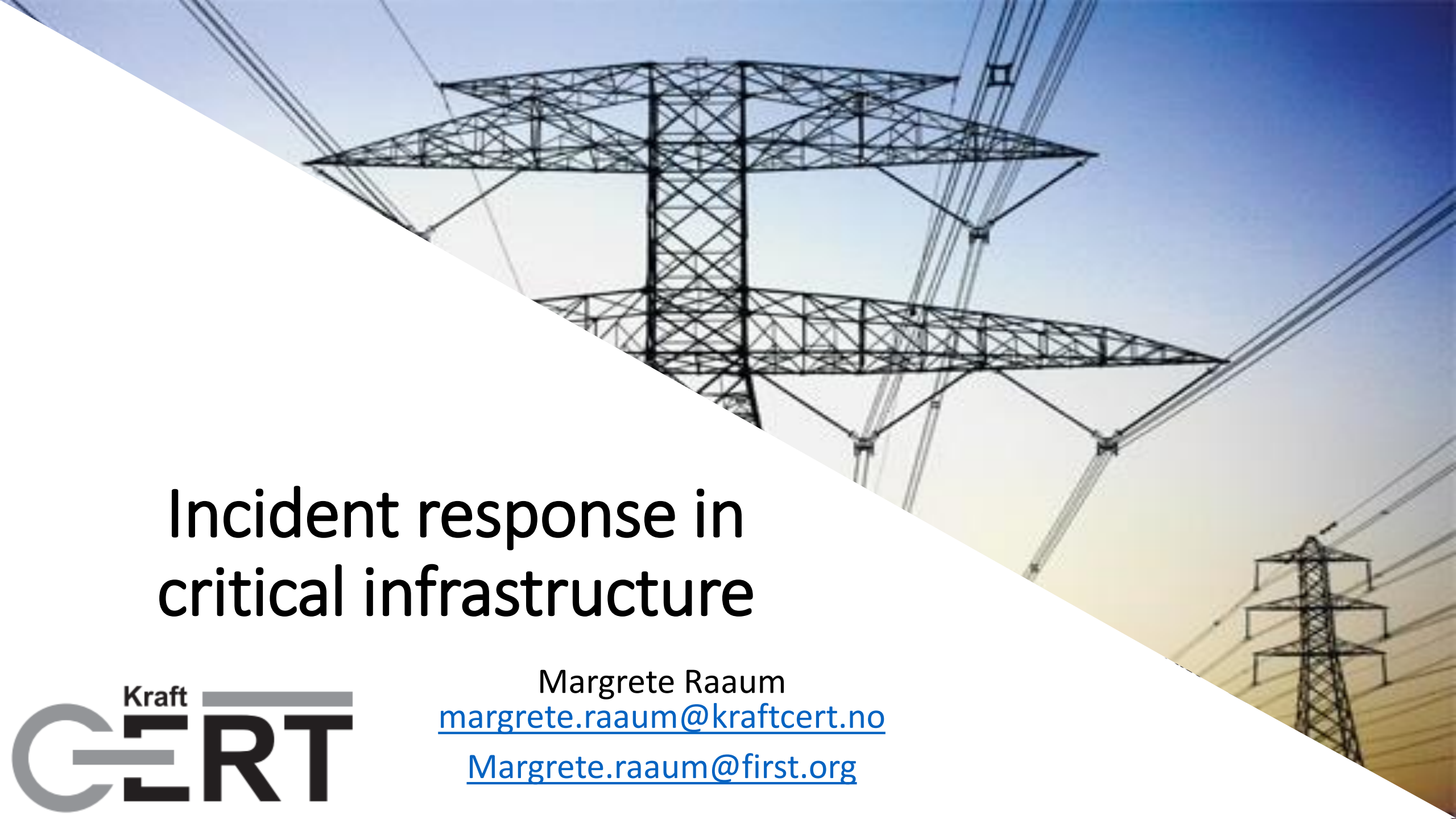


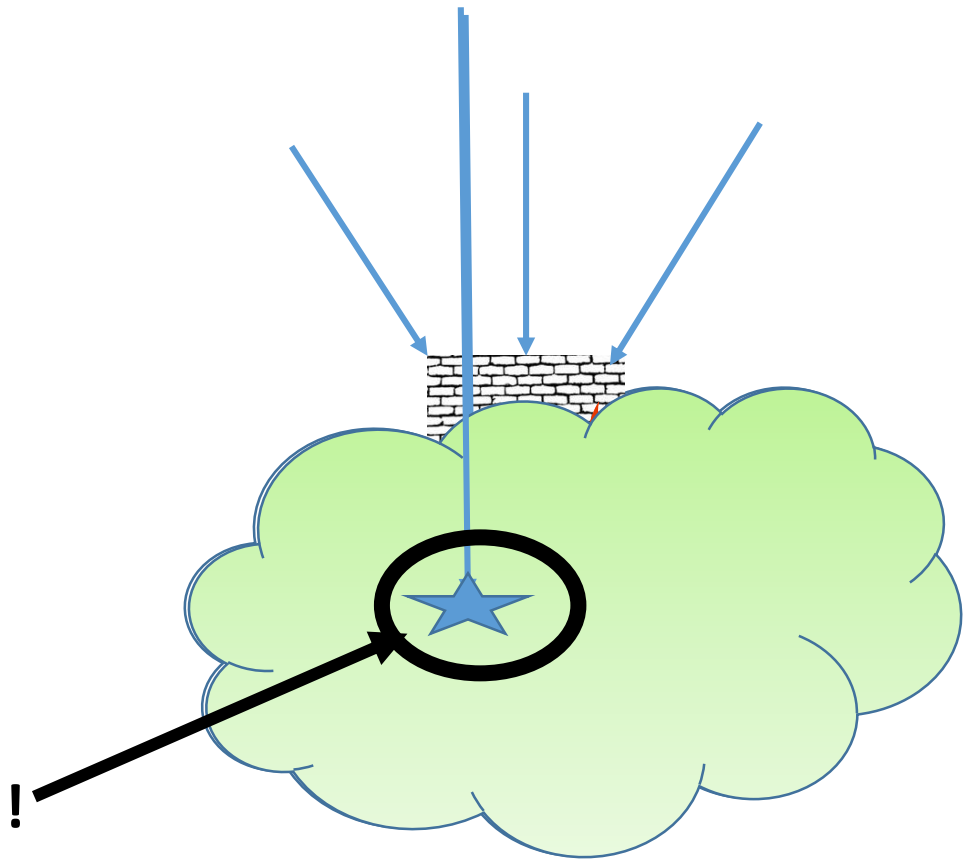
Incident response in critical infrastructure

Margrete Raaum
margrete.raaum@kraftcert.no
Margrete.raaum@first.org

Protection vs readiness

- There is no such thing as absolute security
- Perimeter protection only takes you so far
- Key elements to meet the threats:

- Continuous vulnerability assessment
- Good detection capability
- Incident response readiness



Kraft CERT

Why discussing with industry is difficult

- The perceived security level or threat picture is wrong
- Some do not seek help to avoid exposing themselves as less knowledgeable
- Some are afraid of regulators
- Some think discussing security issues attracts attackers
  - They do not actively attack in particular the ones who care about security
  - It is the internet, they will find you

Kraft CERT

Security capacity issues in companies

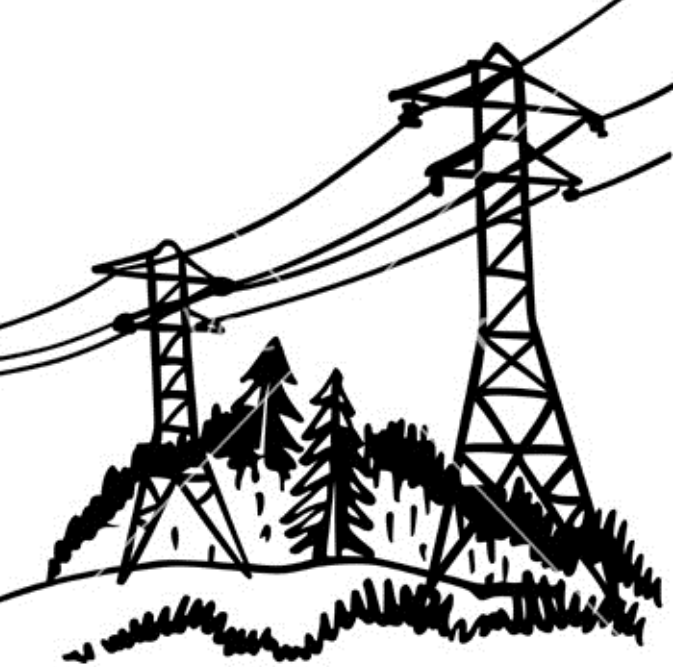
- This work requires highly specialized skill set that has to be maintained continuously
- If there is not a continuous improvement internally, the overall level of security will drop
- Considerations to be done in each company whether other companies be in the same situation, and is this grounds for cooperation?

Kraft CERT

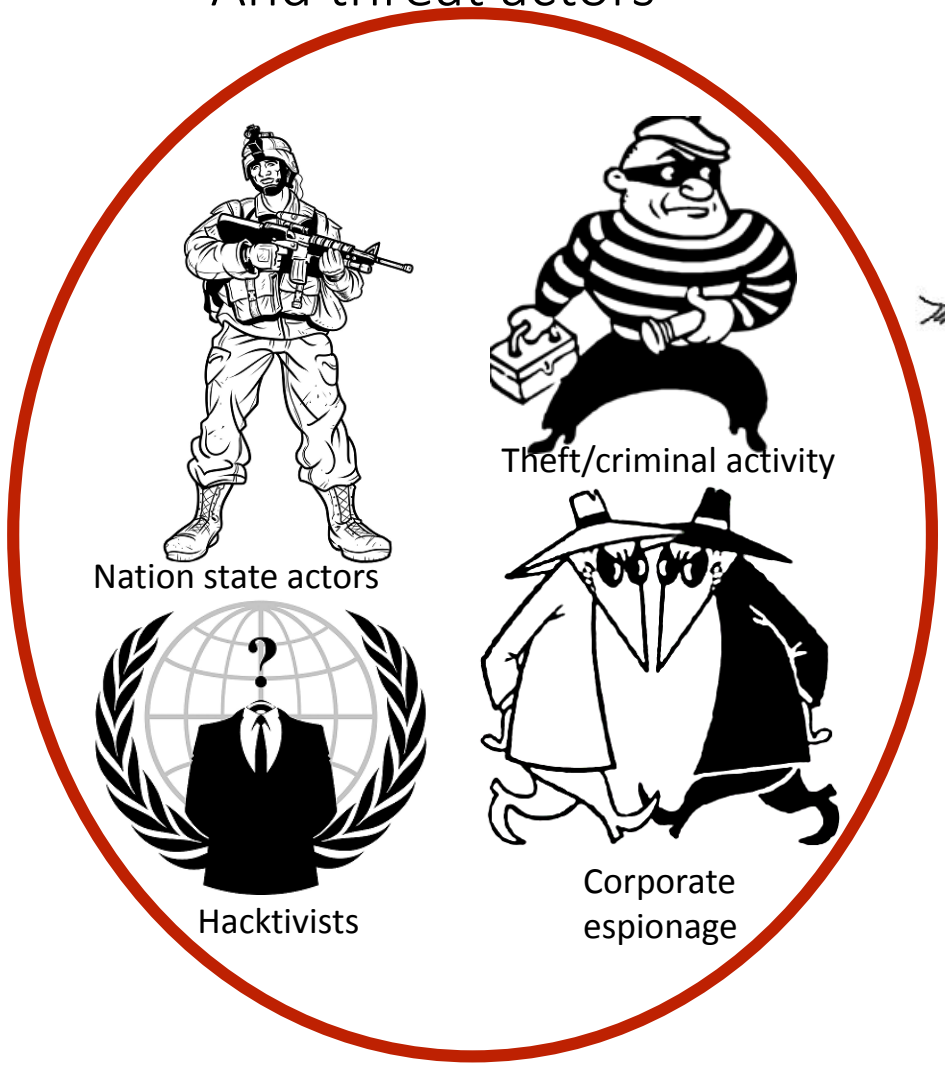
What does it imply, being in the same situation?

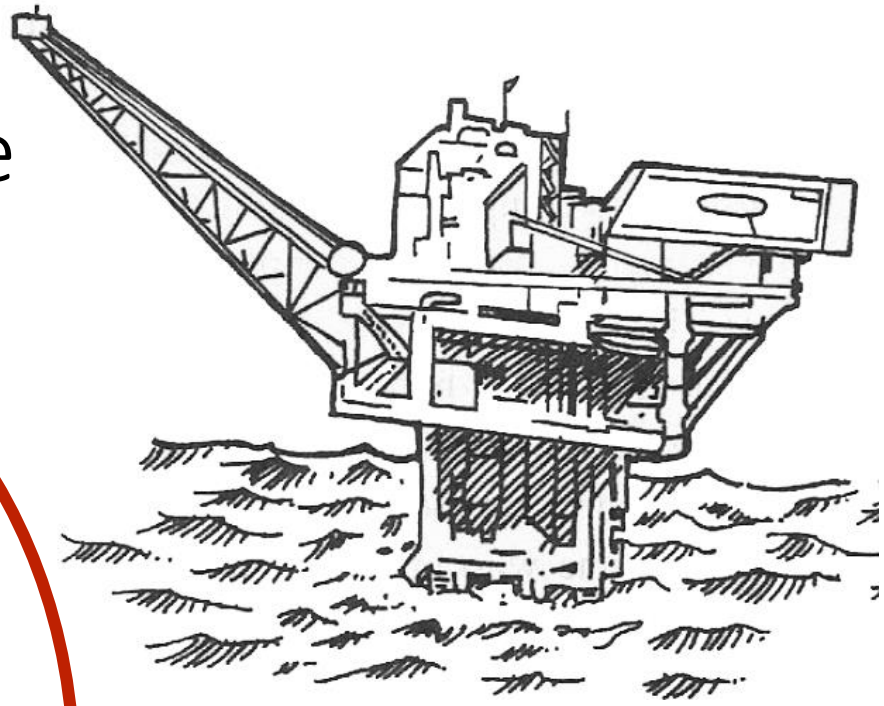
Critical infrastructure

- And threat actors

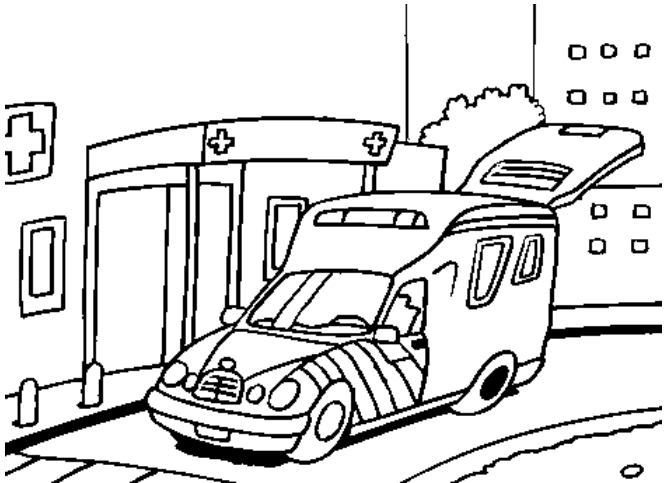


Larger energy companies supply power to many





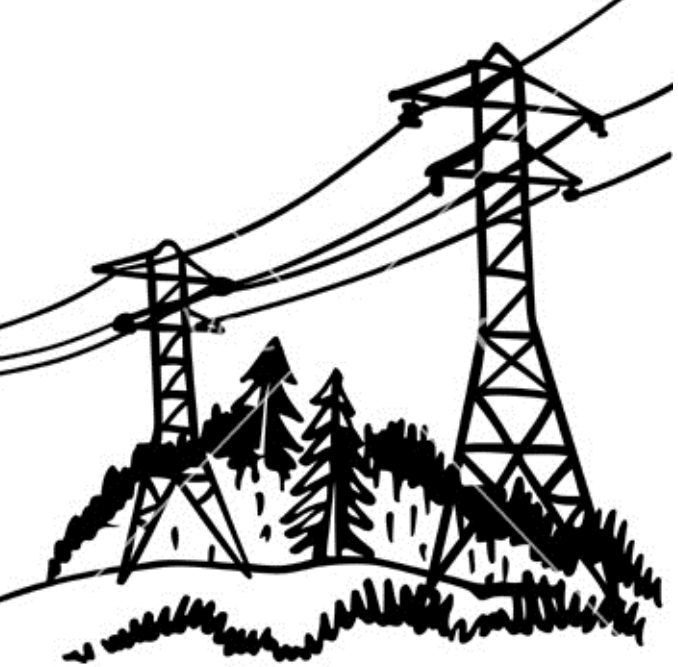
Oil&gas is important to industry, the economy and private parties

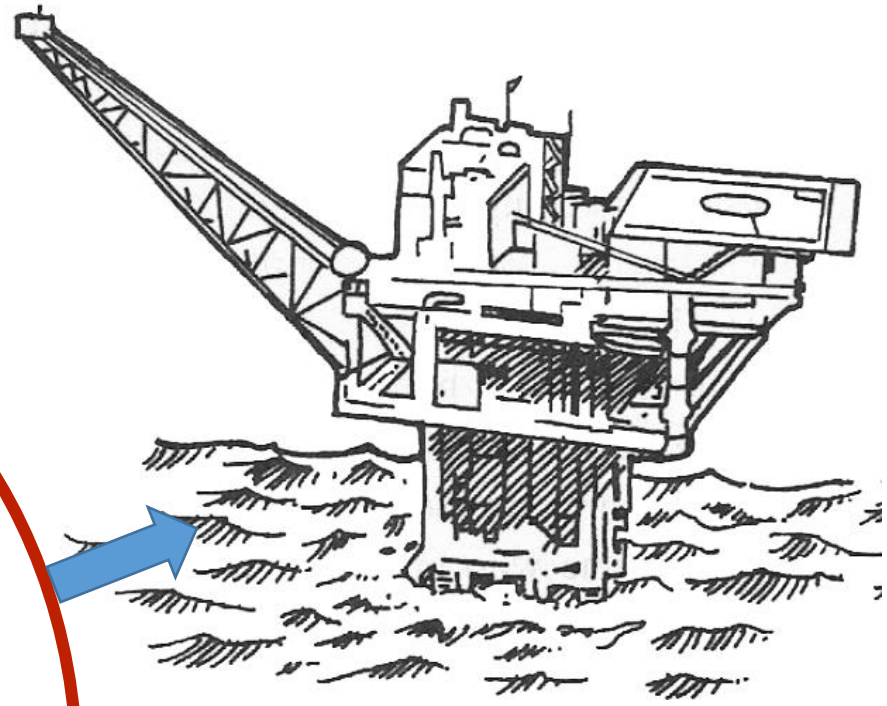


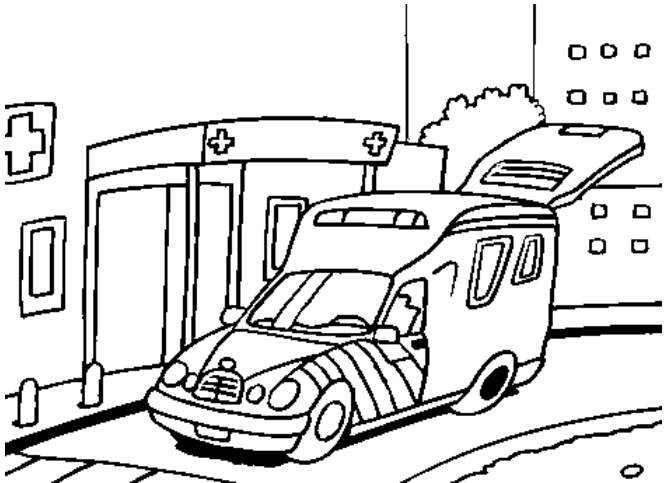
Healthcare – potentially direct loss of life

Smaller utilities provide power to homes

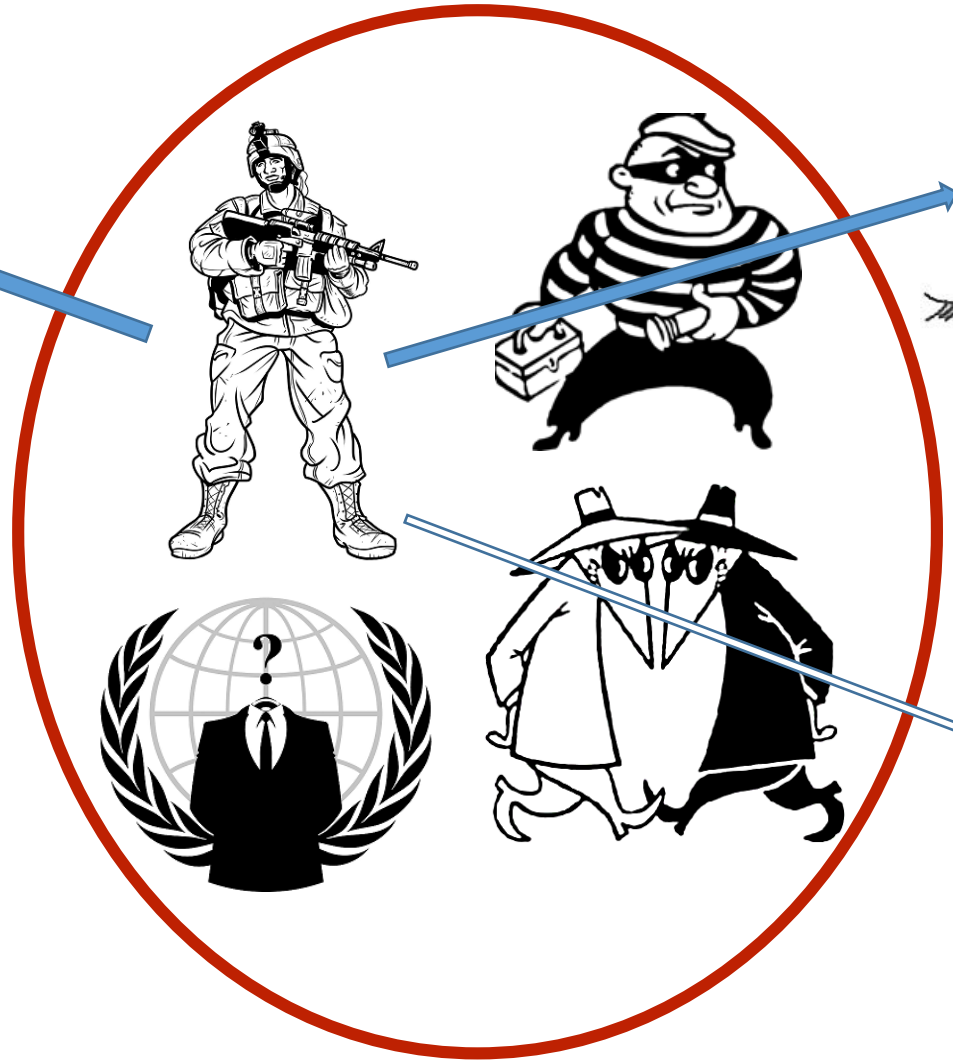
Same attack methods

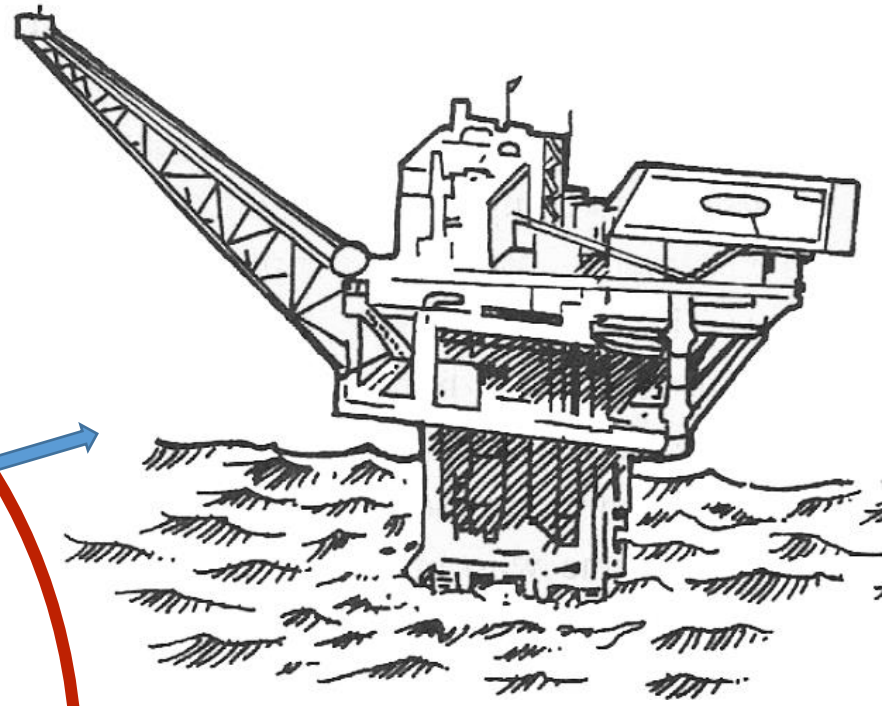


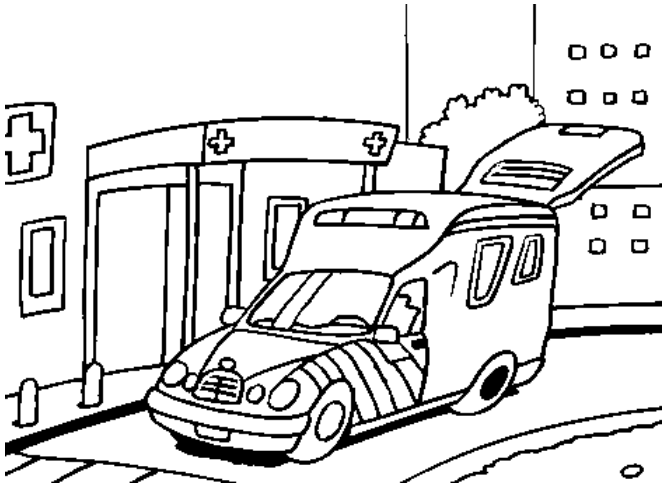


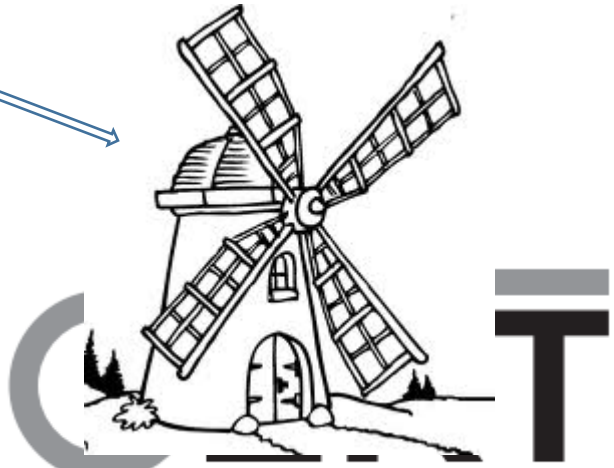


Same threat actors

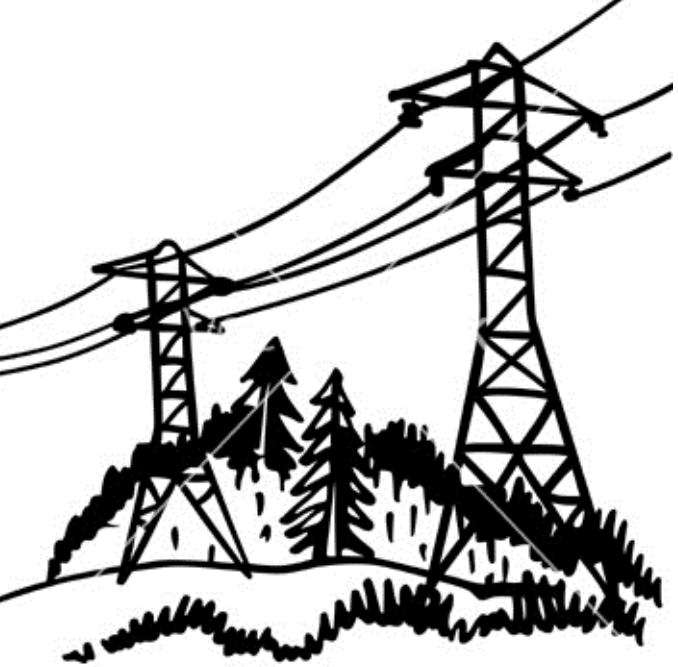


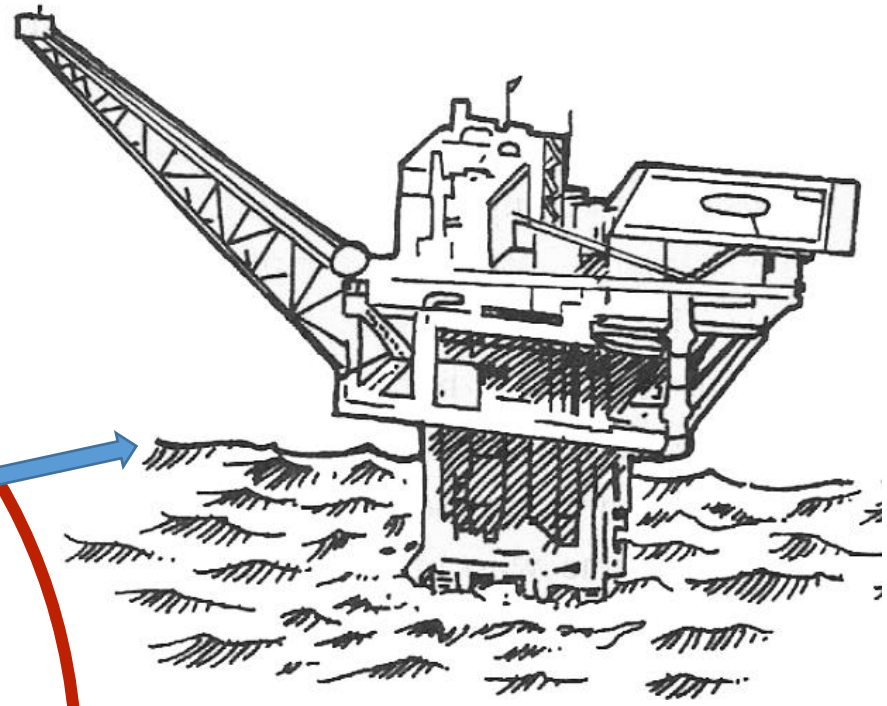


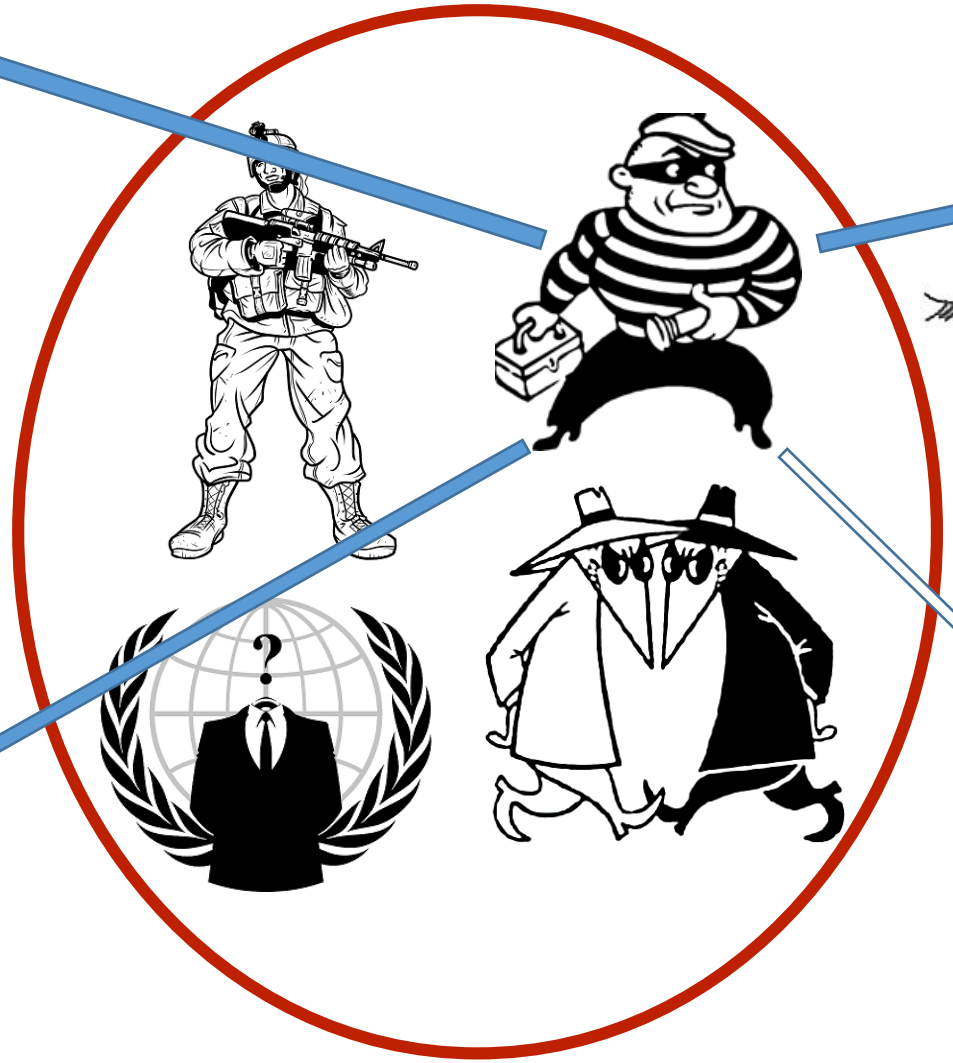


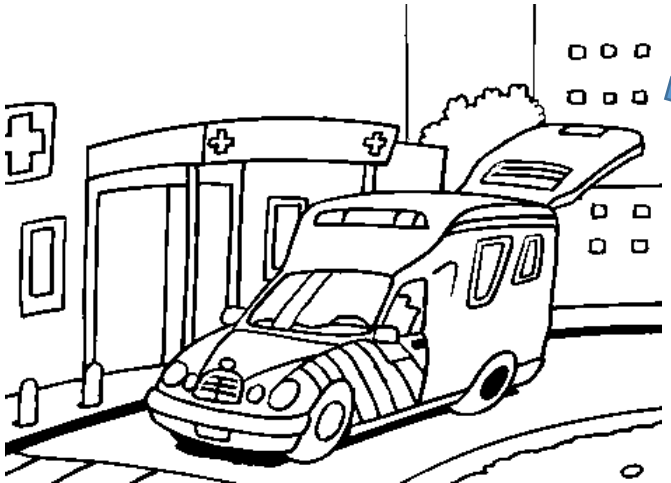


Same threat actors

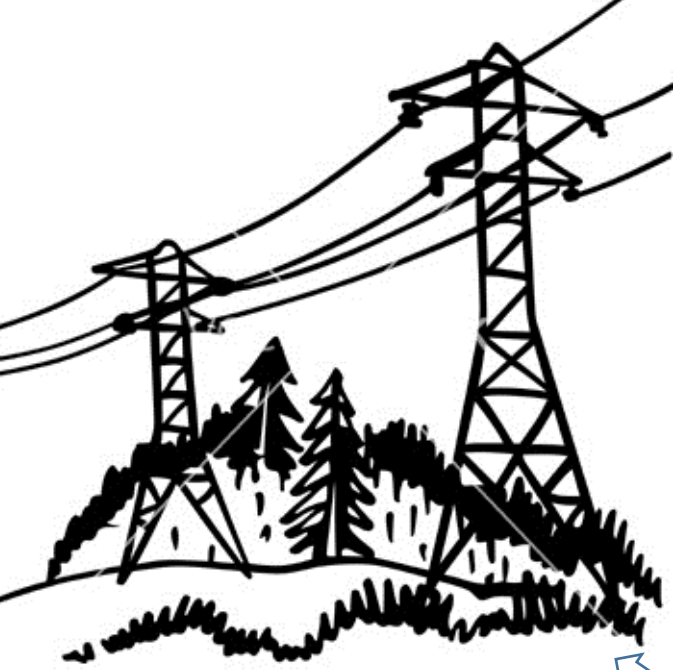


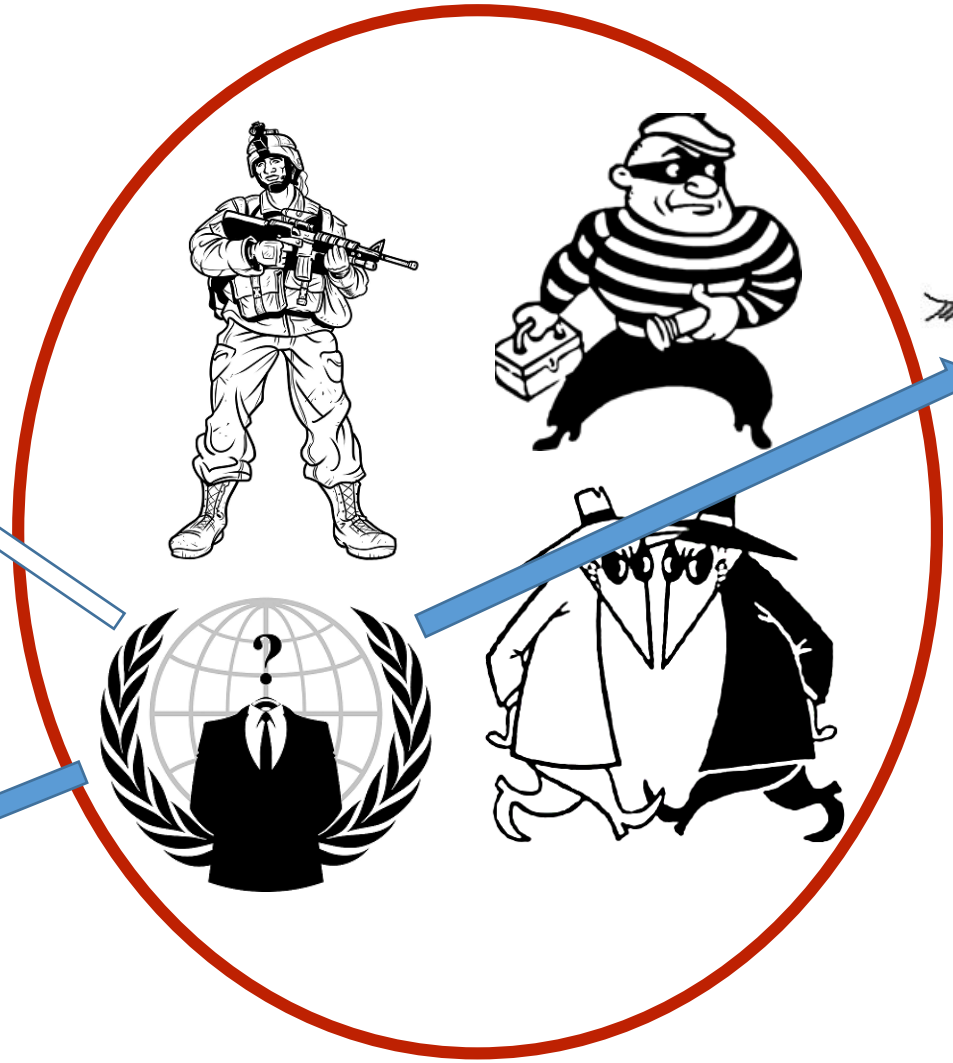


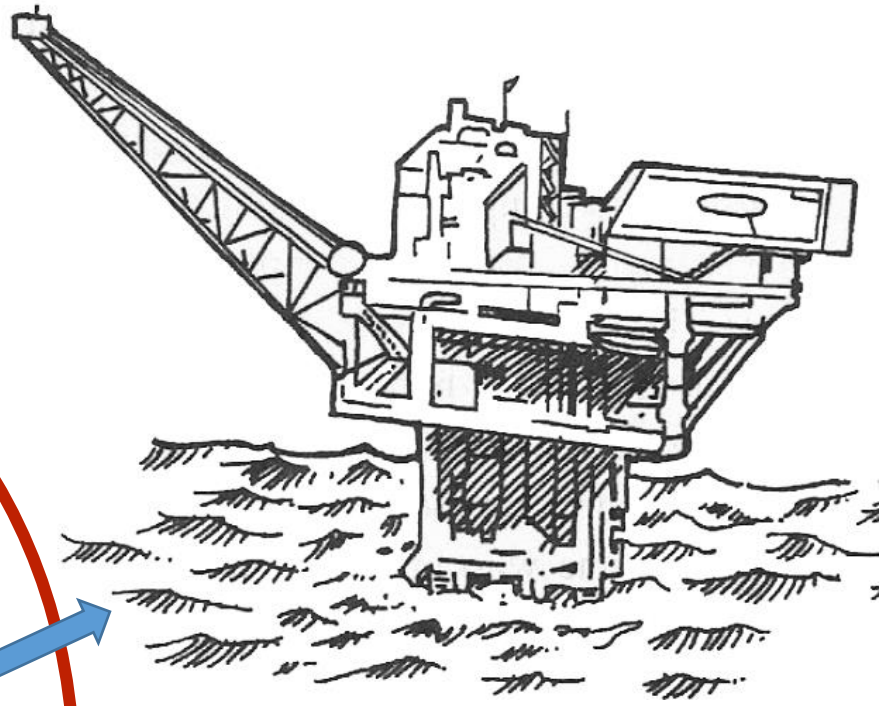


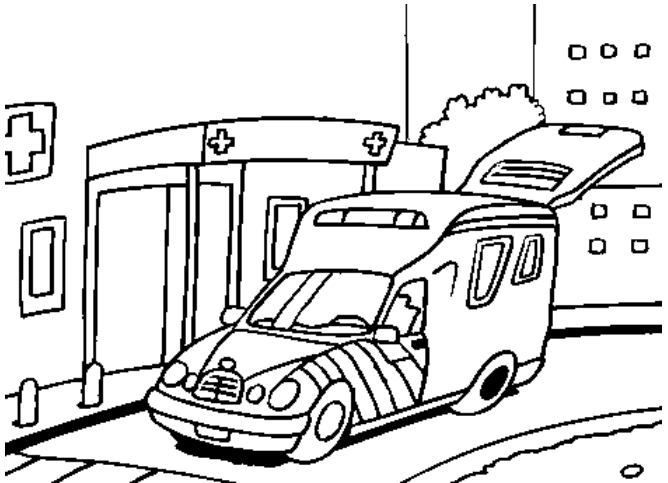


Same threat actors

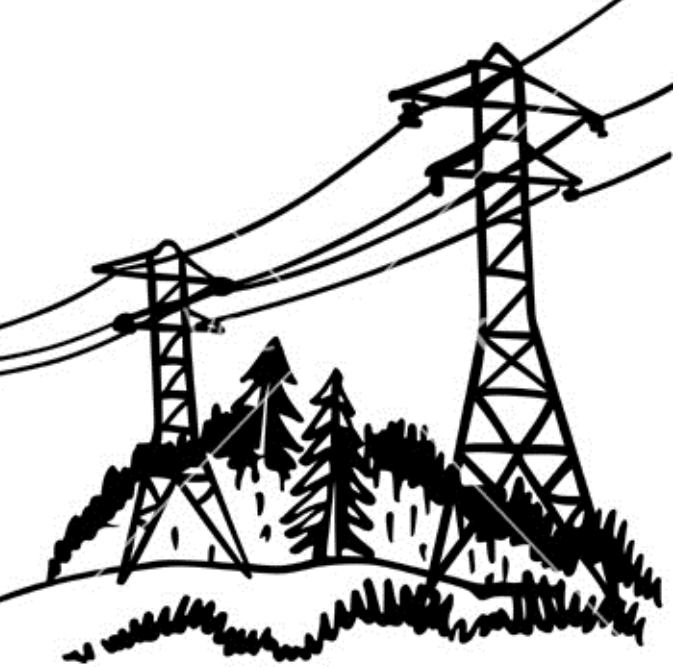


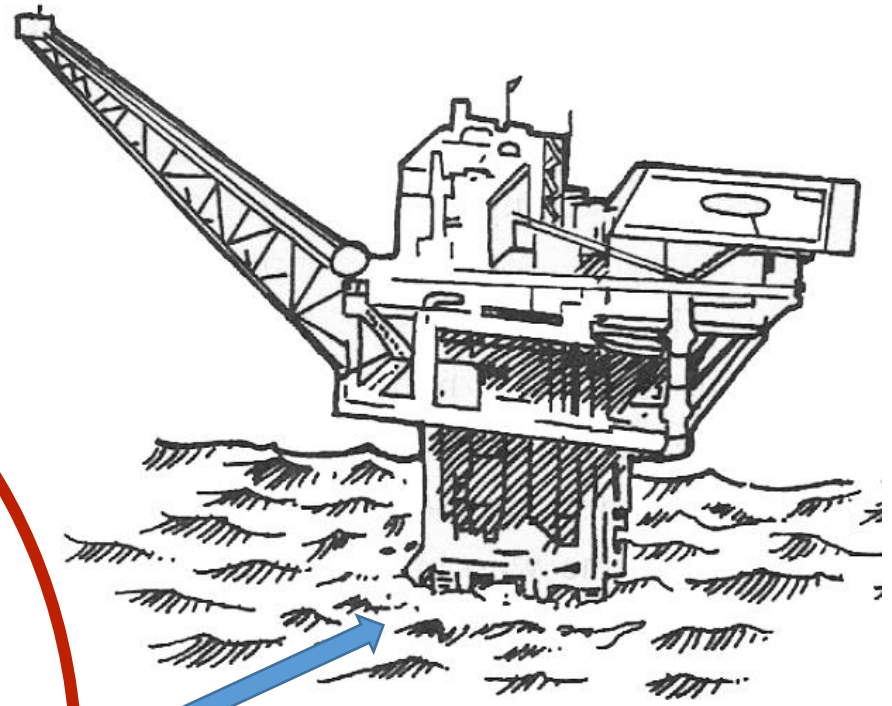


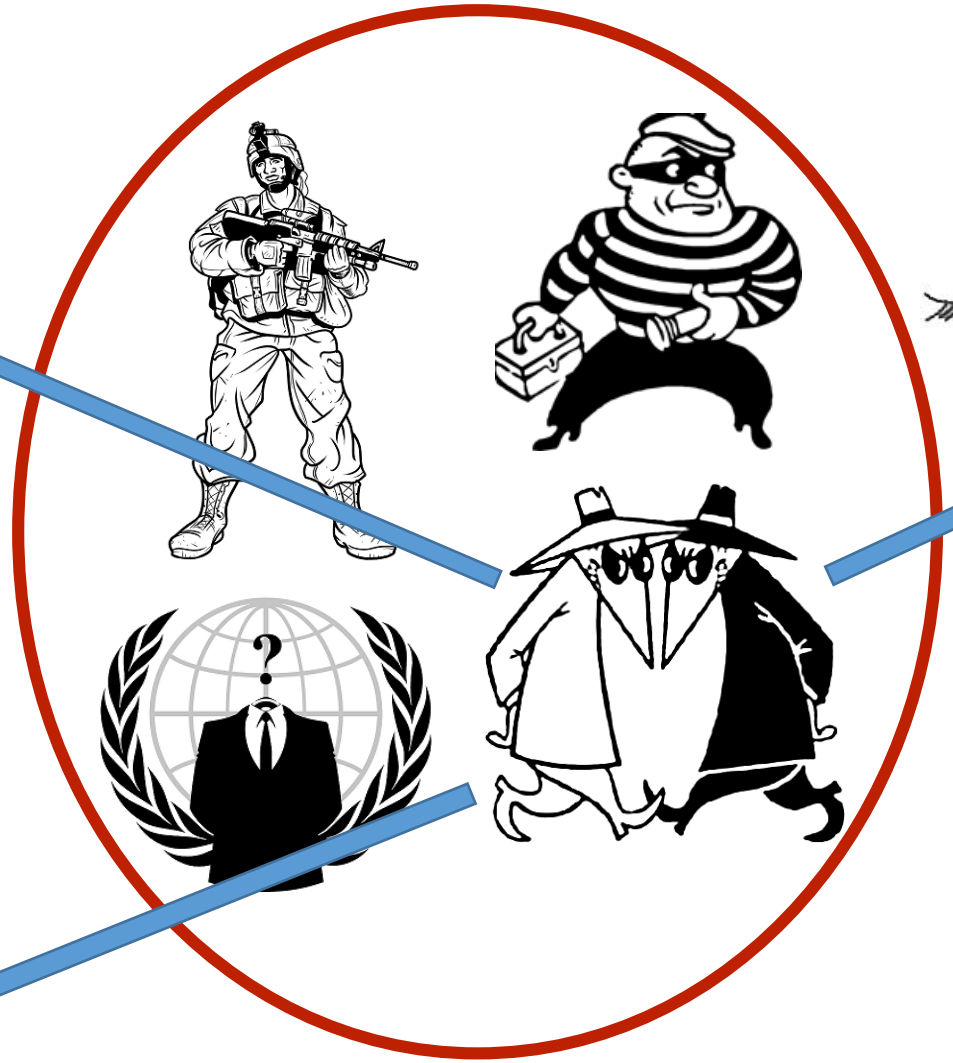


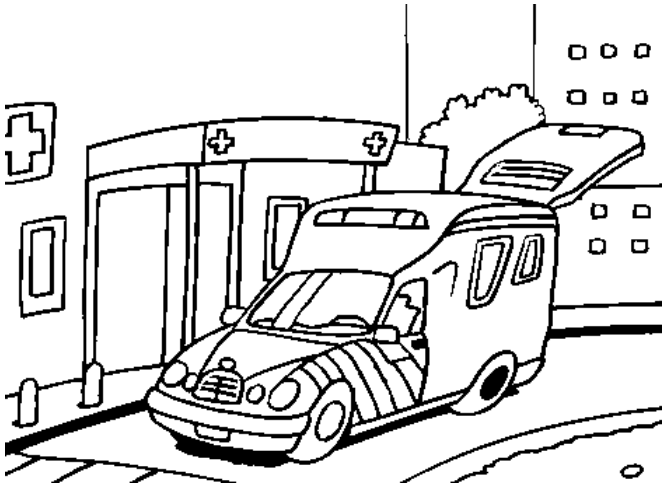


Same threat actors

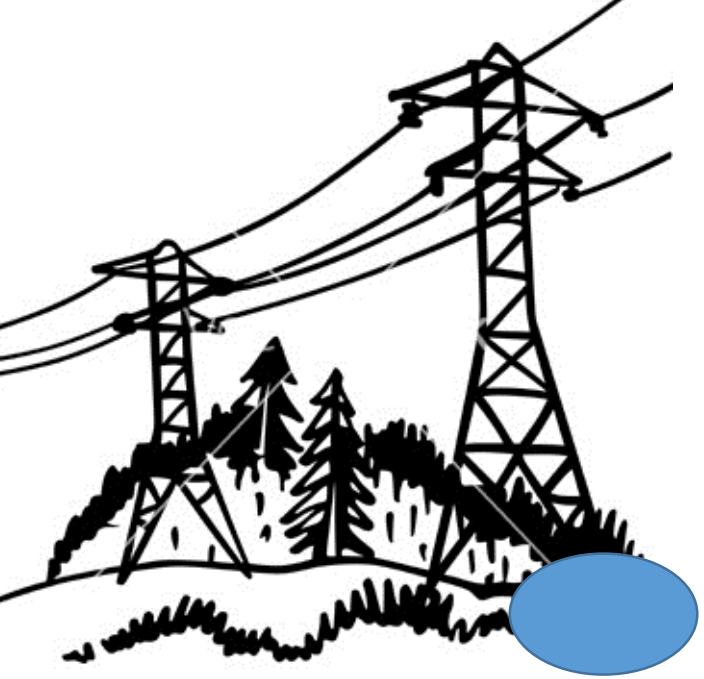


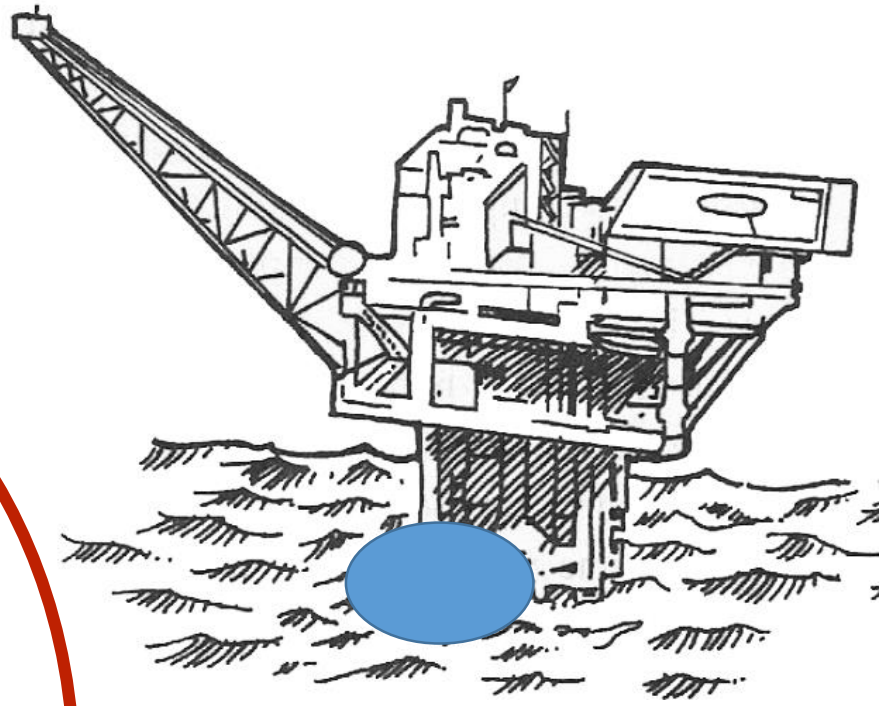


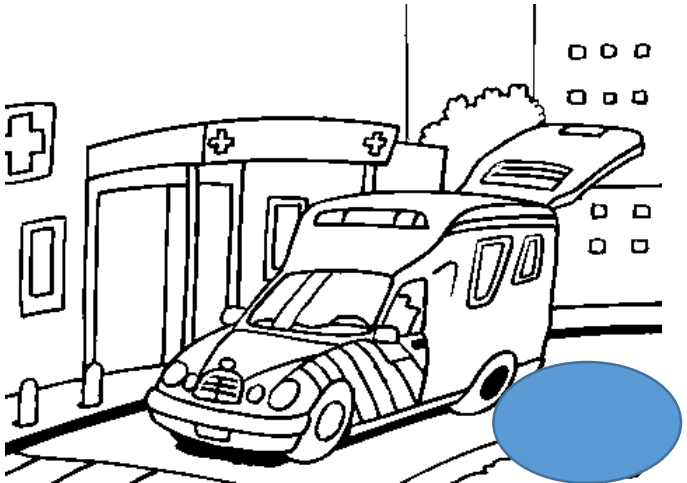




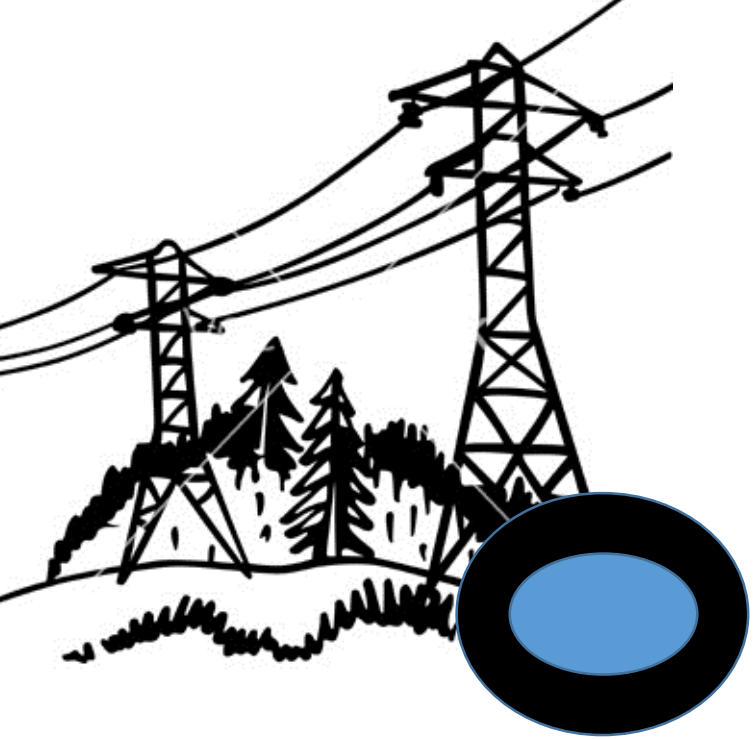
Same vulnerabilities

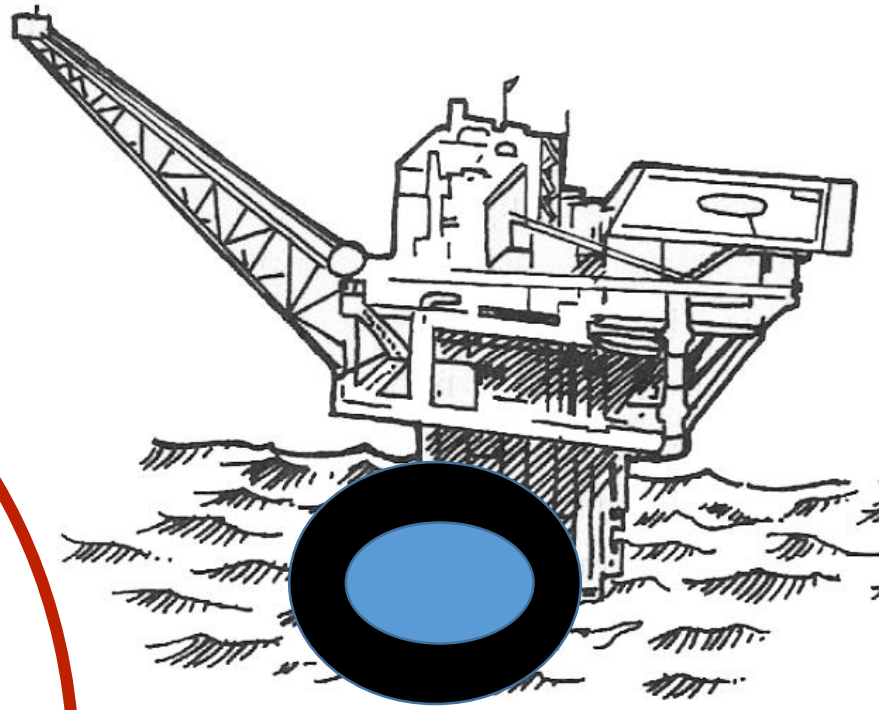


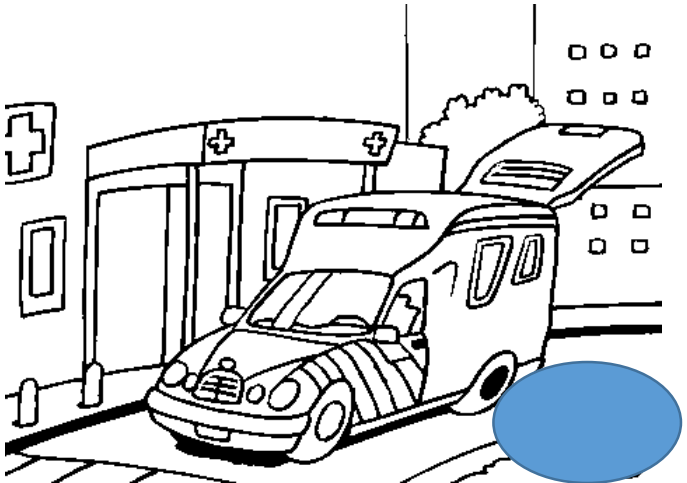




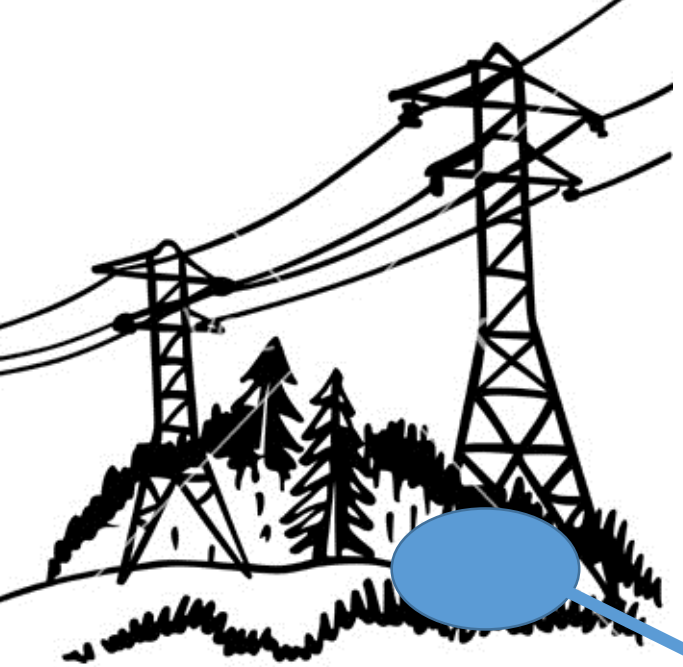
Security maturity

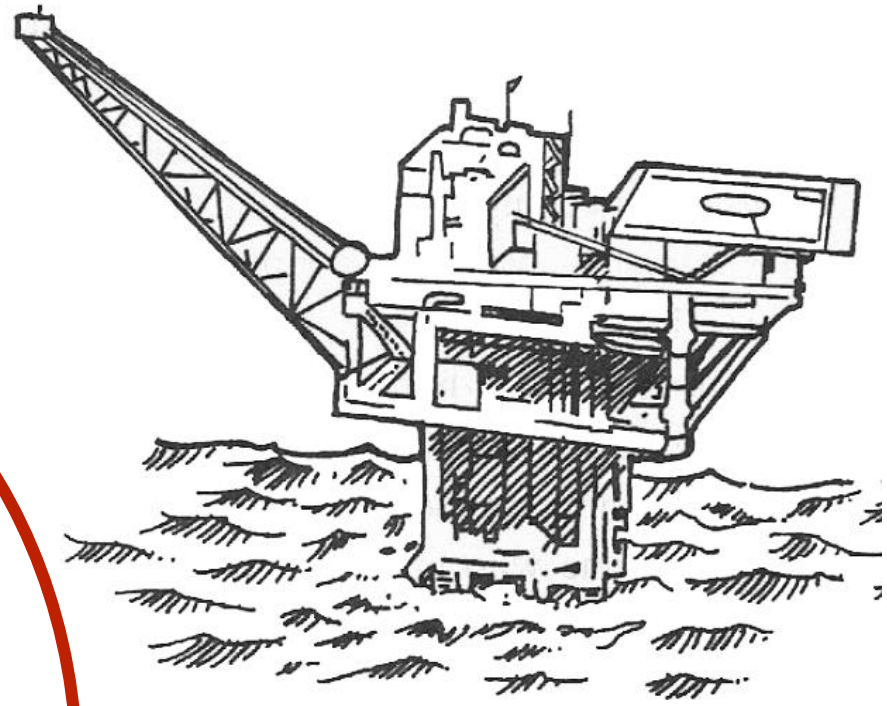


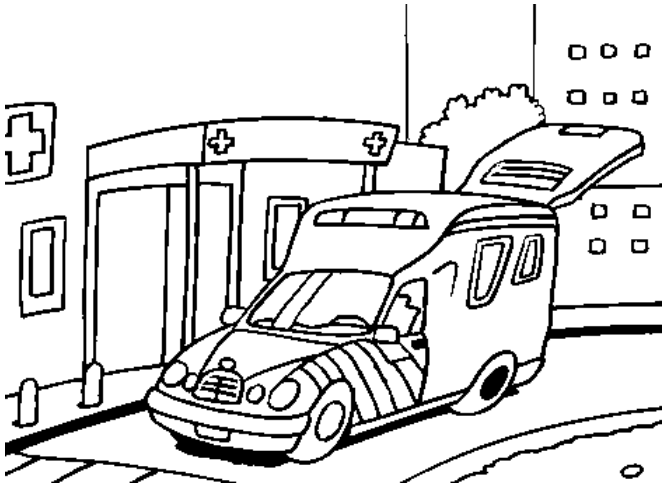




Sector







What now?

- What are we trying to protect?
- Against whom?
- Why do we prepare for the worst?
- How do we prepare?
- How much will this cost me and how mature do we have to be?

Kraft CERT

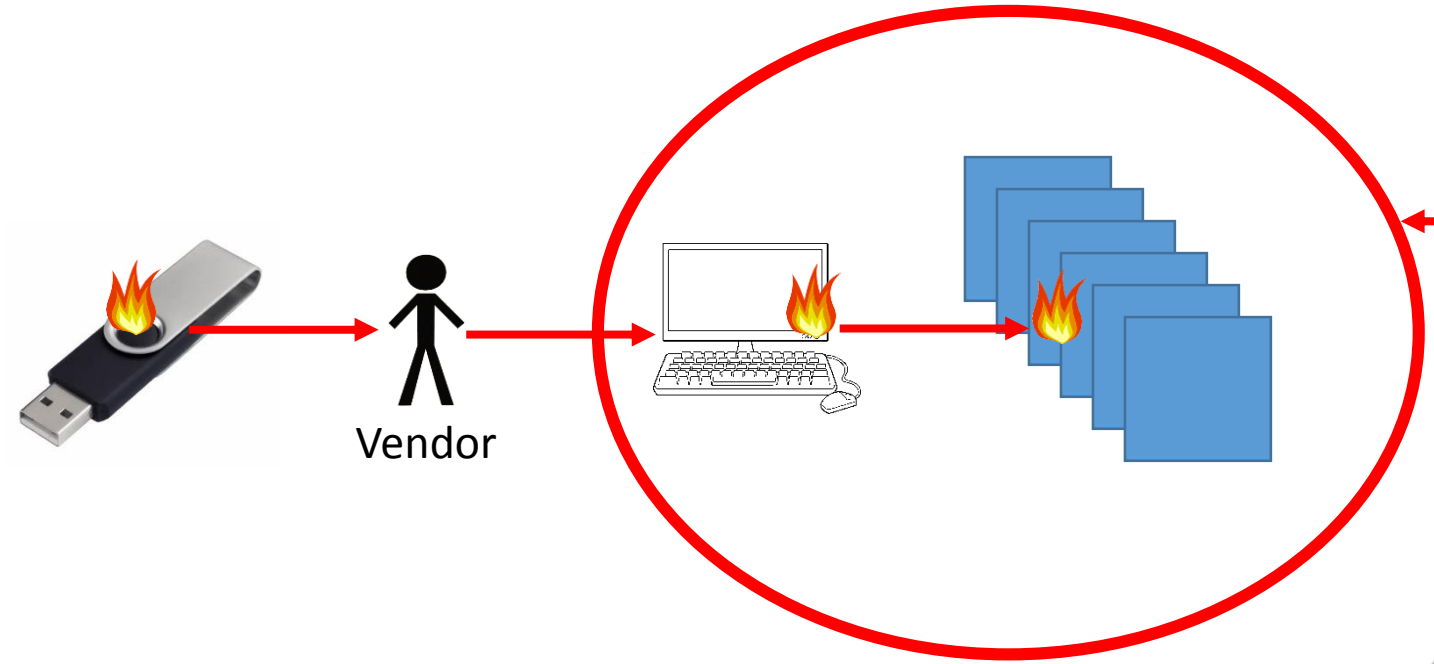
Physical consequences

- 2000: Vitek Boden let out millions of liters of sewage, polluting parks, rivers and buildings
- 2006: Gabriel Murillo and Kartik Patel removed 4 traffic light control boxes from the control grid
- 2008: Polish youth modifies remote control to perform track changes on the tram in Lodz
- 2014: German process industry attacked using APT, the blast furnace ended up in an undefined state

Kraft CERT

And Stuxnet of course

Malware especially designed to destroy Siemens systems



Kraft CERT

This triggers our innermost fears

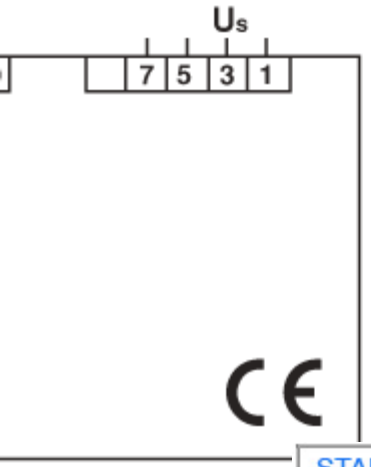
We cannot rely on feedback:

- What we see is not the reality (healthcare, energy, water, food)
- The commands you perform does something other than what it's supposed to do
- Undefined states

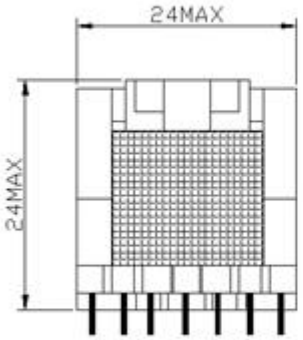
Kraft CERT

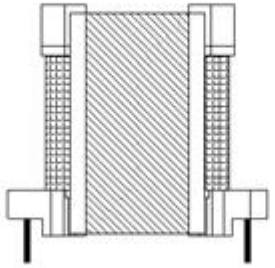
- What kind of leaks are we protecting?

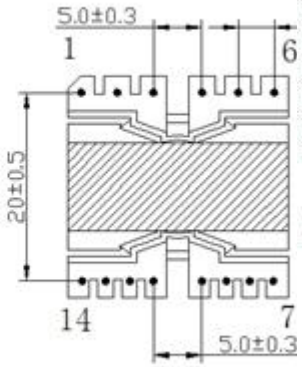
Sensitive information - sabotage



Us
7-1 = 380-415 Vac 7-3 = 220-240 Vac 7-5 = 110-127 Vac-dc
7-3 = 48 Vac-dc 7-5 = 24 Vac-dc





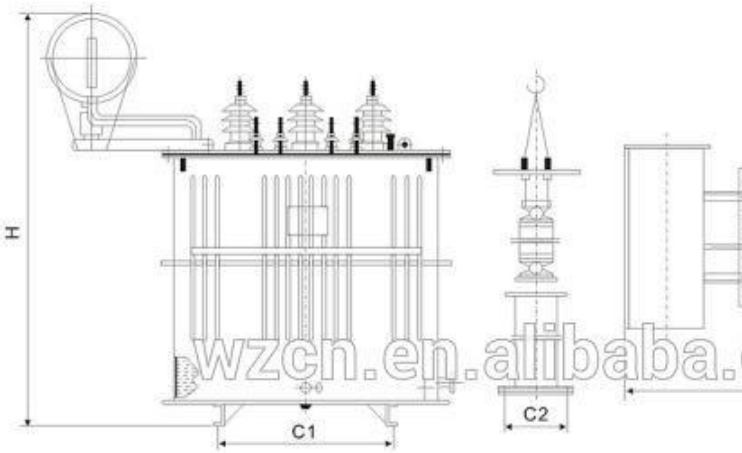


S11 type oil immersed distribution transformer of 6~10kV

Main Technical

Rated capacity (KVA)	Voltage combination (kV) H.V	High voltage tapping range	(kV) L.V	Connection symbol	Loss(kW) Load	No-load
10					0.26	0.06
20					0.44	0.08
30					0.6	0.10
50					0.87	0.13
63					1.04	0.15
80					1.80	0.18
100					1.5	0.20
125	6	± 5%	0.4	Yyno	2.45	0.24
160	6.3	± 2 × 2.5%		Dyn11	2.2	0.28
200	6.6				2.6	0.33
250	10				3.05	0.40
315	10.5				3.65	0.48
400	11				4.3	0.57
500					5.1	0.68
630					6.2	0.81
800					7.5	0.98
1000					10.3	1.15
1250					12	1.36
1600					14.5	1.64
2000					18	1.96

Outline and installation size



Outline and installation size of transformer of S11-10~2000/

STANDART ÖLÇÜLER TEKNİK ÇİZİMİ

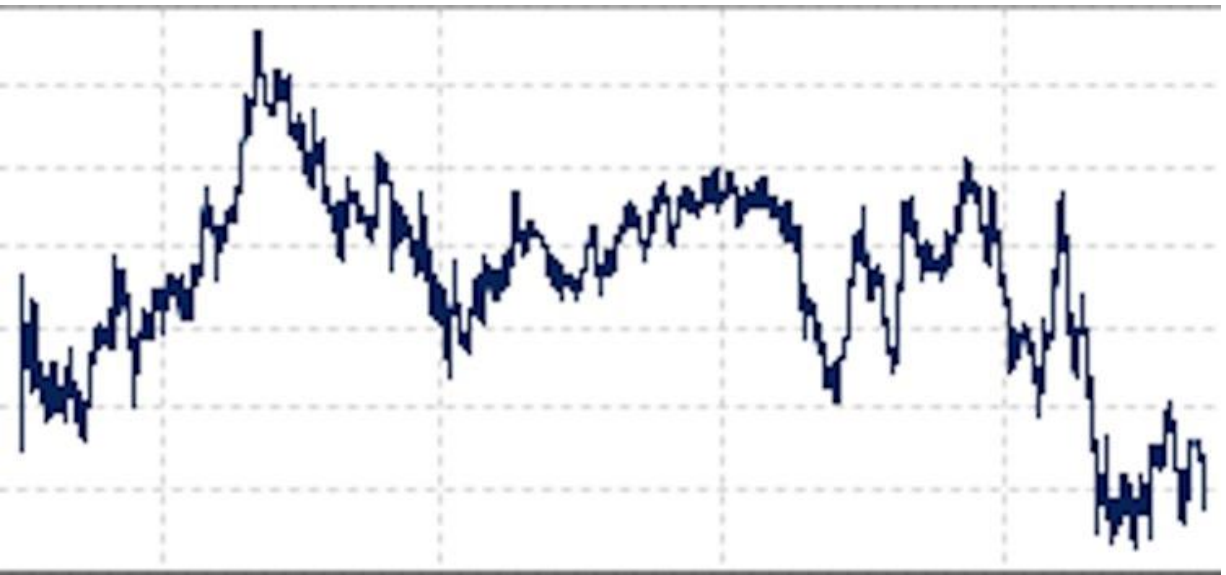
STANDART ÖLÇÜLERİN TEKNİK ÖZELLİKLER

Kod	Kesit	d	d1	d2	L	a	b	s
SKP 06	6	M5	4	5.5	25	10	8	1.3
SKP 10	10	M6	5	6.5	27	11	10	1.5
SKP 16	16	M6	6	8	33	15	11.5	2
SKP 25	25	M8	7	9.5	37	16	13.5	2.5
SKP 35	35	M10	9	11.5	44	19	17	2.6
SKP 50	50	M10	10	13	46	20	18.7	3
SKP 70	70	M10	11.5	14.5	51	24	21	3
SKP 95	95	M12	13	16.5	57	26	23	3.5
SKP120	120	M12	14.5	18	61	27	26.5	3.5
SKP150	150	M12	17.5	22	72	33	32	4.5

Sensitive business information

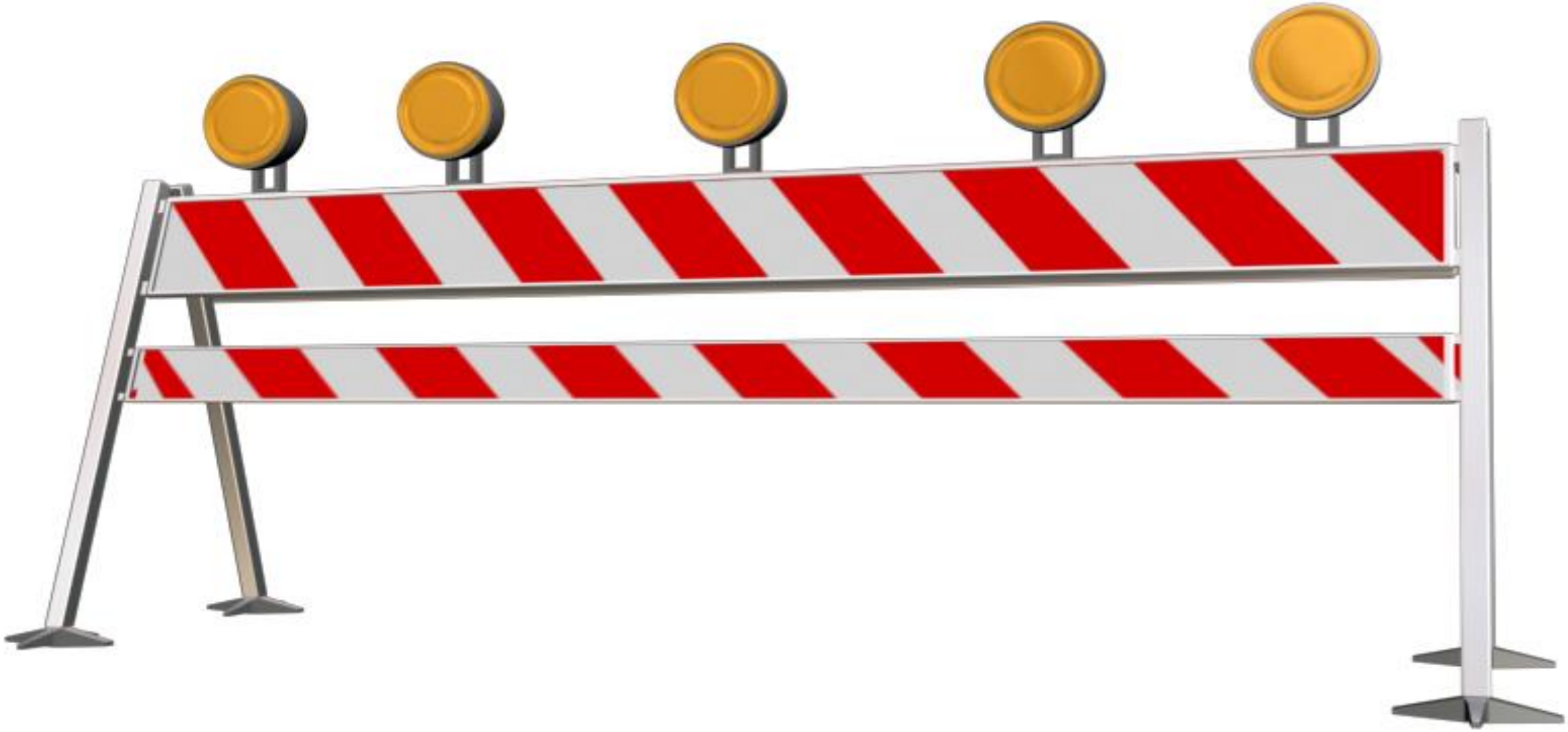
Kraft CERT

Sensitive marked information



Kraft CERT

Privacy-sensitive information



Critical services

- Cannot be taken offline
- Logging, audit or forensic activity cannot affect the system
- 1st priority is to get systems back online
  - Replace, overwrite, reset
- What if the problem already propagated?
- How important is finding root cause?

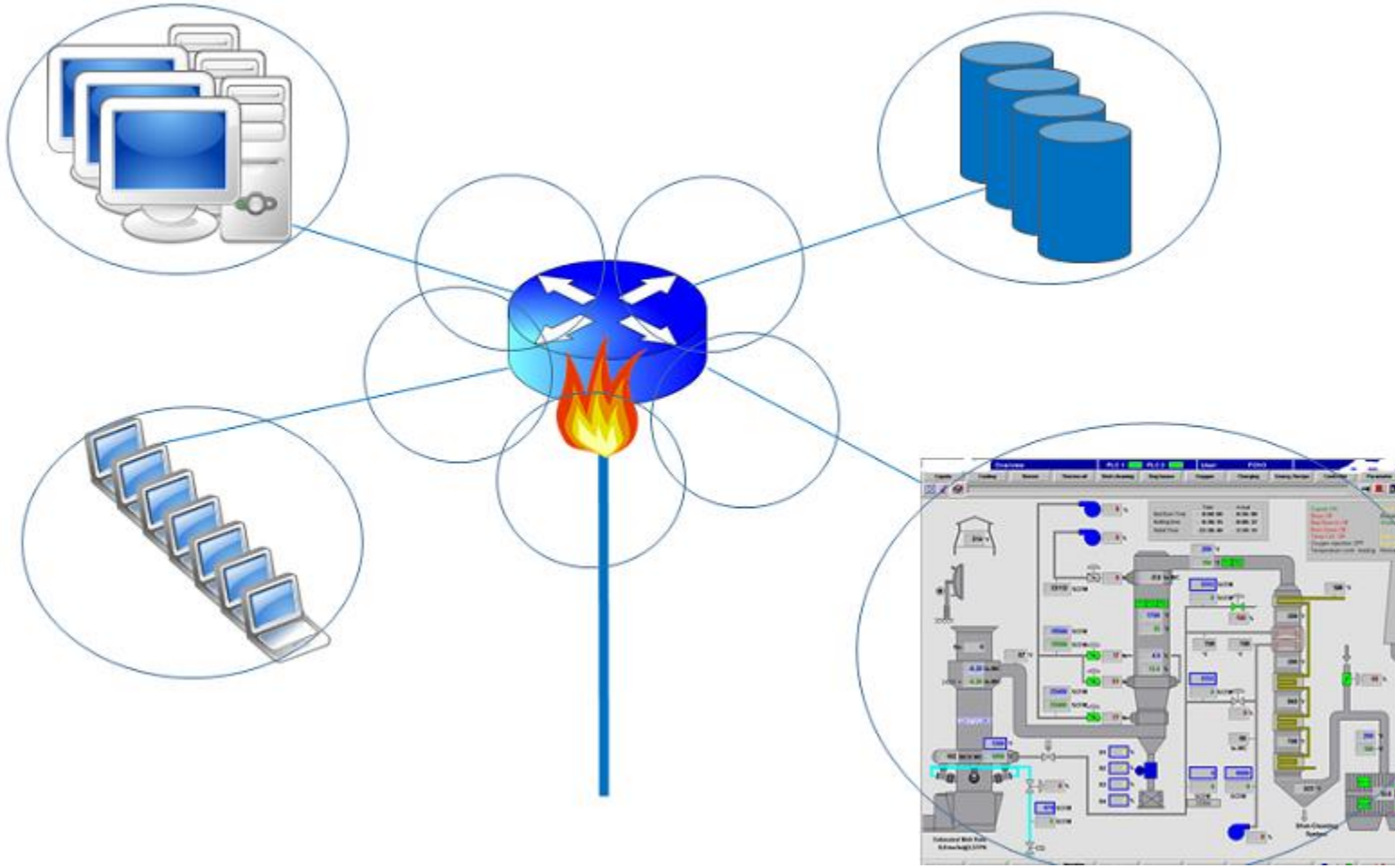
Kraft CERT

Security solution issues

- Sales people want to sell
- Open source is coming but resources are needed
- Who’s first

Asset control

- Where does the data flow
- What kind of data
- Which protocols
- How do you isolate an incident
  - In the critical part of the network
- Is the classification of criticality clear?



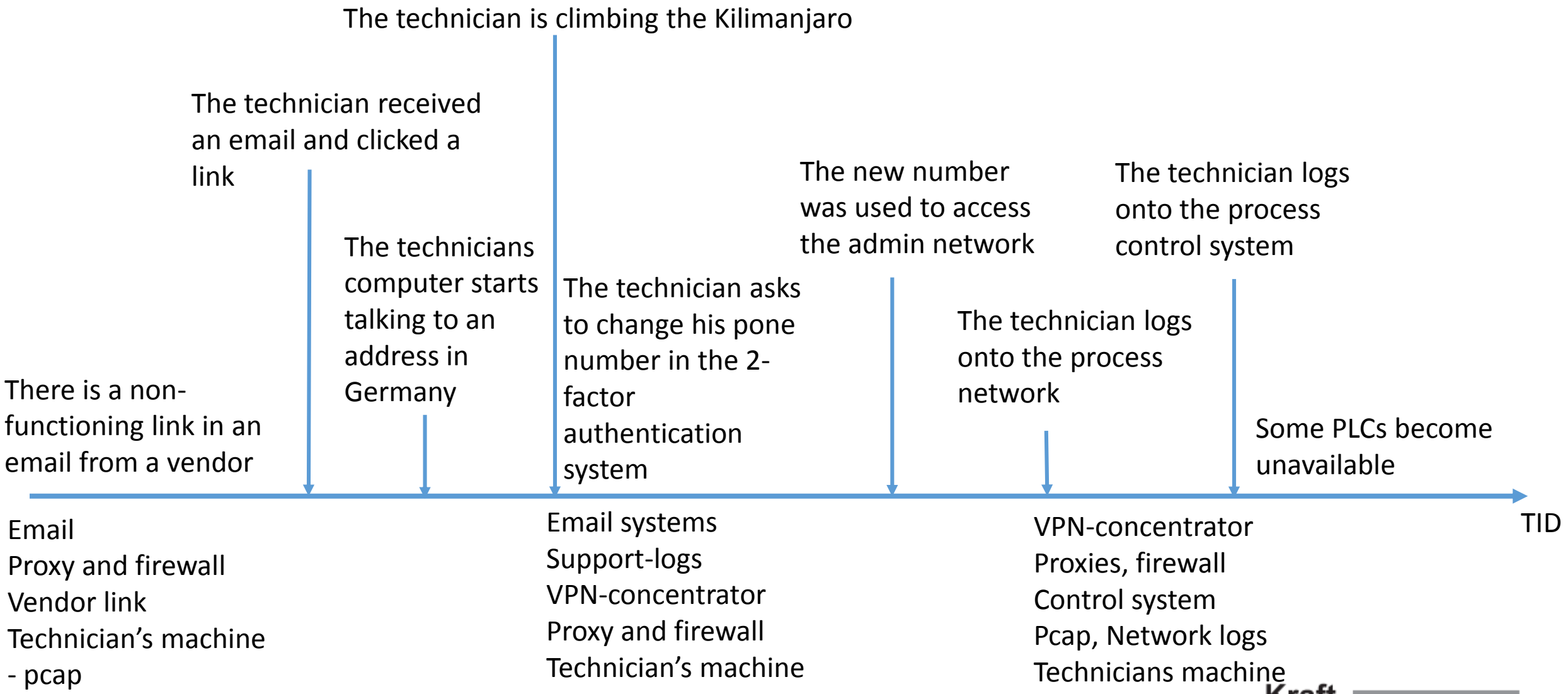
Kraft CERT

Logging in critical infrastructure

Without a timeline this makes no sense:

- The technician asks to change his phone number in the 2-factor authentication system
- Some PLCs become unavailable
- The technician is climbing the Kilimanjaro
- There is a non-functioning link in an email from a vendor

Kraft CERT



Kraft CERT

Evidence:
Testimony/transcripts, logs pcap, forensic image from technician, vendor, control system

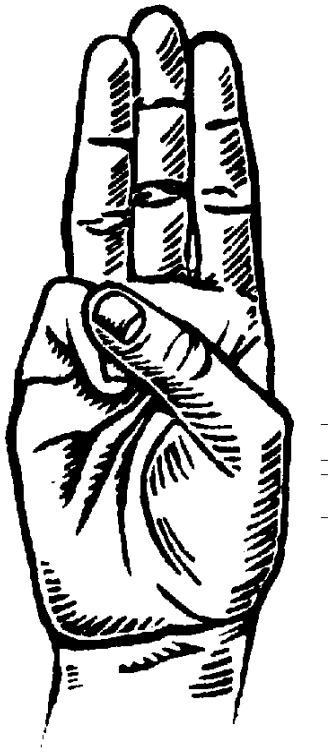
Tidiness

- What happened and why, how do we isolate it?
- Evidence and chain of custody
- How to store evidence
- Digital signing
- Working with legal departments

Kraft CERT

Readiness

- Knowing where the logs are and how to access them
- To be able to look at raw network traffic
- Basic forensic capability
- Keeping the toolbox up to date
- Knowing your network and whom to ask for assistance



Kraft CERT

The dedicated incident response team

- Incident handling will be done quick and consistent
- Avoiding costly mistakes
- The team knows what to do and whom to inform
- They gain control
- The defuse the situation internally and with partners or customers
- They break down the silos
- The ensure learning and provide material for regulator reports

Kraft CERT

Tying it all together across borders

- We can share
  - Attack patterns
  - Target trends
  - Adversary intelligence
  - Vulnerabilities
- We can join forces in assessing the real threat presented by specific vulnerabilities or attacks
- If all are to do this, there will be a lot of overhead

Building a robust network

- Large variations in company size and level of competence
- Larger actors
  - Can be a resource to the others in the sector
  - Can have done investments that can benefit all
  - Can initiate and demonstrate the benefits of information sharing
  - Will also learn from participating
- We hoped that a sector based CERT would facilitate a trusted environment
- Bring the smaller actors are brought up to a level where they can to a larger degree collaborate well with the large actors

Kraft CERT

It is all about trust

- Private non-profit or public support
- Voluntary vs mandatory
  - Mandatory is not trust based, less likely to increase information sharing
- Hierarchical networks
  - Data ownership
  - Delay
  - Sector specific challenges and competence
- Smaller and more homogeneous constituency:
  - Makes it easier to agree on mandate and services
  - Makes it easier to achieve acceptance for extra cost

Kraft CERT