

Physical threats to inside targets

28 June 2023 – TU Delft



Berndt Rif, MSc, MBA

Risk Approach or Threat Approach

the difference



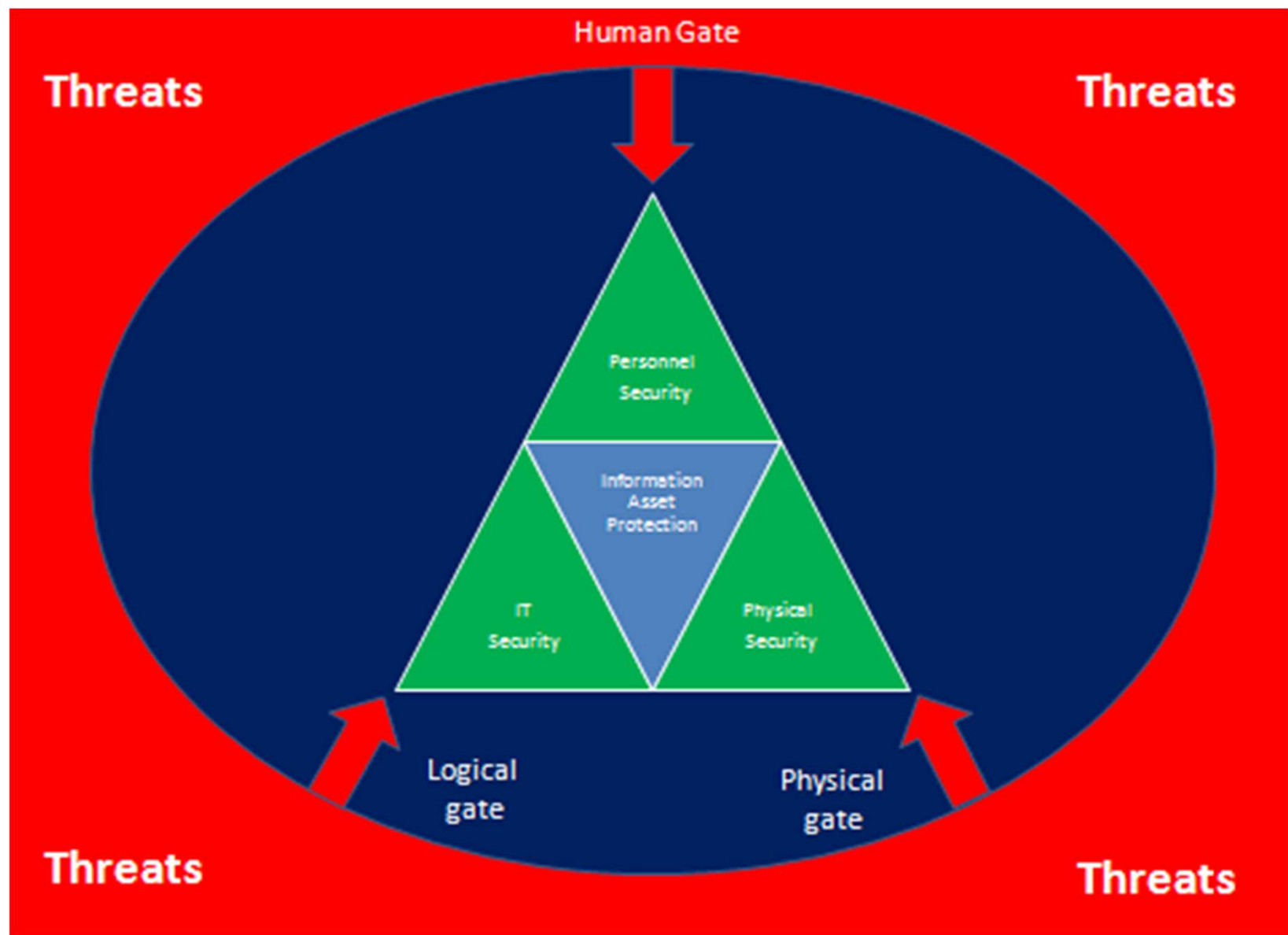
your answer on
10 september 2001 is ?



0 x 100 = ?

0 or 1





In recent years it happened several times that Chinese students and scientists who were (temporarily) studying or working in the West proved to be involved in intelligence activities. These persons usually stay in the West as part of official Chinese government programmes for intensification of knowledge: public programmes aimed at raising the inferior Chinese knowledge economy to a higher level. In some cases participation in such programmes proved to serve as a cover. A couple of years ago, two Chinese students in the US succeeded in collecting American information on the production of a chemical substance that is used in sensors and weapons. They managed to pass the information to China before their activities were discovered.

Reports that Russia's intelligence agencies hold compromising material about Donald Trump have sparked angry denials from the US president-elect and the Kremlin.

The claims that Mr Trump's presidential campaign secretly communicated with Moscow - and that Russia has embarrassing sexual information about him - are unverified.

But there have been allegations circulating in political and media circles for months. Here is what we know about how they came to light.

In February 2003 eavesdropping equipment was discovered in the office of the European Council in Brussels. A major meeting hall, as well as rooms used by the delegations of the United Kingdom, Austria, France, Germany and Spain were tapped. Over the past few years, several important meetings of various European bodies were held in the meeting hall in question. The eavesdropping equipment had probably already been planted during the building of the office in 1995. So far it has been unclear which country is behind the eavesdropping operation. The scope of the system and the connections with extensive cables suggest a large-scale technical operation, possibly set up with help from inside.

Victims of Cold War 'Romeo spies'

By Angus Crawford
BBC News

During the Cold War, the Stasi - East Germany's secret police - sent "Romeo" spies to the West.

They seduced secretaries working in Bonn and tricked them into handing over secrets.

More than 30 of the women were later prosecuted for spying.

Now a former senior Stasi officer has told BBC News the women should be pardoned.



One of those targeted by the Stasi more than 30 years ago is Gabriele Kliem, who still suffers the consequences.

Gabriele Kliem hopes for forgiveness, but expects nothing

A prominent example of clandestine gathering of military-economic information was exposed in 2002, when in Sweden three employees of the telecom company Ericsson were arrested on suspicion of espionage for Russia. Two Russian diplomats who had been active as intelligence officers were expelled. Ericsson is mainly known for its mobile phones, but the company also develops radar and missile guidance systems for the Swedish airforce.

FBI agent Robert P. Hanssen was arrested in the United States in February 2001. It turned out that he had started spying for Russian intelligence services as early as in 1979, in exchange for 1.4 million dollars in money and diamonds. Hanssen's activities allegedly led to the execution of at least two American double agents within the Russian KGB in the days of the Soviet Union. Hanssen was sentenced to life imprisonment in May 2002.

There are many suggested **motives for spying** that an individual may have. In general, **espionage** carries heavy penalties, with spies often being regarded as **traitors**, and so motivating factors must usually be quite large.

There have been various attempts to explain why people become spies. One common theory is summed up by the acronym **MICE**, which stands for **M**oney, **I**deology, **C**ompromise or **C**oercion (depending on source), and **E**go or **E**xtortion (depending on source). Another is the **RASCLS** framework: ^[1] **R**eciprocation, **A**uthority, **S**carcity, **C**ommitment and **C**onsistency, **L**iking, and **S**ocial Proof. Others have stressed the role of disaffection and grudges, or of personal links.

How Pakistan, China agencies are using women to honeytrap Indian army officers

Intelligence agencies have issued an alert for security forces to ask their men to be watchful of attempts made by women to lure them.

Figure 92: Criminal Background of Perpetrator

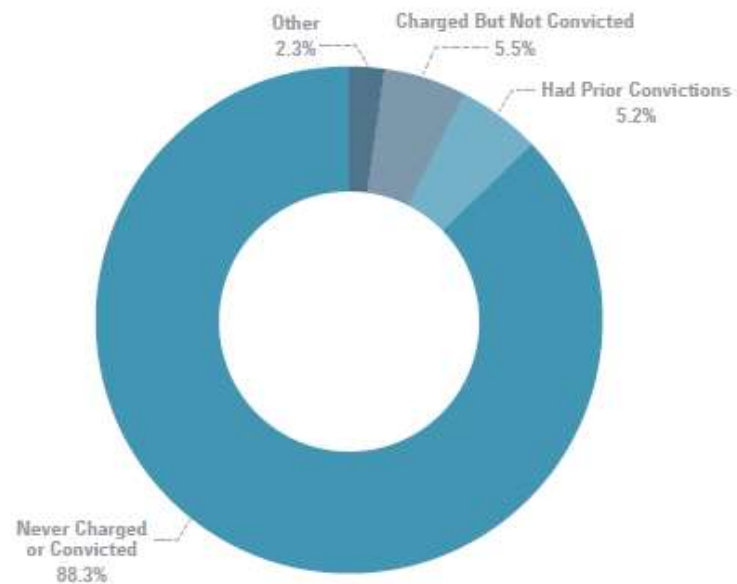
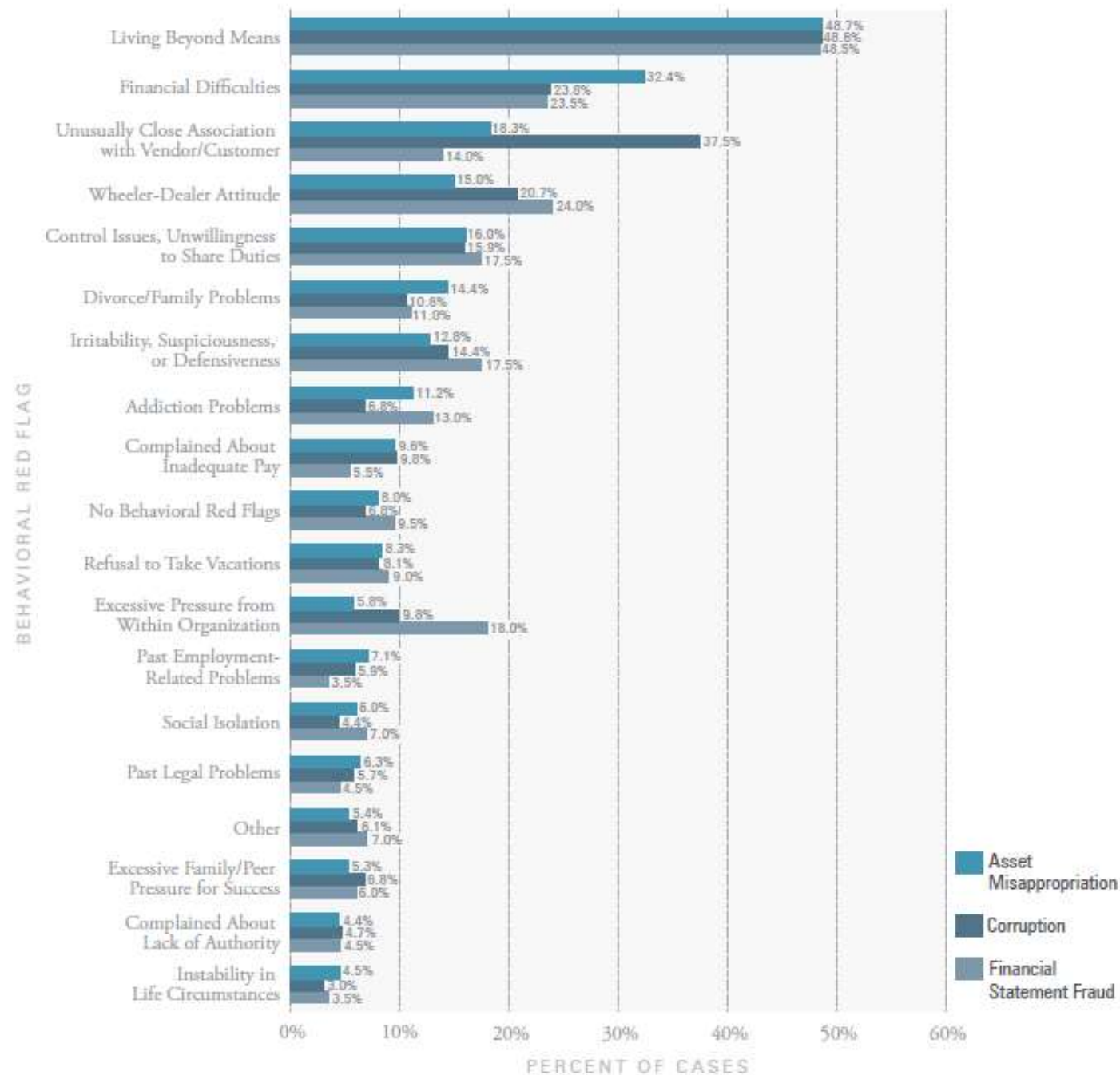


Figure 96: Behavioral Red Flags Based on Scheme Type



Recruitment; how it works?

An example

Cultivate an employee with the aim of 'creating pressure' to make him or her do something that is not allowed...

..... from cultivation to recruitment

- Starting an innocent friendship
- Asking to provide 'public' information
- Going out with the family
- Asking to provide 'confidential' information

Depending on the interests, a process to recruit a person can take between 1 and 5 years (danger is our short-term memory that prevents us from perceiving this).

Criminal organizations have (almost) the same capabilities as intelligence services

Criminal Planning Cycle

- Marking
- Intelligence Gathering
- Surveillance
- Planning
- Tooling up
- Rehearsing/training
- **Execution**
- Getaway

Criminal Planning Cycle

- Marking
- **Intelligence Gathering**
- **Surveillance**
- Planning
- Tooling up
- **Rehearsing/training**
- **Execution**
- Getaway



Program

- Module 1 From cultivation to recruitment; the context
- Module 2 **Threat assessment (identifying opponents)**
- Module 3 Red Teaming (determine modus operandi that affect interests)
- Module 4 Quick Wins

And now mapping the threats 1



Who can attack the interests (crown jewels) the organization wants to protect ?

Exercise 1

- **What are the Crown Jewels**
- **Who is interested in these crown jewels**

Take 30 minutes to answer the two questions





Program

- Module 1 From cultivation to recruitment; the context
- Module 2 Threat assessment (identifying opponents)
- Module 3 **Red Teaming (determine modus operandi that affect interests)**
- Module 4 Quick Wins

And now mapping the threats 2

Think of;

- (Have) physical and electronic values removed (criminals)
- Disrupting vital and/or critical processes (terrorists)
- (Have) valuable information taken away (intelligence services)

**And how
are they going to do that ?**



Infiltration, Human Engineering, Social Engineering

Exercise 2



**Who are you going to get the information from?
How do you make sure you get the information?**

Take 30 minutes to answer the two questions

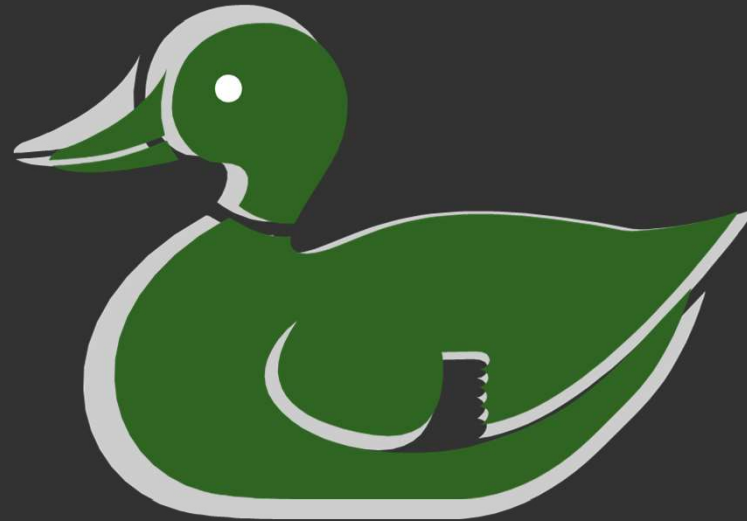


Program

- Module 1 From cultivation to recruitment; the context
- Module 2 Threat assessment (identifying opponents)
- Module 3 Red Teaming (determine modus operandi that affect interests)
- Module 4 **Quick Wins**

Check every situation...

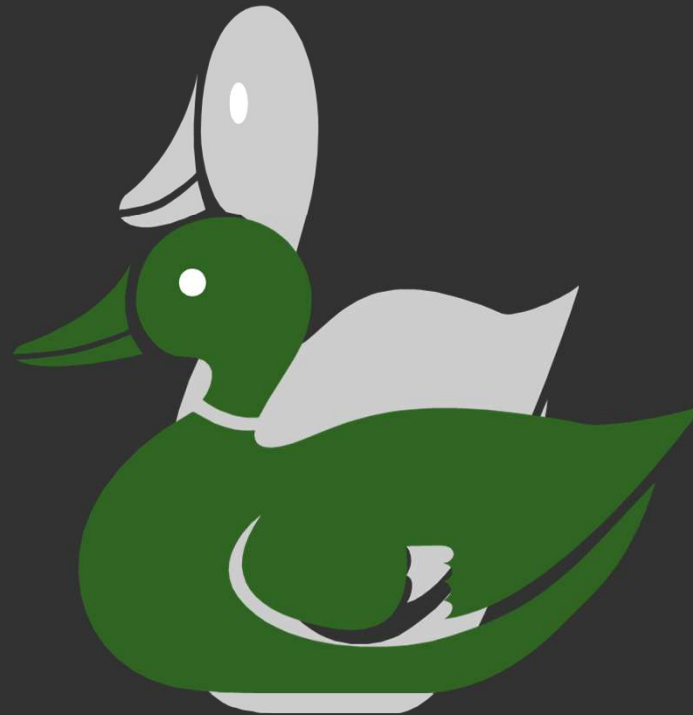
If it looks like a duck,
walks like a duck,
and sounds like a duck...



“Norm”

Check every situation...

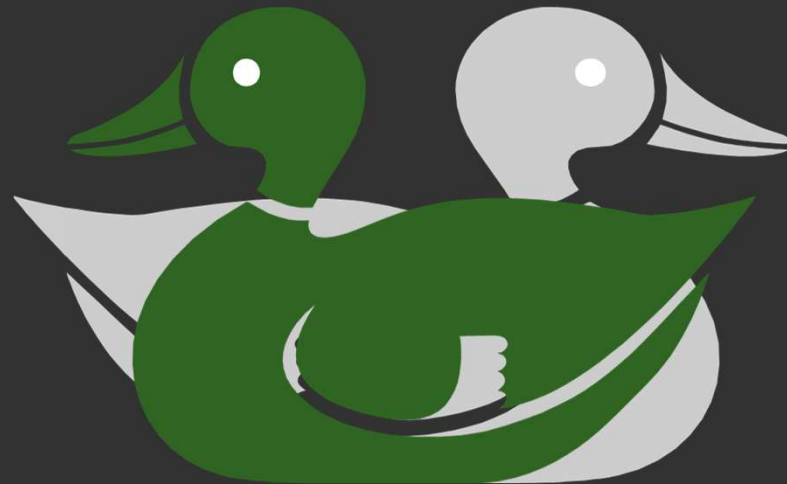
... the duck may look slightly different...



“Norm”

Check every situation...

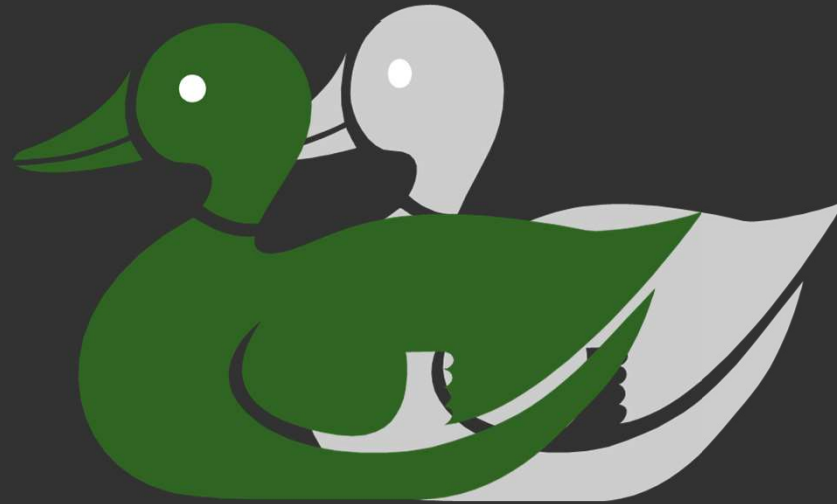
... behave differently...



“Norm”

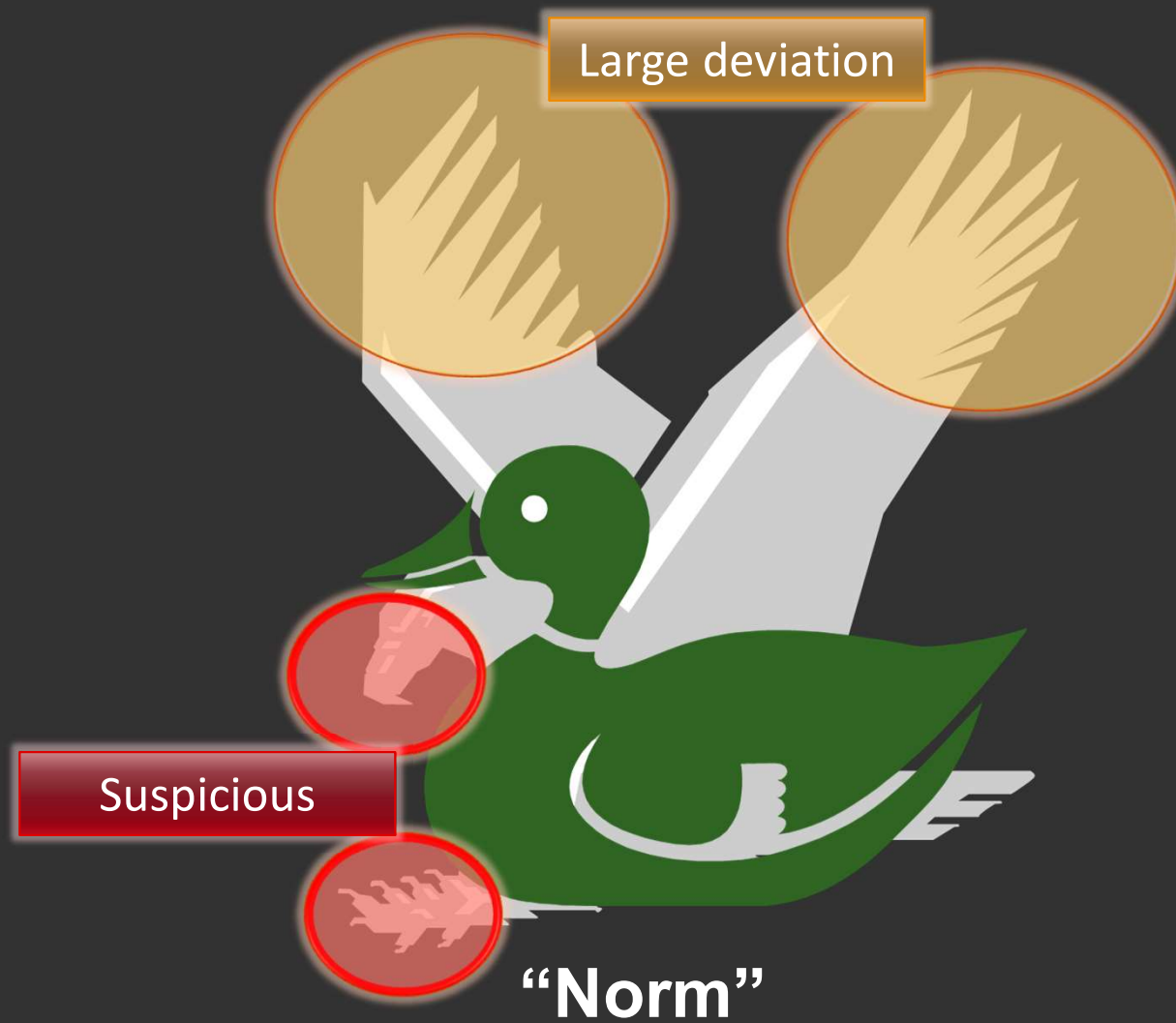
Check every situation...

... have a different color...

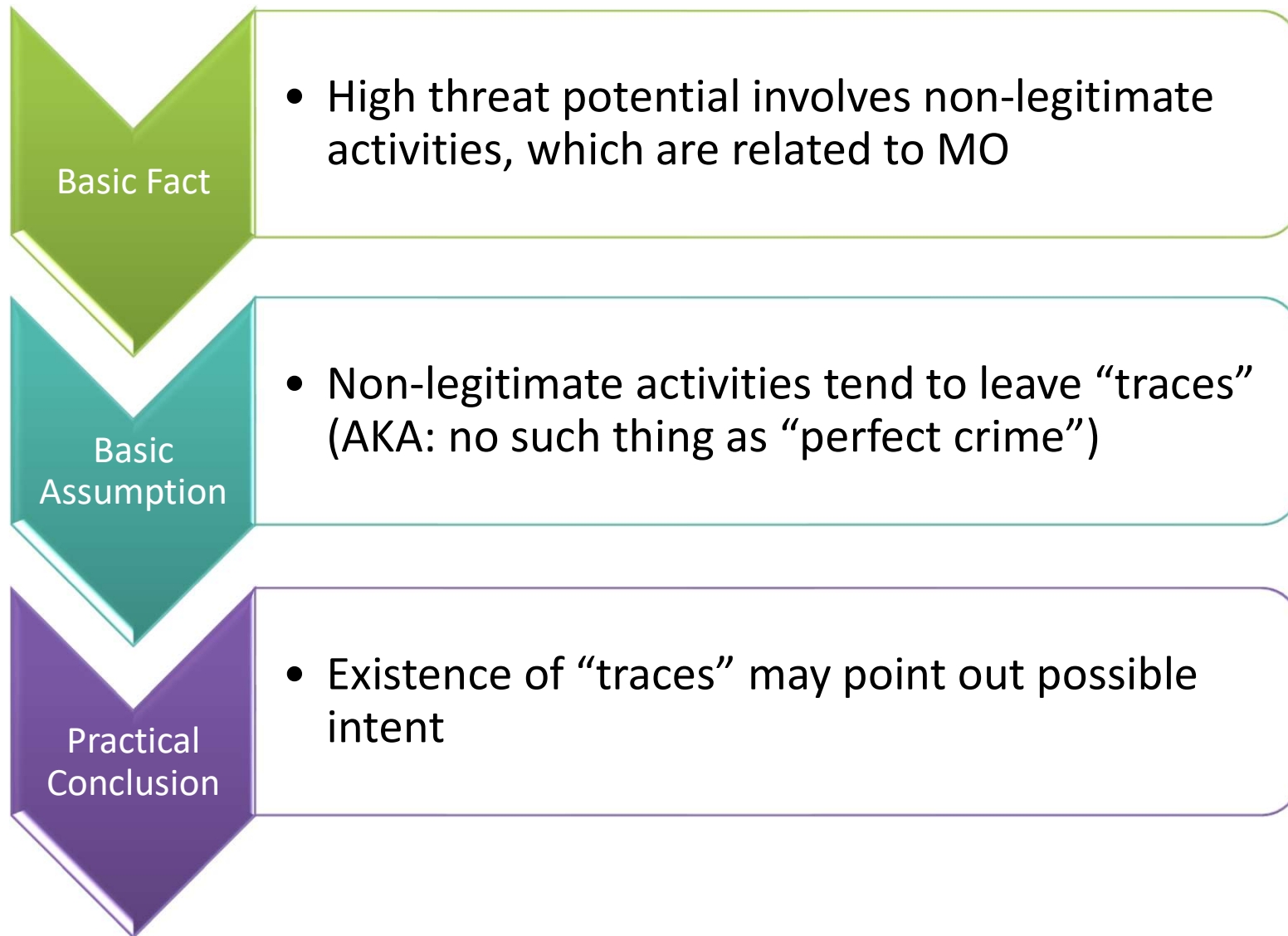


“Norm”

Check every situation...

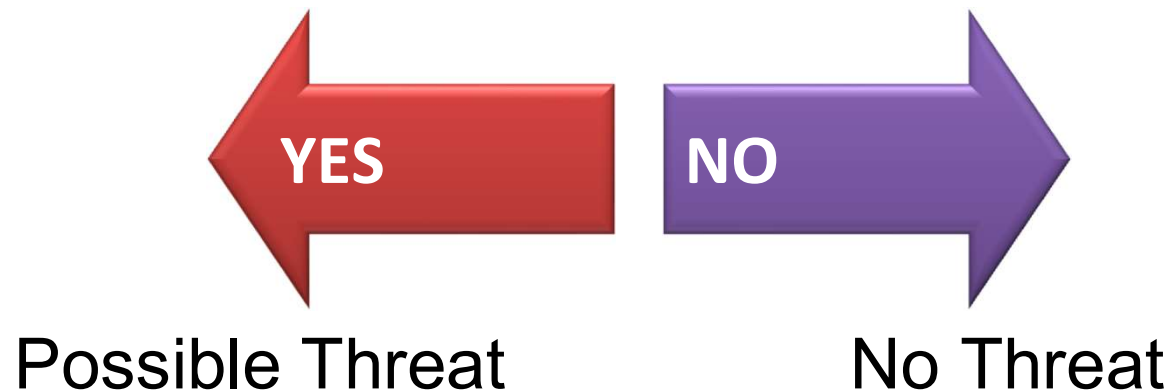


The Foundations



The Basic Process

- Create the “good guy” profile:
Typical Legitimate Instance = “The Norm”
- Examine each instance and look for:
 - Red Flags (suspicious signs)
 - Deviations from the norm



Strange or suspicious?



**What is the adversaries method of operation ?
What is the norm in this environment ?**

deviation from the norm

- ❑ does not look at the track
- ❑ looks at people on the platform

- ❑ shirt over pants
- ❑ dressed differently



Quick Wins



Exercise 3

What measures can we take ourselves?
How can we protect each other?





Physical threats to inside targets

4 July 2023 – TU Delft



Questions ?