



CyWeTa



How to make 5G trustworthy technology (view of the cyber security guy from CEE)

Tomas Pluharik



In the galaxy far far away



In 5G trust you must.



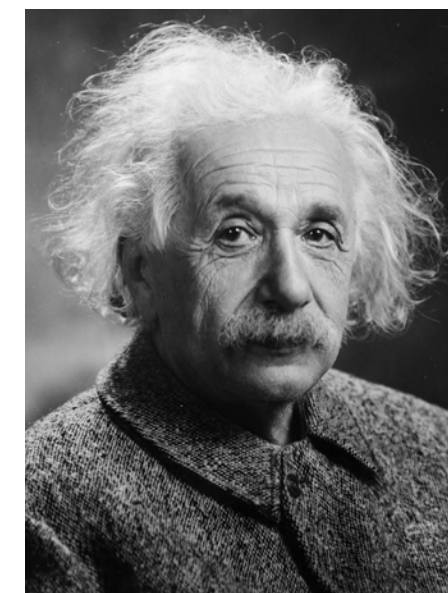
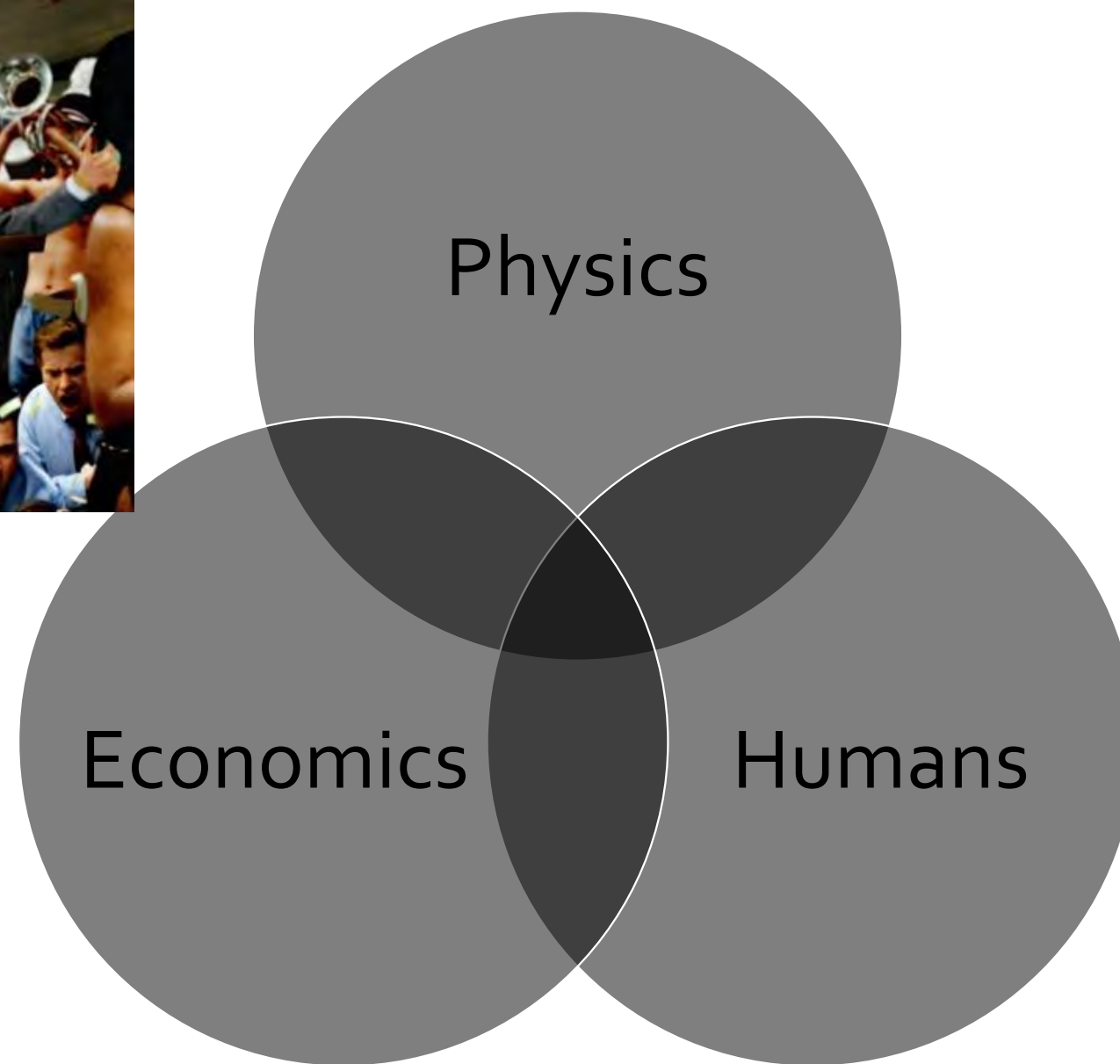
In the galaxy far far away



Fear is the power of the dark side ... well and I am the security guy.



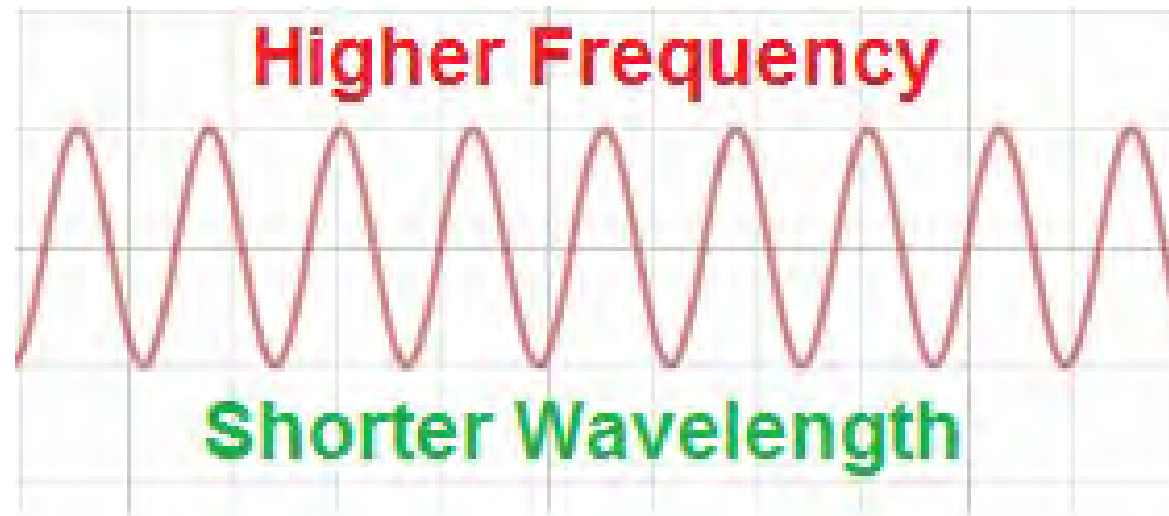
Fundamental forces



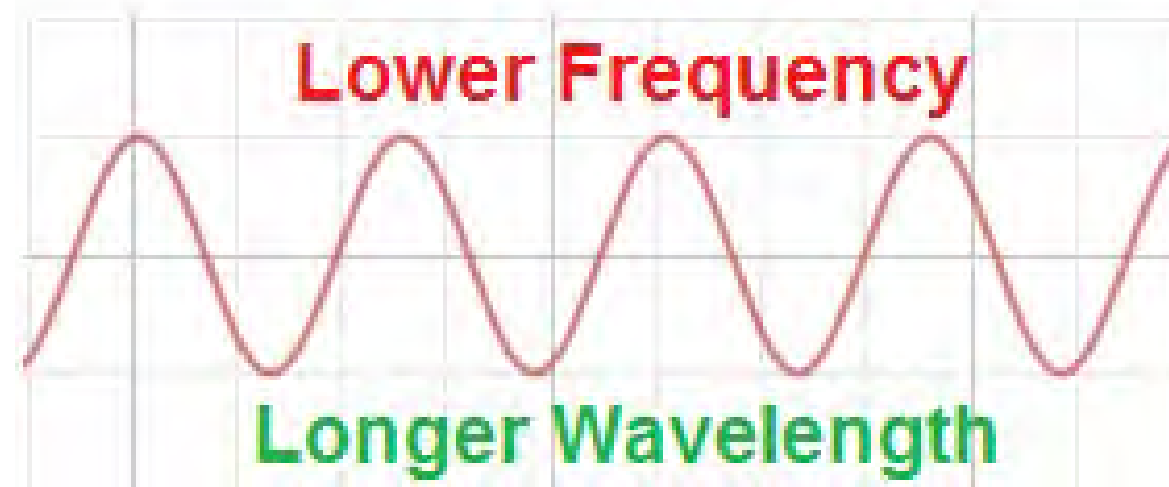
80 percent of cyber incidents are coming from the people.



Physics (oversimplified)



HIGHER DATA THROUGHPUT SHORTER RANGE



LOWER DATA THROUGHPUT HIGHER RANGE

Environment with mixed hardware / bands for various purposes. High frequency for cities, low frequency for rural areas.



2G, 3G, 4G



1X

5G



10X ???

Environment of the cities leads to very deep penetration of the network elements (not just antennas and BTS). Network elements are moving near to the end users.



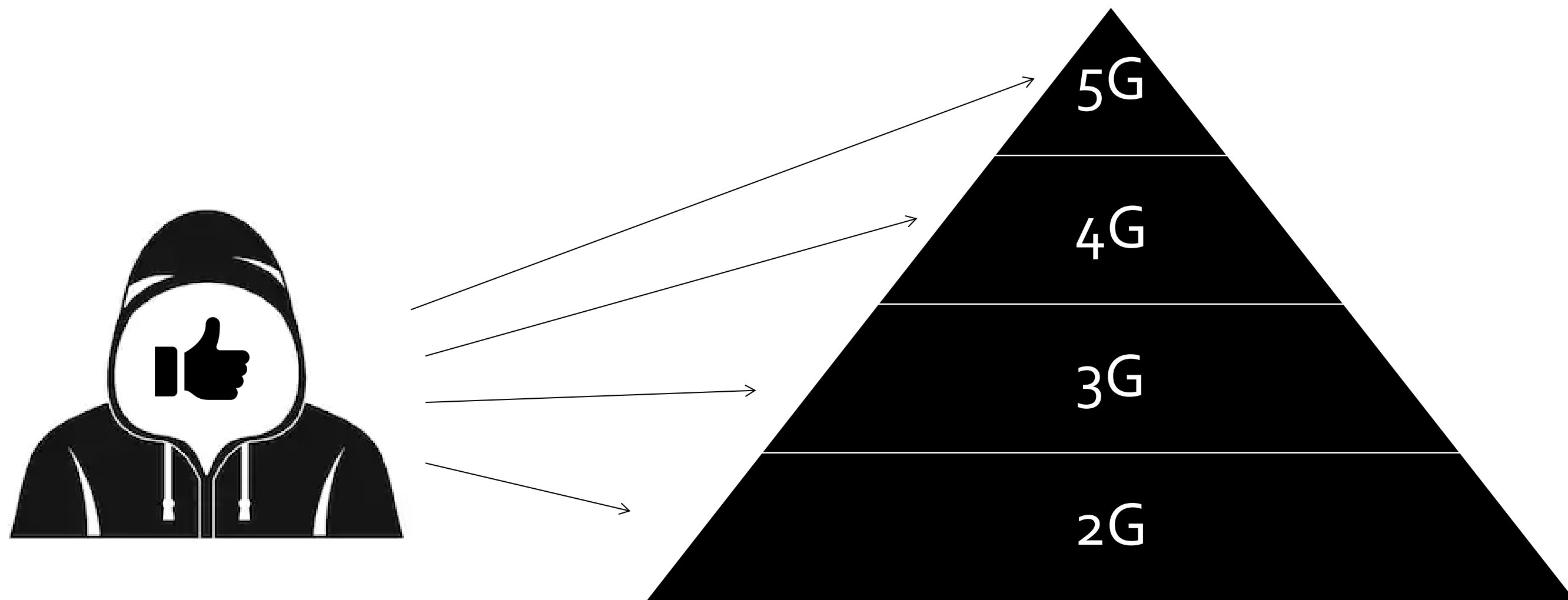
5G is increasing the risk of physical access violation of service interfaces of the infrastructure. It also pushes hard on the physical monitoring of the infrastructure.



5G is communicated as life critical application ready.



Economics – legacy networks



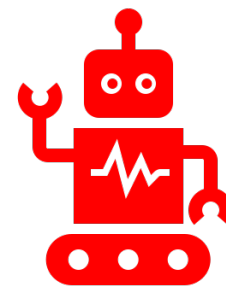
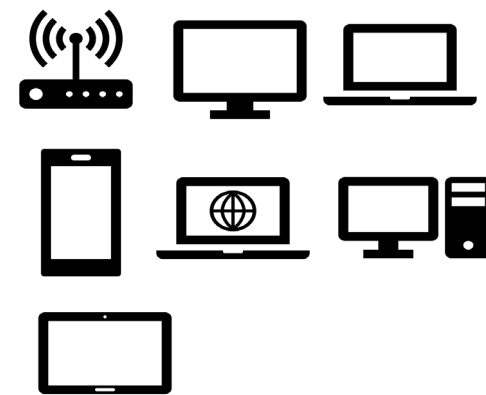
Majority of the initial implementations are based on actual 4G infrastructure. And old infrastructure will not disappear.



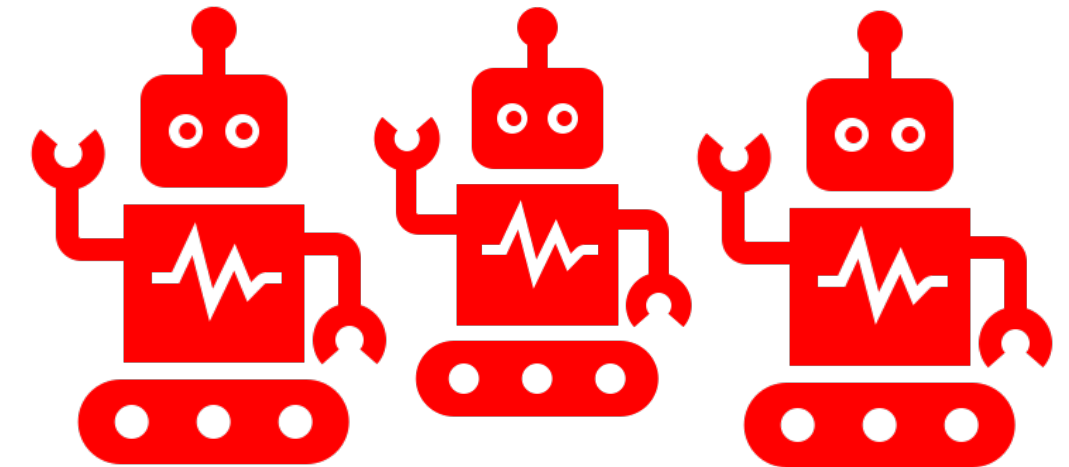
Economics – density of devices



2G, 3G, 4G



5G

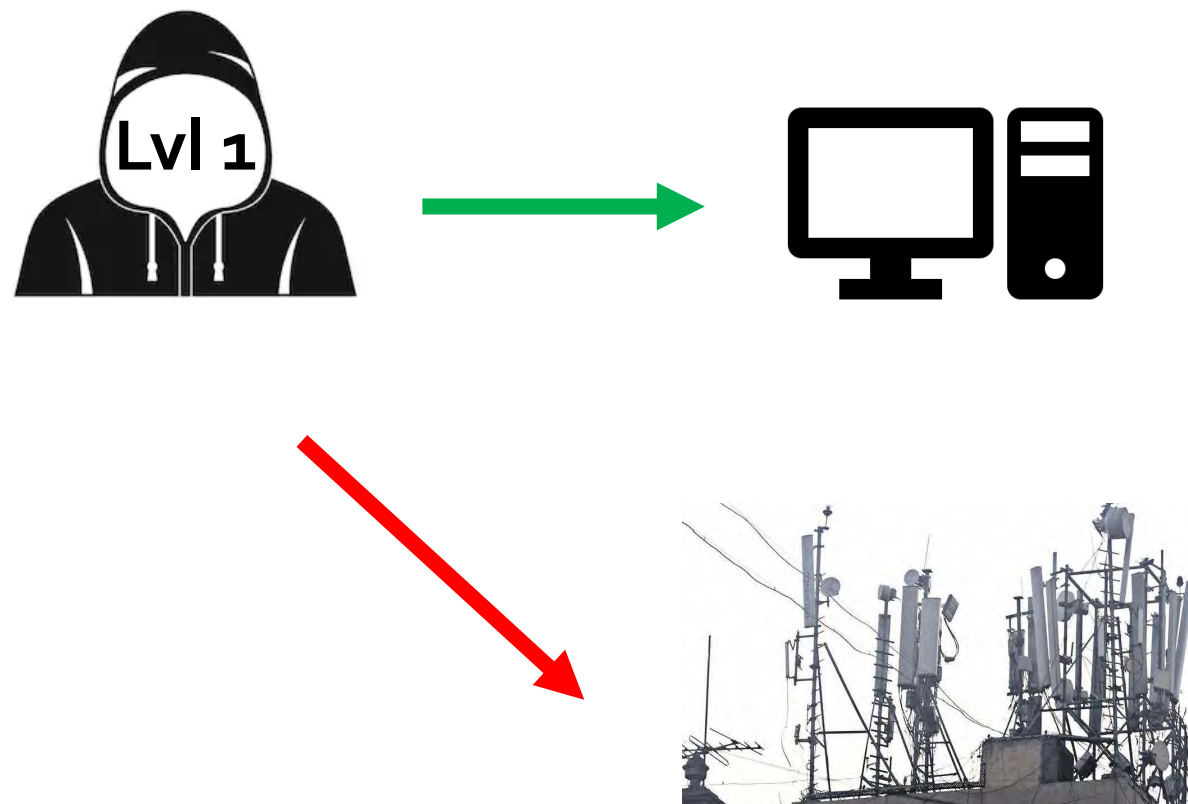


IOT and Edge computing means scalable Botnets plus internal Botnets

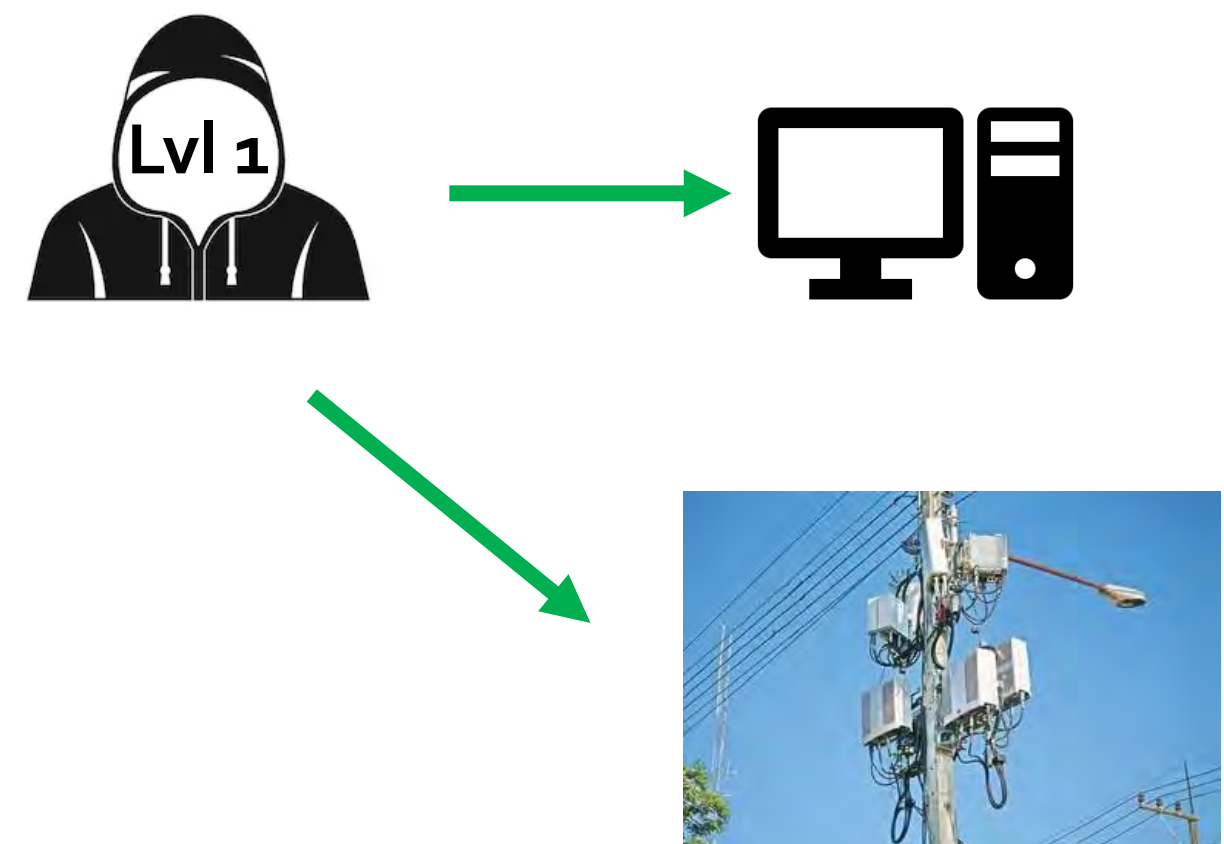


Humans – easier to learn to hack infrastructure (because of softwarization / virtualization)

2G, 3G, 4G



5G



Software based systems are more vulnerable from rookie hackers.



Humans - hackers



Minm

5G AKA



Bidding down

MNmap

IMSI catchers

2G, 3G, 4G generated thousands of zero day flaws and 5G is not different. Actually it is more complex therefore there will be more zero day issues.



Problem of transformation period

- Unproven integrations
- Frequencies not available
- Unproven elements of the 5G (MIMO, EdgeC, Beamforming etc.)
- Not fully virtualized control elements of the 5G
- Security practice driven by legacy technologies
- Etc. etc. etc.

Transformation period will create heterogenic ecosystem full of expectations and gaps.



Any ideas Mr. Spock?





Do cybersecurity for 5G Proposal #1

"SAFE"



NETWORK THINKING

"EVERYTHING IS HACKABLE"



HACKER THINKING

Cybersecurity of 5G should be taken more seriously. Virtualization must lead to shift in network security thinking.



Do cybersecurity for 5G Proposal #1

"EVERYTHING IS HACKABLE"



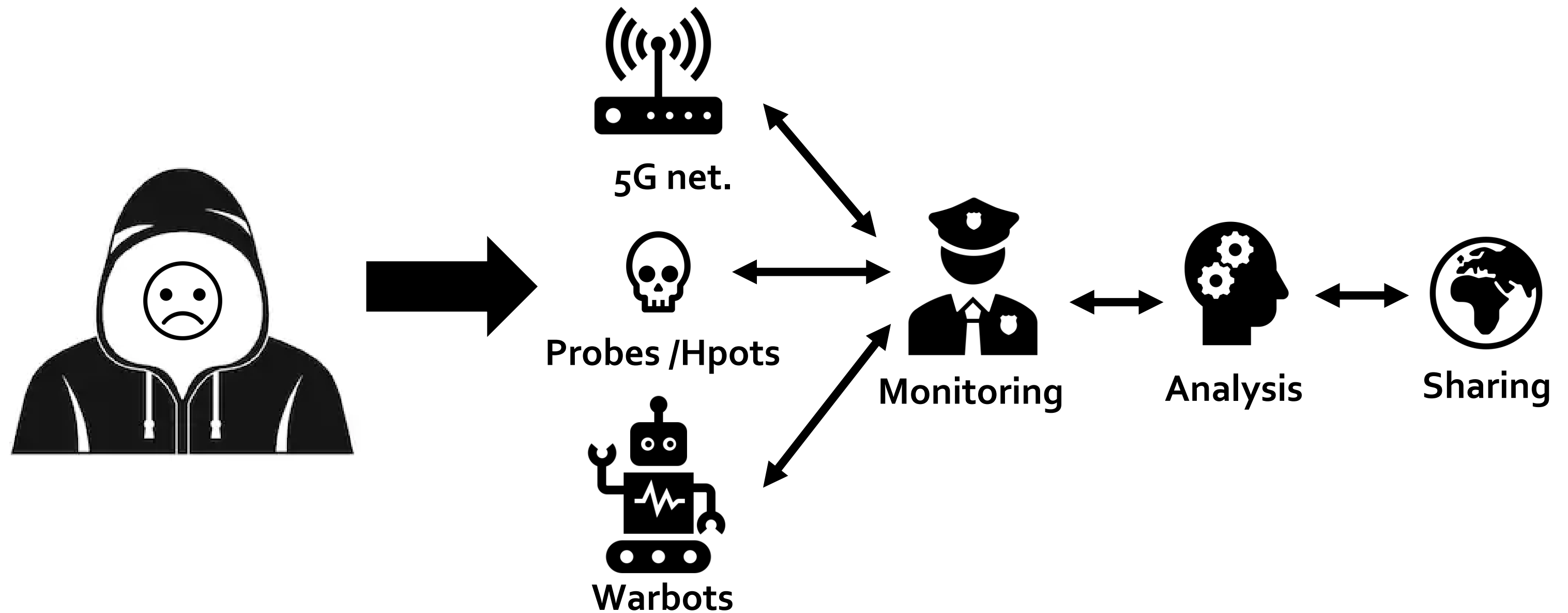
HACKER THINKING

Hire a software hacker.



Distributed probe networks and cybersecurity monitoring – time proven solutions

Proposal #2

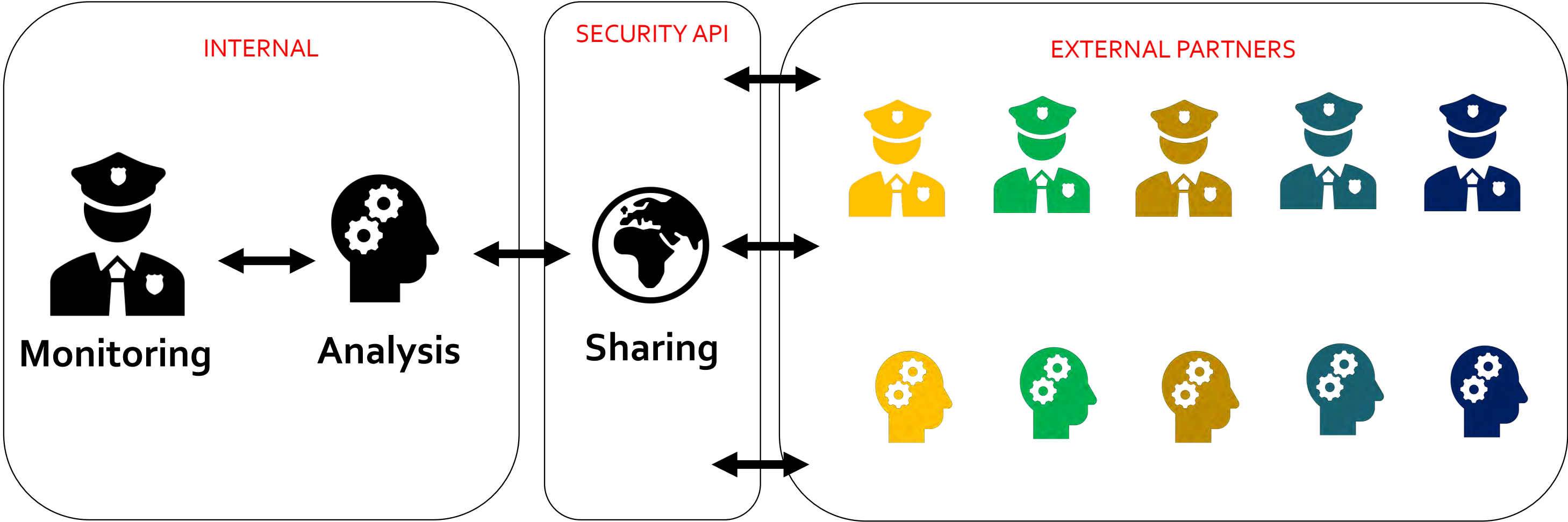


Cybersecurity monitoring and vulnerability assessment is completely different discipline from network monitoring.



Shared realtime security monitoring concepts

Proposal #3



In 5G cybersecurity sharing is protecting (especially with rise of edge computing and 3rd parties operations).



Cognitive detection and response

Proposal #4

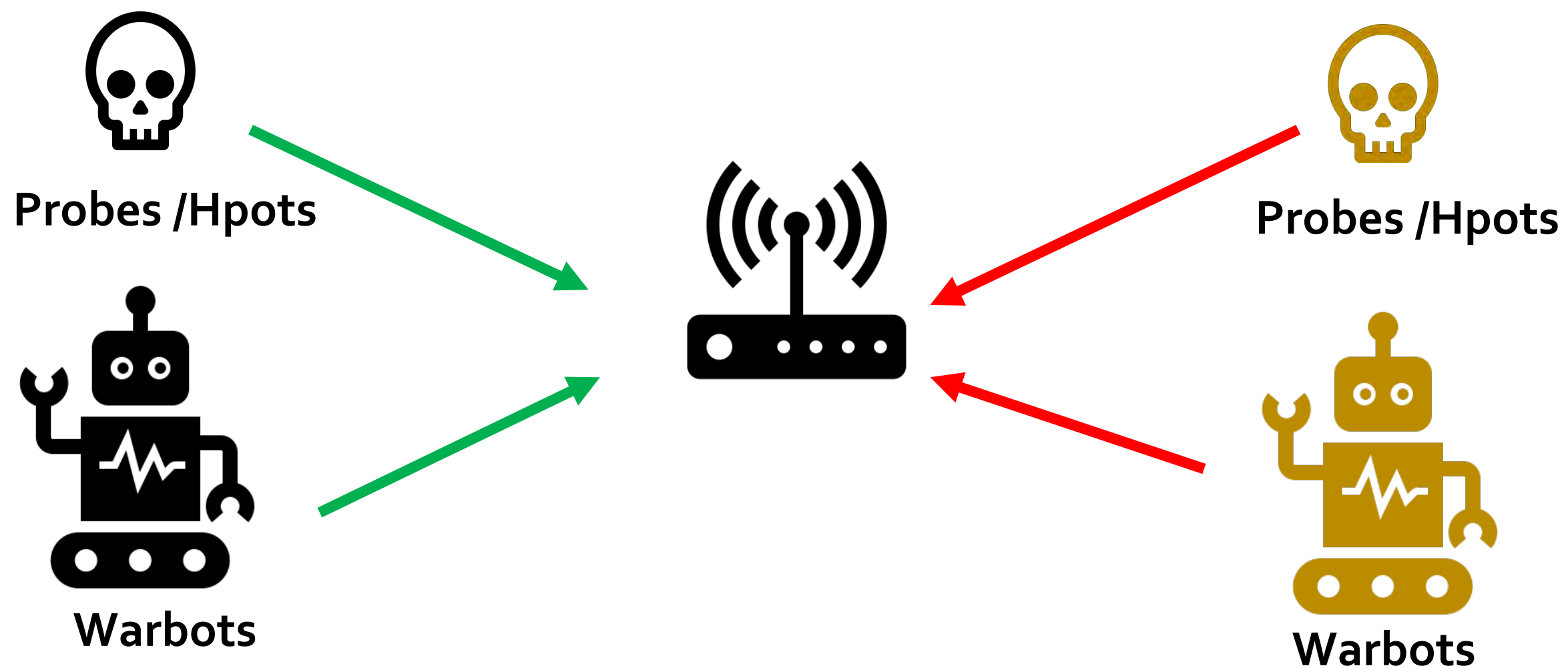
- General problem of overwhelming the human operators.
- AI can preselect threat type
- AI can preselect response
- AI / machine learning can learn new unknown threat and evaluate responses.



Humans cannot manage the load anymore.



Probes /VA / warbots standartization Proposal #5



Any sane network engineer will not allow uncertified active elements into their network.



Probes challenges



WARBOT / VA System



Cybersecurity non commercial hw certification authority (global)

Proposal #6

- Why global?
- Why cyber dedicated?
- Why noncommercial?
- Why 3GPP is not good enough?

We already have examples of such organizations in the life critical applications (ICAO, IAEA etc.).



Summary of 5G situation from the cybersecurity point of view

- We are increasing, not decreasing the complexity of the environment!
- Marketing is pushing 5G as mature solution for life critical applications!
- Virtualization /softwarization of the 5G is not followed by „softwarization“ of the cybersecurity!
- 5G became a political problem.

Perfect storm is coming?



Summary of proposed approaches

- Phase out old technologies as fast as possible
- Change the approach of the cybersecurity to the network – more software hacker thinking
- Include monitoring and VA concepts known from cloud / sw cybersecurity.

I know I am an idealist 😊



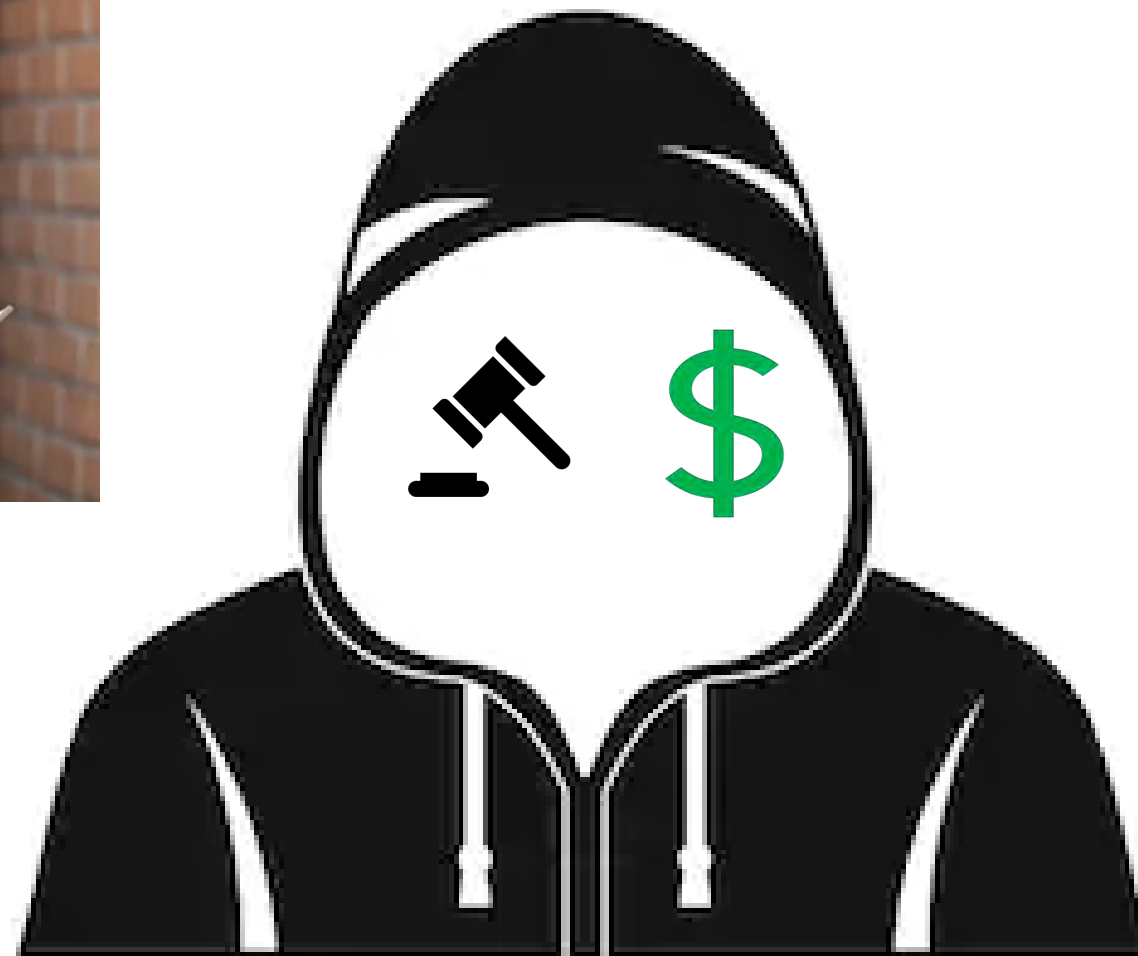
Summary of proposed approaches

- Create independent global non commercial entity covering cybersecurity certifications and standarts for 5G (sorry, but 3GPP is not that type of organization)
- Rationalize view on 5G

I know I am an idealist 😊



Do cybersecurity for 5G with the beancounters and lawyers



Nothing can beat proper financial and compliance damage assessment of successful hack of the network elements.



Contact information

 **Tomas Pluharik, CEO**

tomas.pluharik@cyweta.com

+420 775 013 225

www.cyweta.com

