Social Engineering

Lecture 5: Some psychological aspects

Kaido Kikkas

An only half-joking warning

- "Do not poke shit, it starts to stink." - an Estonian folk wisdom
- The topic is interesting but excessive doses can be harmful
- Remember those guys:

https://upload.wikimedia.org/wikipedia/commons/8/8e/
Hayden_Christensen_as_Anakin_Skywalker.jpg

https://upload.wikimedia.org/wikipedia/en/a/aa/
Christopher_Lee_as_Saruman_LOTR.jpg

Disputed stuff

- We will briefly visit several psychology-related subtopics in SE

- This area of psychology seems to be notoriously riddled with controversies and contradictions

- On the one hand, what is a solid theory for some, can be considered pseudoscience by others (e.g. neurolinguistic programming)

- On the other hand, some stuff gets dismissed for being not in line with some modern prevailing ideas/discourses

- Note: the phenomena and practical applications (incl. in social engineering) are not really disputed, scientific classification and explanations are

- Thus, read, think and decide by yourselves!

Human cognitive biases

- There are bugs in human hardware - and some of them exist in animals as well

- See a list at https://en.wikipedia.org/wiki/List_of_cognitive_biases (a very good overview) and a diagram with links at https://upload.wikimedia.org/wikipedia/commons/6/65/Cognitive_bias_codex_en.svg (note: too large and detailed to fit a slide; again, this is ONE possible interpretation!)

- Most of them can be – and are - used in social engineering!

Examples: decision-making

- Bandwagon thinking (aka groupthink or herd mindset)

- Courtesy bias (aka political correctness / woke / SJW; not offending anyone prevails honesty and truth)

- Curse of knowledge (aka ivory tower; difficulty in understanding 'lesser folks')

- Gambler's fallacy (connecting probabilities of unrelated events; "Heads vs tails")

- IKEA effect (aka "made with my own hands" giving intrinsic value – inflation by participation)

- ...

Examples: social biases

- **Authority bias** (aka "experts have said that", "much better than *ordinary* washing powder" etc)

- **Barnum (-Forer) effect** (aka subjective validation, or "this is exactly about me" - taking well-crafted generic information – e.g. horoscopes – as being personalized)

- **Halo effect** (aka "she is a good actor, let's vote for her")

- **Just world hypothesis** (aka "karma is a bitch" or "he must have deserved it!")

- **System justification / status quo effect** (aka "do not rock the boat!")

- ...

Examples: memory errors/biases

- Bizarreness effect (aka "can't forget something that crazy!")

- Cross-race effect (aka "The Chinese are all alike")

- Hindsight bias (aka "I knew that all along!")

- Picture superiority effect (aka "a picture is worth 1000 words")

- Rosy retrospection (aka "the grass was greener then")

- Suggestibility (aka "thanks for reminding, I remember that now")

- …

Discussion break

- Look at the diagram of biases at https://upload.wikimedia.org/wikipedia/commons/6/65/Cognitive_bias_codex_en.svg . Find a bias/group (one not already discussed above) and its application in SE

Modes of thinking (Hadnagy 2011)

- **Sight (visual thinking)** – remember the scene/situation, learn by seeing, "I see what you mean". Need visual input to decide
  - Light, size, colour, movement speed, focus

- **Hearing (auditory thinking)** – remember the sound, learn by hearing, "Sounds OK". Need careful choice of words
  - Volume, tone, pitch, tempo, distance

- **Feeling (kinesthetic thinking)** – remember the feeling, learn by doing/touch, "I can grasp that". Need recalling the feel
  - intensity, area, texture, temperature, weight

- In SE, understanding the target's dominant mode can help a lot

Microexpressions

- **(Semi)automatic** (hard to control – but can be mimicked by a skilled person) **mechanisms** how people convey emotions. Very short duration (often under a second)

- Haggard and Isaacs 1966, Paul Ekman since the 1990s

- Again, disputed in more recent times

- Negative:
  - Fear
  - Anger
  - Disgust
  - Sadness
  - Contempt

- Positive:
  - Amusement
  - Pride in achievement
  - Satisfaction
  - Relief
  - Contentment

Use in SE (based on Hadnagy 2011)

- **In elicitation** – by using a suitable (emotional) pretext and good impersonation skills (e.g. fear, anger and disgust when playing someone who has just been mugged in the street)

- **In detecting deception** by the other side – looking for different microexpressions when the person
  - Contradicts him/herself
  - Hesitates
  - Notably changes his/her behaviour
  - Uses hand gestures

Rapport (revisited)

- The state of 'clicking' with another person

- Feeling 'sync', kinship, alikeness

- Some ways of building:
    - Coordination/mirroring
        - Emotional ("I am on your side")
        - Posture (matching body language)
        - Voice (tone and tempo)
    - Attentiveness (showing connection, e.g. nodding)
    - Commonality (references to common interests etc)

Neurolinguistic programming

- Richard Bandler and John Grinder (1970s)

- A theory about connecting neurological processes to language and behaviour

- Various aspects and offshoots exist, some of them heavily contested (and some considered BS/pseudoscience)

- Yet, the main point of social engineering – using language to activate some "bugs" in human mind (e.g. memory errors and other biases) to achieve desired behaviour – is close enough

The Voice

- (Apparently, not just the Jedi and Bene Gesserit ;))

- Playing with the tone:
  - "Don't you agree?" (▲) vs "Don't you agree?" (▼)

- NLP suggests using lower tone for subconscious commands:
  - "Remember how clean your room looked last Christmas?" (also refers to a pleasant memory)

- NB! Sentences must be well-crafted

Gestures and posture

- Can be a powerful boost to speech

- Cultural differences!

- Anchoring: repeated use of certain gestures in certain contexts (e.g. Churchill's famous use of "V", but also using right hand for good things, left for bad)

- Mirroring: using similar (but not same) body language

- Placement of hands:
  - Elbows: kept against body in danger
  - Hands: look for subconscious movements

An old Estonian example

- From years ago – probably one of the few examples of written NLP used in Estonian media (selling a sausage brand called "Näpi vorst")
- Note: reconstructed from memory, the original was in Estonian – I've tried to translate the wordplay

always buy

POKE valley

SAUSAGE for

SOME MORE people as

it is tasty and eating it

FEELS GREAT

Discussion break

- Does NLP work? Is it universal?

- If you have any experience/contact with NLP, bring an example

- Could the choice of natural language (English, French, Estonian…) have an impact on NLP attempts? Would any languages be more suitable than others for this?

- Can (skilled) use of expletives ("dirty words") work as a form of NLP?

Dark Psychology

- Suggested by some authors as a separate discipline to study evil behaviour (harming others deliberately) in humans

- Contrasts the Positive Psychology (since around 2000; focuses on the quality of life and positive experiences/traits)

- A thought-provoking idea: 99% of evil behaviour has a purpose, 1% is just 'for shits & giggles' (= rational vs irrational evil)

- For further reading: e.g. *Dark Psychology* by James W. Williams (search the Web for more)

The Dark Triad

- Paulhus & Williams 2002
  - N: inflated ego, no empathy
  - M: manipulative, no morality, self-centred
  - P: antisocial, impulsive, callous, no remorse
- Some authors add sadism – enjoyment of cruelty
- NATURAL SOCIAL ENGINEERS
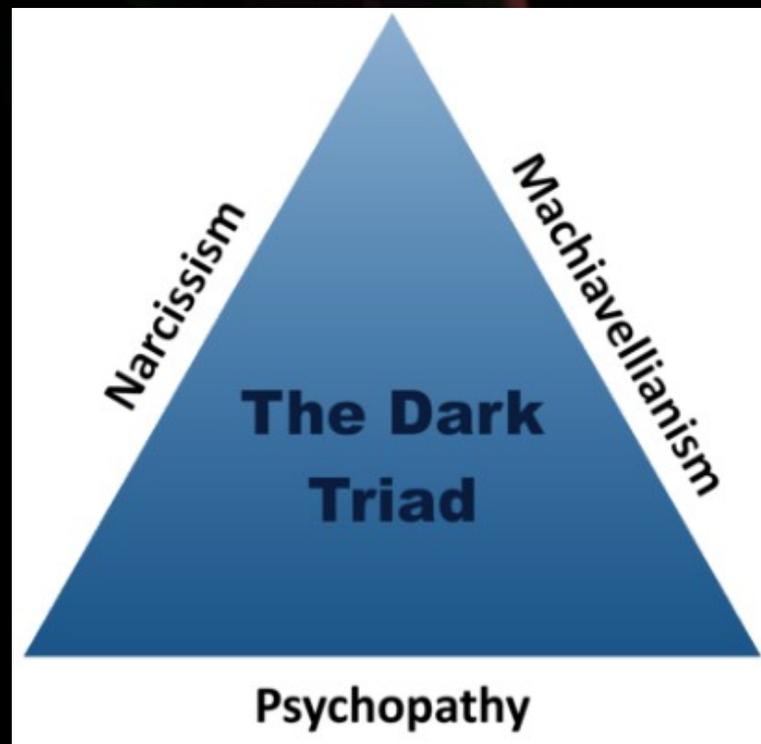
https://upload.wikimedia.org/
wikipedia/commons/b/b5/
The_Dark_Triad.png

A big problem

- Most of us live wearing backpacks:
  - Social norms (e.g. "violence is bad")
  - Moral and religious dogmas
  - Manners and etiquette
  - Guilt and remorse after misbehaving
  - Conscience
- There are people who walk without the backpack…
- … and unfairly but surely reach the top

https://upload.wikimedia.org/
wikipedia/commons/a/a9/
Tropical_Rucksack_3.JPG

Discussion break

- Think (on your own) about your encounters with the Dark Triad

- What can be done when having to deal with a DT person?

- Can a "backpack" be
    - put on someone not having it (education? persuasion? force?)
    - lightened, still without dropping it at one point?

PUA & more

- Seduction by manipulation
- 'Pick-up artists' are mostly male – but there is a parallel, mostly female 'art' of gold-digging
- From just 'guys who want to get laid' to several subcultures ("manosphere")
- Controversial in several ways
  - More obvious: psychological abuse of (mostly) women
  - More subtly, but perhaps more interestingly: the practical effectiveness of some types will challenge the current mainstream understanding of sex/gender – for instance, https://www.apa.org/topics/personality/men-women-difference
- Some practicioners seem to know enough of dark psychology to actually put people in danger
- SE is used both as main method and a marketing tool (quite many of them seem to offer their services as consultants/teachers!)

A brief look on methods

- A common *modus operandi* seems to be
  - preparation phase (ct Information gathering and elicitation)
  - baiting/pickup (sometimes scripted; ct pretexting – preferrable pretext seems to be a 'good catch' – wealth, position. contacts...)
  - raising intrigue/interest (depending on the Short vs Long game)
  - rapport-building (depending on the Short vs Long game)
  - 'roller-coaster' phase (alternating between positive and negative feedback cycles)
  - attack (various scenarios; can involve additional means)
  - disengaging (Short) or further manipulation (Long)

A social engineering view on PUA etc

- A specific branch

- In general, specific groups/direction (men => women)

- Uses a variety of techniques from general SE (see lecture 1)

- Can be both Short and Long Game

- Communication is the key (the 4 questions of initial contact should also apply to these scenarios)

- Elicitation is used more widely (response rather than information!)

- Initial contact scripting <= "Click, whirr!"

- Pretexting is important, but might be somewhat narrower

Discussion break

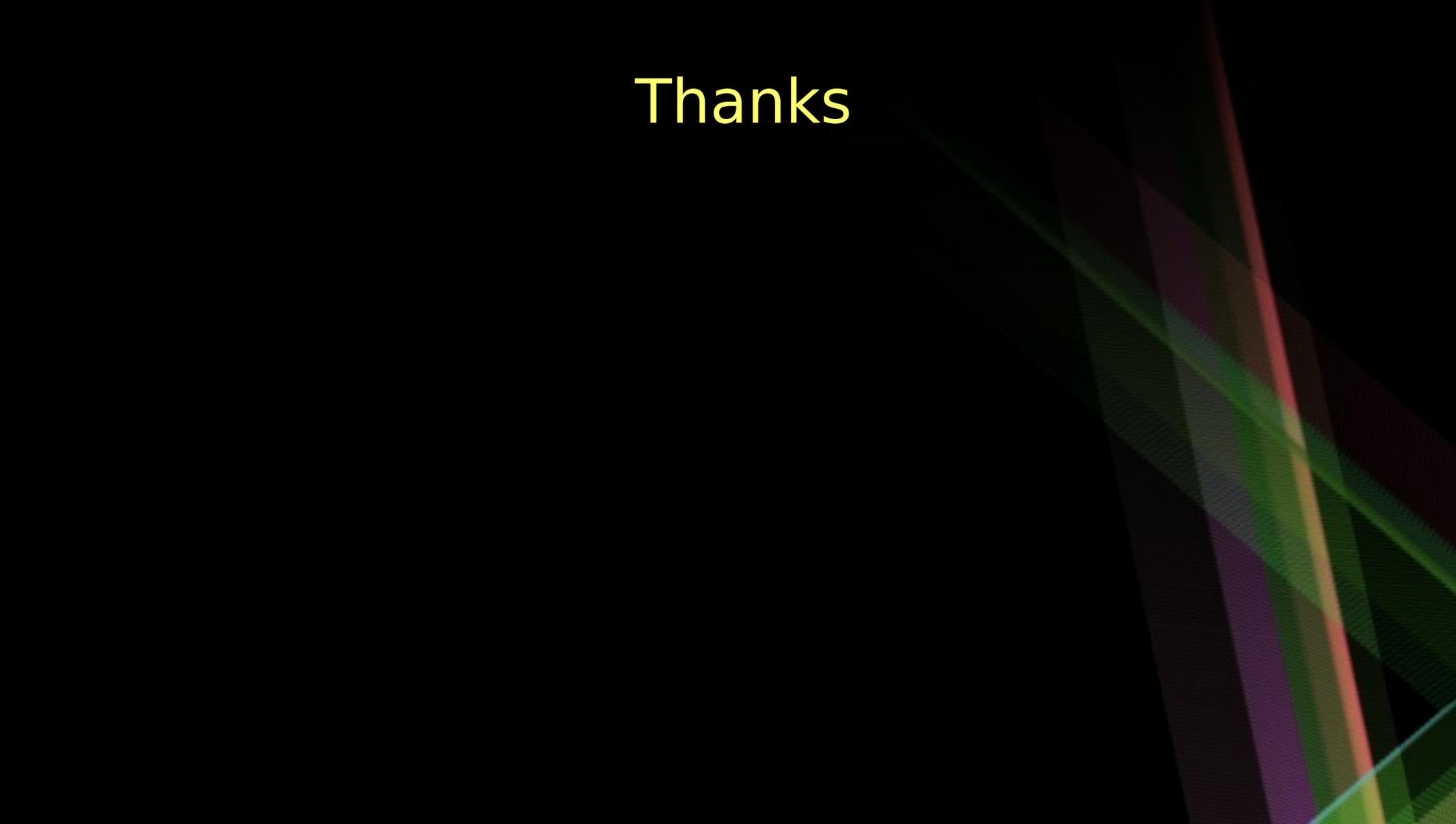- Could PUA etc work on deeper emotional level (sex vs love)?

Summing up

- Another well-known (and small) hero:
  - When you look at the dark side, careful you must be. For the dark side looks back.

  - Is the dark side stronger? No, no. no. Quicker, easier, more seductive.

  - A Jedi uses the Force for knowledge and defense, never for attack.

  - May the Force be with you. :)

- Next time: Influence

https://en.wikipedia.org/wiki/File:Yoda_Empire_Strikes_Back.png

Thanks