



<https://www.nccgroup.com/us/safety-security-privacy-prompts-cyber-resilience-in-the-age-of-artificial-intelligence/>



CODE FOR ALL, SECURITY FOR ALL?

The AI driven Paradigm Shift in IT

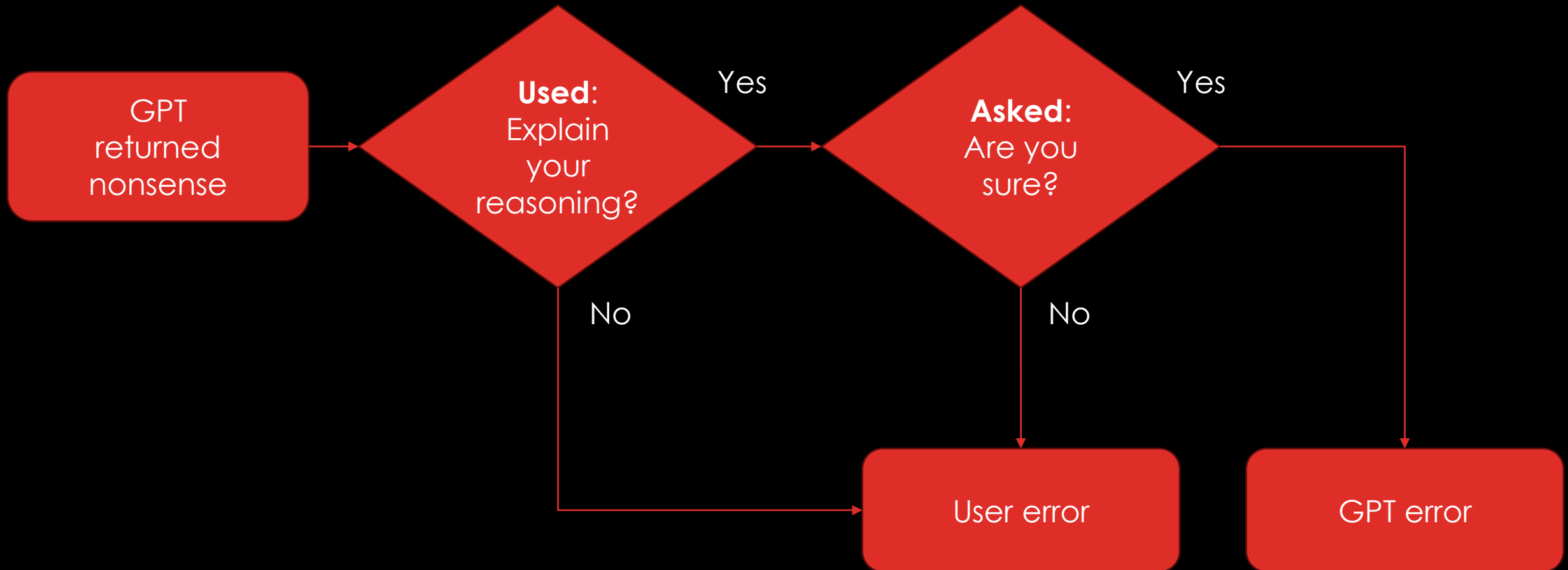
GERBEN VAN DER LEI



FOX IT
part of nccgroup



NOT OUR TOPIC



NOT OUR TOPIC



OUR TOPIC



"Predictions are hard, especially about the future"

OUR TOPIC - AGENDA

- Software
- ChatGPT assisted software development
- Common causes of security problems
- AI – where we stand
- Crystal ball

- Question: How would we get to Terminator?

WHAT IS SOFTWARE?

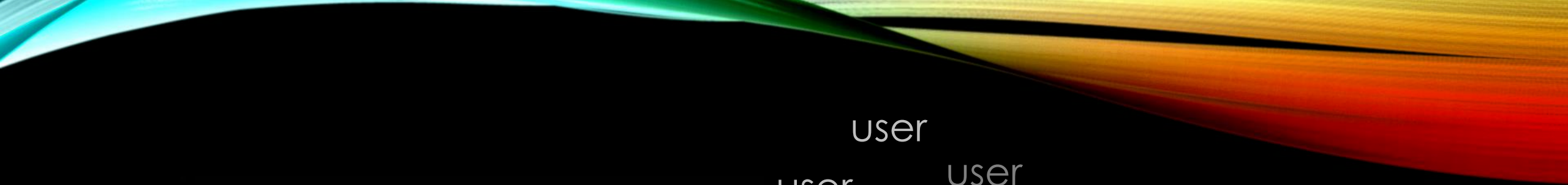


“a set of instructions that tells the computer how to perform specific tasks”

WHAT IS SOFTWARE?



- Written by specialists
- Requires specific skills
- Hard to make
- Easy to copy
- Driver of economic growth



user
user user
user user
user user



coder

code



intent

SO AI CAN WRITE SOFTWARE?

- Yes, it can!



You

Can you write software?



ChatGPT

Yes, I can write software code in various programming languages like Python, JavaScript, C++, and others. If you need help with writing a script, developing an algorithm, or solving a programming-related problem, feel free to ask! Just let me know what you need, including the specific task, the programming language, and any other relevant details.



GE

You

You are a python programmer, we collaborate on a bigger software project.

Can you write me a python function that will check if a number is prime? that I can copy/paste to my codebase?

python

Copy code


```
def is_prime(num):  
    """  
    Check if the provided number is a prime number.  
  
    Args:  
    num (int): The number to check.  
  
    Returns:  
    bool: True if the number is prime, False otherwise.  
    """  
    # Check if num is less than 2, which is not a prime number  
    if num < 2:  
        return False  
  
    # Check for factors from 2 to the square root of num  
    for i in range(2, int(num**0.5) + 1):  
        if num % i == 0:  
            return False  
  
    return True
```

GE

You

You are an experienced software tester and you know how to find all corner cases. I have a Python function that will test if a number is prime (`is_prime()`). Please write me a test for this function.

python

 Copy code

```
import unittest

class TestIsPrime(unittest.TestCase):
    def test_negative_numbers(self):
        self.assertFalse(is_prime(-1))
        self.assertFalse(is_prime(-10))

    def test_zero_and_one(self):
        self.assertFalse(is_prime(0))
        self.assertFalse(is_prime(1))

    def test_small_primes(self):
        for prime in [2, 3, 5, 7, 11, 13]:
            self.assertTrue(is_prime(prime))

    def test_small_non_primes(self):
        for non_prime in [4, 6, 8, 9, 10, 12]:
            self.assertFalse(is_prime(non_prime))

    def test_large_prime(self):
        # Example large prime could be any known large prime
```



Question: WHY does IT security as an industry exist?

IT PARADIGM ANNO 2022

- **Making** software is **hard** & **expensive**
- **Distributing** software is **easy**
- So: we must all use the *same* software

SOURCES OF IT SECURITY PROBLEMS

- User error (system functions as intended, user not -> phishing etc.)
 - Admin error (system & user function as intended, wrong configuration)
 - ...
- Exploitable software error -> 0 day, unpatched, etc.
 - Supply chain compromise

COMPUTING BASE GROWS

- And grows
 - And grows
 -
 - Add more security software!
 - ...
 - And grows
 -
-
- What could possibly go wrong?

ROOT CAUSE

- Making secure code (systems) is VERY hard
 - ~10x to 100x more expensive
- Business model is: “build 1 sell many”
- Less hours built = more profit
- Selling with bugs is the norm but SW companies prefer to call it “Agile”, “OTA updateable” or “As A Service”, “time to value”

BUT WAIT!

- AI is making this problem bigger, right?
- Yes, perhaps...



WHAT IF...

- Making software would be easy, fast and cheap?



<https://www.nccgroup.com/us/safety-security-privacy-prompts-cyber-resilience-in-the-age-of-artificial-intelligence/>

WHAT HAPPENED HERE???

GE

You

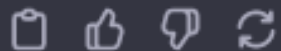
Can you make me a QR code for the url: <https://www.nccgroup.com/us/safety-security-privacy-prompts-cyber-resilience-in-the-age-of-artificial-intelligence/>



ChatGPT

I have generated a QR code for the URL you provided. You can download and use the QR code image from the link below:

[Download QR Code \[↗\]](#)



Analysis

python

Copy code

```
import qrcode

# URL for the QR code
url = "https://www.nccgroup.com/us/safety-security-privac

# Generate QR code
qr = qrcode.QRCode(
    version=1,
    error_correction=qrcode.constants.ERROR_CORRECT_L,
    box_size=10,
    border=4,
)
qr.add_data(url)
qr.make(fit=True)

# Create an image from the QR Code instance
img = qr.make_image(fill_color="black", back_color="white
```

- Write
- Run
- Return

Single use software!

This is a BIG thing!



FYI

- Chat GPT was released 30 nov '22...
- Less than 1 year ago!

SMALL EXCURSION

- 1997 Deep Blue
- 2015 Alpha GO
- 2017 Alpha GO zero



SELF IMPROVE?



ChatGPT

All tests have passed successfully for the `is_prime` function. It correctly identifies prime numbers, handles negative numbers, zero, one, small primes, small non-primes, large primes, large non-primes, and very large numbers. Additionally, it appropriately raises a `TypeError` for invalid input types. [\[>-\]](#)



COMPLEXITY

- Real-life Software is very complex, right?
- ChatGPT can only make simple things, right?

AGENTS....

- Specific task
- Fine tuned for task

Example:

<https://github.com/microsoft/autogen>



NEXT LEVEL:
MULTI AGENT

OUR TOPIC



- Step 1: writing code
- Step 2: self test
- Step 3: self improve
- Step 4: execute
- Step 5: going on a mission

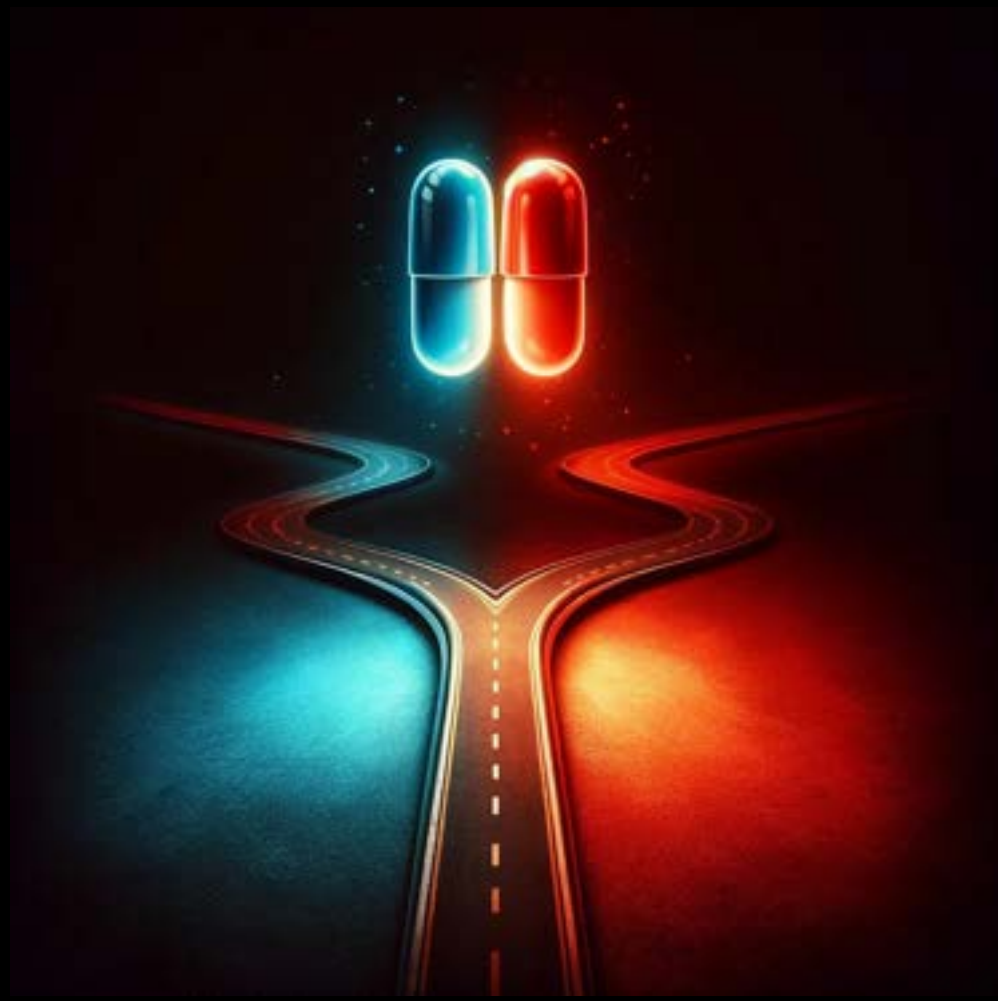
WHAT IT BRINGS

Positives I see:

- Single use code -> less code volume, less common code
- Self improving code -> higher quality

Risks I see:

- Larger code volume in old business model
- Too fast to go to market
- Development too fast to keep up







<https://www.nccgroup.com/us/safety-security-privacy-prompts-cyber-resilience-in-the-age-of-artificial-intelligence/>