

DeepSec 2016

Social Engineering...



DEEPSEC

DeepSec 2016

Social Engineering...



DEEPSEC

Social Engineering by Dominique C. Brack

Introduction
Security
(Information
Security) Stuff

2-day
is
About
U
not
me

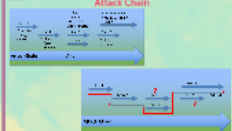
Sounds a bit like a whatsapp breakup :-)

`chmod -R 755 /humanroot`
Human
in
debug mode

How?



Attack Chain



Introduction

Security

(Infor^m~~r~~nation

Security) Stuff

Speak
Write
Publish

Politicize
Volunteer
Mentor

Hack & research and experiment

2-day

is

About

not

me

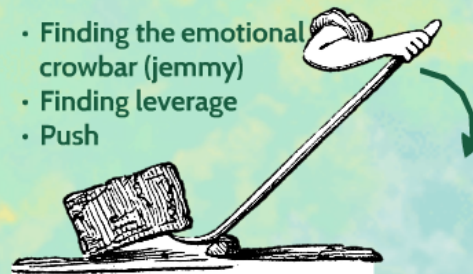
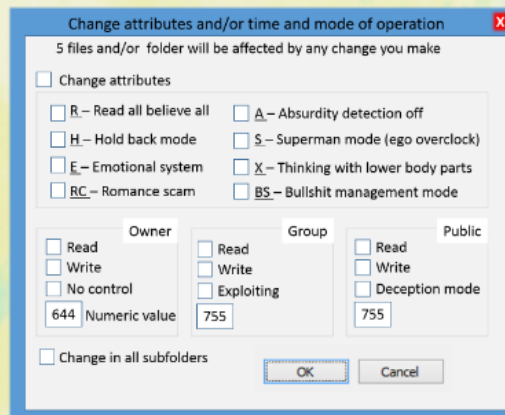
Sounds a bit like a whatsapp breakup ;-)

```
chmod -R 755 /humanroot
```

Human

in

debug mode



Change attributes and/or time and mode of operation



5 files and/or folder will be affected by any change you make

Change attributes

R – Read all believe all

A – Absurdity detection off

H – Hold back mode

S – Superman mode (ego overclock)

E – Emotional system

X – Thinking with lower body parts

RC – Romance scam

BS – Bullshit management mode

Owner

Read

Write

No control

Numeric value

Group

Read

Write

Exploiting

Public

Read

Write

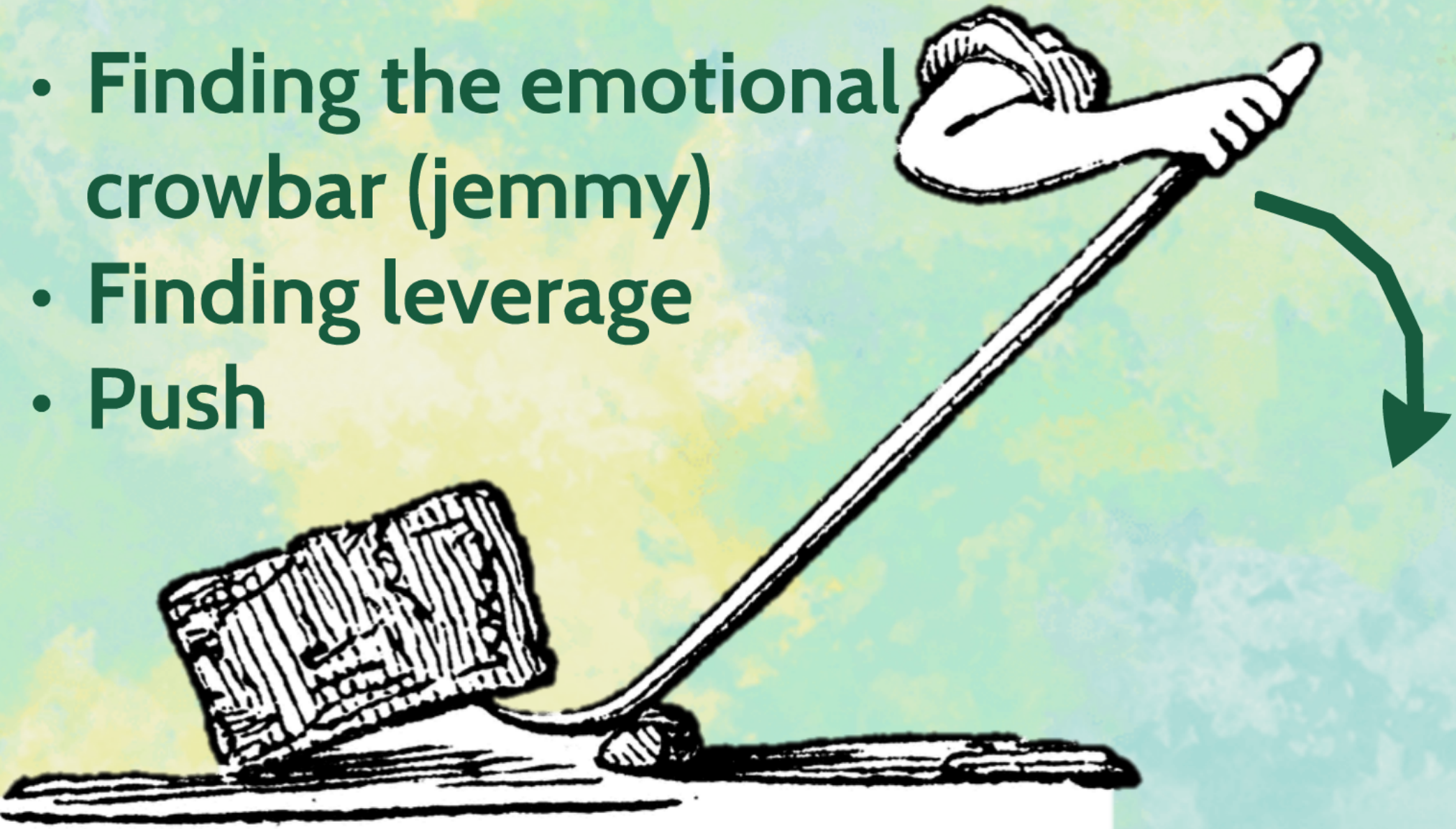
Deception mode

Change in all subfolders

OK

Cancel

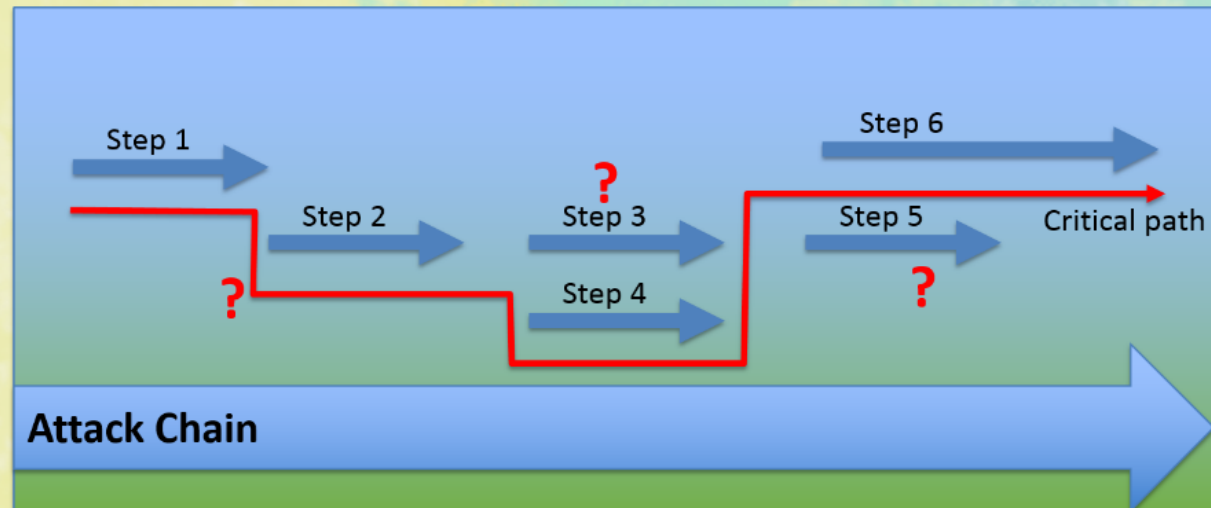
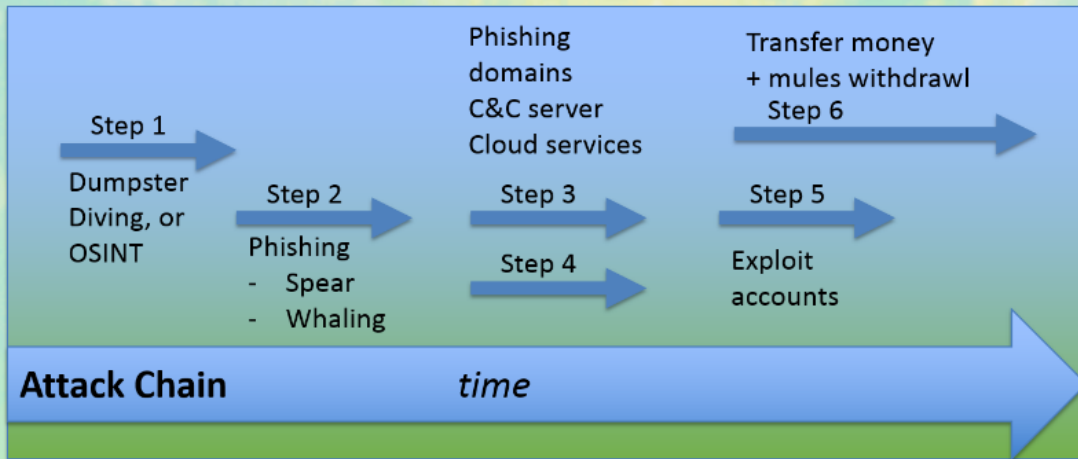
- Finding the emotional crowbar (jemmy)
- Finding leverage
- Push



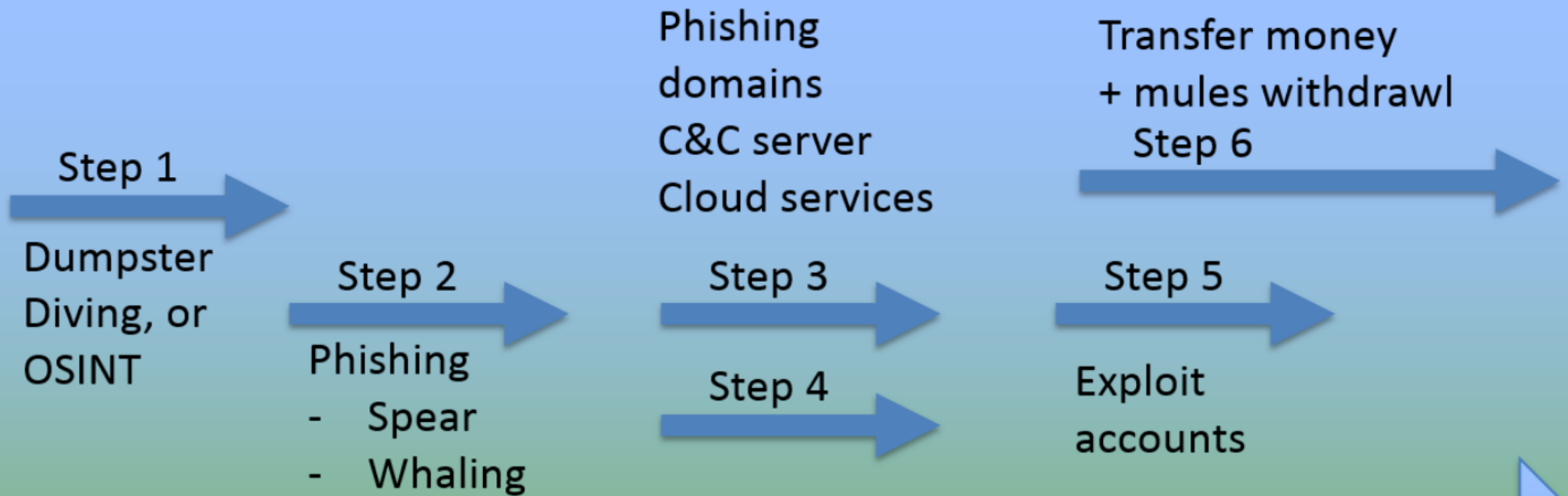
How?



Attack Chain



Attack Chain

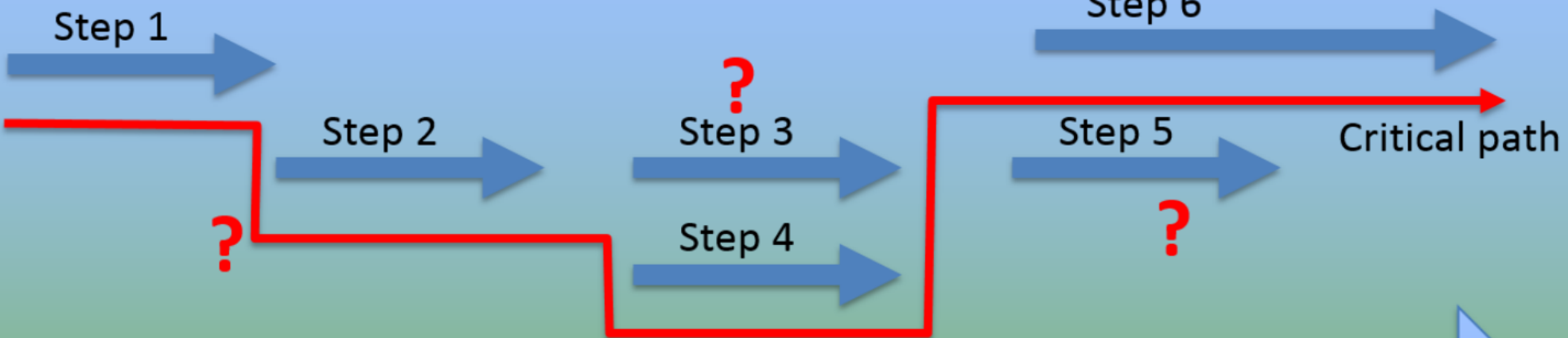


Attack Chain

time

Step 1

accounts



Attack Chain

Social Engineering Engagement Framework - SEEF

You will get the
free ebook and
the Icons too!



Structure and method for SE



**"THE ELICITATION OF
INFORMATION FROM
SYSTEMS, NETWORKS OR
HUMAN BEINGS
THROUGH METHODS
AND TOOLS"**

SEEF definition of Social Engineering

Topics:

- SEEF Engagement Management
- Governance, Risk and Compliance and ++
- Intensity Levels
- Approach Selection Method (ASM)
- Attack Vector Development (AVD)
- Interpersonal Distance (Concept of space)



"THE
INFO
SYST
HUM
THRO
AND



20'000 feet



6 feet

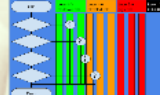
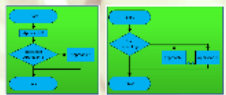
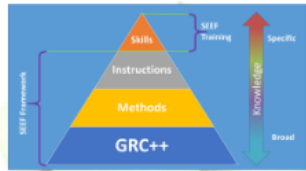
Beware of motion sickness from sudden altitude changes.



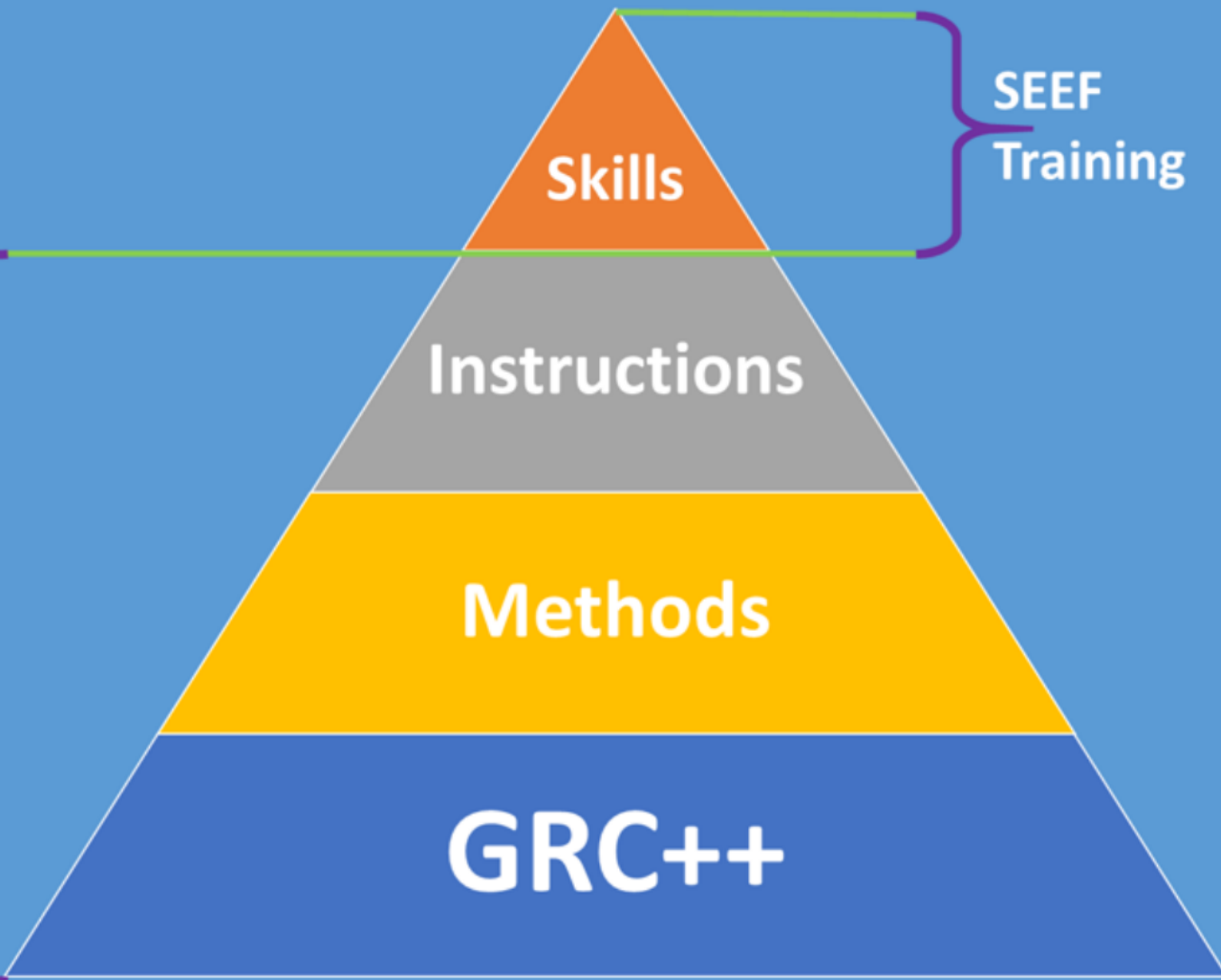
Those topics didn't made the cut.

- SEEF Framework
- SEEF Engagement Management
- Governance, Risk and Compliance (++)
- Approach Selection Method (ASM) & Approach Modelling

For completeness I will speed-present them to you... 30sec each.



SEEF Framework

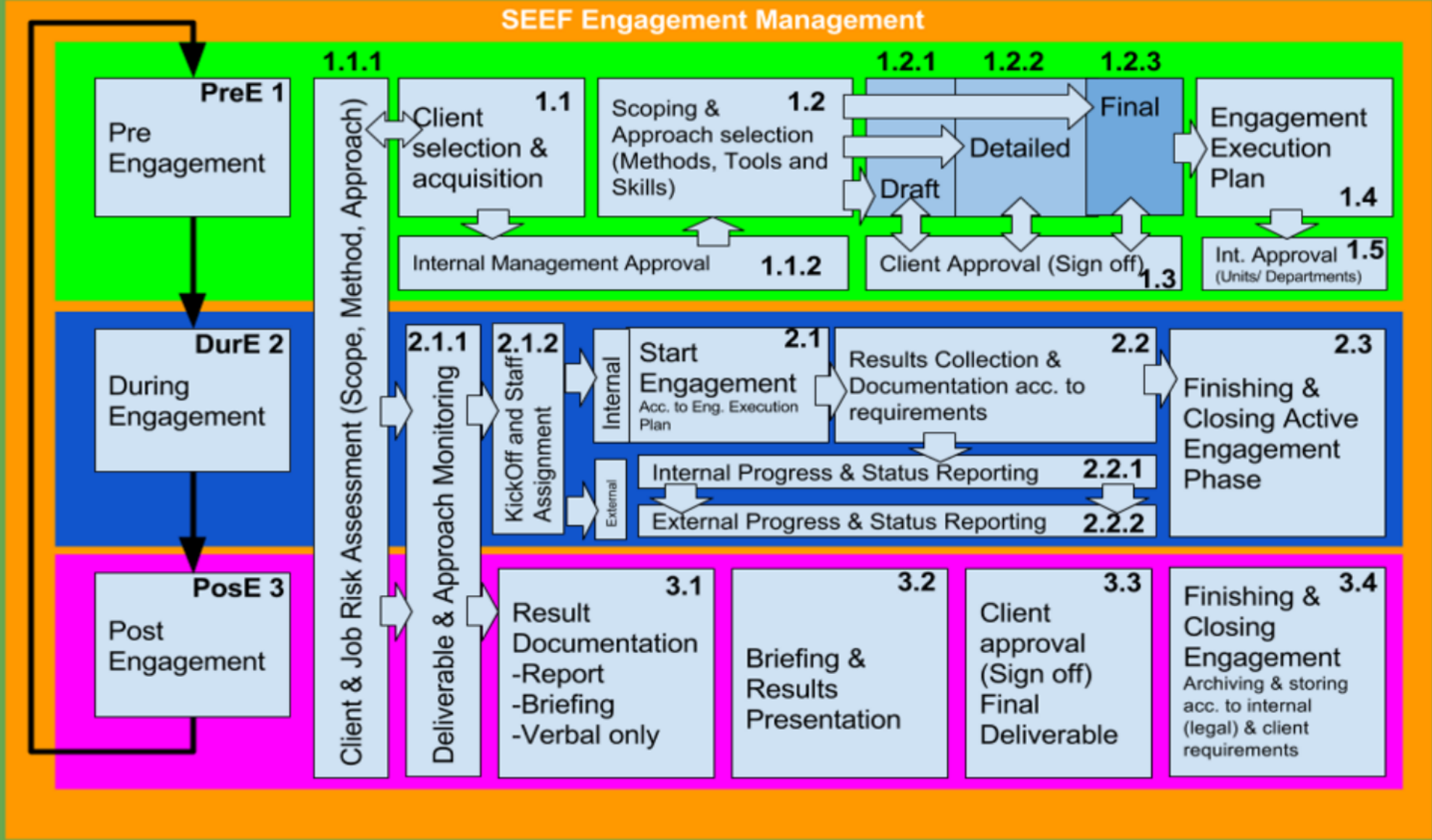


Start

Level 1-3
moderate risk

Level 4-6
elevated risk

Start



Governance, Risk and Compliance (GRC) ++

Governance

Risk
Management

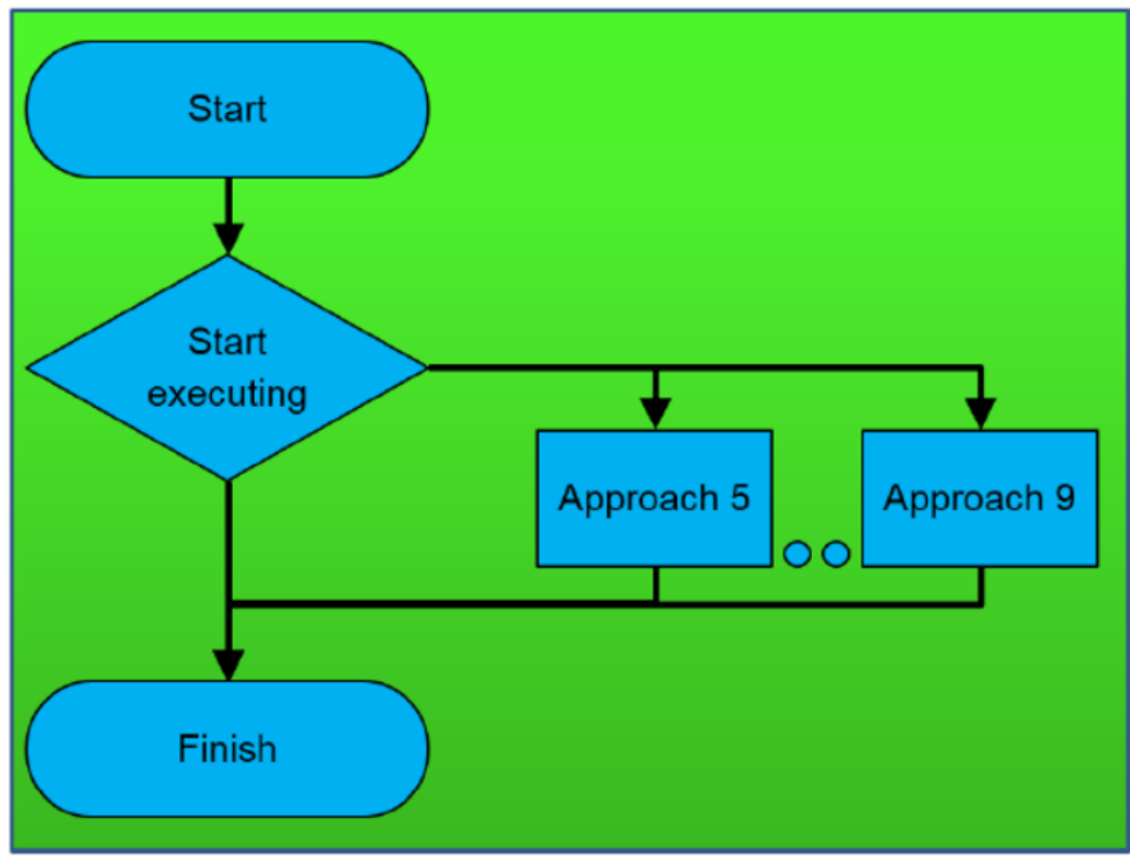
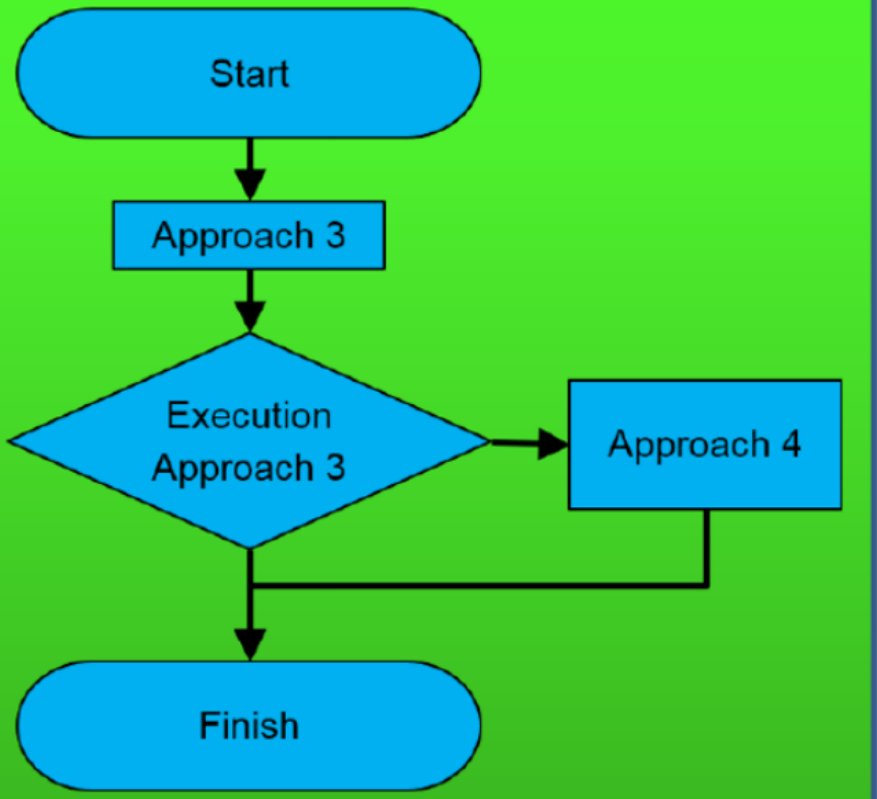
Compliance

Intensity
Levels

Engagement
Management

Ethics

Culture



Start

Level 1-3
moderate risk

Level 4-6
elevated risk

Level 7-9
high risk

Level 10-12
do not engage



A
1



A
2

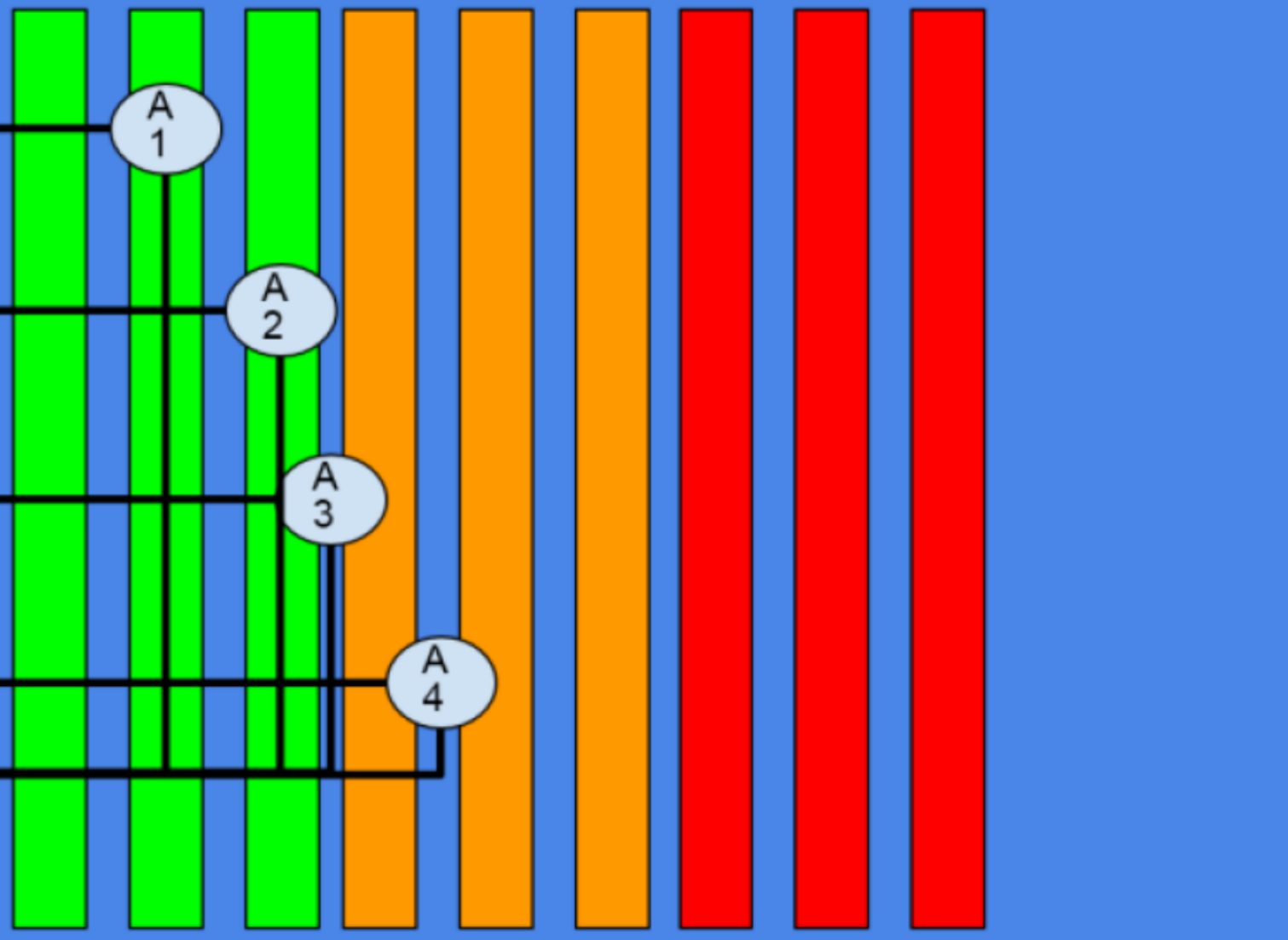


A
3



A
4

Finish



Intensity Levels

Level	Risk Appetite, Possible Consequences and Techniques used
1	Legal, non-invasive, OSINT
2	simple, local or national, standard corporation
3	preservation of person/ company integrity
4	Invasive, intrusive, medium complexity, international, well known corporation
5	Ethically questionable
6	Occasional risk of illegal (misdemeanours) activity, legal implications not known entirely
7	Invasive, intrusive, highly complex, international, high profile political or medially present organization,
8	Coercion, unethical, risk of collateral damages
9	Illegal (felonies), active crime, bodily harm
10-12	Highly illegal, treason, breach of international law, possible death sentence, cyber warfare, industrial espionage, cost of lives

Level	Risk Appetite, consequences	Signoff, approval, comment
1	Legal, non-invasive, OSINT	Engineer or specialist on the engagement can execute assigned tasks on his own after his tasks have been released for execution. Use own staff. Simple tasks i.e. OSINT can be outsourced. Risk to be assessed by engagement manager.
2	simple, local or national, standard corporation	
3	preservation of person/ company integrity	Tasks have to be signed off by the responsible project manager of the engagement. Risks have to be mitigated or respective assurances collected. Official formal sign off by the client management. Definition of a contingency plan. Instruct team about identified risks. Compartmentalize tasks and split risk. Only Senior resources. Constant monitoring of status and progress. Legal advice required and mandatory. Engagement to be approved by two company directors.
4	Invasive, intrusive, medium complexity, international, well known corporation	
5	Ethically questionable	
6	Occasional risk of illegal (misdemeanours) activity, legal implications not known entirely	
7	Invasive, intrusive, highly complex, international, high profile political or medially present organization,	
8	Coercion, unethical, risk of collateral damages	
9	Illegal (felonies), active crime, bodily harm	
10-12	Highly illegal, treason, breach of international law, possible death sentence, cyber warfare, industrial espionage, cost of lives	DO NOT ENGAGE! DO NOT ENGAGE! DO NOT ENGAGE!

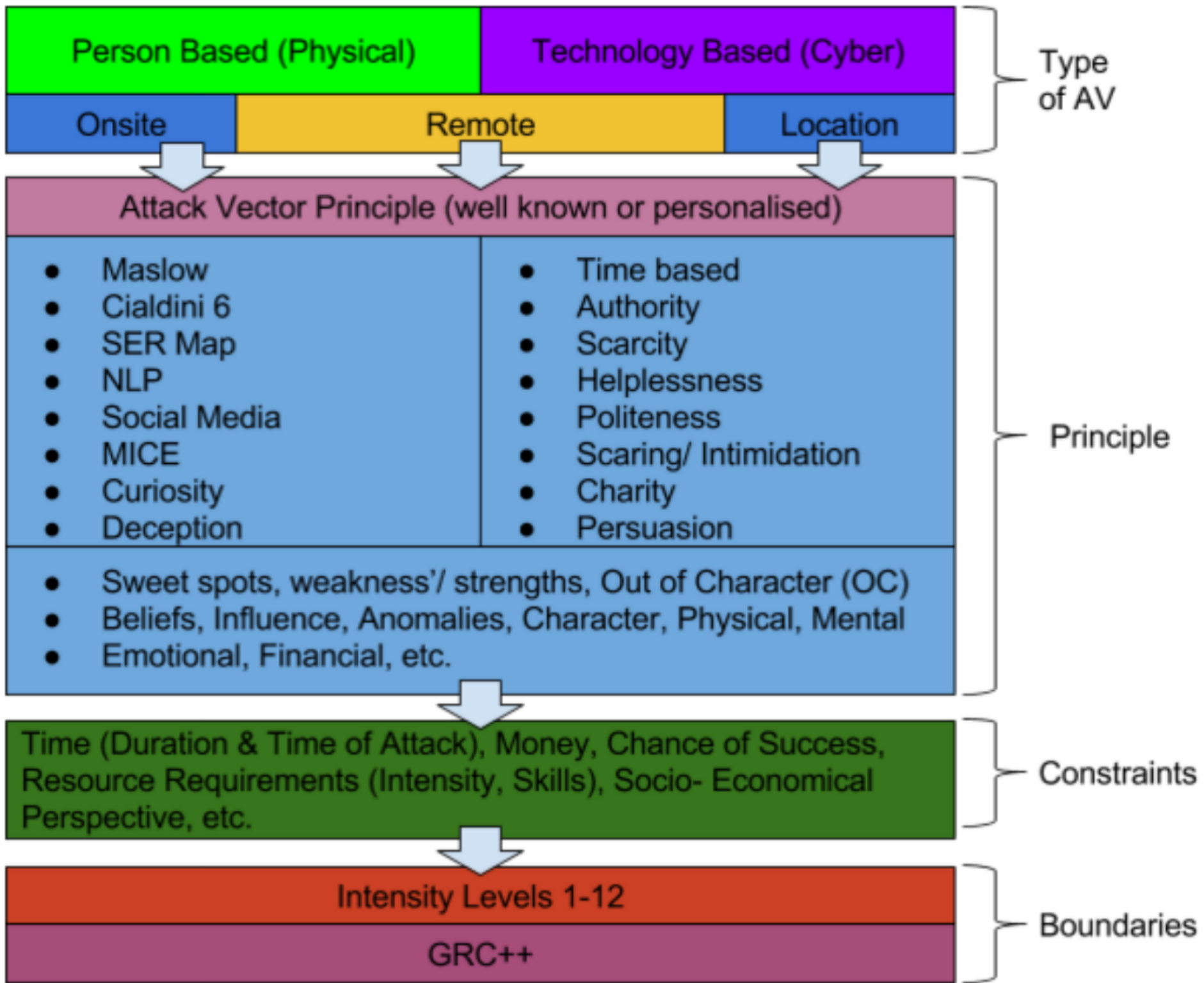
Level	Risk Appetite, Possible Consequences and Techniques used
1	Legal, non-invasive, OSINT
2	simple, local or national, standard corporation
3	preservation of person/ company integrity
4	Invasive, intrusive, medium complexity, international, well known corporation
5	Ethically questionable
6	Occasional risk of Illegal (misdemeanours) activity, legal implications not known entirely
7	Invasive, intrusive, highly complex, international, high profile political or medially present organization,
8	Coercion, unethical, risk of collateral damages
9	Illegal (felonies), active crime, bodily harm
10-12	Highly illegal, treason, breach of international law, possible death sentence, cyber warfare, industrial espionage, cost of lives

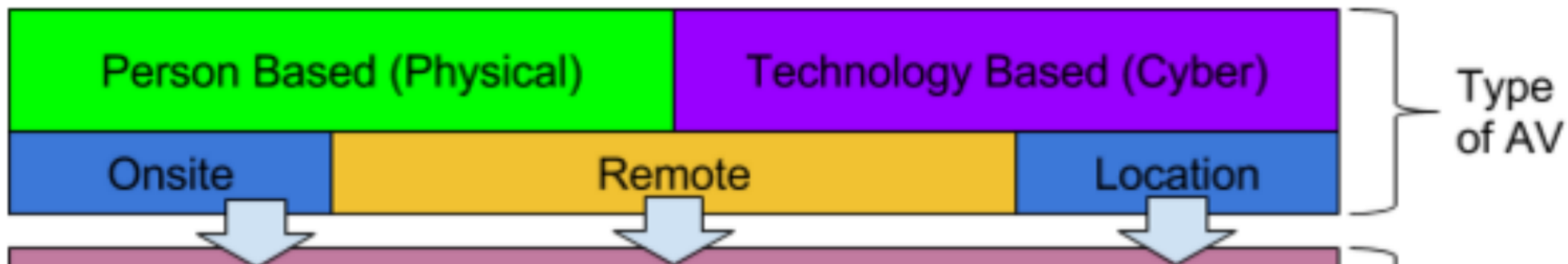
Level	Risk Appetite, consequences	Signoff, approval, comment
1	Legal, non-invasive, OSINT	Engineer or specialist on the engagement can execute assigned tasks on his own after his tasks have been released for execution. Use own staff. Simple tasks i.e. OSINT can be outsourced. Risk to be assessed by engagement manager.
2	simple, local or national, standard corporation	
3	preservation of person/ company integrity	
4	Invasive, intrusive, medium complexity, international, well known corporation	Tasks have to be signed off by the responsible project manager of the engagement. Risks have to be mitigated or respective assurances collected. Official formal sign off by the client management. Definition of a contingency plan. Instruct team about identified risks. Compartmentalize tasks and split risk. Only Senior resources. Constant monitoring of status and progress. Legal advice required and mandatory. Engagement to be approved by two company directors.
5	Ethically questionable	
6	Occasional risk of Illegal (misdemeanours) activity, legal implications not known entirely	
7	Invasive, intrusive, highly complex, international, high profile political or medially present organization,	If during the engagement you have been reached higher levels try to mitigate immediately to acceptable levels. Stop continuation of risk loaded tasks. Immediately stop the engagement. Offer active support to investigating authorities. Obligation to report discovered crime. Compartmentalize engagement from company resources. Use of outsourcing contracts for execution.
8	Coercion, unethical, risk of collateral damages	
9	Illegal (felonies), active crime, bodily harm	
10-12	Highly illegal, treason, breach of international law, possible death sentence, cyber warfare, industrial espionage, cost of lives	DO NOT ENGAGE! DO NOT ENGAGE! DO NOT ENGAGE!

Attack Vector Development (AVD)

Anything can (and will)
be used as an attack
vector (AV) against you!

You have the right to use no
consultant. If you cannot afford a
consultant, one will be provided
for you at exorbitant costs.
- faithfully yours skills shortage





Attack Vector Principle (well known or personalised)

- Maslow
- Cialdini 6
- SER Map
- NLP
- Social Media
- MICE
- Curiosity
- Deception

- Time based
- Authority
- Scarcity
- Helplessness
- Politeness
- Scaring/ Intimidation
- Charity
- Persuasion

- Sweet spots, weakness'/ strengths, Out of Character (OC)
- Beliefs, Influence, Anomalies, Character, Physical, Mental
- Emotional, Financial, etc.

Principle

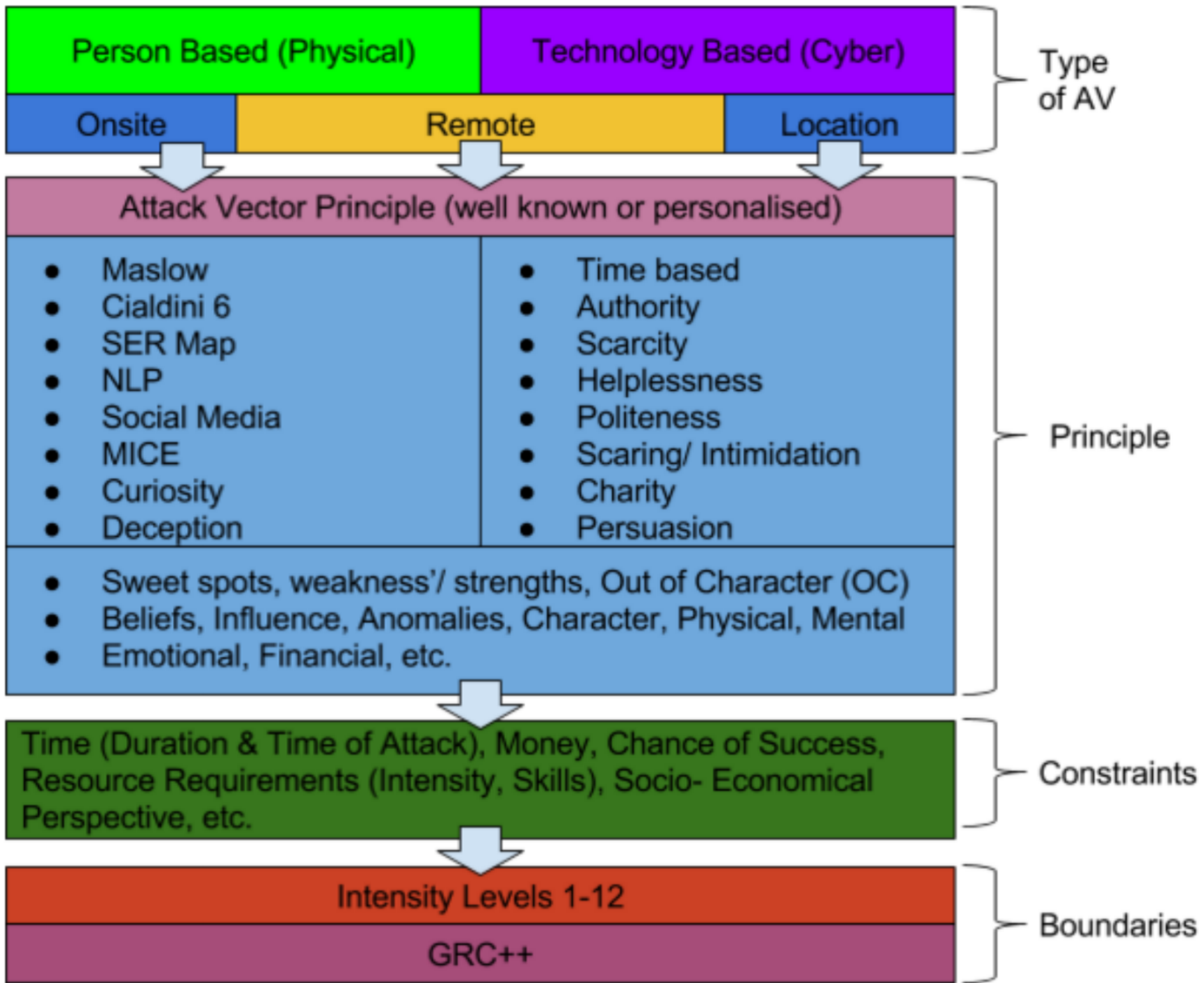
Time (Duration & Time of Attack), Money, Chance of Success, Resource Requirements (Intensity, Skills), Socio- Economical Perspective, etc.

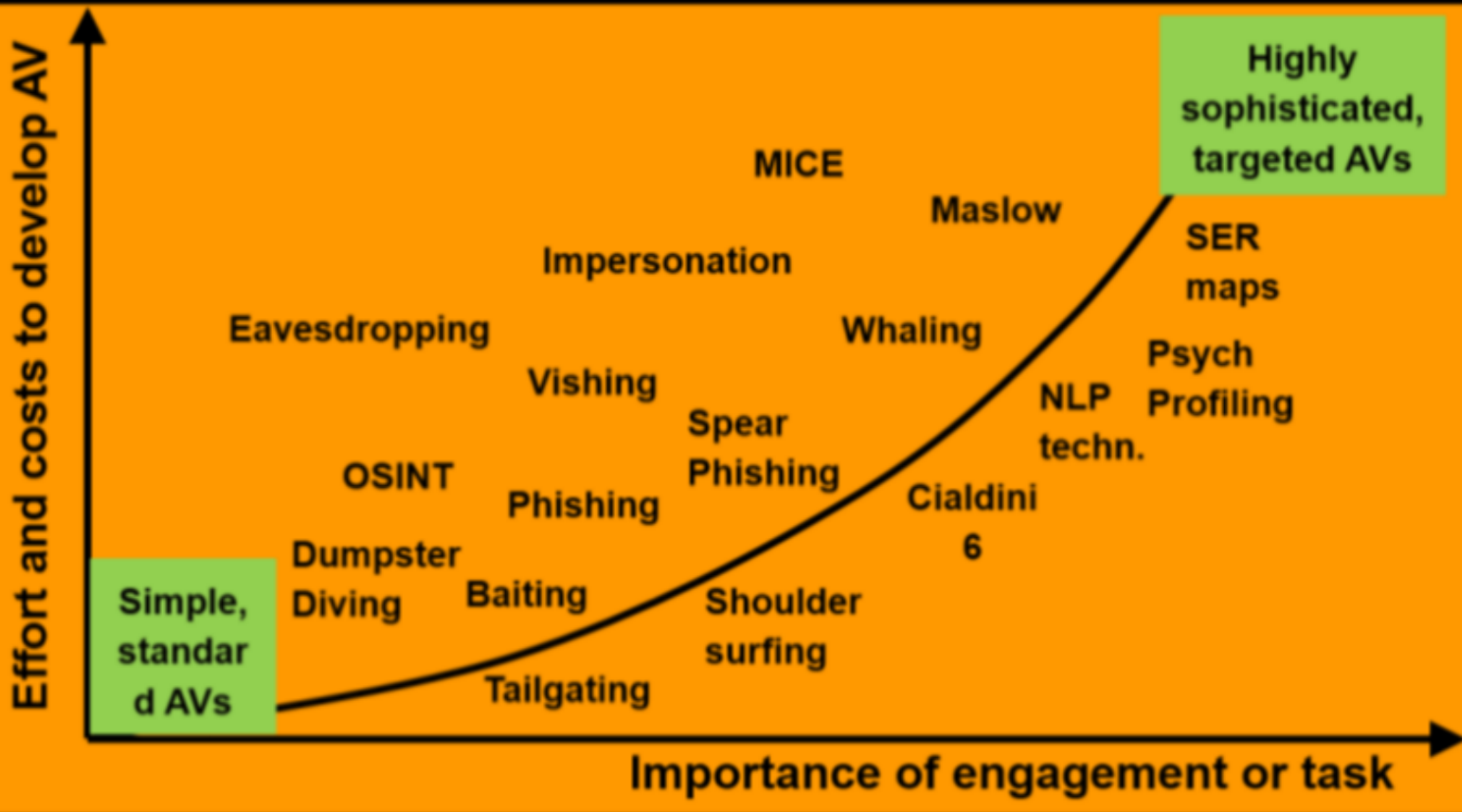
Constraints

Intensity Levels 1-12

GRC++

Boundaries







you gotta dig bick.
you that read wrong.

You read that wrong too...

I got a pet wussy.
you that read wrong.

You read that wrong too...

S

D

I

K

U

C

M

Y



Depending on what you have been reading you should seriously consider additional testing.

For example based on the Rorschach Inkblot test.

What do you C here?

How does this make you feel?

Going back to normal... Standard AV examples

Phishing

Tactics and Experience

PHISHME ≠ Phishermen

is not the same (obviously)

Spearphishing

Whaling

Phishing Tactics

- Ask how well they know you
- Ask how they got your info
- Ask how they got your info
- Ask how they got your info
- Ask how they got your info
- Ask how they got your info

Tailgating

Description: Tailgating is when an employee opens a door and then holds it open for others who are following him. This could include visitors without badges, tech personnel with spare parts or the passive acceptance of a uniformed worker. It can also occur covertly when a person waits after the door has been opened by a legitimate employee and then slips in or blocks the door just before the door closes.

Intensity Level: Tailgating can be done within acceptable intensity levels (green, levels 1-5) if specified rules are followed. Tailgating can be done within acceptable intensity levels (green, levels 1-3) if specified rules are followed, which only include working on politeness and speed without coercion, forcing entry or the stealing of access cards or credentials.

GRC++: The "tailgater" requires crystal clear instructions about the behavior and boundaries he or she is expected to act in. There must be instructions about how, when and to whom the identity will be revealed. This could be planned as an open book exercise with the knowledge of the client and security staff. Or a closed book exercise with no more informed beforehand.

Eavesdropping

Description: Eavesdropping is secretly listening to the verbal or digital communication of others through wiretapping or the interception of e-mail and cell phone calls.

Intensity Level: Eavesdropping can be done within acceptable intensity levels (green, levels 1-3) if rules are followed. Wiretapping is very delicate and can easily reach intensity levels 6 and above.

GRC++: Federal law allows recording of phone calls and other electronic communications with the consent of at least one party to the call. Twelve states, including California, require the consent of all parties to the call under most circumstances.



Eavesdropping

Description: Eavesdropping is secretly listening to the verbal or digital communication of others through wiretapping or the interception of e-mail and cell phone calls.

Intensity Level: Eavesdropping can be done within acceptable intensity levels (green, levels 1-3) if rules are followed.

Wiretapping is very delicate and can easily reach intensity levels 6 and above.

GRC++: Federal law allows recording of phone calls and other electronic communications with the consent of at least one party to the call. Twelve states, including California, require the consent of all parties to the call under most circumstances.



Tailgating

Description: Tailgating is when an employee opens a door and then holds it open for others who are following him. This could include visitors without badges, tech personnel with spare parts or the passive acceptance of a uniformed worker. It can also occur covertly when a person waits after the door has been opened by a legitimate employee and then slips in or blocks the door just before the door closes.

Intensity Level: Tailgating can be done within acceptable intensity levels (green, levels 1-3) if specified rules are followed. Tailgating can be done within acceptable intensity levels (green, levels 1-3) if specified rules are followed, which only include working on politeness and speed without coercion, forcing entry or the stealing of access cards or credentials.

GRC++: The “tailgatee” requires crystal-clear instructions about the behavior and boundaries he or she is expected to act in. There must be instructions about how, when and to whom the identity will be revealed. This could be planned as an open book exercise with the knowledge of the client and security staff. Or a closed book exercise with no one informed beforehand.



Phishing

Tactics and Experience

PHISHME

≠

phishrney

is not the
same
(obviously)



Spearfishing



Whaling



Facts & Figures

- We have >20'000 users
- We test monthly sending to blocks of -320 users
- 110 clicked on the link
- Only 16 reported the phishing email (me of course)
- First click after about 6 minutes
- Some clicked multiple times!!!

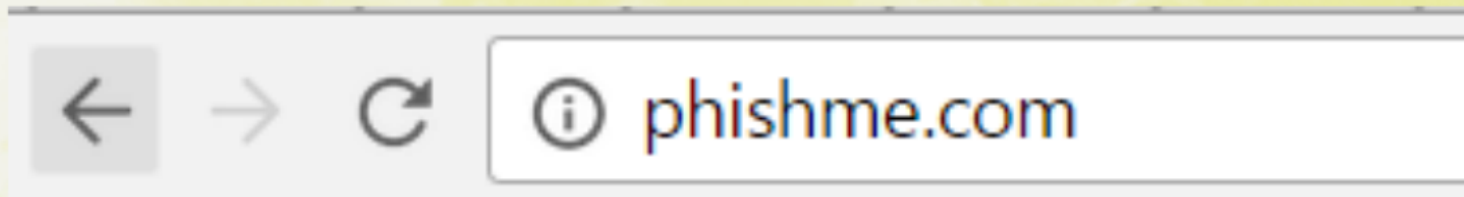


Tactics and Experience

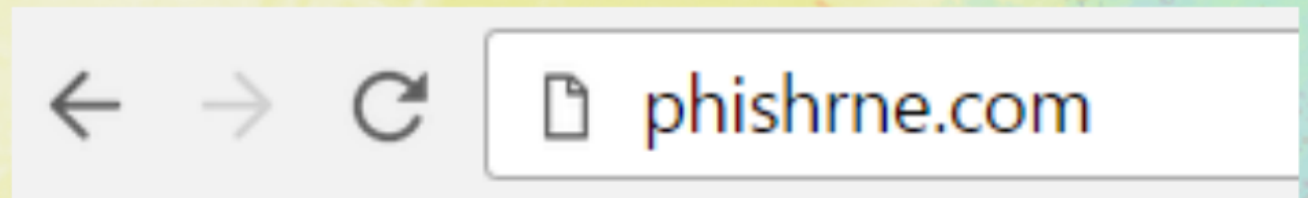
PHISHME



is not the
same
(obviously)



Wow very
the same



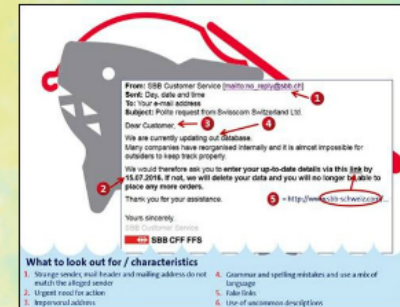
Homographic attack...
--> Shark eats little fish.

We used this technique
too for our phishing
campaigns.



Facts & Figures

- We have >20'000 users
- We test monthly sending to blocks of ~320 users
- 110 clicked on the link
- Only 16 reported the phishing email (me of course)
- First click after about 6 minutes
- Some clicked multiple times!!!





What to look out for / characteristics

1. Strange sender, mail header and mailing address do not match the alleged sender
2. Urgent need for action
3. Impersonal address
4. Grammar and spelling mistakes and use a mix of language
5. Fake links
6. Use of uncommon descriptions

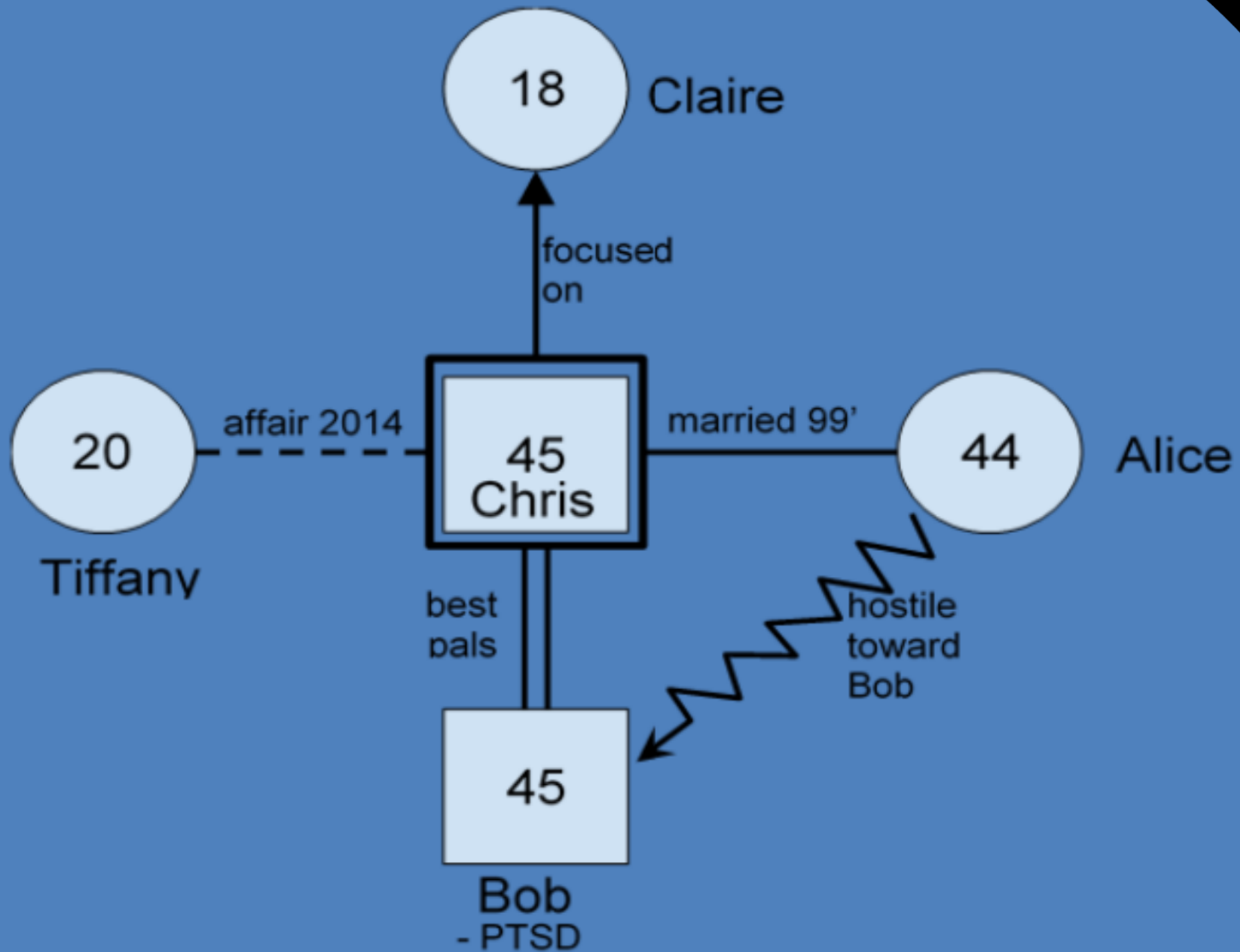
Advanced AV examples

- 1.) Pattern recognition
- 2.) Out of character (OC) behavior
- 3.) Emotionally loaded areas
- 4.) Incongruency in personal and business life
- 5.) Strong or highly developed areas
- 6.) Weak or underdeveloped areas

Social and emotional relationship (SER) map

Pattern recognition: Since Chris had an affair with 20-year-old Tiffany, in addition to the focus he shows toward 18-year-old Claire, there is a possible fixation on young women. Chris would eventually respond well to phishing emails with pictures of young girls and contact requests over social media based on young women.

Emotionally loaded areas: Alice, Chris' wife, is hostile toward Bob, Chris' best pal. Tiffany, Chris' affair from 2014, might hold a grudge against Chris and could act as an information repository. Bob could be used to gain information about Alice and ultimately about Chris.

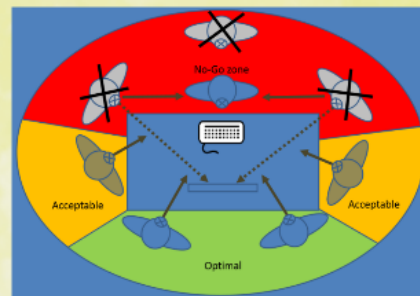
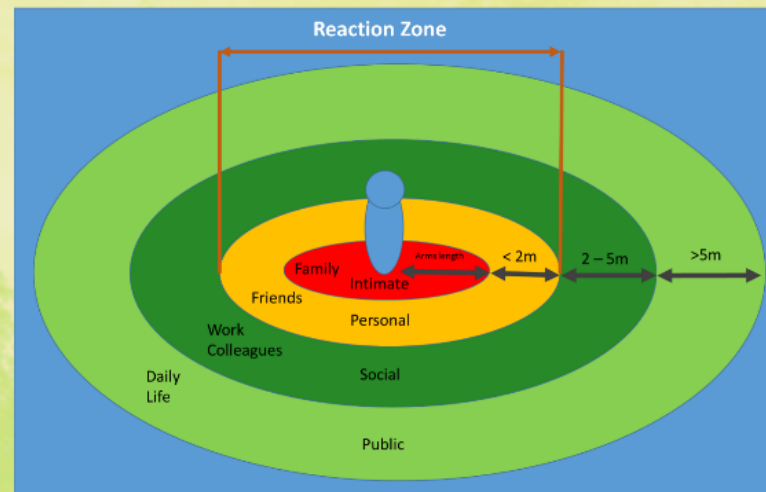


- 1.) Pattern recognition
- 2.) Out of character (OC) behavior
- 3.) Emotionally loaded areas
- 4.) Incongruency in personal and business life
- 5.) Strong or highly developed areas
- 6.) Weak or underdeveloped areas

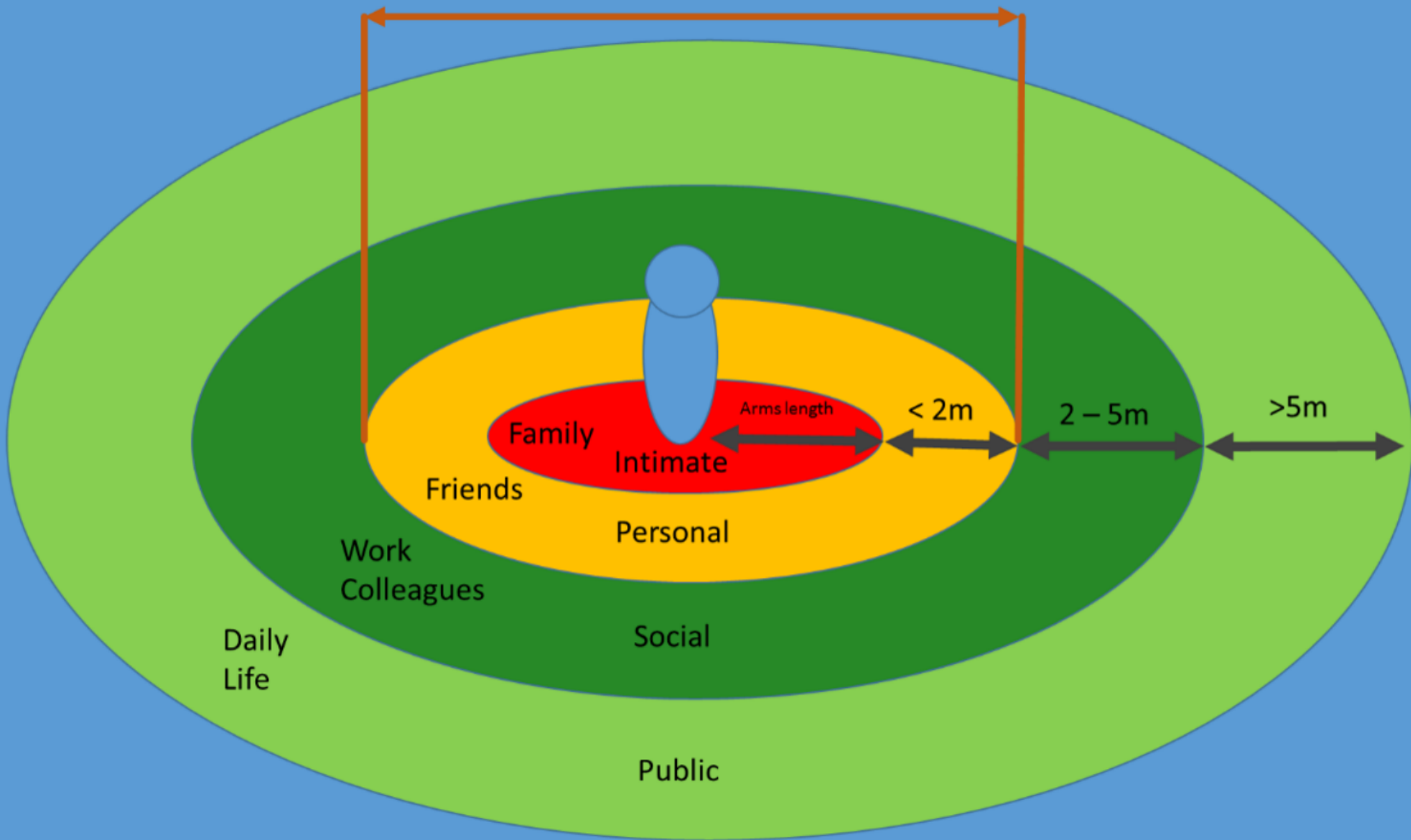
Pattern recognition: Since Chris had an affair with 20-year-old Tiffany, in addition to the focus he shows toward 18-year-old Claire, there is a possible fixation on young women. Chris would eventually respond well to phishing emails with pictures of young girls and contact requests over social media based on young women.

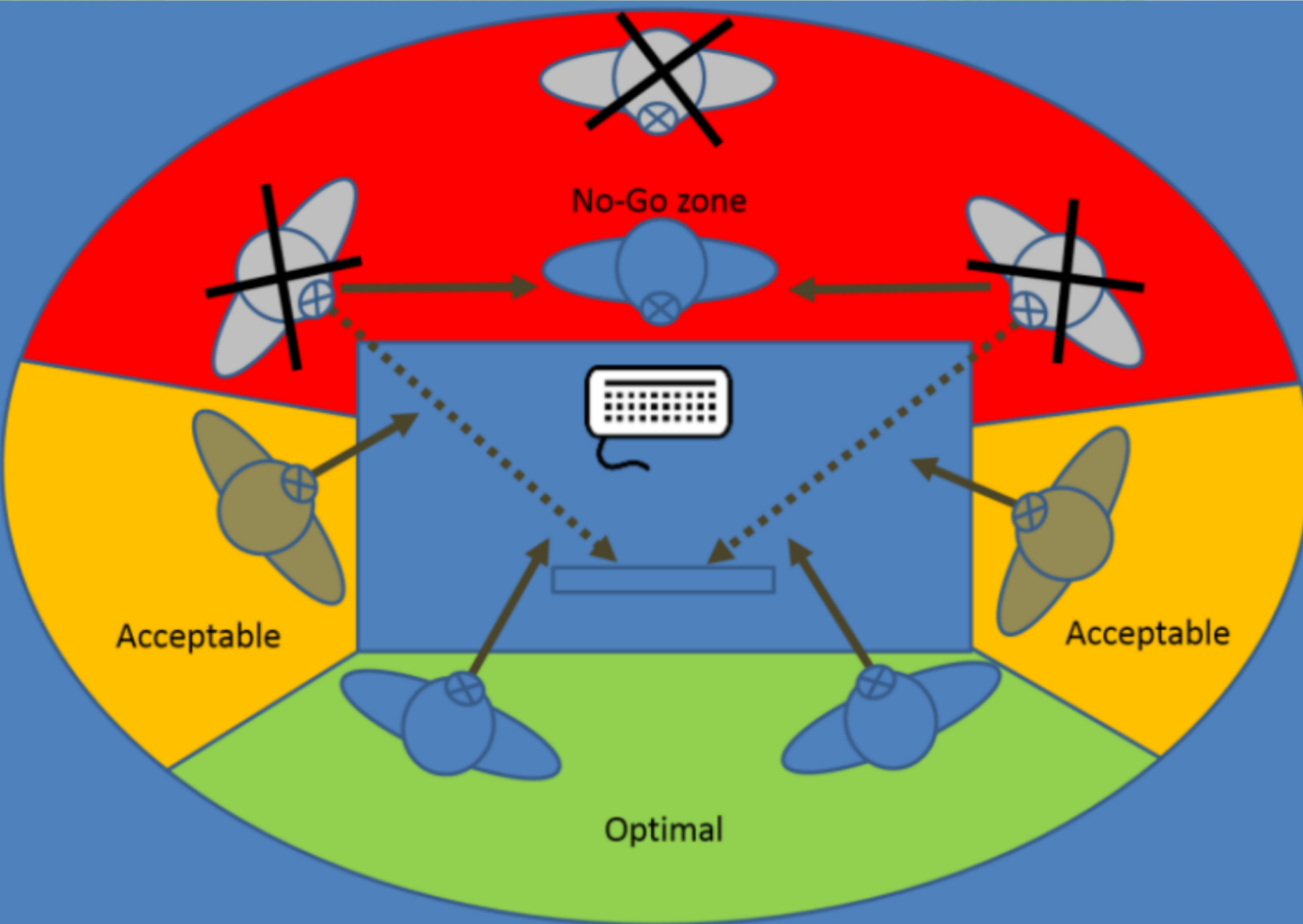
Emotionally loaded areas: Alice, Chris' wife, is hostile toward Bob, Chris' best pal. Tiffany, Chris' affair from 2014, might hold a grudge against Chris and could act as an information repository. Bob could be used to gain information about Alice and ultimately about Chris.

Interpersonal Distance (Concept of space)



Reaction Zone





No-Go zone

Acceptable

Acceptable

Optimal

https://www.xing.com/profile/DominiqueCedric_Brack

<http://ch.linkedin.com/in/dominiquebrack>

<http://www.slideshare.net/slideshare807am>

<https://twitter.com/Reputelligence>

<https://seef.reputelligence.com/>

Icons download:

<http://selz.co/Ny-y91s5Z>

Book QR code

<http://bit.ly/1IYHDoN>

<https://reputelligence.selz.com>

Punch this in: 4ONLLC6X

First name, last name and email is required (use a valid (for U accessible) email you will get the eBook sent there...)



Micro Expressions

Micro expressions are very brief facial expressions, lasting only a fraction of a second. They occur when a person either deliberately or unconsciously conceals a feeling.

Sadness, Surprise, Anger, Disgust,
Fear, Contempt

www.paulekman.com/micro-expressions/ i.e «Lie to me» TV series

Guess the expression



Sadness, Surprise, Anger, Disgust, Fear, Contempt

Guess the expression



Toolbox

SE's use tools too. Although seen by some as the "unskilled" little brother of real hackers.

- Shoes (redteaming)
- Superglue
- Welding 2 component
- Hook
- Glasses
- Hand cuff key
- etc.

Tech equipment (Hack 5 i.e.):

- WiFi Pineapple NANO
- LAN Turtle
- USB Rubber Ducky Deluxe

P.S: Your SE knows how to place them with a smile...

