OASIS

CyberDetective

COMIC PART 3 OF 6

PART 3/6

Welcome to the World of Oasis where its inhabitants are kept safe by the technology they surround themselves with as they try to rebuild their lives. In this episode the detective has to visit an unexplored building.

Chief Editor &
Transmedial Producer:
Vincent "South-Blessed" Baidoo
Artist: Connor Rawlings
Front Cover: Jonathan Tonello
Writer: Vincent Baidoo
Editor: Niki Baidoo
Writer & Researcher: Patrick Shortis
Extra Art: Vladimir Rikowski, Francisco Ruiz
Special Thanks: Jeremy Charles, Tomas Hall

CyBOK

CROWNROOT publications

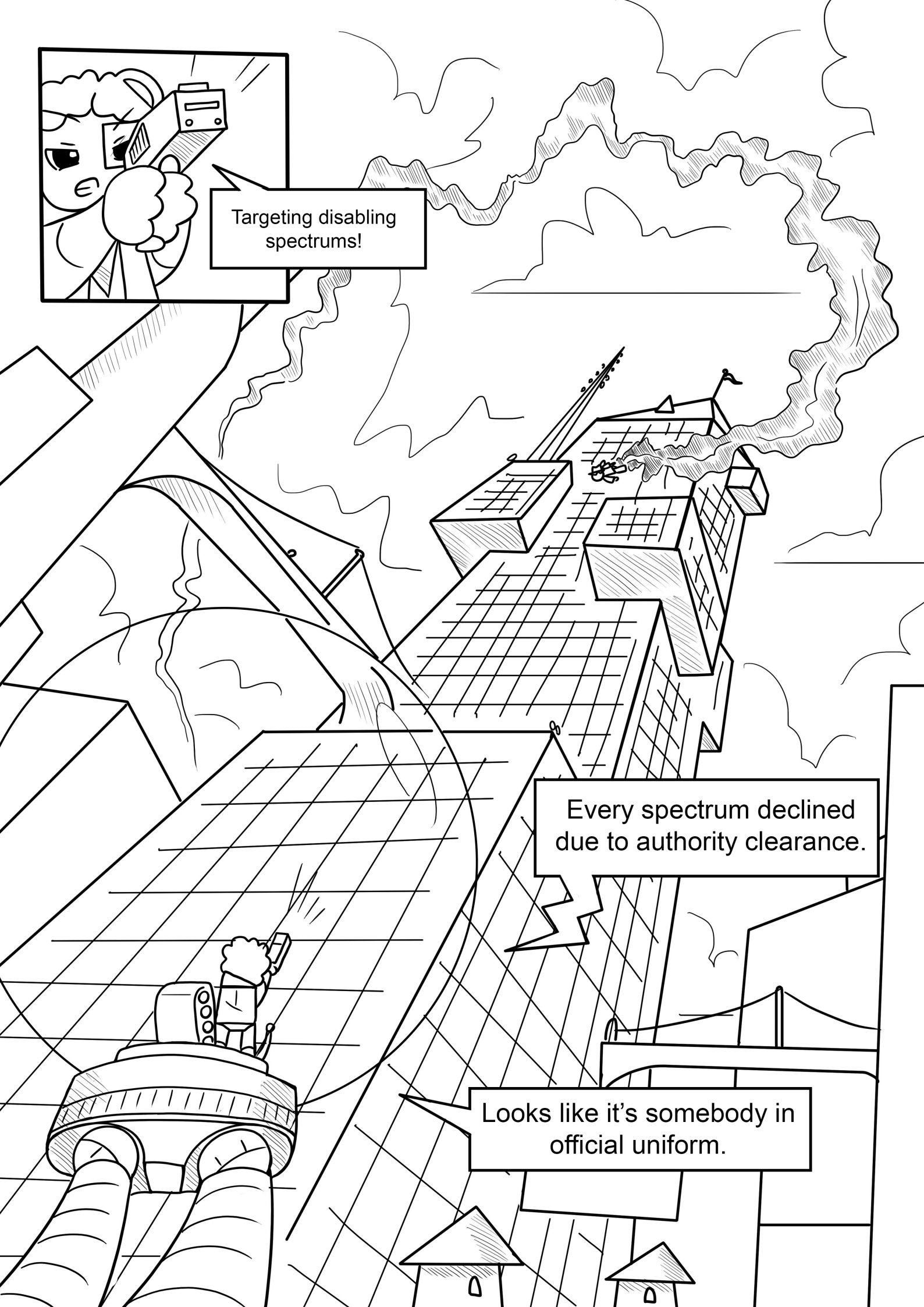
University of BRISTOL

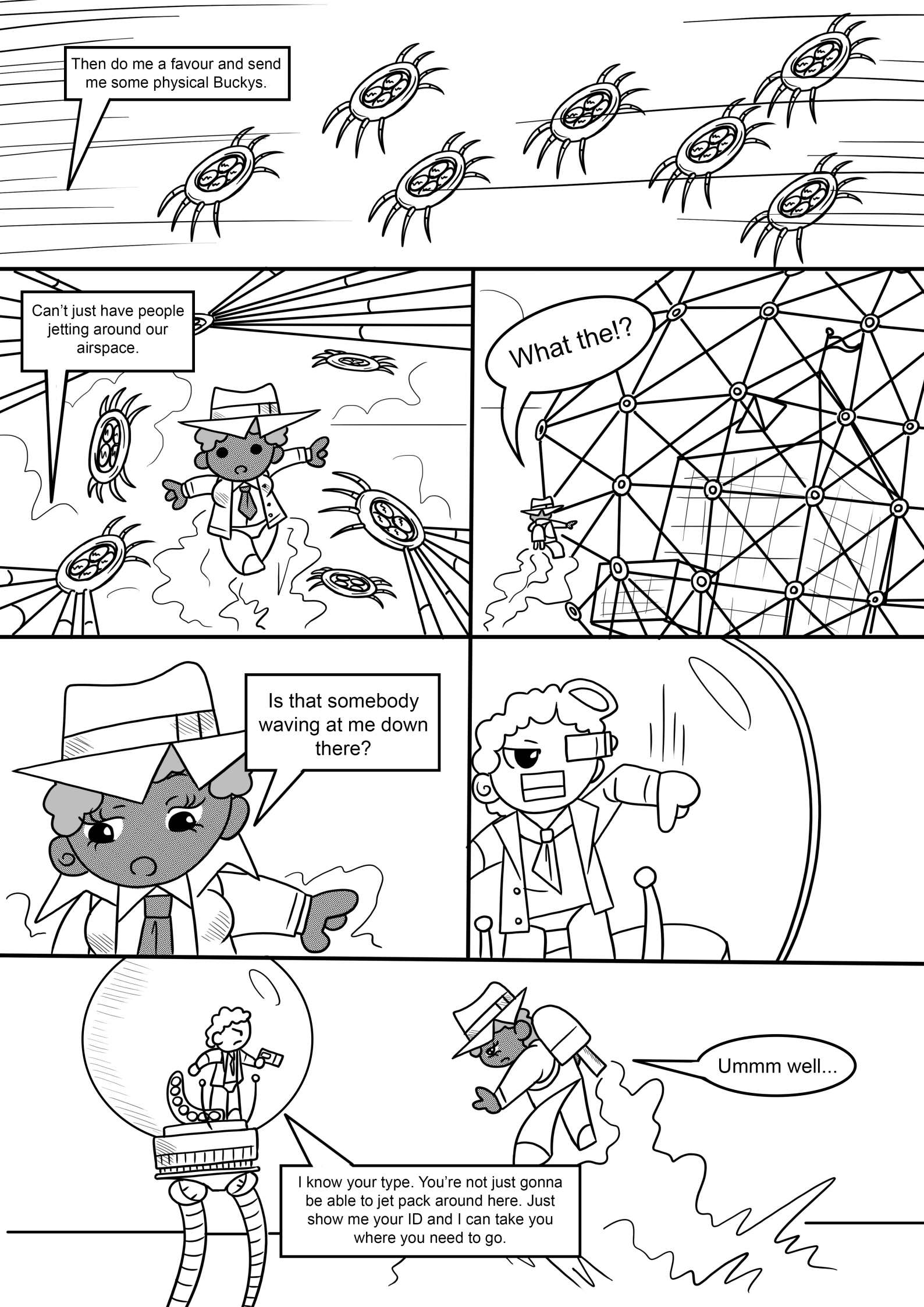
UKRI Research England

THIS PUBLICATION IS A RESULT OF CYBOK AND CROWNROOT PUBLICATIONS FUNDED BY BRISTOL UNIVERSITY AND RESEARCH ENGLAND

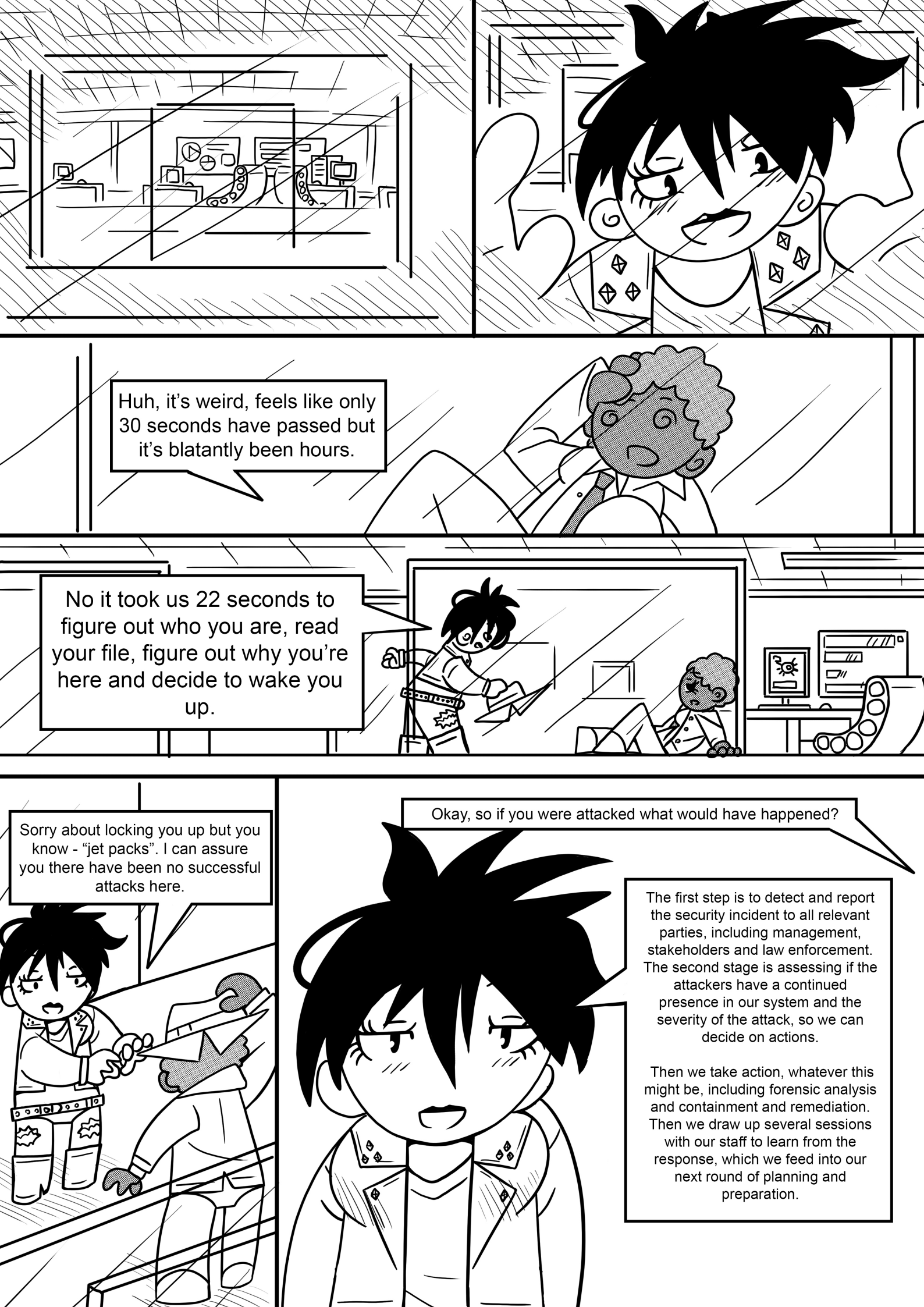

I should have told you beforehand but somebody came around asking about the drones that end up at the food bank.
And you just told this person everything they wanted to know?
They weren't a stranger, they had an energy plant ID and everything. I did kinda recognise them but looking back on it it was weird, that's why I'm caling you.
Well at least you let me know. Anyway my Chief is gonna call you in a second. Tell him everything and don't forget anything this time.
Alright Chief, turns out the guy from the automation plant did have an unusual visit so this is all making more sense now.
Well I will get some Juniors over to him, I've also got the warrant, we've got clearance to forensically analyse the energy systems and collect evidence.
Okay, well given everything I have heard I can think of 50 ways to get into their system.
No, that's not legal. We're only criminally exempt from using the warranted technique, so get over to the Data Centre and find out more about the exploits.

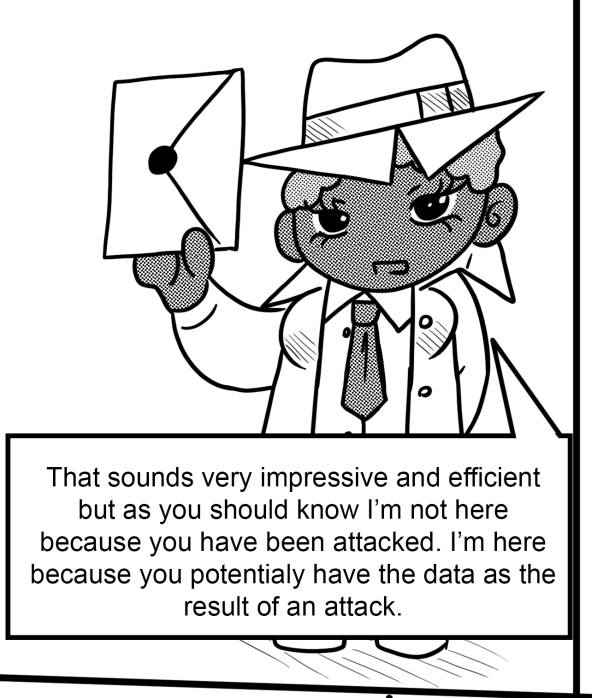

Ok, I'm off to the Data Centre. Take that encrypted voice note to the Chief.
Grrr that Jet Pack will be her end as well!
Oooh, I've never caught a shiny Poltergeist before!
SCORE - 237
What is that!?
Is this a registered projectile?
That is a negative on projectile authentication - over.


Targeting disabling spectrums!
Every spectrum declined due to authority clearance.
Looks like it’s somebody in official uniform.

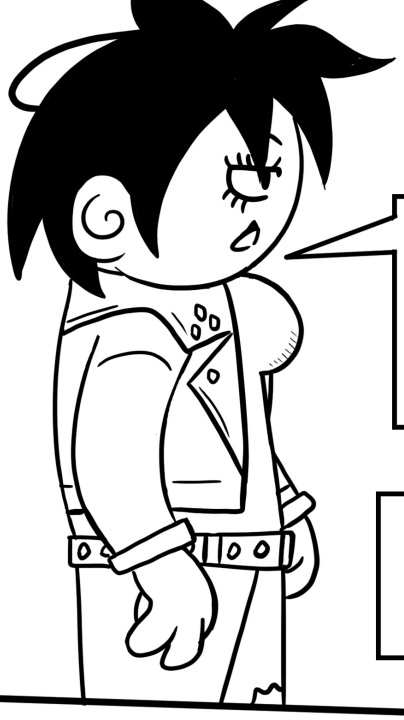

Then do me a favour and send me some physical Buckys.
Can't just have people jetting around our airspace.
What the!?
Is that somebody waving at me down there?
Ummm well...
I know your type. You're not just gonna be able to jet pack around here. Just show me your ID and I can take you where you need to go.


This is actually the first time I've been here so I don't have an ID yet.
Grrr!! I can't believe you! Code Red!
HA HA HA! You're actually pretty funny. No one's been this obvious with an attack.
XYZ correct! Position targeted!
KCHUNK
WAAAAAAAA!?


Huh, it's weird, feels like only 30 seconds have passed but it's blatantly been hours.
No it took us 22 seconds to figure out who you are, read your file, figure out why you're here and decide to wake you up.
Sorry about locking you up but you know - "jet packs". I can assure you there have been no successful attacks here.
Okay, so if you were attacked what would have happened?
The first step is to detect and report the security incident to all relevant parties, including management, stakeholders and law enforcement. The second stage is assessing if the attackers have a continued presence in our system and the severity of the attack, so we can decide on actions.
Then we take action, whatever this might be, including forensic analysis and containment and remediation. Then we draw up several sessions with our staff to learn from the response, which we feed into our next round of planning and preparation.

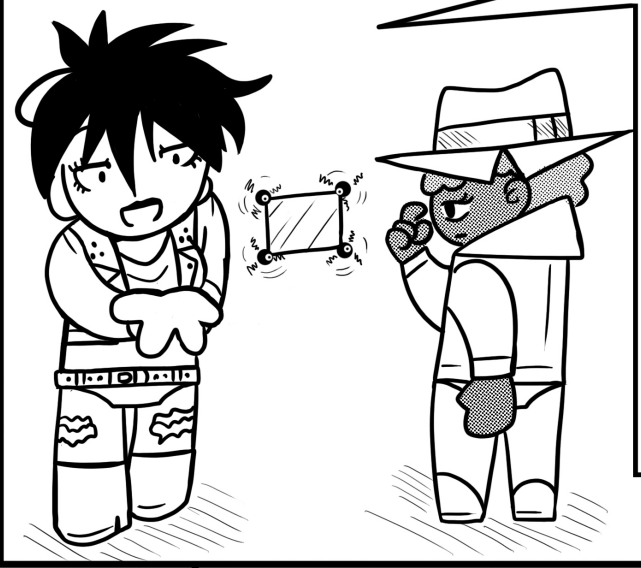


That sounds very impressive and efficient but as you should know I'm not here because you have been attacked. I'm here because you potentialy have the data as the result of an attack.



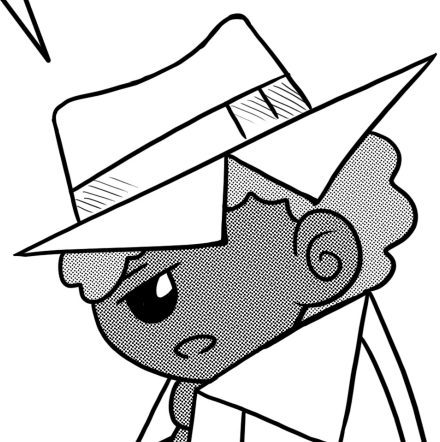
Oh. If you had just shown that letter to Sam outside you could have saved yourself getting sucked into the floor.

Quick question? Did they not try to attack your cloud services at all?

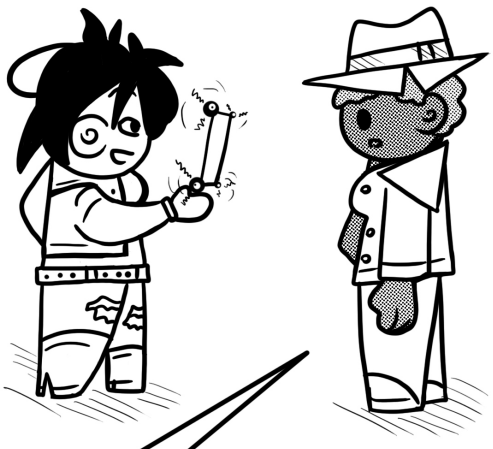


Our cloud service provider has a dedicated cyber security team and some top-of-the-line intrusion detection systems. They also periodically carry out ID authentication queries as well as look for anomalies in the system state, to ensure IDs are not compromised. It would be a hell of a struggle if they did try it.

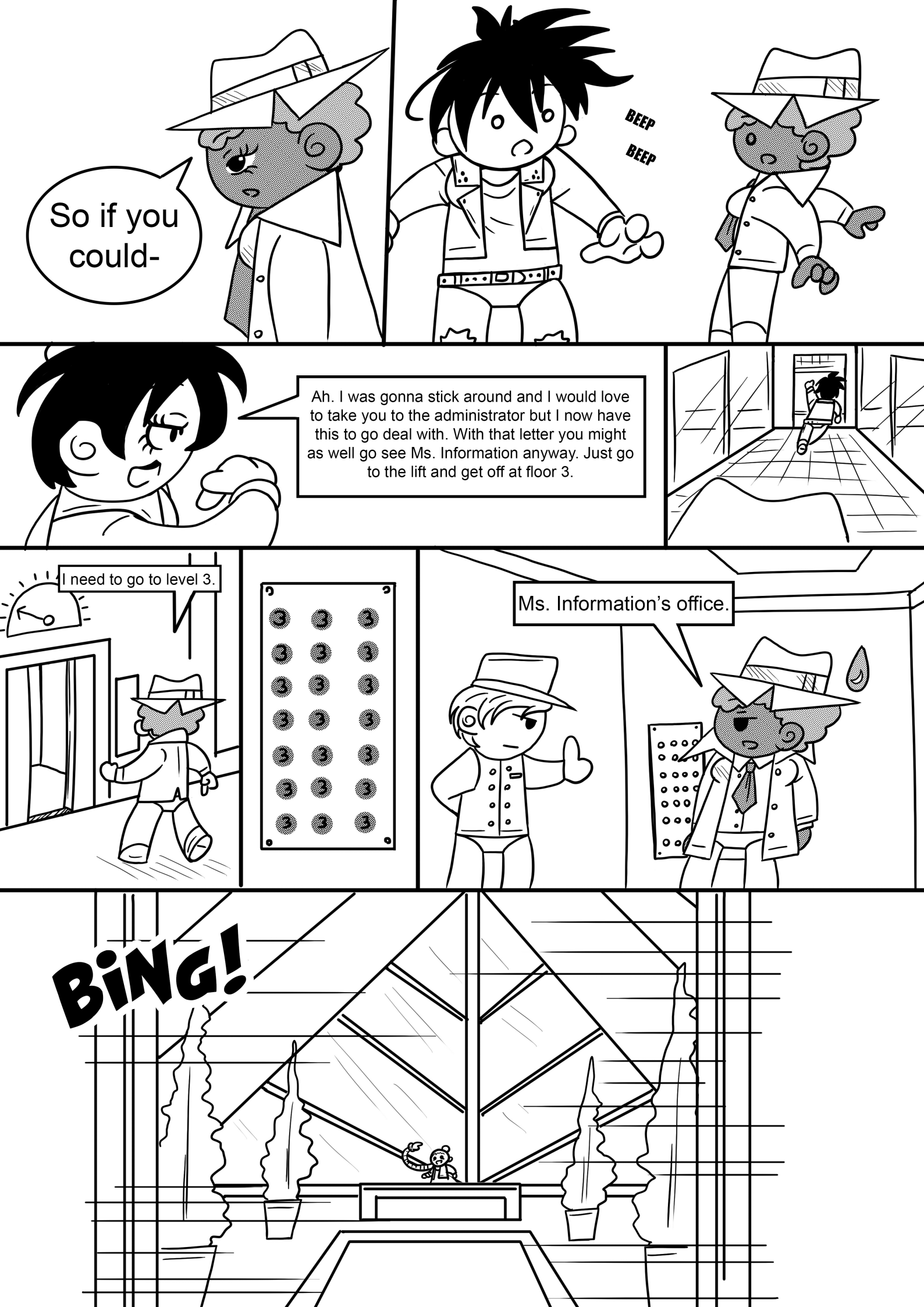
I want to talk to your administrator about your audit policies. If they've been done well they should have logs of all the successful and failed authentication attempts and any information on sensitive access requests from access control decision algorithm.



With that letter I am sure you will be welcome to look, but I doubt you'll find anything. I checked them myself and found no access attempts. Our system was pen-tested by some of the best ethical hackers in the business, we profiled all the attacks and believe me they leave signatures. Our machine learning algorithms would have picked them up and flagged them to me at once. There's nothing.

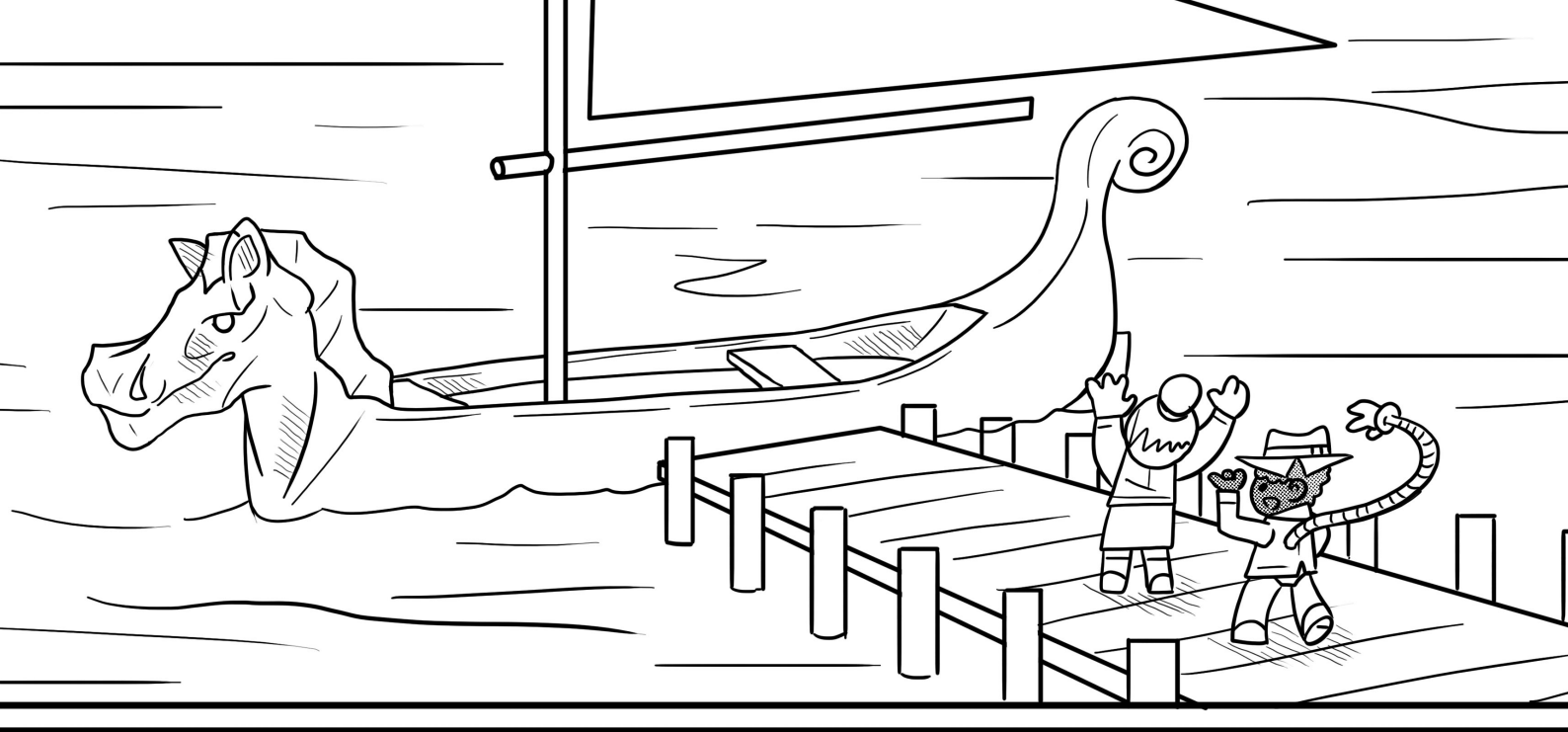


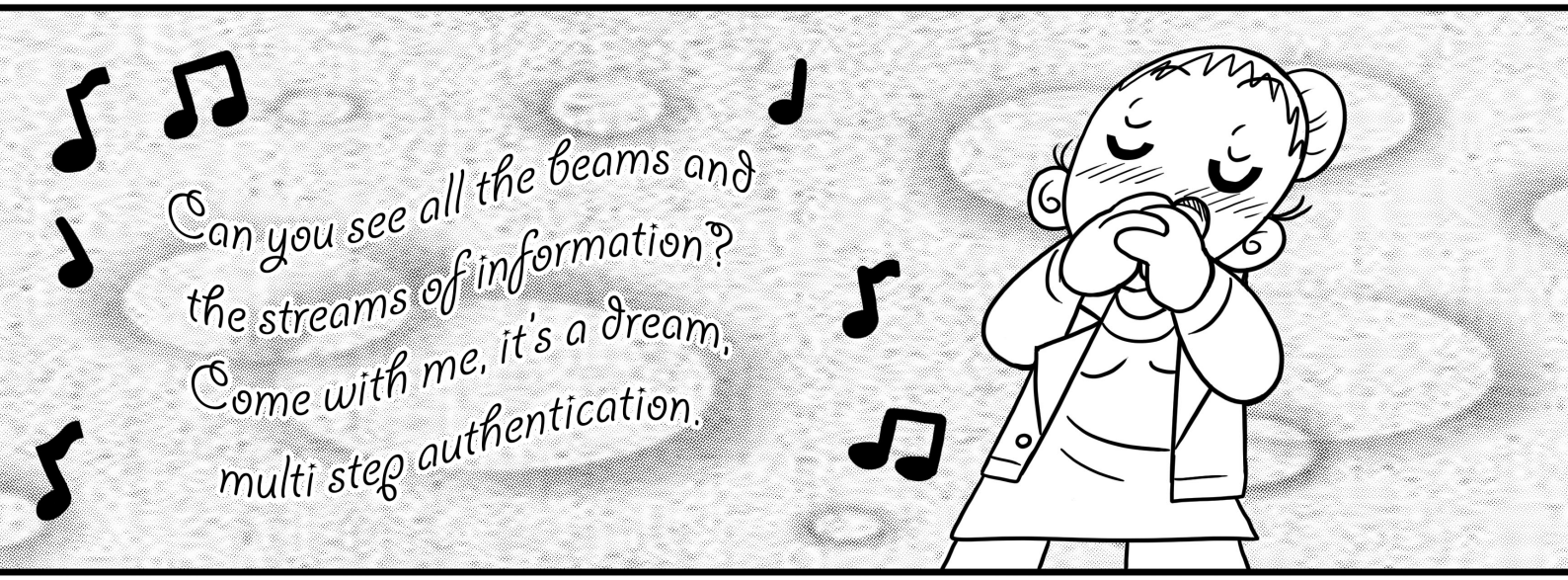
I want to see them anyway.


So if you could-
BEEP
BEEP
Ah. I was gonna stick around and I would love to take you to the administrator but I now have this to go deal with. With that letter you might as well go see Ms. Information anyway. Just go to the lift and get off at floor 3.
I need to go to level 3.
Ms. Information's office.
BiNG!


Victoria! Where does a bad light end up?
Bad light? I don't know what you mean.
In a Prism.
I know you're gonna go through and change everything back but we added a light feature. Hope you don't mind.
I suppose I should just be happy to get it back at this point...
That's the positive attitude we're looking for around here. And now we can just skip straight to you asking me loads of questions I can't answer due to privacy issues.
You say that...
But I'm gonna need some answers actually.
Oooooooohh!!
murmur
whisper
murmur
whisper
murmur
whisper
murmur
murmur


Do you know Archie Baylies is always on Psychic Readings.com.
Disgusting isn't it? But jokes aside I need access to your servers because of Archie's private habits.
You want our servers??! Are you mad? They're running half of our business...
We'll make copies –
Hmmmmmmmm...
And the originals will go into our evidence lockers until this case is over.
I suppose they could use a good holiday. Look they're hard work to access so how about you take a snapshot of the current system starting with Archie's system, as well as copies of the backups.
Yeah that sounds fine.
OAE34515NRGZZ4 is the physical machine hosting most of the information systems and servers for Archie so start there. I'll take you there now, it's a nice little boat trip.

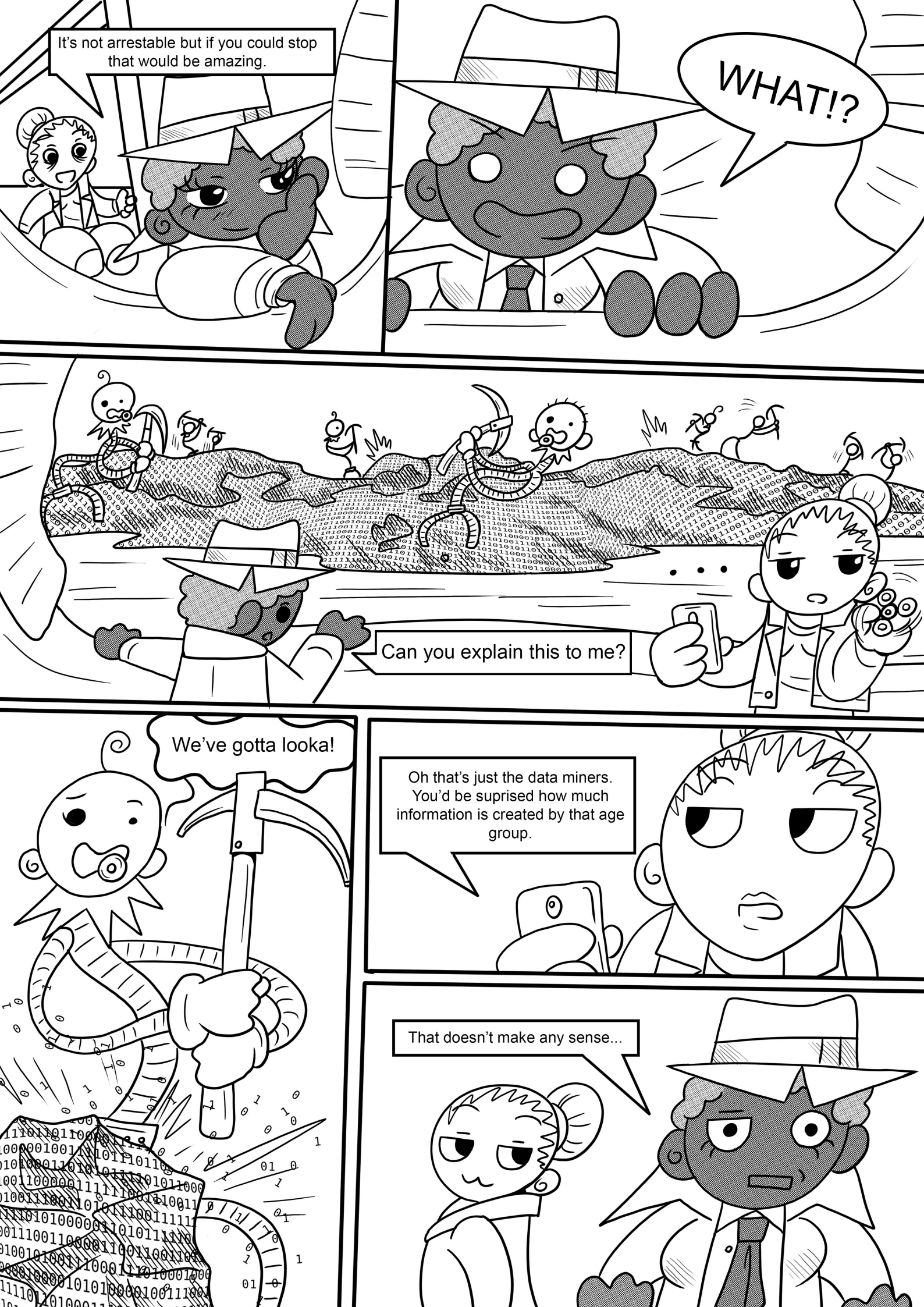


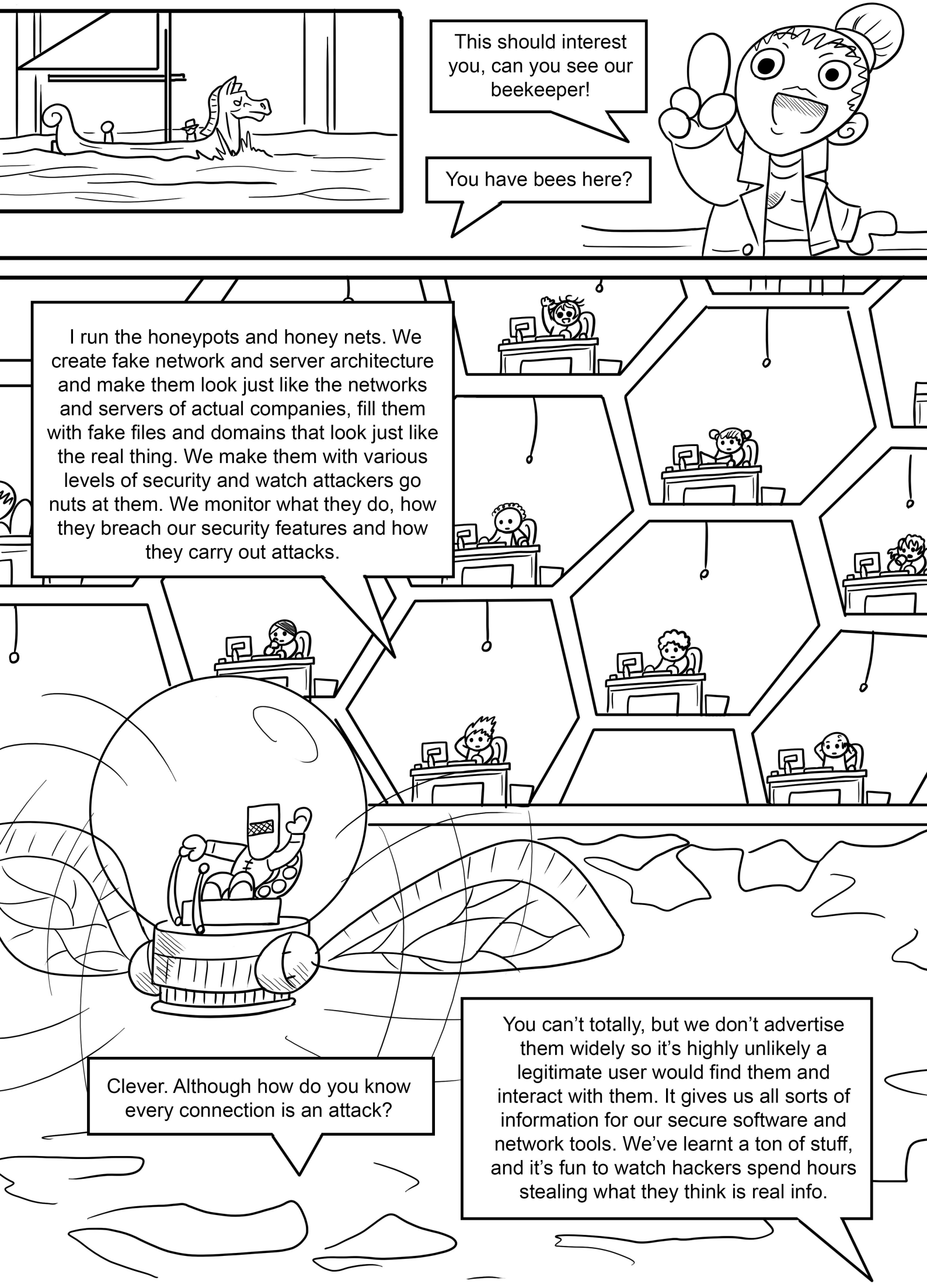

Can you see all the beams and
the streams of information?
Come with me, it's a dream,
multi step authentication.


Could everyone stop singing!

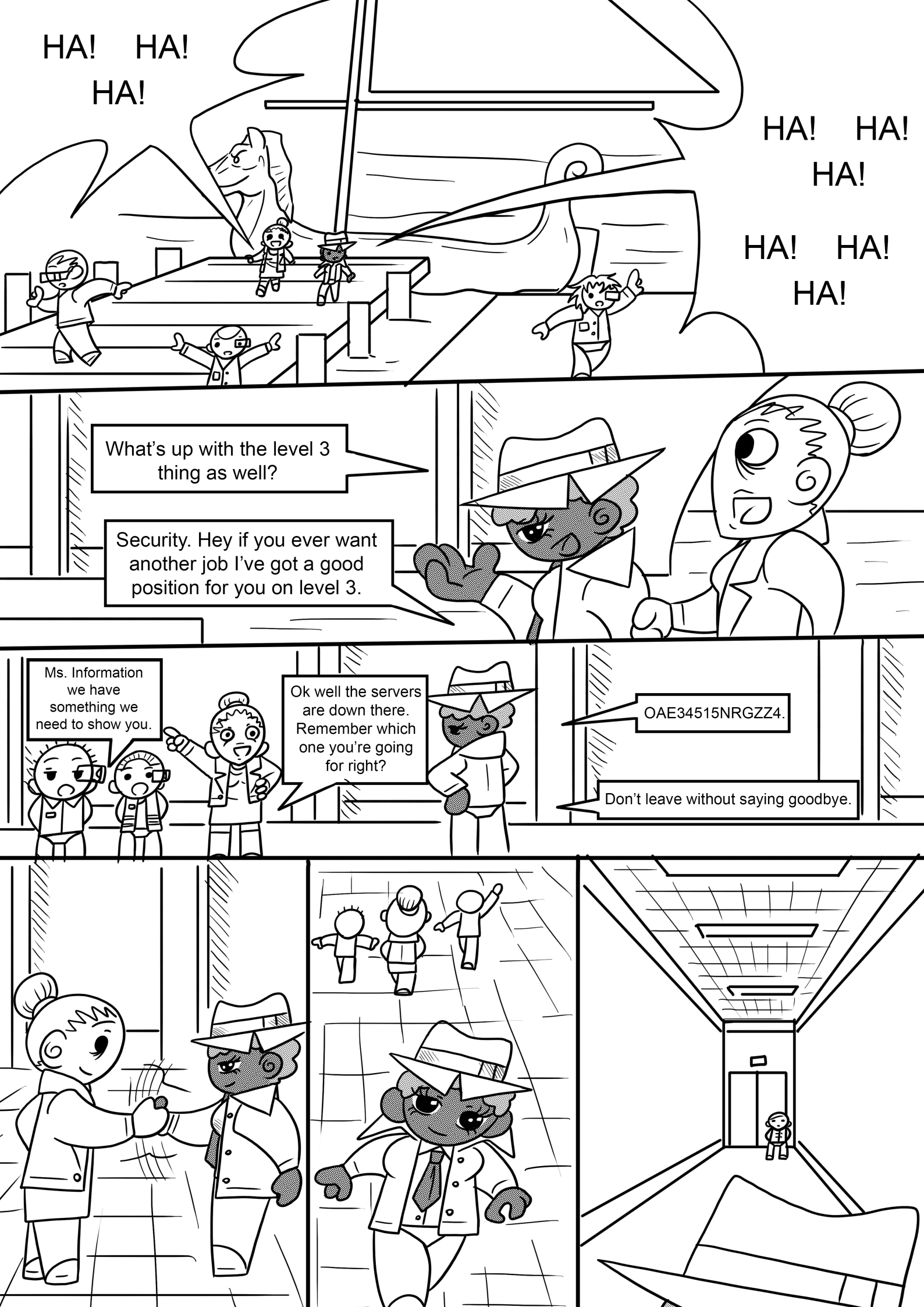

Oh you don't like singing? Let me give you the drum and bass version -

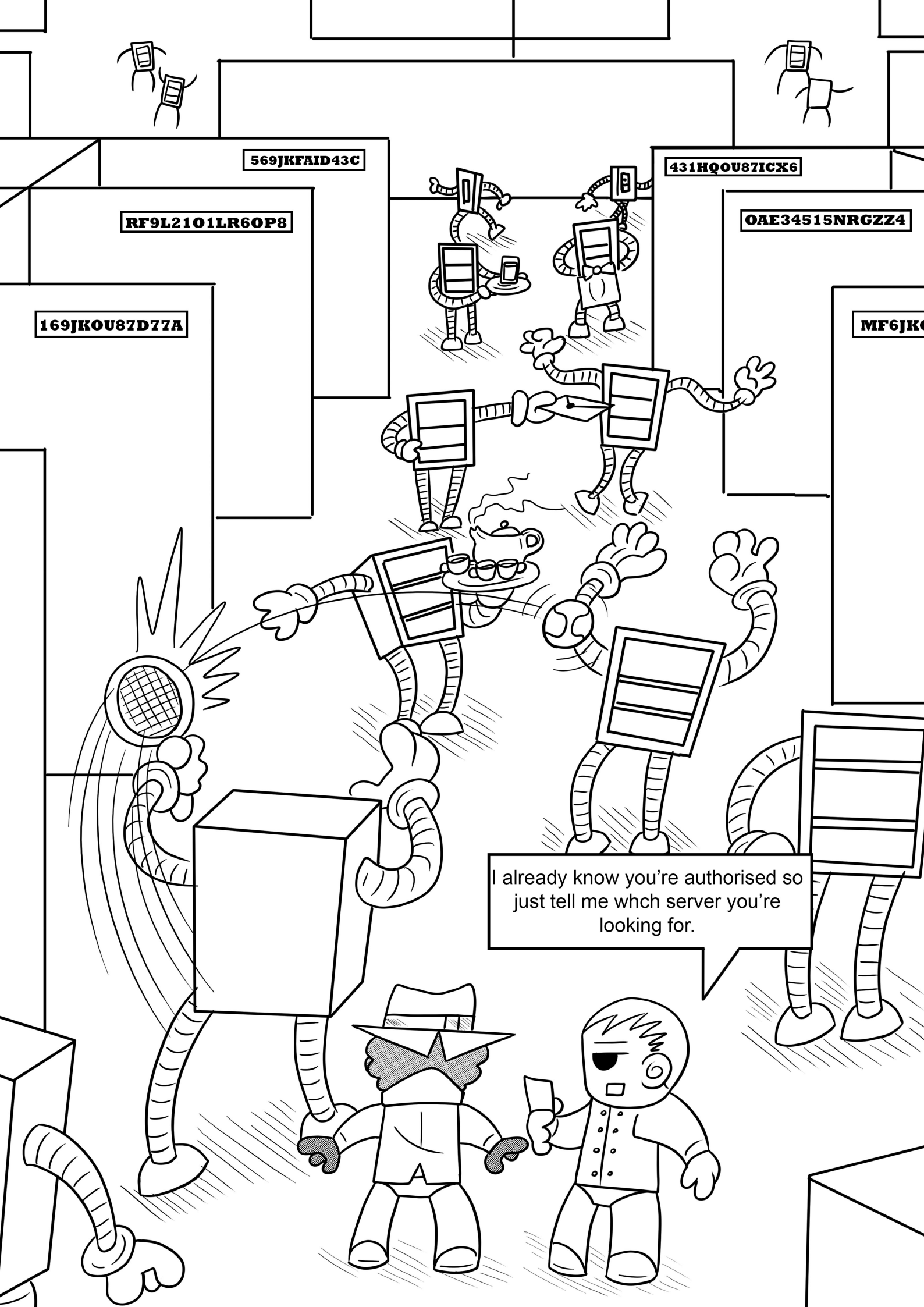

DATA
DAYTAH

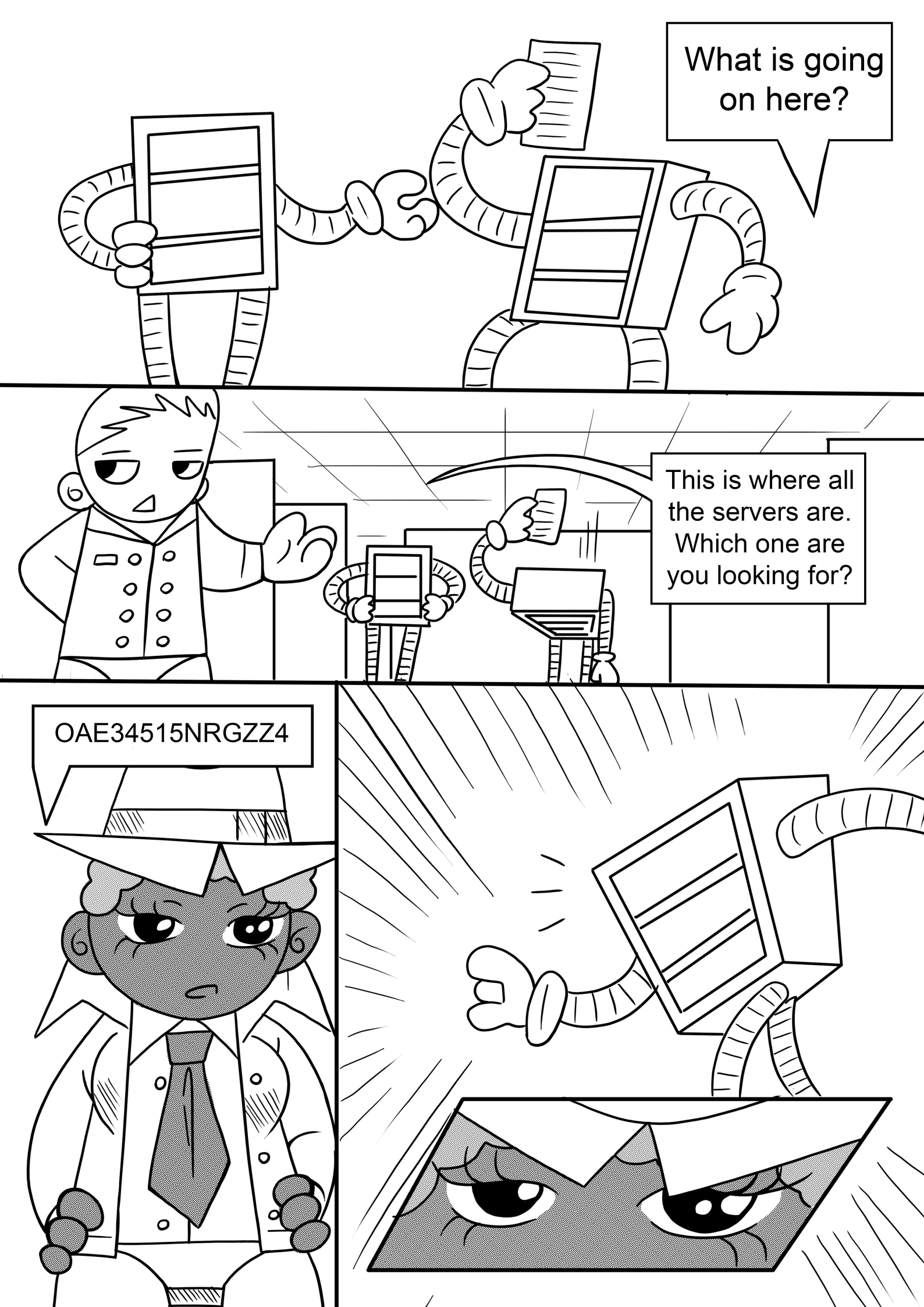

It's not arrestable but if you could stop that would be amazing.
WHAT!?
Can you explain this to me?
We've gotta looka!
Oh that's just the data miners. You'd be suprised how much information is created by that age group.
That doesn't make any sense...


This should interest you, can you see our beekeeper!
You have bees here?
I run the honeypots and honey nets. We create fake network and server architecture and make them look just like the networks and servers of actual companies, fill them with fake files and domains that look just like the real thing. We make them with various levels of security and watch attackers go nuts at them. We monitor what they do, how they breach our security features and how they carry out attacks.
Clever. Although how do you know every connection is an attack?
You can't totally, but we don't advertise them widely so it's highly unlikely a legitimate user would find them and interact with them. It gives us all sorts of information for our secure software and network tools. We've learnt a ton of stuff, and it's fun to watch hackers spend hours stealing what they think is real info.

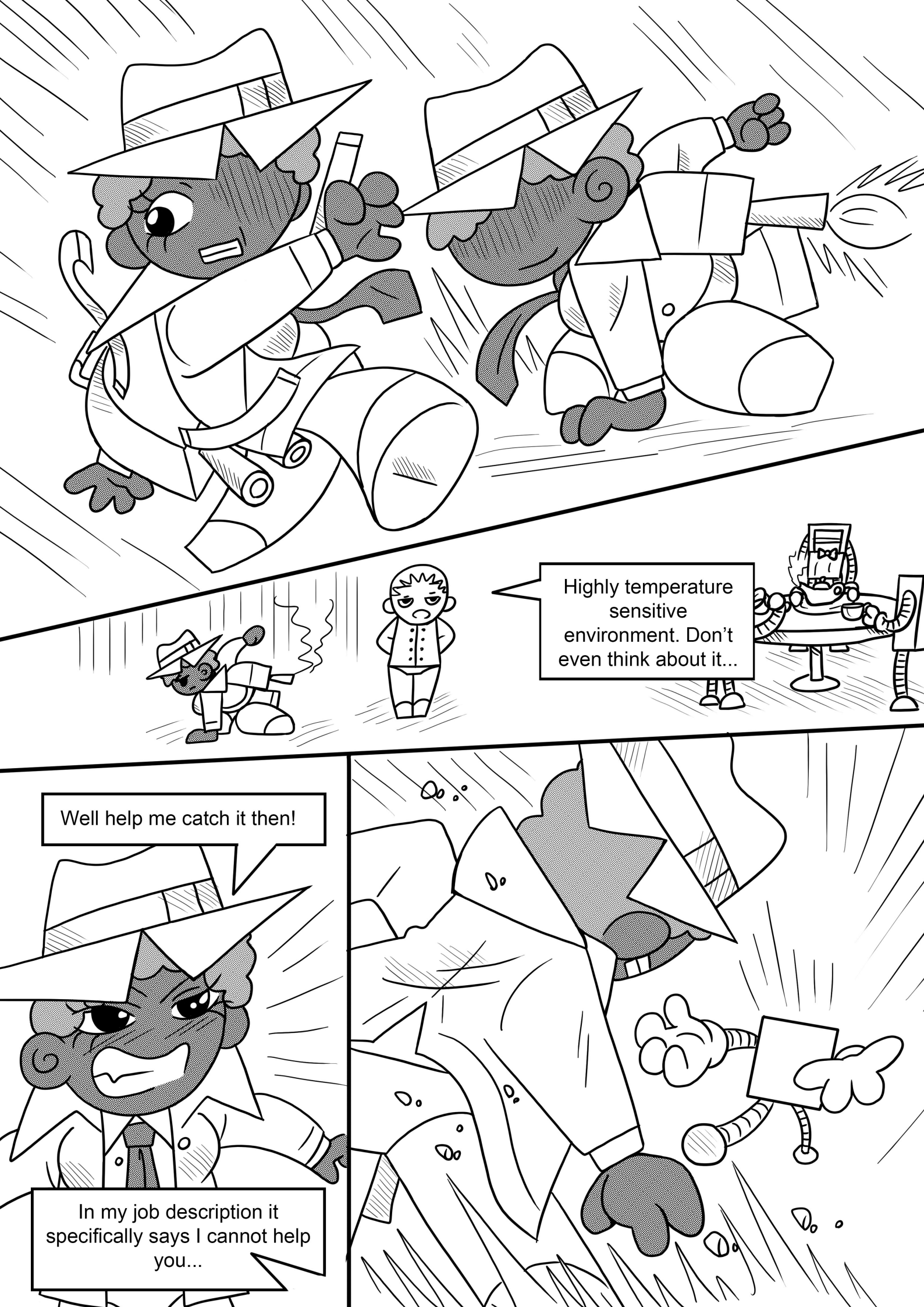

And I take it this is how you spy on everyone?
It's the job that's never started as takes the longest to finish.
Getting information in real time and storing it in one place must be dangerous no?
The burnt hand teaches best. After that advice about fire goes to the heart.
So you're just doing the cryptic answer thing. Well not much I can do as I'm not investigating you. You remind me of my fiancé.
I understand your frustration but in reality as soon as you trust someone fully your security has been breached.
As you can imagine we get a lot of data from lots of different sources.
Including reading your emails...


HA! HA!
HA!
HA! HA!
HA!
HA! HA!
HA!
What's up with the level 3 thing as well?
Security. Hey if you ever want another job I've got a good position for you on level 3.
Ms. Information we have something we need to show you.
Ok well the servers are down there. Remember which one you're going for right?
OAE34515NRGZZ4.
Don't leave without saying goodbye.


569JKFAID43C
431HQOU87ICX6
RF9L2101LR6OP8
OAE34515NRGZZ4
169JKOU87D77A
MF6JK
I already know you're authorised so just tell me whch server you're looking for.


What is going on here?
This is where all the servers are. Which one are you looking for?
OAE34515NRGZZ4


You have to chase it...
? ?


Highly temperature sensitive environment. Don't even think about it...
Well help me catch it then!
In my job description it specifically says I cannot help you...


ACTIVATE ANCHOR MODE!
TBC