CYBER CUPULA

Operation “Baobab” : Neutralizing an active cyber gang operating from Nigeria and UK, targeting commercial banks worldwide

The strategy of offensive cyber operation to achieve technical and psychological supremacy

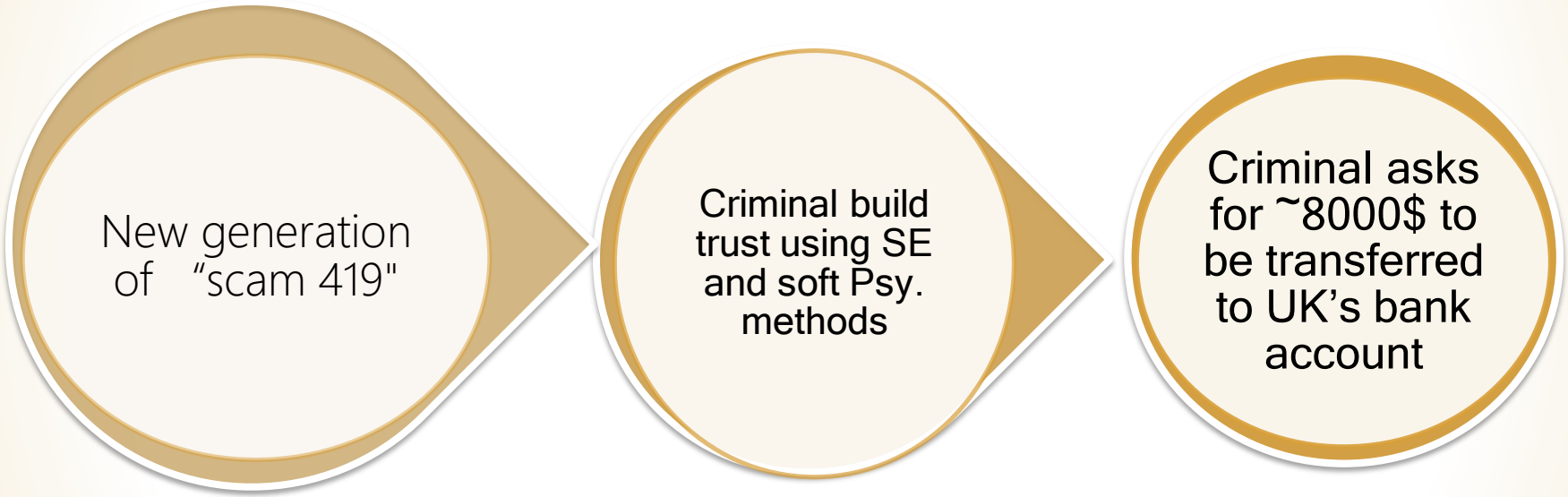
February 2019

CYBER CUPULA

Who am I?

- Active Defense Cyber Humint specialist
- Israeli intelligence
- Serial entrepreneur
- Studied History
- Doing Judo

Operation "Baobab" – cybercriminals *modus operandi*



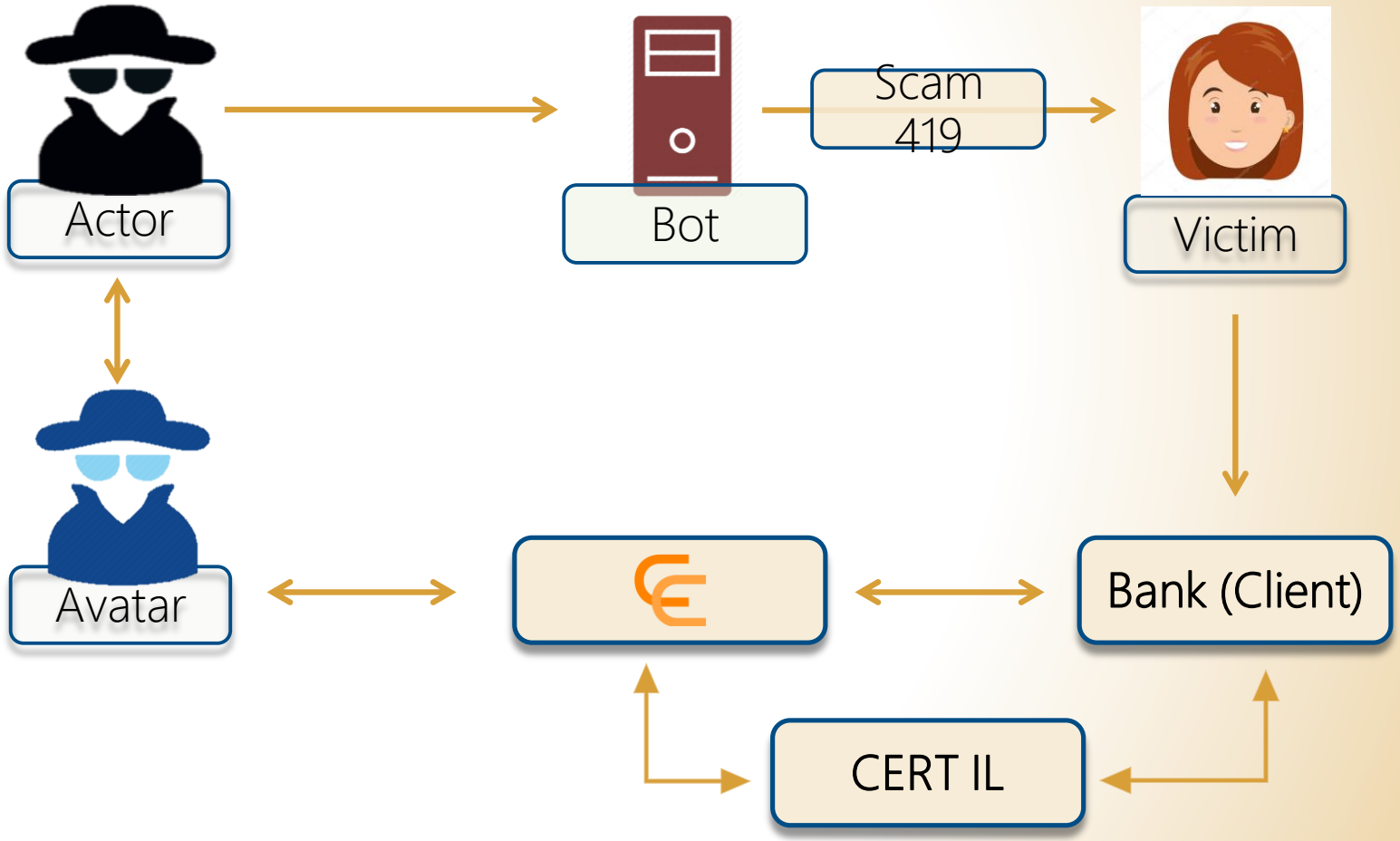
A new generation of scam 419: Cyber gangs well organized not the *script kidos* anymore.

"Baobab" operation - the 4 phases

- Establishing direct contact with presumed actor using several avatars, creating trust relationship, data collection
- Data fusion and analysis of the collected data of this campaign (emails, addresses, name, domains)
- Contact is established in the Clearnet, mapping the cyber gang actors
- Contacts with CERT IL, European bank, Law enforcement agencies, neutralization

"Baobab" operation phase 1: establishing contacts

- Victim informed Bank
- Collaboration with CERT IL
- Avatar Creates contact



Trust created using HUMINT capabilities

"Baobab" operation - the 4 phases

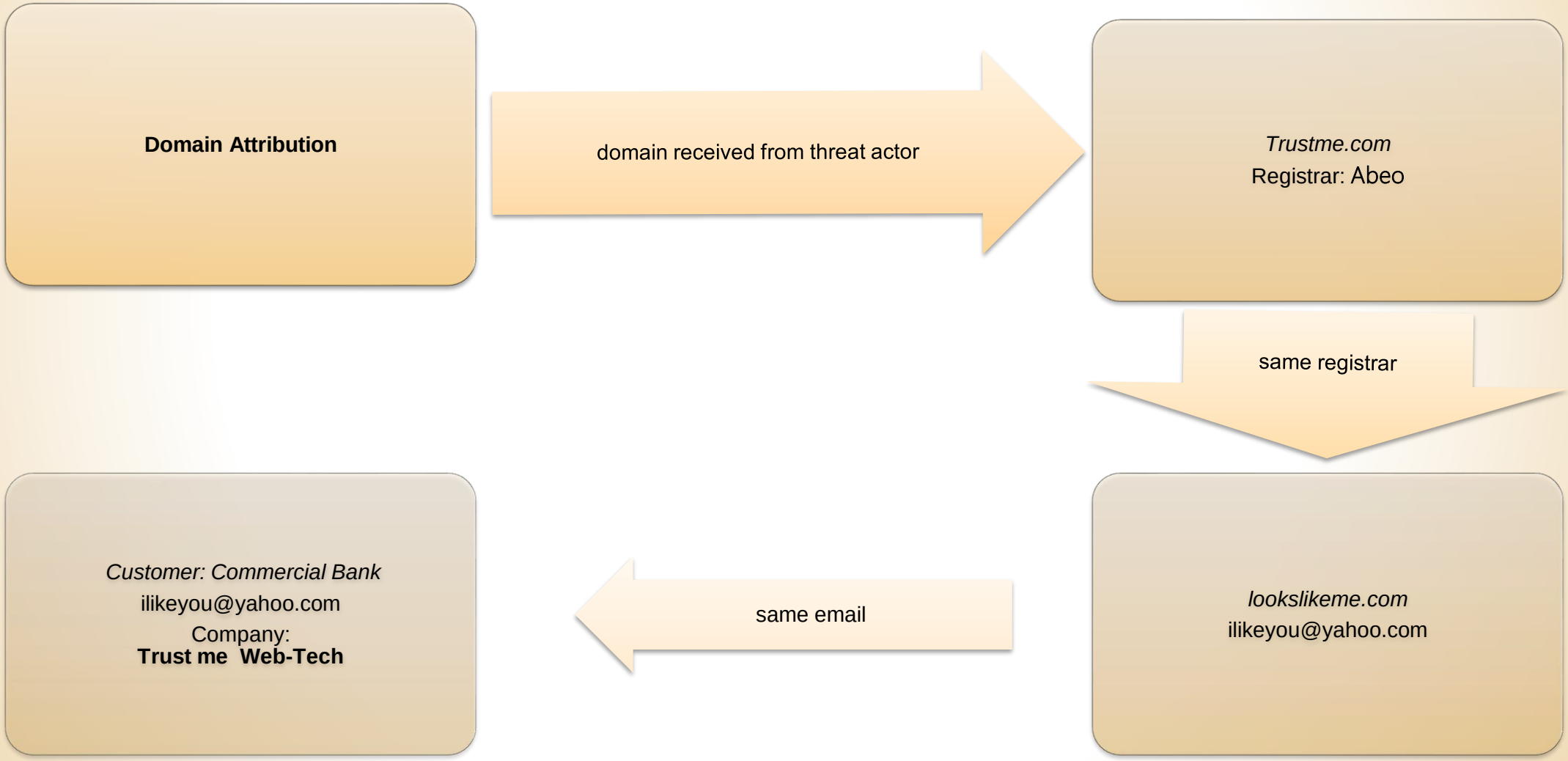
- Establishing direct contact with presumed actor using several avatars, creating trust relationship, data collection
- **Data fusion and analysis of the collected data of this campaign (emails, addresses, name, domains)**
- Contact is established in the Clearnet, mapping the cyber gang actors
- Contacts with CERT IL, European bank, Law enforcement agencies, neutralization

Threat Actors' Details	
Trust me Web-Tech	• https://www.facebook.com/pages/Trust meWeb-Tech/849221142932317
Trust me.com	• https://www.facebook.com/pages/trustme-IT-product-FH/73762938532387 • Trust me.org • Trust me.net
Abeo Okafor	• Nigerian male in his 40s, Lives in Lagos City, Nigeria. • Studied Computer Sciences at *University of Lago* (UNILAG). • Abeo expertise is in the web hosting / domains registration field • DOB: March 14, 1976 • Phone #: +234 909 749 2387 • https://twitter.com/abeo • https://www.facebook.com/abokafor • Personal email: abeo.okafor@Yahoo.com
Bako Eze CTO at *Trustme.com*	• Skype: bako. eze327 • https://twitter.com/bakoeze2889 • Mail: bako.eze3776@gmail.com • https://www.facebook.com/bako.eze3776 • Avatar name: Champion
M**aria Awa** (Finance)	• 34 Canal Street, Manchester M2 4NH. United Kingdom https://www.facebook.com/maria.awa • https://twitter.com/mariaawa36 • https://www.instagram.com/hindimaria5

“Baobab” operation phase 2 : Phishing campaigns

“BAOBAB” gang Associated Phishing Campaigns			
Fake Site	**Legitimate Site**	**Comment**	**Threat Actor Details**
online-lloyed.net	lloydsbank.com (US)	ACTIVE	abeo.okafor@Yahoo.com
Baobab	**Baobab**	**INACTIVE**	abeo.okafor@Yahoo.com
ABM Amroo.com	ABN Amro.com	ACTIVE	bako.eze3776@gmail.com
Online.Banking.CITI.org	Citi.com	INACTIVE	abeo.okafor@Yahoo.com
BMP Paribass.com.sg	BNP Paribas.com.sg	INACTIVE	bako.eze3776@gmail.com
onlinecitibike.com, citi-bankos.net	online.citi.com (EU)	INACTIVE	bako.eze3776@gmail.com

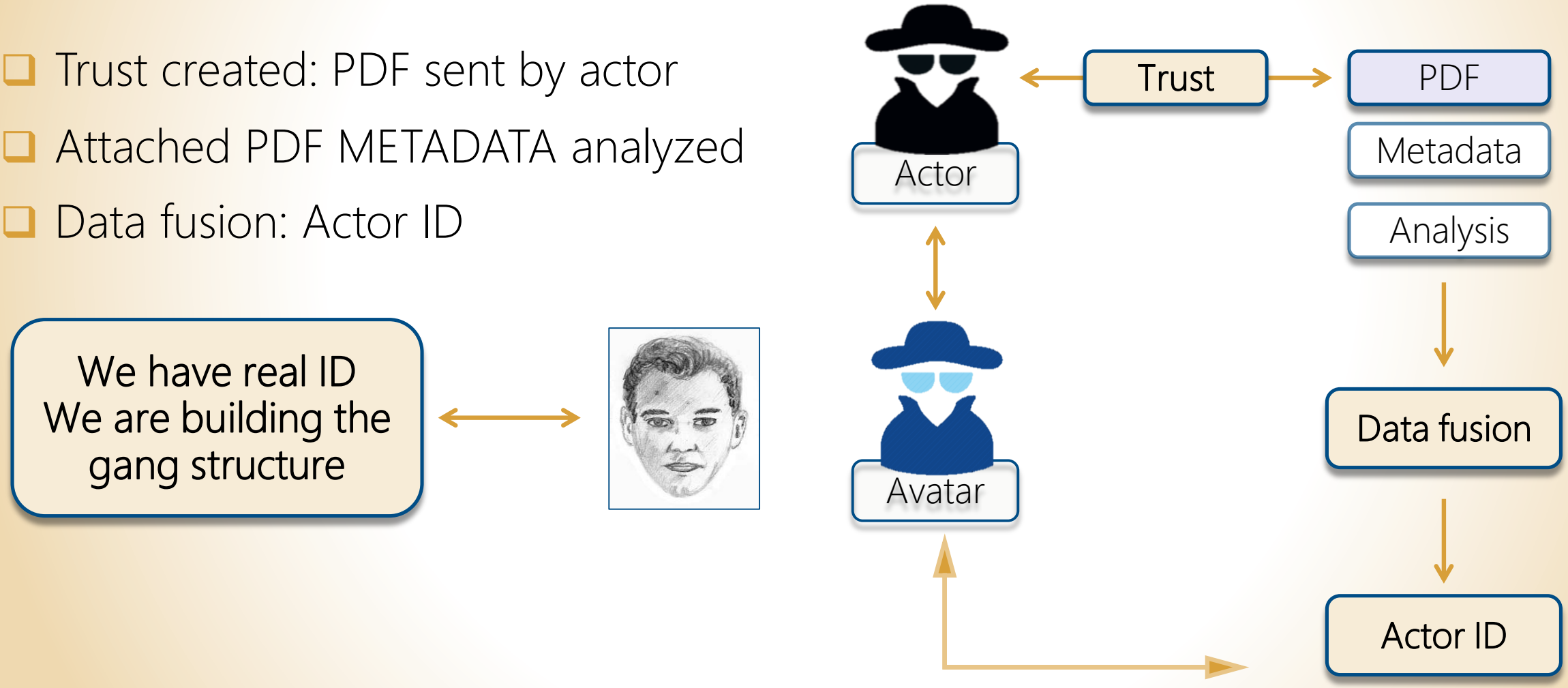
“Baobab” operation phase 2 : Domain attribution



CYBER CUPULA

"Baobab" operation phase 2: Data fusion & analysis

- Trust created: PDF sent by actor
- Attached PDF METADATA analyzed
- Data fusion: Actor ID

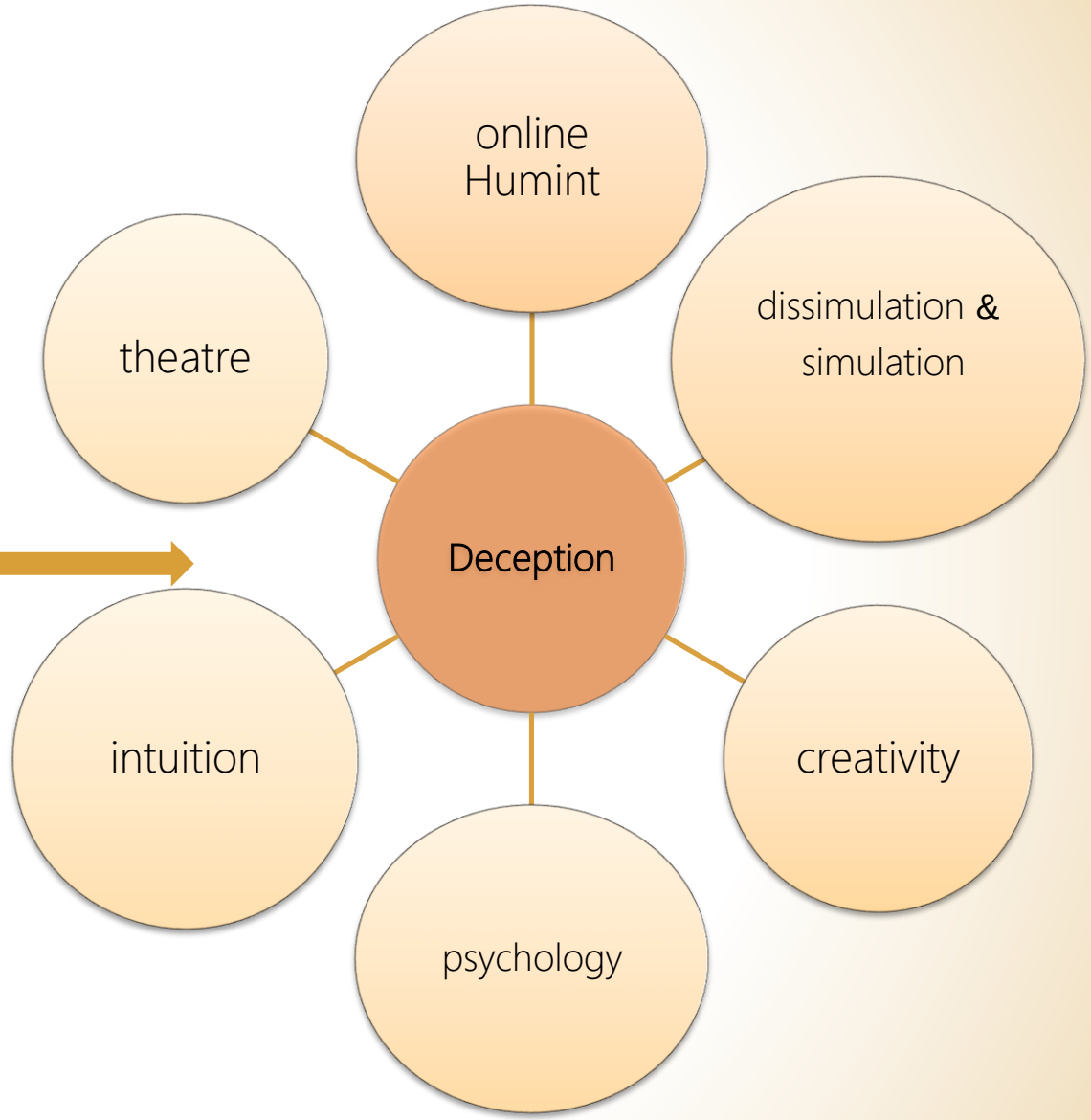


"Baobab" operation - the 4 phases

- Establishing direct contact with presumed actor using several avatars, creating trust relationship, data collection
- Data fusion and analysis of the collected data of this campaign (emails, addresses, name, domains)
- **Contact is established in the Clearnet, mapping the cyber gang actors**
- Contacts with CERT IL, European bank, Law enforcement agencies, neutralization

Cyber Humint deception: few words on this….

Trust and dependency

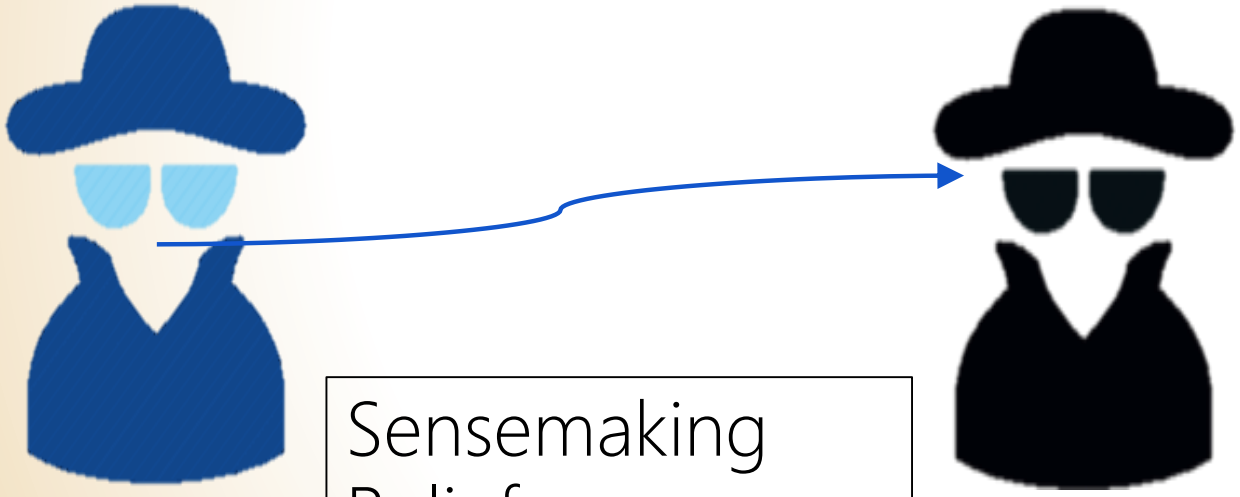


CYBER CUPULA

Deception: using human psychology

undercover AVATAR

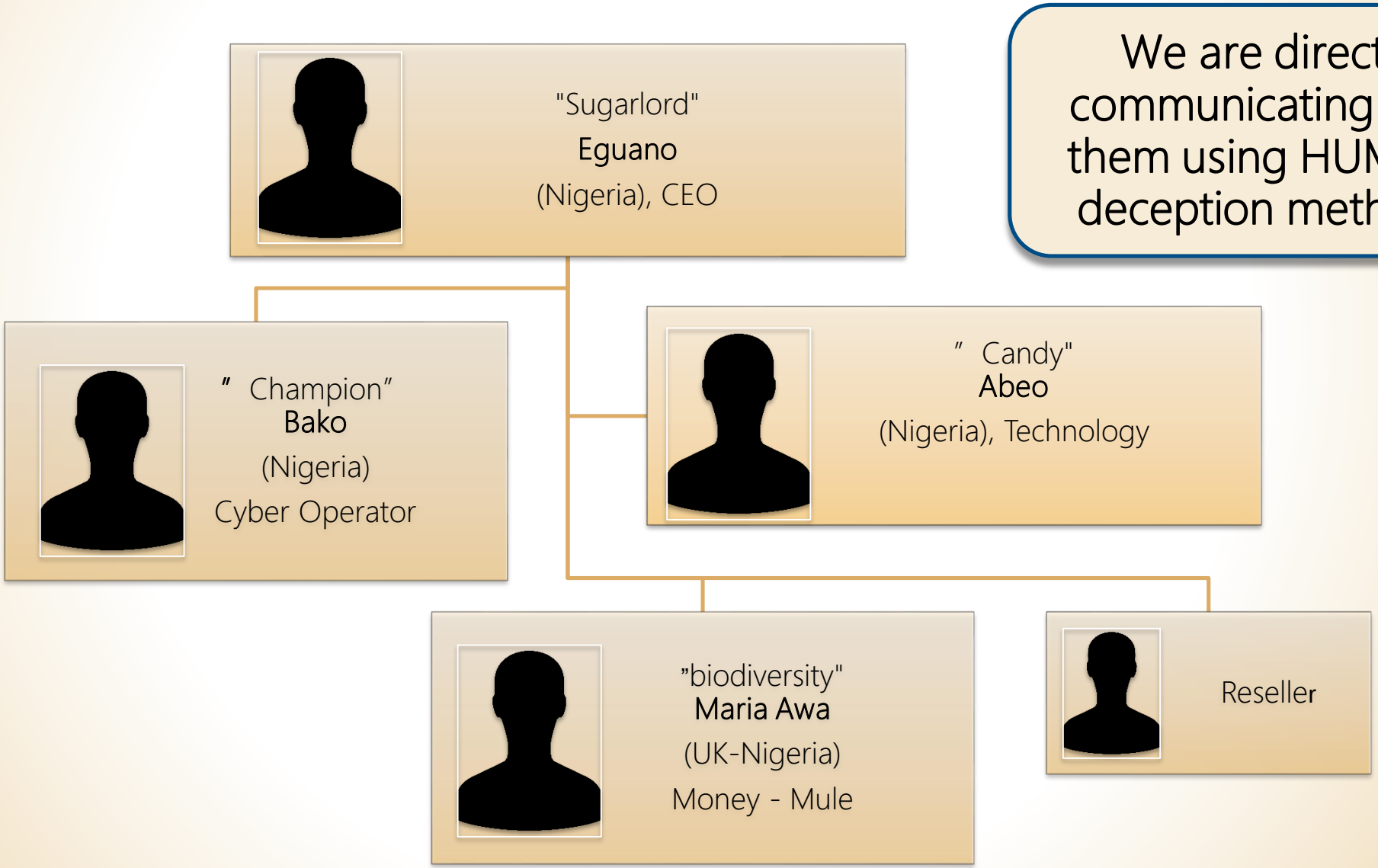
Cybercriminal in Africa



Sensemaking
Beliefs
Emotions
fears

"Baobab" operation phase 3: cyber gang structure

We are directly communicating with them using HUMINT deception methods



"Baobab" operation - the 4 phases

- Establishing direct contact with presumed actor using several avatars, creating trust relationship, data collection
- Data fusion and analysis of the collected data of this campaign (emails, addresses, name, domains)
- Contact is established in the Clearnet, mapping the cyber gang actors
- Contacts with CERT IL, European bank, Law enforcement agencies, neutralization

Last mile: follow the money

Bank Name - UK Bank

Bank Address - 155 circle Rd, Manchester, M2 4DU, United Kingdom.

Account Name – Maria Awa

Account No – 42993359

Sort Code - 8828

SWIFT Code: ABCDEK34H18

IBAN: GB67 ABCD 6934 9376 3728 84

Beneficiary Address - 34 Canal Street, Manchester M2 4NH. United Kingdom

Like in the war on terrorism – this is very efficient

The Art of War, Sun Tzu*

- "All warfare is based on deception. Hence, when we are able to attack, we must seem unable;…
- "If you know the enemy and know yourself, you need not fear the result of hundred battles…"
- "The supreme art of war is to subdue the enemy without fighting."

*Chinese military strategist, Master Sun, 5th century BC