones, that are OSINT related or, sorry, social media related. So this year at Civil Service Live we've been giving examples of how we've used people's social medias against them to get access into departments. And one of them is, you know, everyone posts pictures of their keys when they buy a house. It is so easy to just cut those keys from a picture and just replicate those keys and then you've got access to someone's house. There's geolocation tools, like even just tweaking a picture of your balcony, we can use geolocation tools to kind of find that tree, with how the sunlight hits it, what floor you live on, and then it's just, you know, all you have to do is go on Zoopla, Rightmove, old records, and find floor plans, where they live, and then how to get in as well. That was all from just one person's social media. And again, they don't think they're doing anything wrong, but it's just how those small innocuous... Harmless or seem harmless actions can be put together by someone who's really capable and keen to actually, you know, make a, make, make a life out of you.

Another one that we're quite keen, to share is Instagram posts of like pets and stuff like that. People post their pets all the time, but it's also really obvious security, question as well. I don't know if everyone's like seen, you know, what is the name of your pet as like a security question. Someone posting their dog online and then even if they haven't named it, people in the comments will name and be like, Oh, great picture of Alfie or whatever. And then, you know, even though you haven't breached your personal security, someone else has, but it's a way that we've, you know, been able to access emails and things like that and bypass security questions.

Yeah, so there's, there's so many different ways, whether it's social engineering, or OSINT, or social media, or, you know, physical access into a building, getting past guards, or reception, talking to the right people, or personnel, and like, just putting the right person into, who's trusted in a team, or using phishing, scams to get people to click on a link. These are all ways, and they generally work.

Isabella: Yeah, it sounds like a testament to open source intelligence.

Umaira: Yeah, yeah.

Isabella: And also, hopefully, for everyone to sort of clean up their digital footprints as well.

Umaira: Oh yeah. I'm very paranoid all the time.

Isabella: Definitely made me even more paranoid, so thank you. But good, good tips to have from somebody that is definitely in the know. Sort of further from that, what are the most common findings during a red teaming exercise?

Umaira: Usually an over reliance or optimism of one area of security. So just thinking your cyber security will be able to handle all attacks, so your physical, your...

and not realising that one area that's not given as much attention could be the entryway to your cyber system or building.

Like I mentioned before, the polite Britishness of people allowing tailgating, but also not really challenging, not having a challenge culture. Bad password hygiene as well, writing them down when they shouldn't have written them down. Or, you know, we do need to store passwords in some way, but not doing it properly.

And then again, bad social media habits, even like organisational, social media, like from government departments can be bad.

Those are all examples of things that we see. Often, but then there's also the weird and wonderful stuff that aren't common findings, but I would say those four are probably the ones that we see in any and every exercise.

Isabella: I think this is a really good learning curve for a lot of people that are listening as well, just, you know, it's not necessarily blame, it's just, if it's a culture of everyone else doing it. it's realising that, you know, maybe we shouldn't be...

Umaira: Yeah, yeah, yeah, yeah, you just need to be aware. Um, and again, like you said, it's not a blame game, we're not pointing fingers, it's something that a lot of people trip up on, senior people trip up on. Um, but it's just, you know, talking about it, making people aware and making sure you don't do it again.

Isabella: So once you've, you know, run a red team exercise, do you then provide recommendations to teams to improve their security posture? And then also how do people sort of respond to that feedback you give them?

Umaira: We do, we have we have both senior and technical team debriefs where we summarize the main findings and the key takeaways, and then there's a detailed bespoke report for each department that highlights the areas of improvement and how to mitigate them.

Whether it's implemented on is mostly in the hands of the department, but we work closely with NTAs and policy teams and GSECs and engagement teams and security teams to make sure that the findings are acted on. The assurance cycle allows us to see results are changing and hopefully we'll get even better insight after GovAssure being launched recently and across government.

So we do try to kind of stick with them, not to sort of come in, break things, tell them what they did bad and leave. We do try and keep that. relationship going. And generally, departments respond really well. And sometimes the findings can be alarming or worrying, but again, we make sure to highlight that it can be a managed risk and so it can be dealt with. And our results can be quite motivating as well. They can be good evidence based for funding and for more senior attention later on. So... Generally, we always try and help them with any of the findings that come back and implementing the

mitigations and if we can't do anything then we point them towards the right people or providing the evidence base for them to go away and actually do something about it with the seniors and usually people are really happy to have us in the room which is nice to hear.

Isabella: So security can be a male dominated environment. Do you feel this impacts how you work? If so, what measures do you take or have other people taken to ensure that you are considered equal?

Umaira: So I think it's true, it is quite a male dominated, area. When I joined the red team I was the only woman in the team but now the head of the red team is a woman and you know I just, I've never really felt like, I've been treated differently. I think the men that surround me in my team, in my directorate and in GSG general have been incredibly supportive and welcoming and have always looked out for me in my development. I'm quite young compared to them, so they're always trying to help me develop and learn new things.

But to be fair, the panel that we were at with, that we met, I was there because my other team member, who was a man, was on, originally supposed to be on the panel. And he stepped aside and said no, I think you should go because you're going to, you know, you're knowledgeable and you're going to be great. And not just because I'm a woman, but obviously he did want that representation there as well. And to step aside and give me a seat at the table is another way to do it. And it's brilliant. I was scared being on that panel, surrounded by men who are more senior than me and older than me and just more important than me. But being on that stage and being allowed a seat at that table because another man opened that up for me is what other people should be doing. Whether you're a woman or a man, you should be opening up that space for other people. And I'm so grateful to be in a team where that happens and we all look out for each other.

And what I do know is that I don't want to change how I am to fit in. So I'm quite a feminine person. I wear these flowery skirts to work and I send smiley faces in emails. And I'm, I'm generally a really friendly, smiley person. I don't want to have to act serious in emails or in exchanges with people, whatever department they're from, to, you know, seem more appropriate for the situation or for working in security. You know, you should be able to bring your whole self to work and feel confident in how you are.

I will say the one thing I have changed is using the word ‘just’ in emails. I think it's so easy, especially for women, to just be like, Oh, I'm just sending this email, you know, sorry, I just need help with this. And, you know, trying to be more confident in my language, on emails at least, but not really changing my whole self to kind of fit into what other people's ideas are of how I should be acting at work.

So it is a male dominated area, but I feel so comfortable, where I work in GSG at least, to come to work however I am and be accepted. And I've never really had to complain about being felt like a young woman at work when, you know, that's just, that's how it should be.

Isabella: No, it sounds like a really lovely work environment. I don't think you would have stayed for as long as you had if you weren't, you know, in a really comfortable place. But it's always nice to hear when you get colleagues that are allies to you.

Umaira: Yeah, yeah, yeah.

Isabella: Where do you think the areas of improvement are for increasing diversity in security?

Umaira: So I think the two areas I would say are recruitment and vetting. I get asked to sit on recruitment panels all the time and, um, I do think it's because I'm from a BAME background and I'm a young woman, um, so that helps to have, you know, me on a panel and I really enjoy it. I always, I do like being asked to be on panels. The recruitment panels are so daunting in the first place and, you know, entering a room in which people look nothing like you or have not had the same experiences, you can be even more daunting.

So just seeing someone the same colour as you, the same gender as you. can be a massive help. And then vetting is so important in building trust as well. People from foreign backgrounds can feel nervous about vetting and not put themselves forward for roles in security because they're scared of, you know, the kind of questions they might get asked. I know I was really scared, having come from Pakistan, what they're going to ask or, you know, if I'm even going to be allowed, if it's going to get rejected, all of these things. And I do think that the mysterious element of vetting and having that bit of a facade around it is beneficial and it can help. But not to the detriment, and we are taking the right steps, there's the DV initiative where they give DV to people from diverse backgrounds even before they need to apply. And, you know, there's the new vetting framework allows for more representation for LGBTQ backgrounds. So we're making the right steps, I just think there's a bit more that can be done in those areas.

Isabella: No, definitely. So, what is the most valuable advice you have received at work?

Umaira: I've gotten so many bits and pieces of advice that I feel like it's hard to pick just one. But there's like the general just work related ones like, save everything that you do because you will forget that you've done it. You know, write it down, keep a log, keep a record. I'm really bad at that but I try and

come back to it every now and then. So just remember what I've done because you do just, things come out, get out of control and you, time goes by, by so quickly. You do just forget.

You care more about you than anyone else in the room. So like, don't worry, you're overthinking it, it's fine. You know, just because you made a mistake in that meeting, it's, it's not the end of the world. No one really probably even noticed or bothered. Like, don't make a mountain out of a molehill, that sort of thing. Because I know I get my, like, my anxiety or like my worry is really like looking dumb in a meeting or something like that. Because I try and think about how many times I notice a mistake in a meeting and I don't, so. Trying to like, not be, not have main character syndrome, basically. And like, just think that not everyone in the room is worried about what you're thinking right now. Is quite, something that I quite like. But my, my colleague did like, remind me, remind me when I was talking about this advice is, this doesn't work for if you're feeling bullied or harassed. Like, at that point, you probably should say something, but this is more about just making mistakes and, you know.

Isabella: Definitely. I think in a professional capacity, I'm so similar. I just don't, I don't want everyone to focus on the bad stuff and it's like, no, they're just focusing on their own bad stuff anyway, it's all okay. And then further from that, what advice would you give to someone wanting to go into red teaming?

Umaira: So we look for people that are open minded and you know, there's no real fit into it. Something that you need to have studied or something that you need to have experienced. We've got people who went to university, who didn't go to university. I think that's what makes our work so rich. Having all these different perspectives into a room to avoid groupthink. We like someone who's a challenger, who doesn't mind speaking truth to power. And is good at kind of convincing people to come on to their, to their way of thinking. And changing minds and challenging everyday mindsets, I think is integral to what we do in red teaming and being creative and thinking outside of the box.

Isabella: And then onto the final, and arguable the hardest question.

Umaira: It is, it is.

Isabella: Do you have any recommendations, books, TV shows, podcasts for our listeners relevant to security, work, or just simply anything you're enjoying.

Umaira: So relevant to security, but not at all realistic. I recently watched Slow Horses. Have you seen that on Apple TV? It's really good. It has Gary Oldman and it's basically, about the misfits or the bad MI5 agents and all the ones that have messed up at some point and he, he leads that little misfit group of bad MI5 agents and then they go off on all these missions and adventures and it's

really funny and really good. It's actually a book series turned, turned into a TV series. And there's two seasons out, or three, I can't remember. Obviously not realistic at all than MI5, but a really fun show to watch if you're interested in that sort of stuff.

Isabella: Security adjacent.

Umaira: Yeah, exactly.

Isabella: Thank you so much for giving up some of your time today, it was really interesting hearing all about red teaming. And thank you for your recommendations at the end as well.

Umaira: No worries, thanks so much for having me, it was really fun.

Isabella: Of course.

[Outro music.]

Thank you for listening to Off Mute. And a special thank you to today's guest, Omera. This episode was hosted by Isabella, written by Sophie, and produced by Sam.

[Outro music.]