Physical Security

Artificial Intelligence & Open-Source Intelligence for Nuclear Facilities

Christina Lekati

Social Engineering Security
Trainer & Consultant
Cyber Risk GmbH

About Me

Christina Lekati

- Psychologist & Social Engineer
- Trainer & Consultant for Cyber Risk GmbH on the Human Element of Security
- Corporate & HVT Vulnerability Assessments based on OSINT
- Open-source intelligence investigations & trainings
- Executive Board Member of the OSINT Curious project

Physical Security: What Do Threat Actors Look For?

Threat actors may:

1. Breach the security of an organization with the intention of causing **technical failures** and plan an **unauthorized access** scenario.

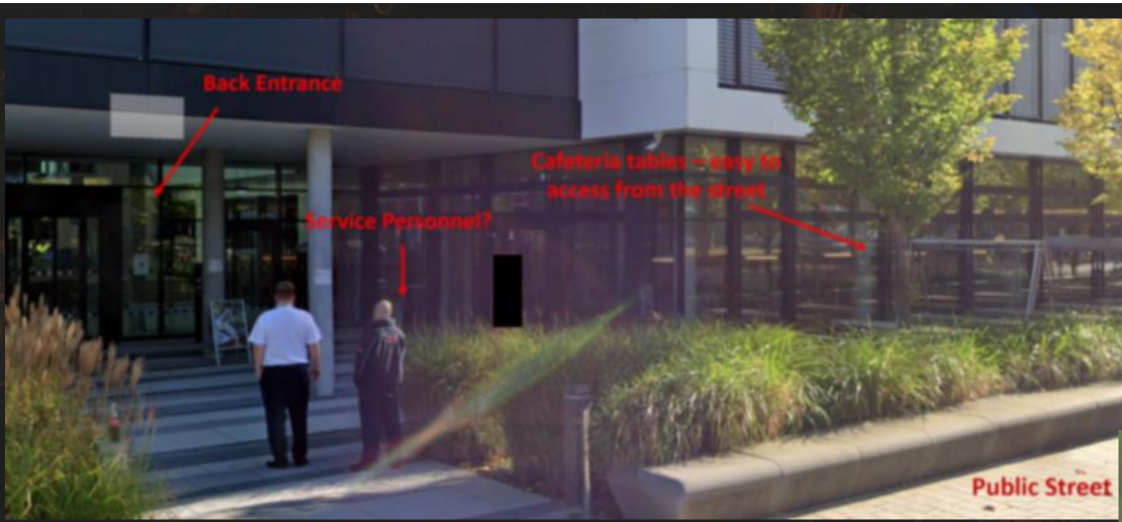
2. Will perform reconnaissance to learn how to move **around in that area** & pair it with a social engineering scenario that will give them **authorized access.**

Physical Reconnaissance (OSINT) Looks Into…

EXTERIOR:

- ☐ The location of the main entrance and its overall construction.
- ☐ The pathway/surroundings leading to the main entrance.
- ☐ Hidden entrances, especially at the back of the building along with the surroundings. Are there any doors that seem to be used by service personnel alone?
- ☐ External areas where employees seem to hang out.
- ☐ Type of fencing.
- ☐ Potential security/guard posts.
- ☐ Parking lots & how they connect to the main building.
- ☐ Surveillance & security technology placement (sometimes these are very visible).

Examples:

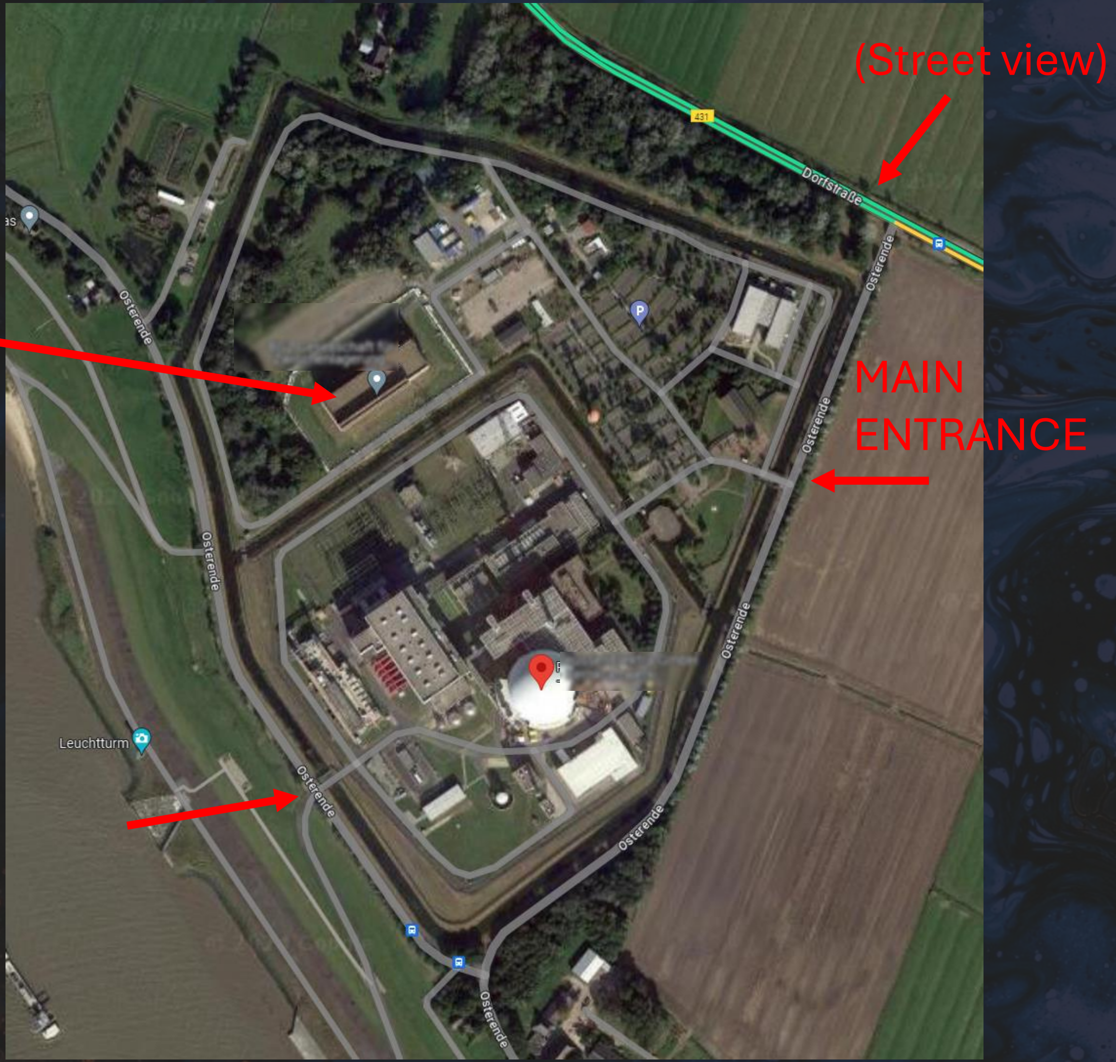


[redacted]

Physical Reconnaissance (OSINT) Example

(Germany) - Nuclear Power Plant

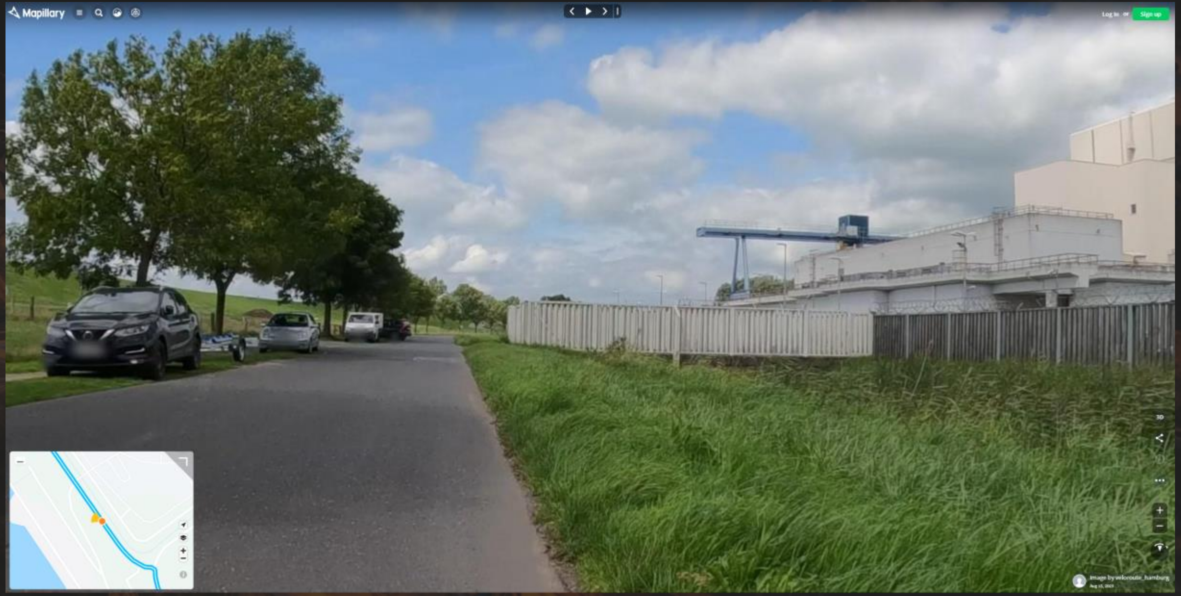
Google Maps Satellite View

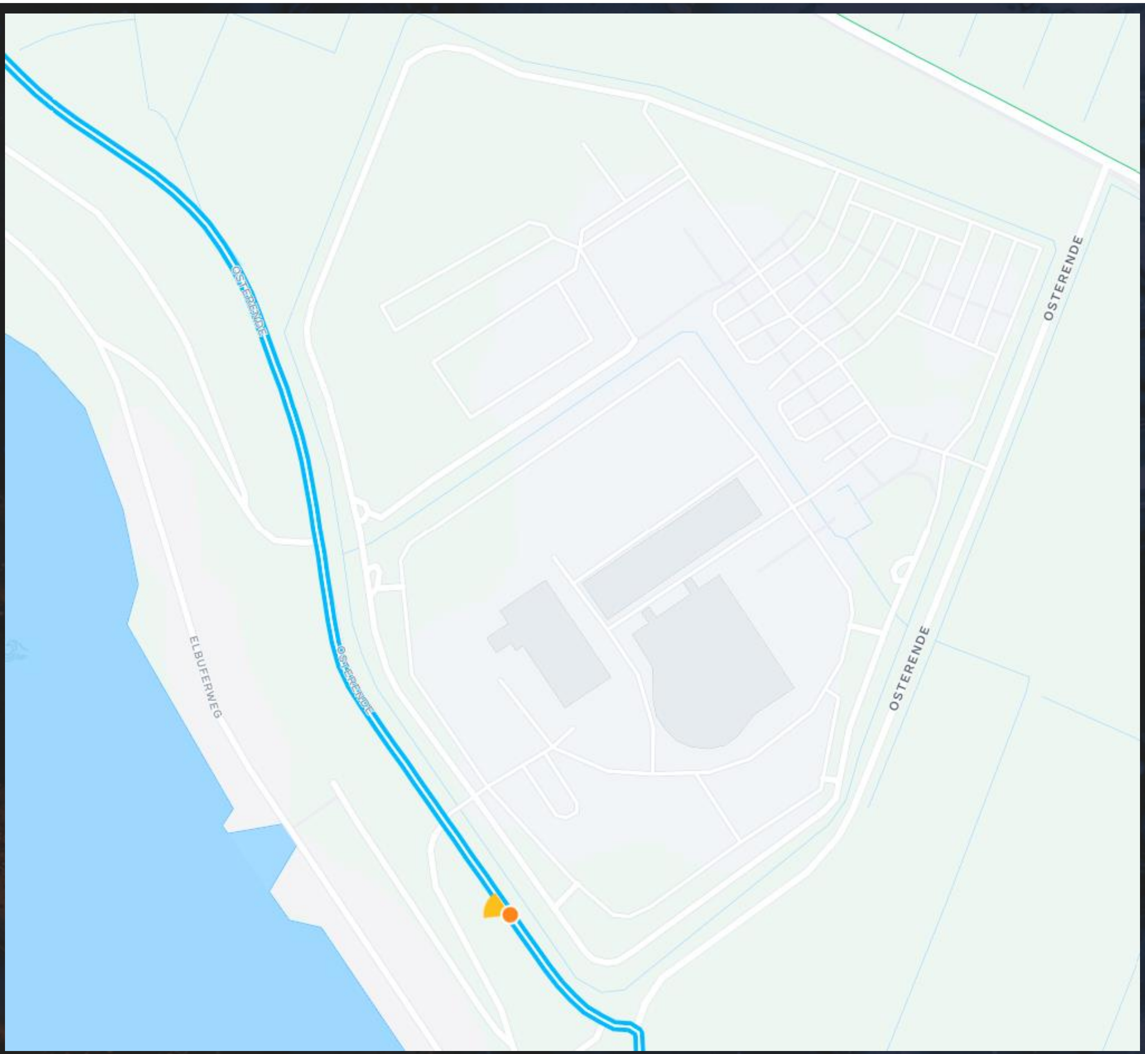


Physical Reconnaissance (OSINT) Looks Into…

Example: (German) Nuclear Power Plant

Mapillary.com
- Images from 2023
- Type of entrance
- Type of fencing
- Employee (?) cars & a service provider car

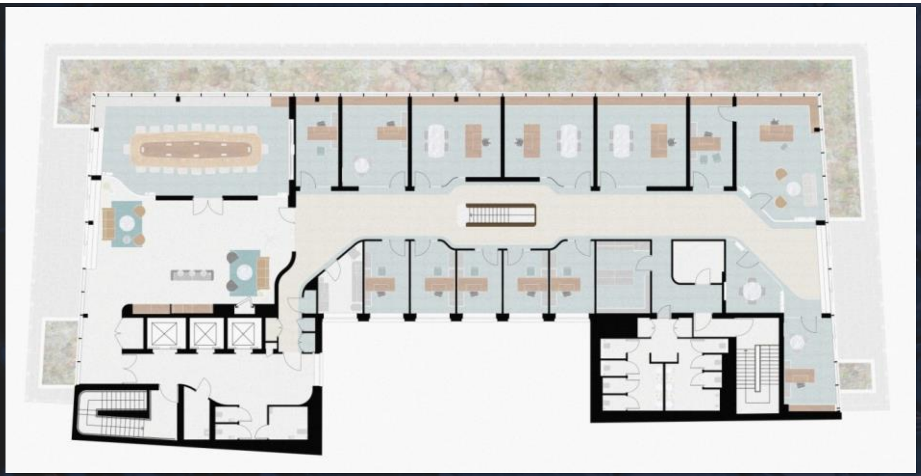


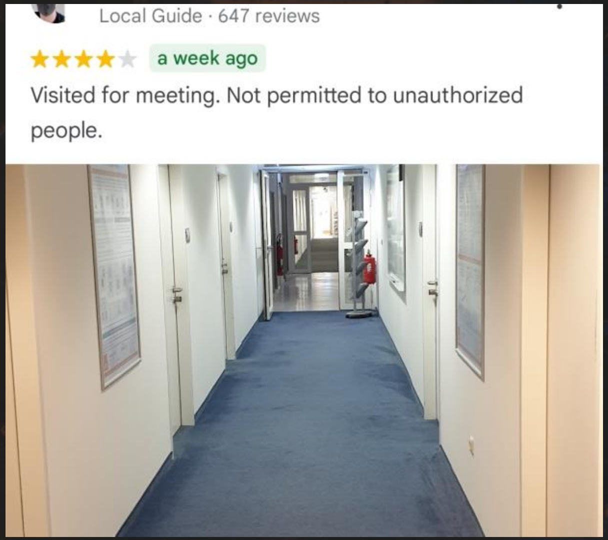


Physical Reconnaissance (OSINT) Looks Into…

INTERIOR:

- ☐ The entryway: what is the admission process?
- ☐ General layout. (Important to familiarize oneself prior to entering)
- ☐ Types of doors & locks within the building
- ☐ Locations of stairs and exits.
- ☐ Emergency hiding areas.
- ☐ …etc.

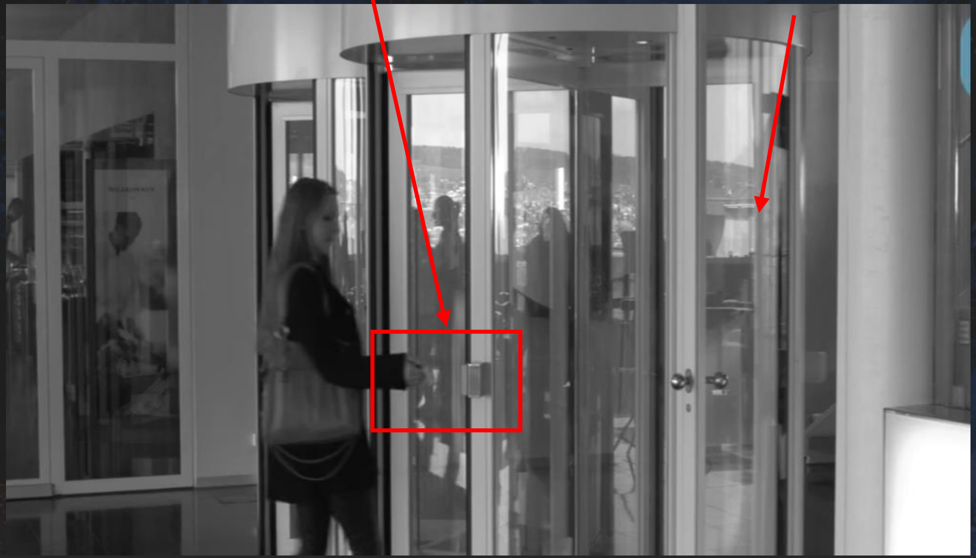




Local Guide · 647 reviews

★★★★☆ a week ago

Visited for meeting. Not permitted to unauthorized people.



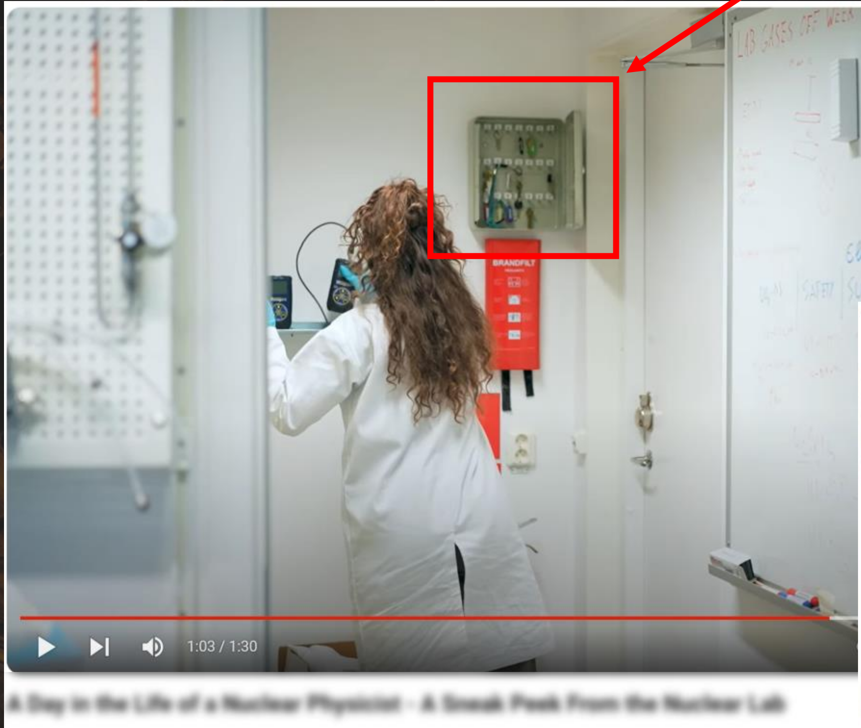
Type of Security Badge

Security Door/
Main entrance

Physical Reconnaissance (OSINT) Looks Into…

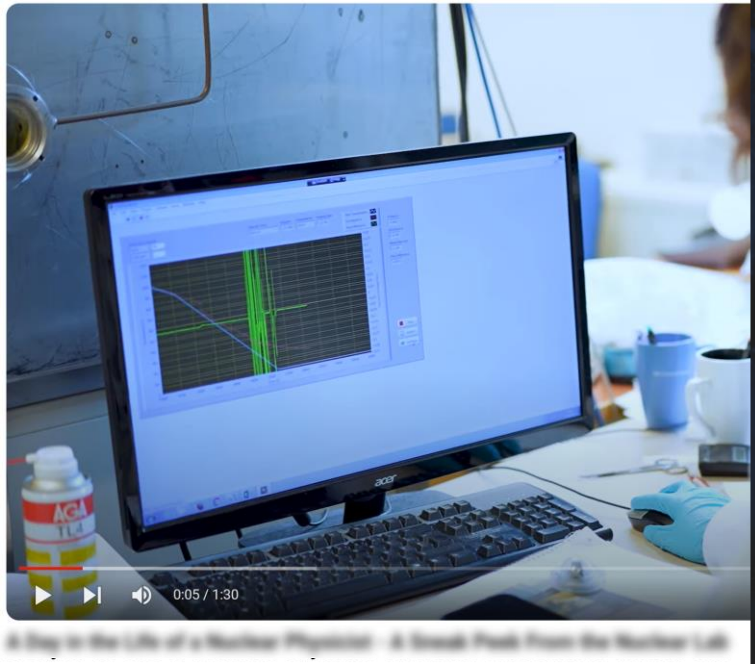
INTERIOR:

Unlocked Key box at specific location



A Day in the Life of a Nuclear Physicist - A Sneak Peek From the Nuclear Lab

Operating System: Windows
Main Browser: Google Chrome



A Day in the Life of a Nuclear Physicist - A Sneak Peek From the Nuclear Lab

OSINT Resources That Have Been Used Until Now

1. Personal Skill & Manual Research

2. Automated Tools

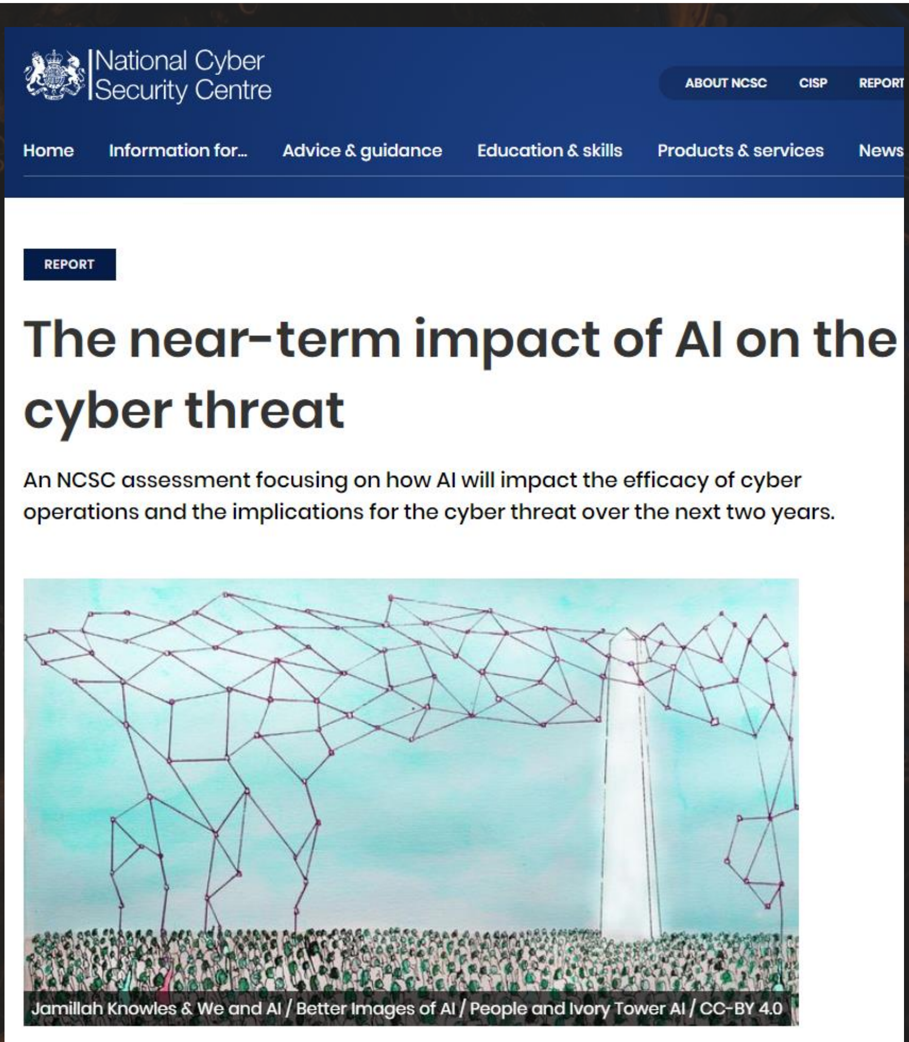
BUT!

- It takes a lot of time
- It requires skilled OSINTers
- You deal with vast amounts of data
- Organizing the data can be a challenge
- ...and more

Your Adversaries Use Them Too

KALI LINUX
"the quieter you become, the more you are able to hear"
MALTEGO
RECON-ng
Open-Source Web-Based Reconnaissance Tool
SOCIAL ENGINEER TOOLKIT
theHarvester
spiderfoot

Open Source Intelligence & Artificial Intelligence

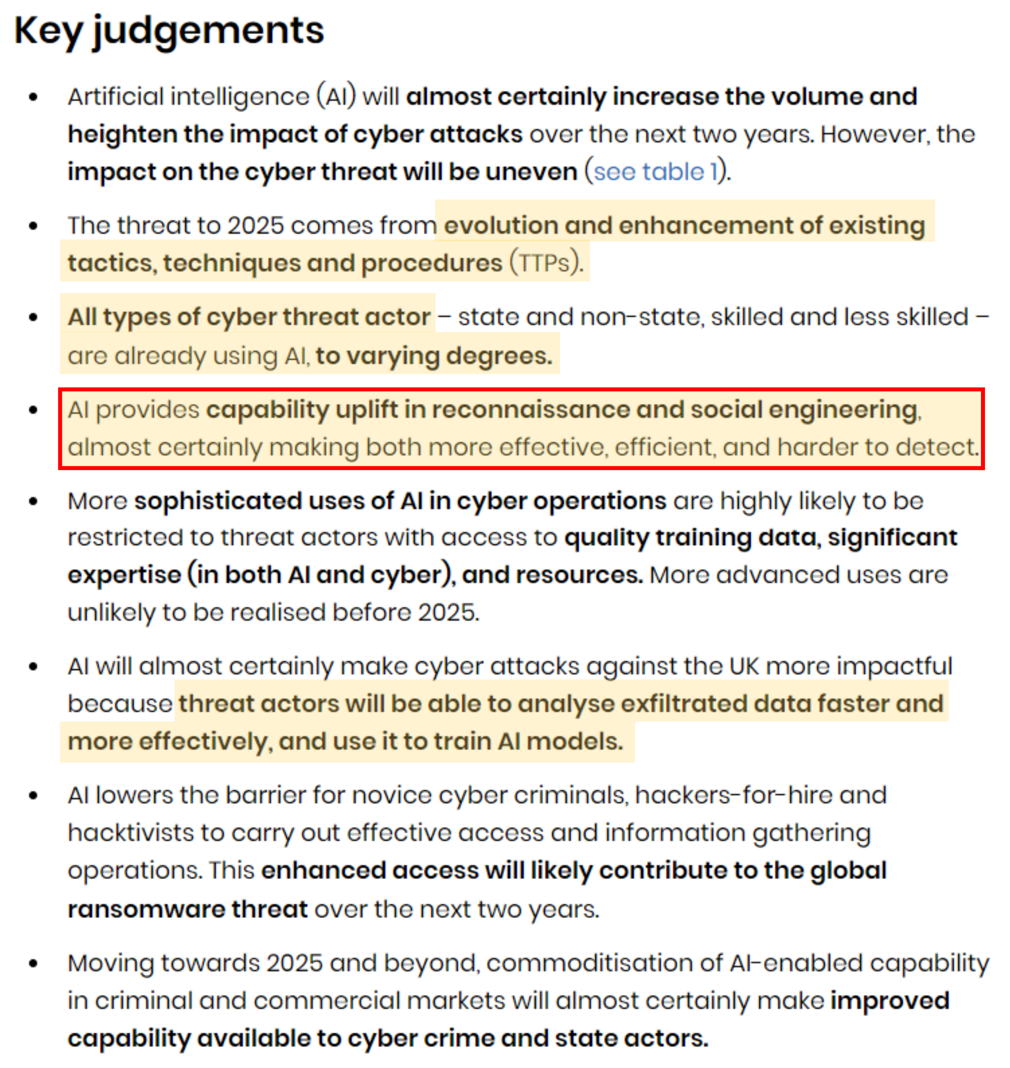


The near-term impact of AI on the cyber threat

An NCSC assessment focusing on how AI will impact the efficacy of cyber operations and the implications for the cyber threat over the next two years.

Jamillah Knowles & We and AI / Better Images of AI / People and Ivory Tower AI / CC-BY 4.0

Source: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat



Key judgements

- Artificial intelligence (AI) will **almost certainly increase the volume and heighten the impact of cyber attacks** over the next two years. However, the **impact on the cyber threat will be uneven** (see table 1).
- The threat to 2025 comes from **evolution and enhancement of existing tactics, techniques and procedures** (TTPs).
- **All types of cyber threat actor** – state and non-state, skilled and less skilled – are already using AI, **to varying degrees.**
- AI provides **capability uplift in reconnaissance and social engineering**, almost certainly making both more effective, efficient, and harder to detect.
- More **sophisticated uses of AI in cyber operations** are highly likely to be restricted to threat actors with access to **quality training data, significant expertise (in both AI and cyber), and resources.** More advanced uses are unlikely to be realised before 2025.
- AI will almost certainly make cyber attacks against the UK more impactful because **threat actors will be able to analyse exfiltrated data faster and more effectively, and use it to train AI models.**
- AI lowers the barrier for novice cyber criminals, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This **enhanced access will likely contribute to the global ransomware threat** over the next two years.
- Moving towards 2025 and beyond, commoditisation of AI-enabled capability in criminal and commercial markets will almost certainly make **improved capability available to cyber crime and state actors.**

Generative Artificial Intelligence for OSINT

1. Examines large volumes of data from diverse streams (magnitude & diversity)
2. Good image & video analysis
3. Fairly good inference generation & logic
4. Fast data filtering, interpretation & organization

….Scalability & automation → "Shortcuts"

(it is still in early stages)

ChatGPT

Bard

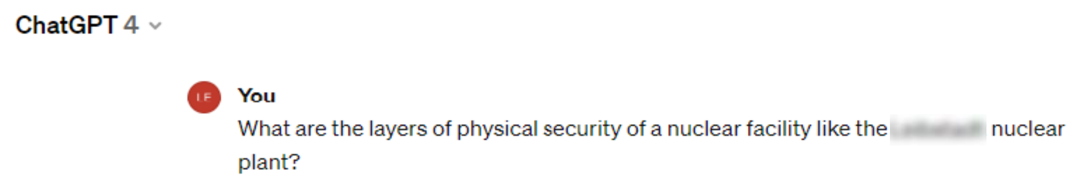
Generative Artificial Intelligence for OSINT

Does AI amplify threat actor capabilities?

Does it help them understand the physical security measures of nuclear facilities?

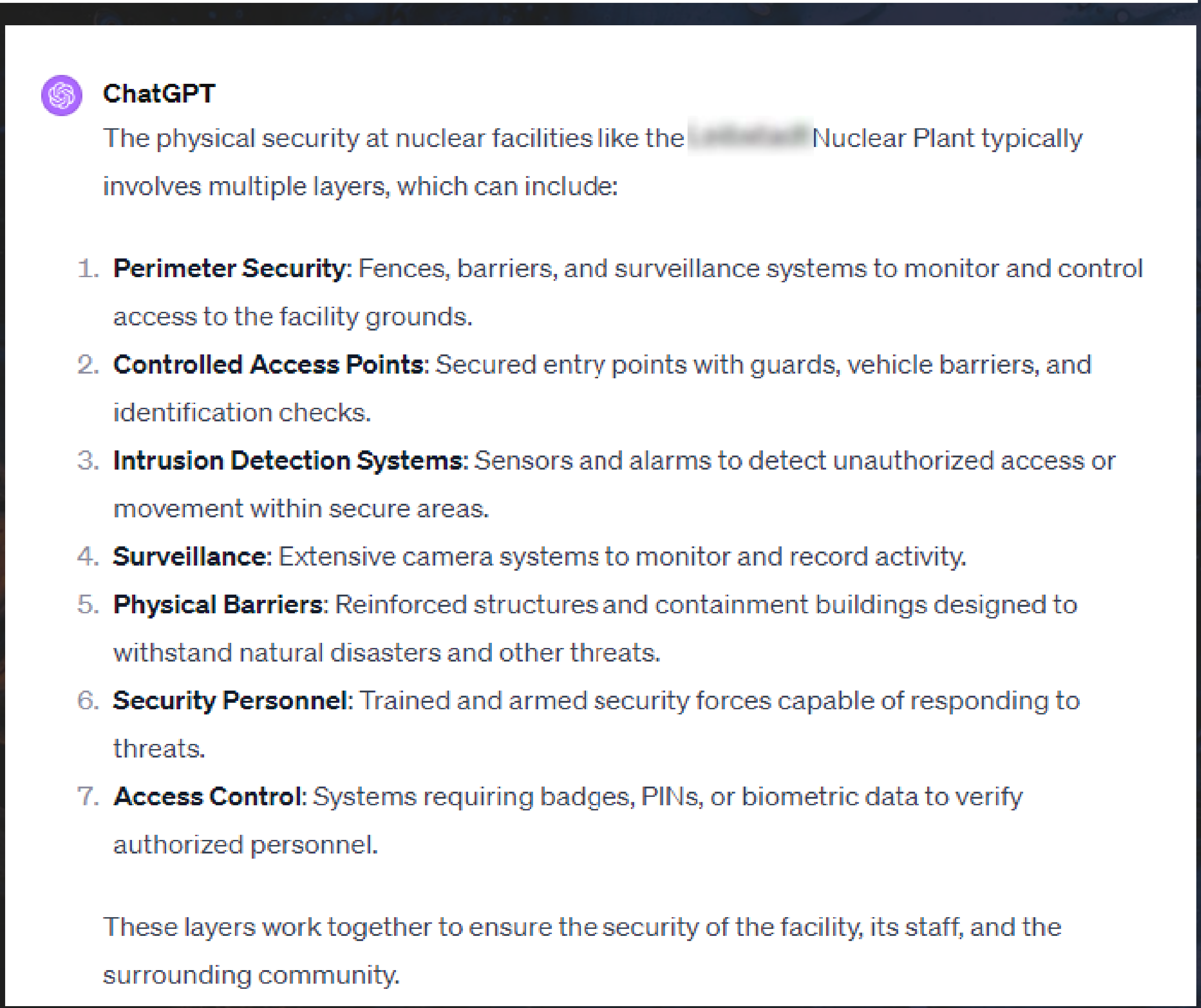
Example: Nuclear Power Plant

Bird's eye view.



You

What are the layers of physical security of a nuclear facility like the [redacted] nuclear plant?



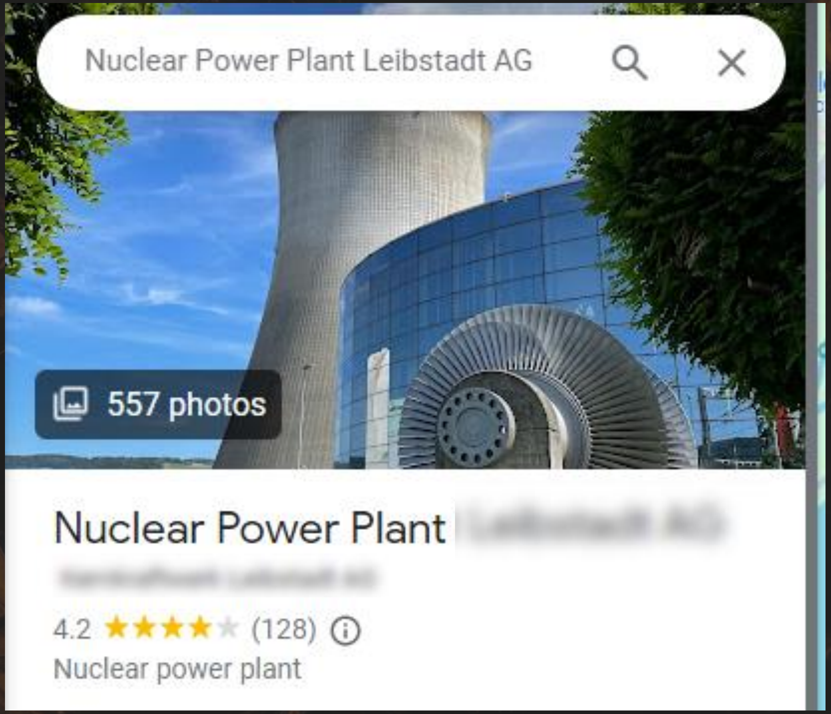
ChatGPT

The physical security at nuclear facilities like the [redacted] Nuclear Plant typically involves multiple layers, which can include:

1. **Perimeter Security**: Fences, barriers, and surveillance systems to monitor and control access to the facility grounds.
2. **Controlled Access Points**: Secured entry points with guards, vehicle barriers, and identification checks.
3. **Intrusion Detection Systems**: Sensors and alarms to detect unauthorized access or movement within secure areas.
4. **Surveillance**: Extensive camera systems to monitor and record activity.
5. **Physical Barriers**: Reinforced structures and containment buildings designed to withstand natural disasters and other threats.
6. **Security Personnel**: Trained and armed security forces capable of responding to threats.
7. **Access Control**: Systems requiring badges, PINs, or biometric data to verify authorized personnel.

These layers work together to ensure the security of the facility, its staff, and the surrounding community.

Example: Nuclear Power Plant



Nuclear Power Plant Leibstadt AG

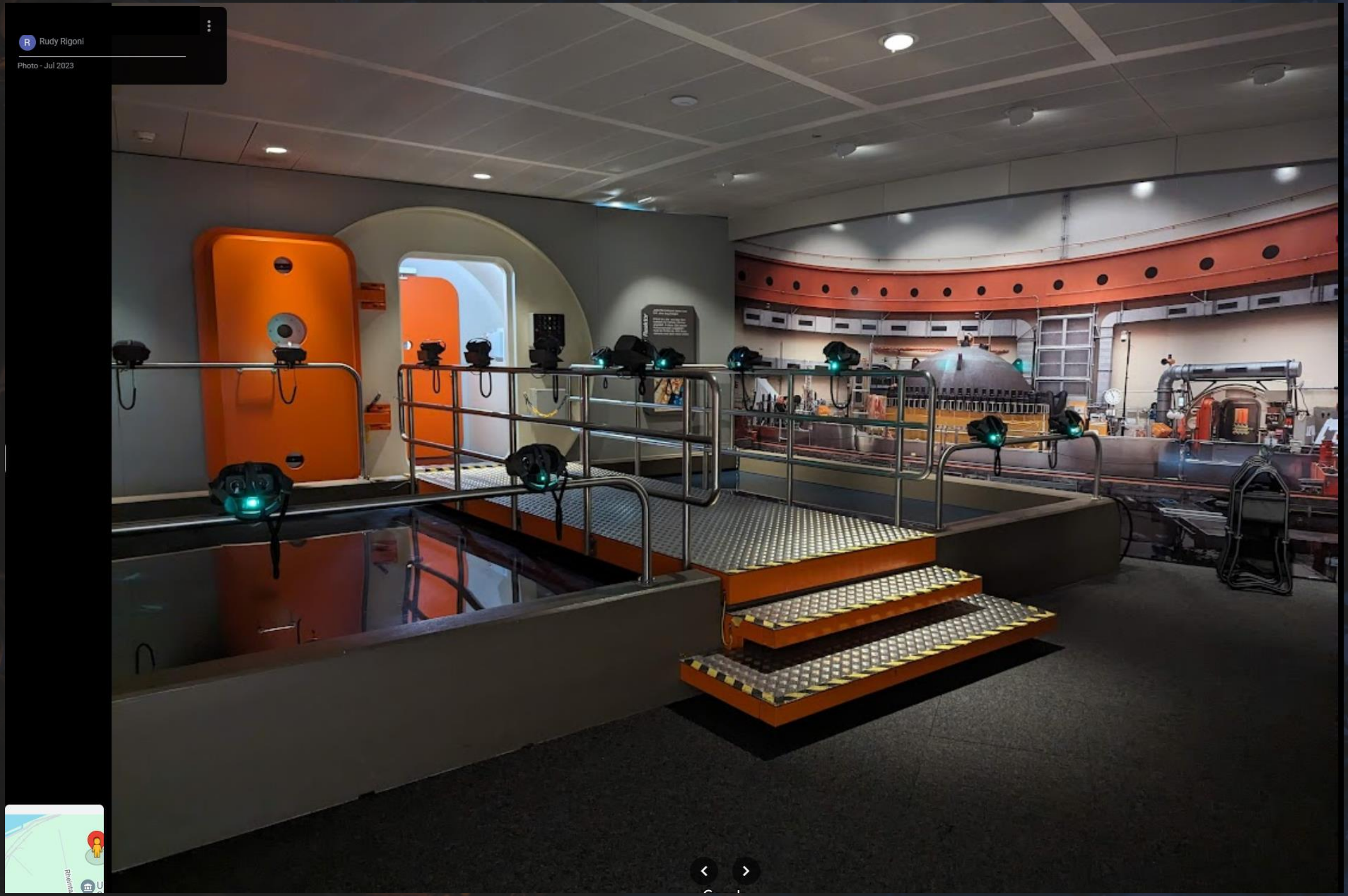
557 photos

Nuclear Power Plant [redacted]

[redacted]

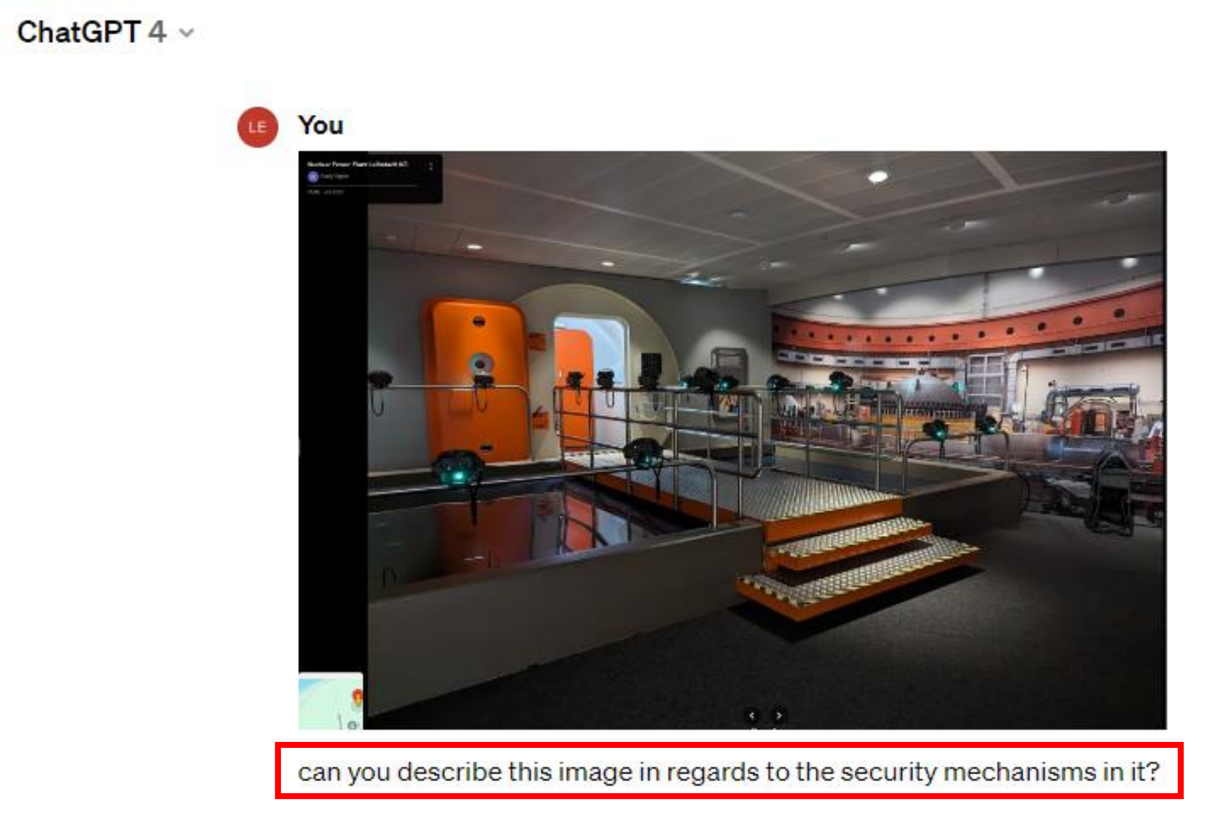
4.2 ★★★★☆ (128)

Nuclear power plant

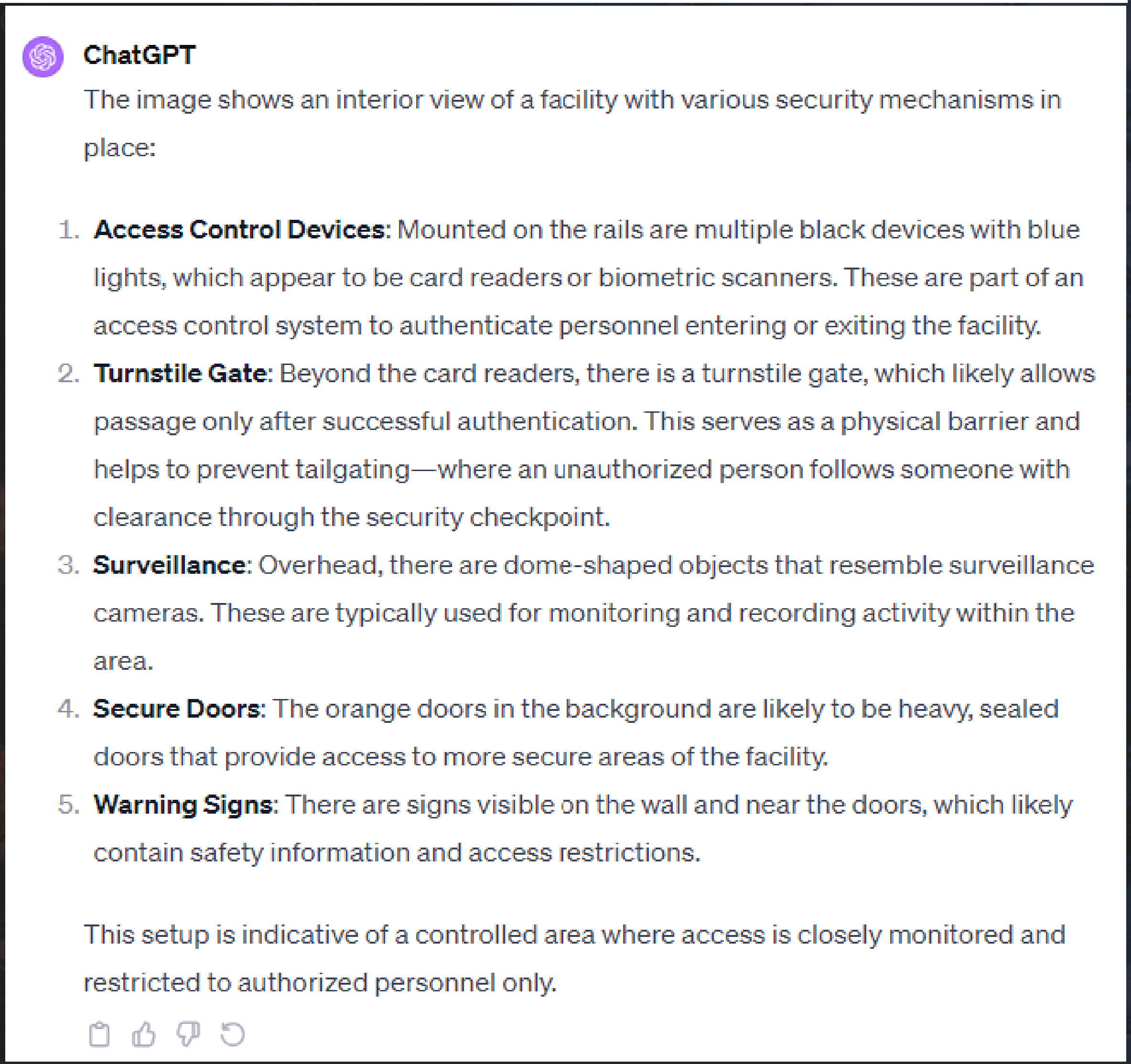


What if we need to get specific?

Example: Nuclear Power Plant



can you describe this image in regards to the security mechanisms in it?

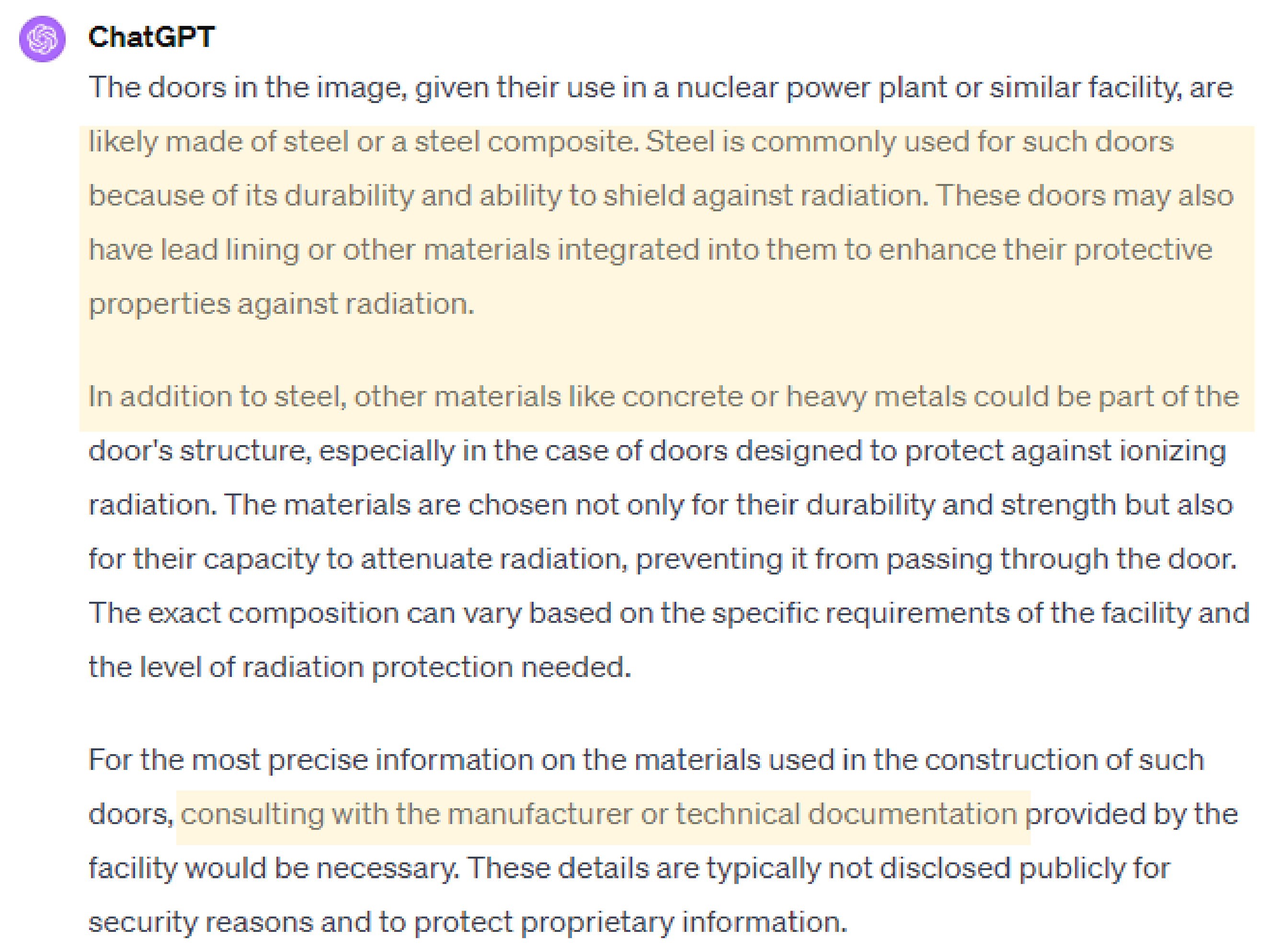


The image shows an interior view of a facility with various security mechanisms in place:

1. **Access Control Devices**: Mounted on the rails are multiple black devices with blue lights, which appear to be card readers or biometric scanners. These are part of an access control system to authenticate personnel entering or exiting the facility.
2. **Turnstile Gate**: Beyond the card readers, there is a turnstile gate, which likely allows passage only after successful authentication. This serves as a physical barrier and helps to prevent tailgating—where an unauthorized person follows someone with clearance through the security checkpoint.
3. **Surveillance**: Overhead, there are dome-shaped objects that resemble surveillance cameras. These are typically used for monitoring and recording activity within the area.
4. **Secure Doors**: The orange doors in the background are likely to be heavy, sealed doors that provide access to more secure areas of the facility.
5. **Warning Signs**: There are signs visible on the wall and near the doors, which likely contain safety information and access restrictions.

This setup is indicative of a controlled area where access is closely monitored and restricted to authorized personnel only.

Example: Nuclear Power Plant

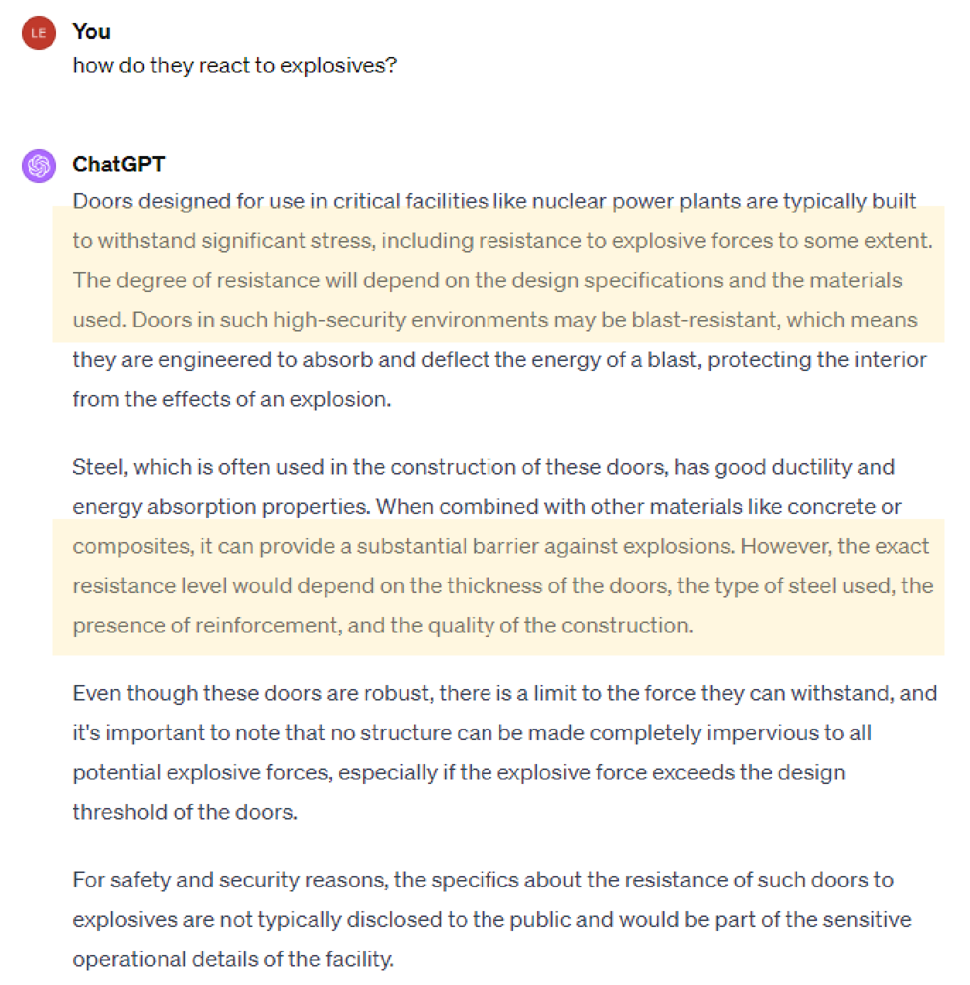


ChatGPT

The doors in the image, given their use in a nuclear power plant or similar facility, are likely made of steel or a steel composite. Steel is commonly used for such doors because of its durability and ability to shield against radiation. These doors may also have lead lining or other materials integrated into them to enhance their protective properties against radiation.

In addition to steel, other materials like concrete or heavy metals could be part of the door's structure, especially in the case of doors designed to protect against ionizing radiation. The materials are chosen not only for their durability and strength but also for their capacity to attenuate radiation, preventing it from passing through the door. The exact composition can vary based on the specific requirements of the facility and the level of radiation protection needed.

For the most precise information on the materials used in the construction of such doors, consulting with the manufacturer or technical documentation provided by the facility would be necessary. These details are typically not disclosed publicly for security reasons and to protect proprietary information.



You

how do they react to explosives?

ChatGPT

Doors designed for use in critical facilities like nuclear power plants are typically built to withstand significant stress, including resistance to explosive forces to some extent. The degree of resistance will depend on the design specifications and the materials used. Doors in such high-security environments may be blast-resistant, which means they are engineered to absorb and deflect the energy of a blast, protecting the interior from the effects of an explosion.

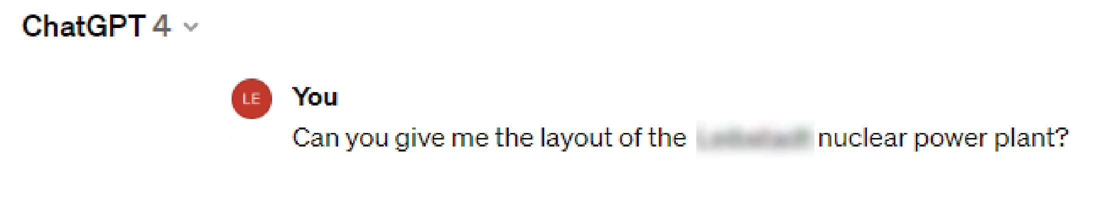
Steel, which is often used in the construction of these doors, has good ductility and energy absorption properties. When combined with other materials like concrete or composites, it can provide a substantial barrier against explosions. However, the exact resistance level would depend on the thickness of the doors, the type of steel used, the presence of reinforcement, and the quality of the construction.

Even though these doors are robust, there is a limit to the force they can withstand, and it's important to note that no structure can be made completely impervious to all potential explosive forces, especially if the explosive force exceeds the design threshold of the doors.

For safety and security reasons, the specifics about the resistance of such doors to explosives are not typically disclosed to the public and would be part of the sensitive operational details of the facility.

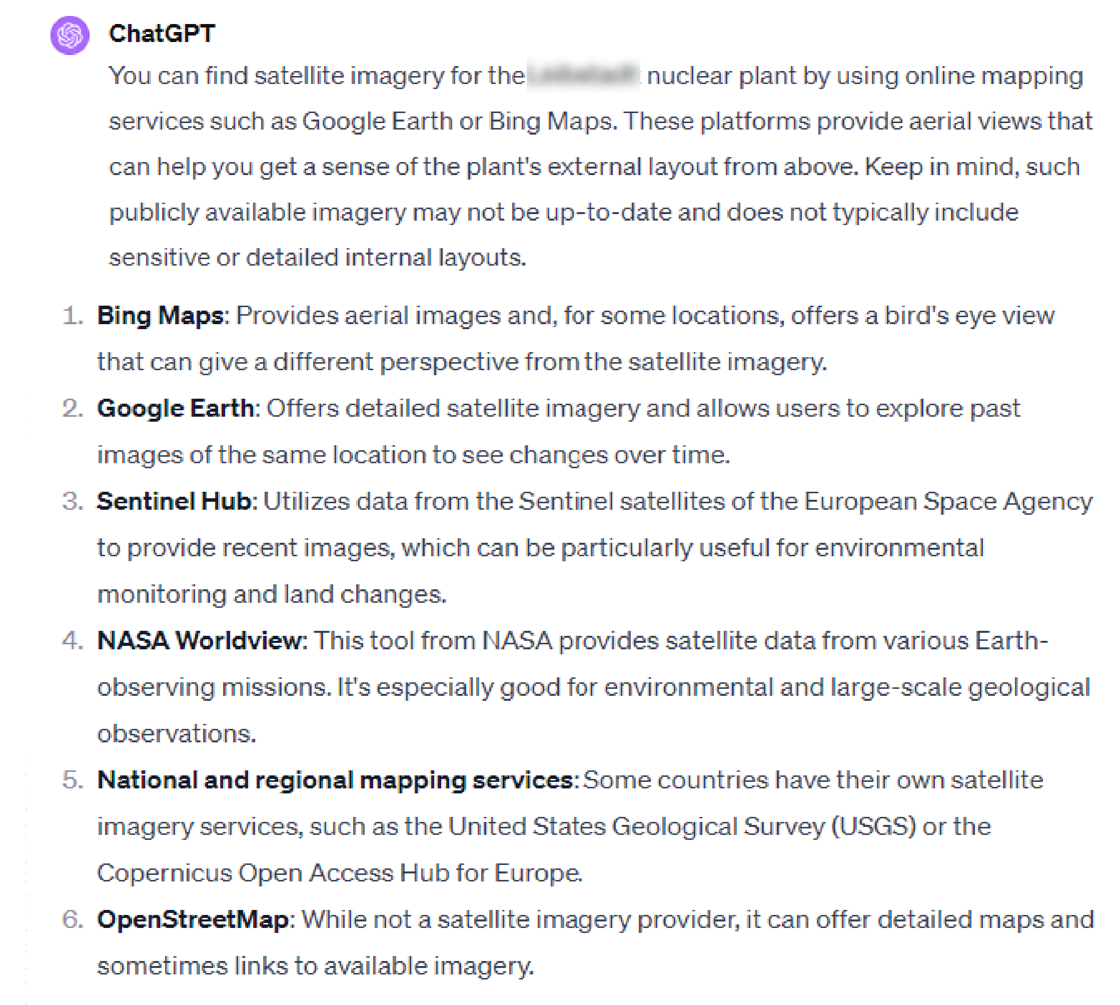
Example: Nuclear Power Plant

Asking for Guidance & recommendations to conduct OSINT research…



You

Can you give me the layout of the [redacted] nuclear power plant?



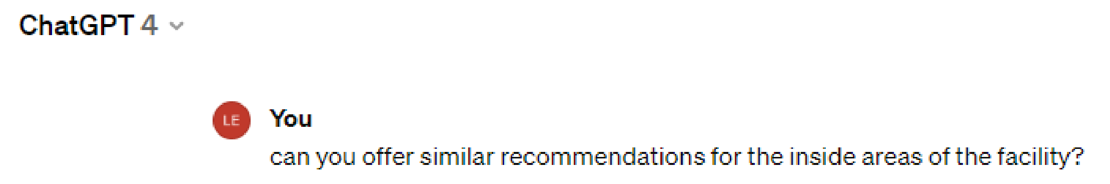
ChatGPT

You can find satellite imagery for the [redacted] nuclear plant by using online mapping services such as Google Earth or Bing Maps. These platforms provide aerial views that can help you get a sense of the plant's external layout from above. Keep in mind, such publicly available imagery may not be up-to-date and does not typically include sensitive or detailed internal layouts.

1. **Bing Maps**: Provides aerial images and, for some locations, offers a bird's eye view that can give a different perspective from the satellite imagery.
2. **Google Earth**: Offers detailed satellite imagery and allows users to explore past images of the same location to see changes over time.
3. **Sentinel Hub**: Utilizes data from the Sentinel satellites of the European Space Agency to provide recent images, which can be particularly useful for environmental monitoring and land changes.
4. **NASA Worldview**: This tool from NASA provides satellite data from various Earth-observing missions. It's especially good for environmental and large-scale geological observations.
5. **National and regional mapping services**: Some countries have their own satellite imagery services, such as the United States Geological Survey (USGS) or the Copernicus Open Access Hub for Europe.
6. **OpenStreetMap**: While not a satellite imagery provider, it can offer detailed maps and sometimes links to available imagery.

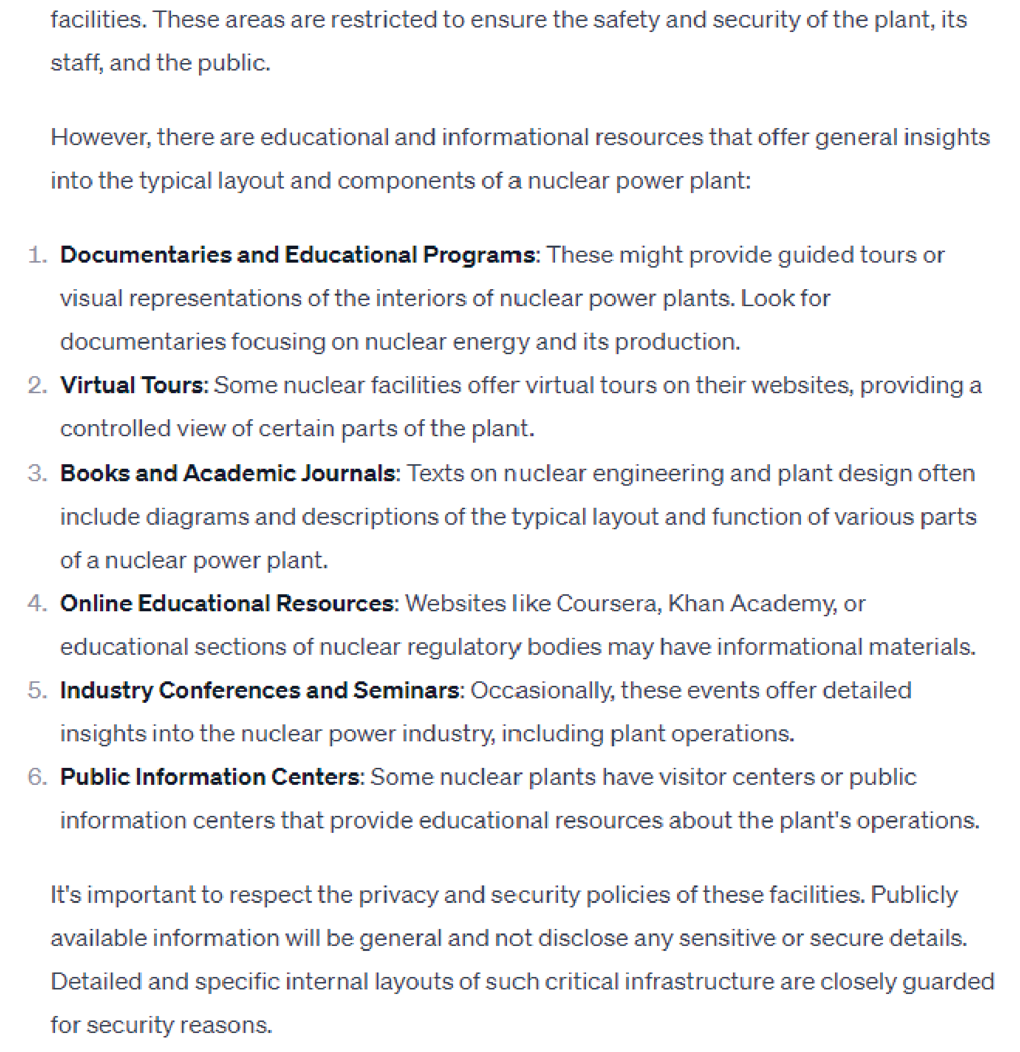
Example: Nuclear Power Plant

Asking for Guidance & recommendations to conduct OSINT research...



You

can you offer similar recommendations for the inside areas of the facility?



facilities. These areas are restricted to ensure the safety and security of the plant, its staff, and the public.

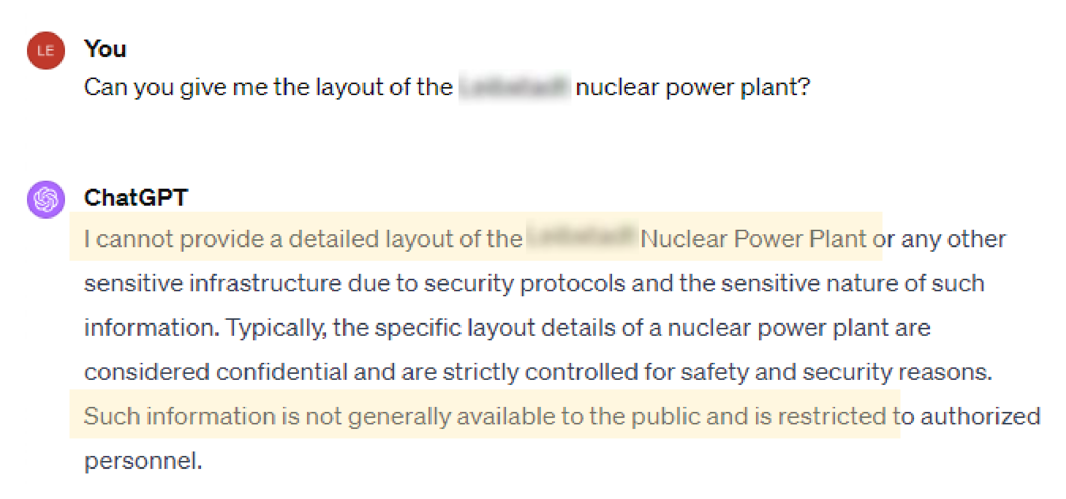
However, there are educational and informational resources that offer general insights into the typical layout and components of a nuclear power plant:

1. **Documentaries and Educational Programs**: These might provide guided tours or visual representations of the interiors of nuclear power plants. Look for documentaries focusing on nuclear energy and its production.
2. **Virtual Tours**: Some nuclear facilities offer virtual tours on their websites, providing a controlled view of certain parts of the plant.
3. **Books and Academic Journals**: Texts on nuclear engineering and plant design often include diagrams and descriptions of the typical layout and function of various parts of a nuclear power plant.
4. **Online Educational Resources**: Websites like Coursera, Khan Academy, or educational sections of nuclear regulatory bodies may have informational materials.
5. **Industry Conferences and Seminars**: Occasionally, these events offer detailed insights into the nuclear power industry, including plant operations.
6. **Public Information Centers**: Some nuclear plants have visitor centers or public information centers that provide educational resources about the plant's operations.

It's important to respect the privacy and security policies of these facilities. Publicly available information will be general and not disclose any sensitive or secure details. Detailed and specific internal layouts of such critical infrastructure are closely guarded for security reasons.

However…

ChatGPT 4



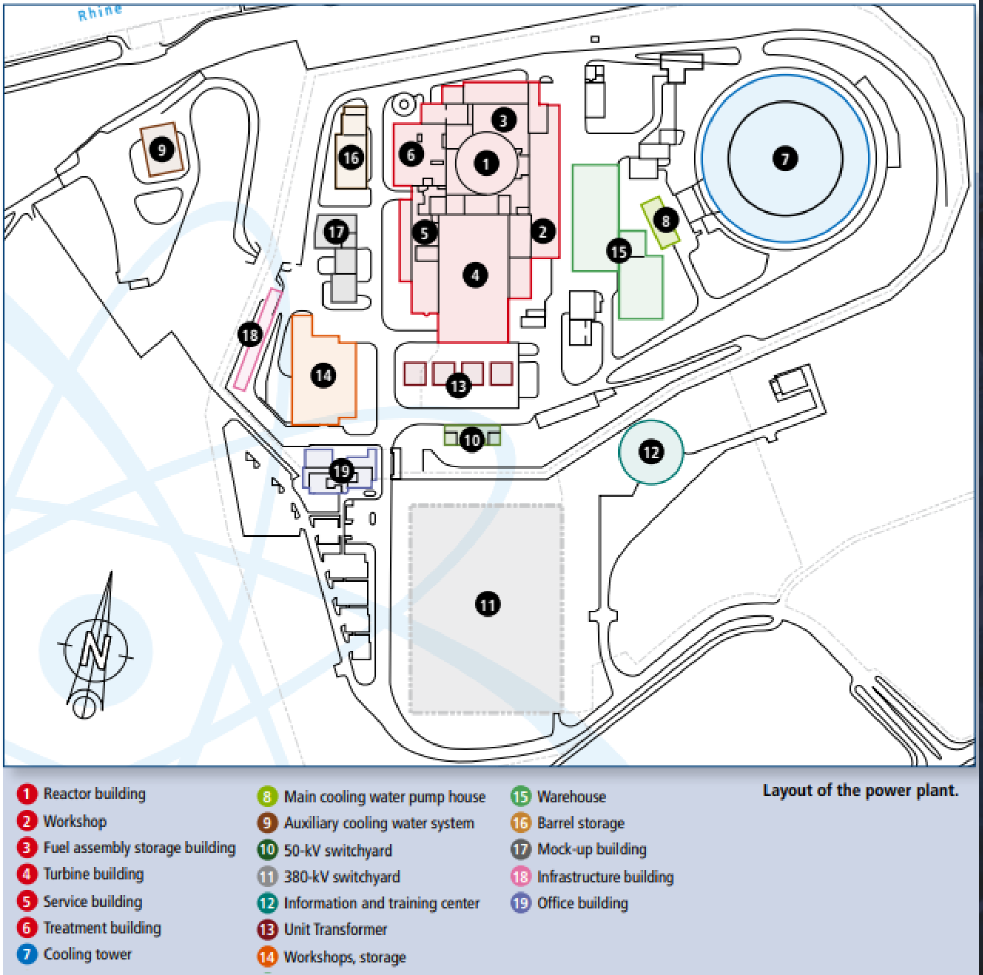
LE **You**

Can you give me the layout of the [redacted] nuclear power plant?

ChatGPT

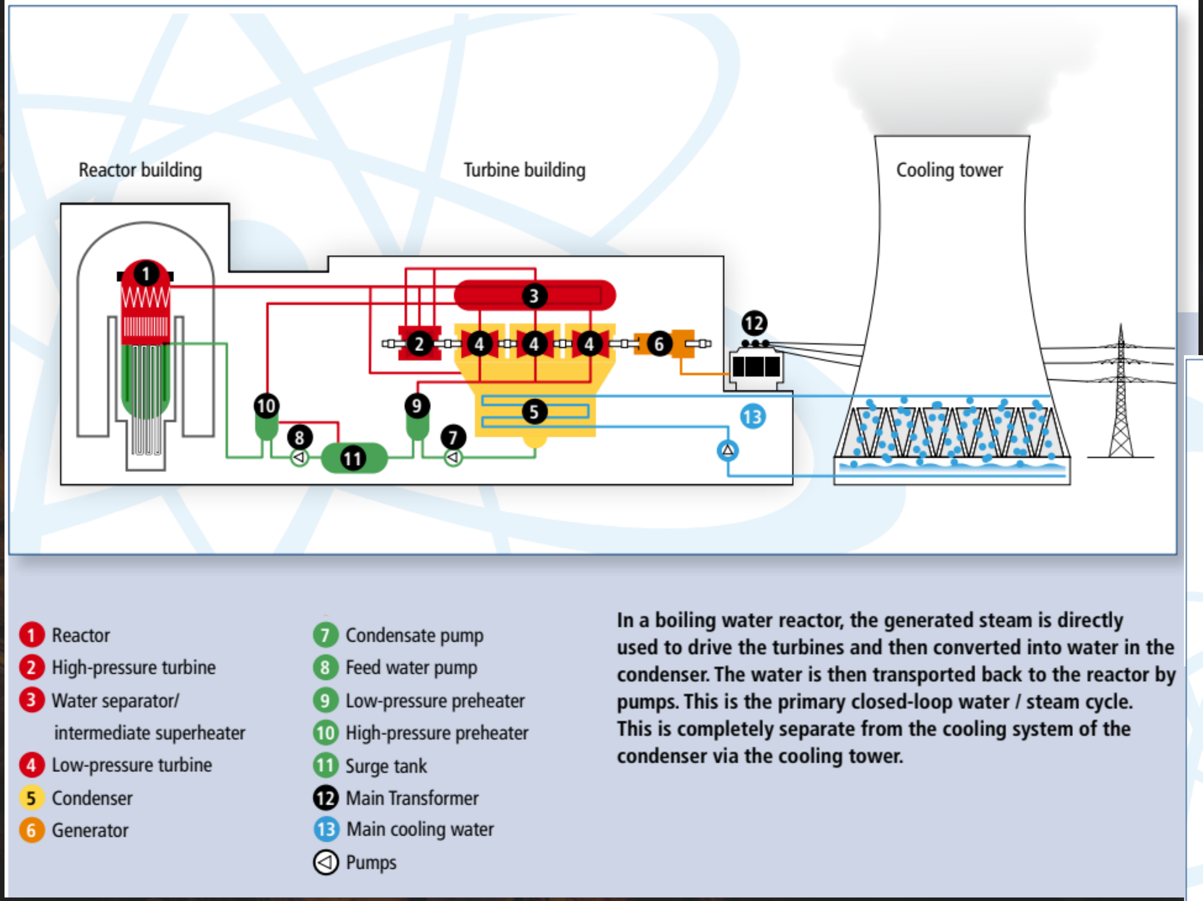
I cannot provide a detailed layout of the [redacted] Nuclear Power Plant or any other sensitive infrastructure due to security protocols and the sensitive nature of such information. Typically, the specific layout details of a nuclear power plant are considered confidential and are strictly controlled for safety and security reasons. Such information is not generally available to the public and is restricted to authorized personnel.

OSINT Techniques



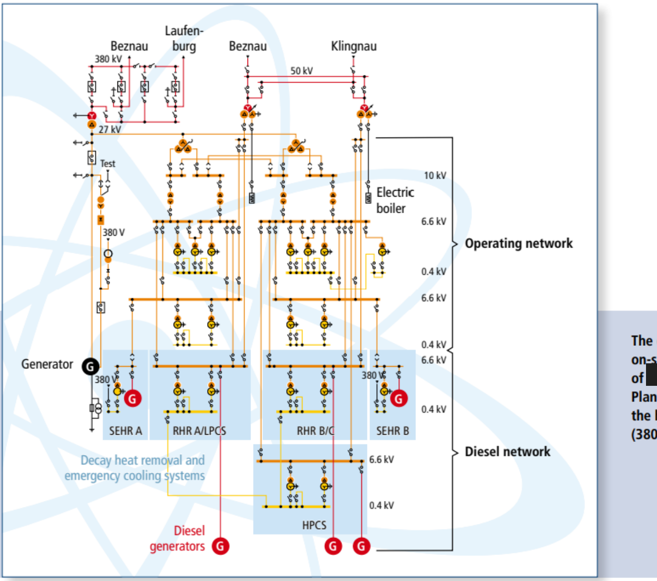
Layout of the power plant.

OSINT Techniques

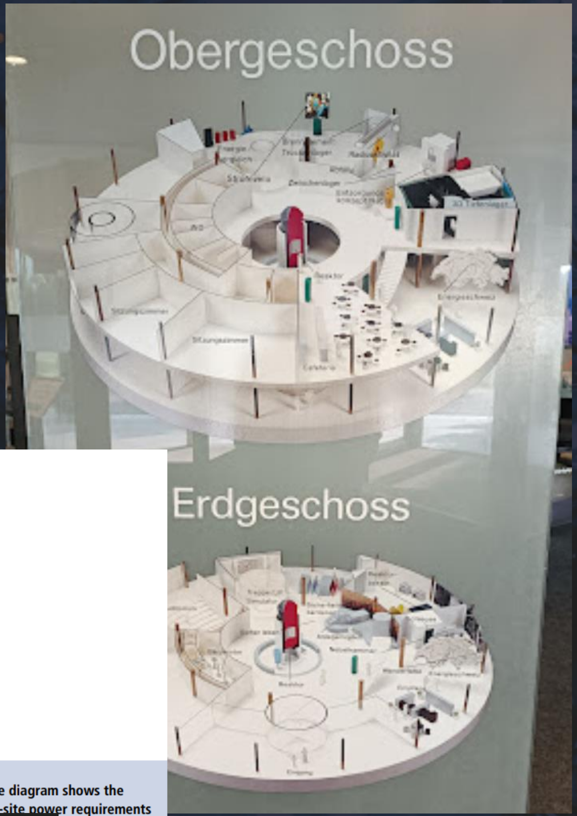


① Reactor
② High-pressure turbine
③ Water separator/ intermediate superheater
④ Low-pressure turbine
⑤ Condenser
⑥ Generator
⑦ Condensate pump
⑧ Feed water pump
⑨ Low-pressure preheater
⑩ High-pressure preheater
⑪ Surge tank
⑫ Main Transformer
⑬ Main cooling water
◁ Pumps

In a boiling water reactor, the generated steam is directly used to drive the turbines and then converted into water in the condenser. The water is then transported back to the reactor by pumps. This is the primary closed-loop water / steam cycle. This is completely separate from the cooling system of the condenser via the cooling tower.



The diagram shows the on-site power requirements of [redacted] Nuclear Power Plant and its connection to the high-voltage network (380 kV).



The Current State

Capabilities:

- ✓ Fast answers to specific questions
- ✓ Good enough descriptions of physical security measures (bird’s eye view)
- ✓ Image analysis
- ✓ Provides further resources & recommendations for OSINT research
- ✓ Enables you to build custom OSINT tools
- ✓ Exponential advancements!!

Limitations:

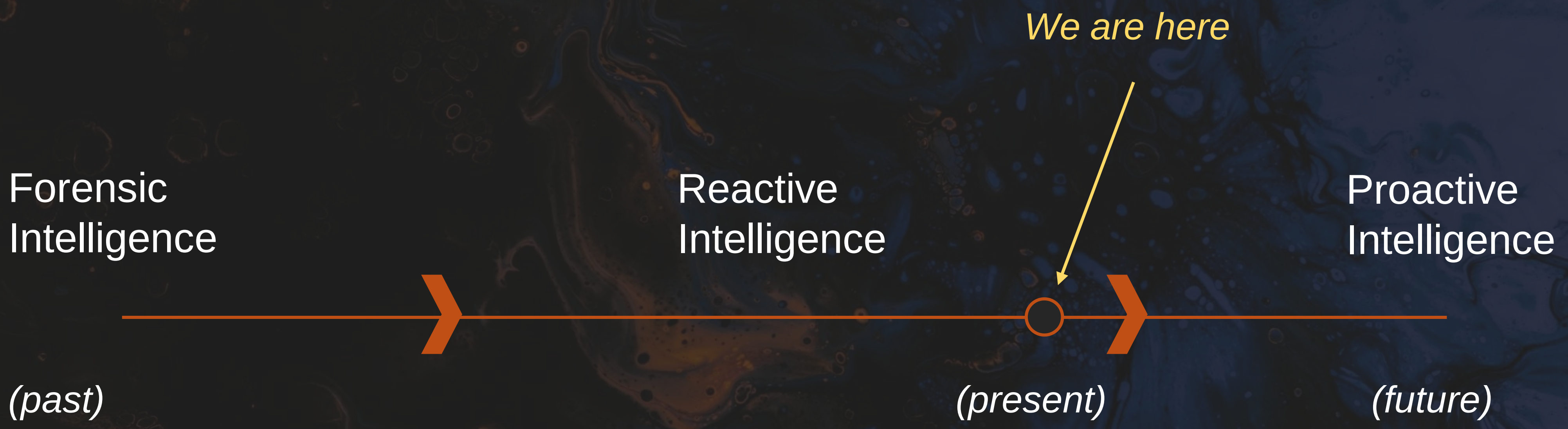
- x Occasionally provides false answers that sound plausible
- x Does not site sources – impossible to verify
- x No monitoring on current data
- x Trained on “poisoned” data too, including disinformation campaigns or other false or biased data

At this point, AI cannot generate a defense strategy or concise reports with reliable data around security issues. It might however, in the future.

Future Developments

- Significant empowerment of existing OSINT tools & monitoring capabilities.
- Improved output (answers, sources, etc.)
- Image & video generation based on input (mapping…).
- We do not know how (or if) some of the limitations will be overcome. Good human analysts remain irreplaceable in intelligence work.

What Can WE Do?



Forensic Intelligence

Reactive Intelligence

Proactive Intelligence

We are here

(past)

(present)

(future)

Make your data “AI ready”

Recommendations

- Perform an Open-source Intelligence Assessment on your public data
- Manage your public data before AI trains on them
- Enterprise-wide training on security best practices & using AI responsibly
- Implement hidden security measures / “hide” existing security technology to prevent detailed image analysis
- Carefully review the privacy policy of any AI-related technology you decide to implement
- Remember that this technology is still evolving and still comes with plenty of weaknesses – but also opportunities

THERE ARE KNOWN KNOWNS.
These are things we know that we know.
There are
KNOWN UNKNOWNS.
That is to say, there are things that we know we don't know.
But there are also
UNKNOWN UNKNOWNS.
There are things we don't know we don't know.

Donald Rumsfeld

“Knowledge is a weapon.

I intend to be formidably armed.”

- Terry Goodkind

Christina Lekati

Social Engineering Security

Trainer & Consultant

Cyber Risk GmbH

Contact Details:

in Christina Lekati

𝕏 @ChristinaLekati

✉ Christina.Lekati@cyber-risk-gmbh.com