Guardians of the Digital Realm

Exploring the Symbiosis of Artificial Intelligence and CyberSecurity

(Looking for a needle in a haystack of needles)

Dr. Dev R. Sainani
Associate Dean
School of Information Technology
Fanshawe College

What I will cover today

01

Introduction

The School of Information Technology, Fanshawe College

02

Cyber Security

CybSec, The CyberRange, and the HPC Cluster

03

Artificial Intelligence

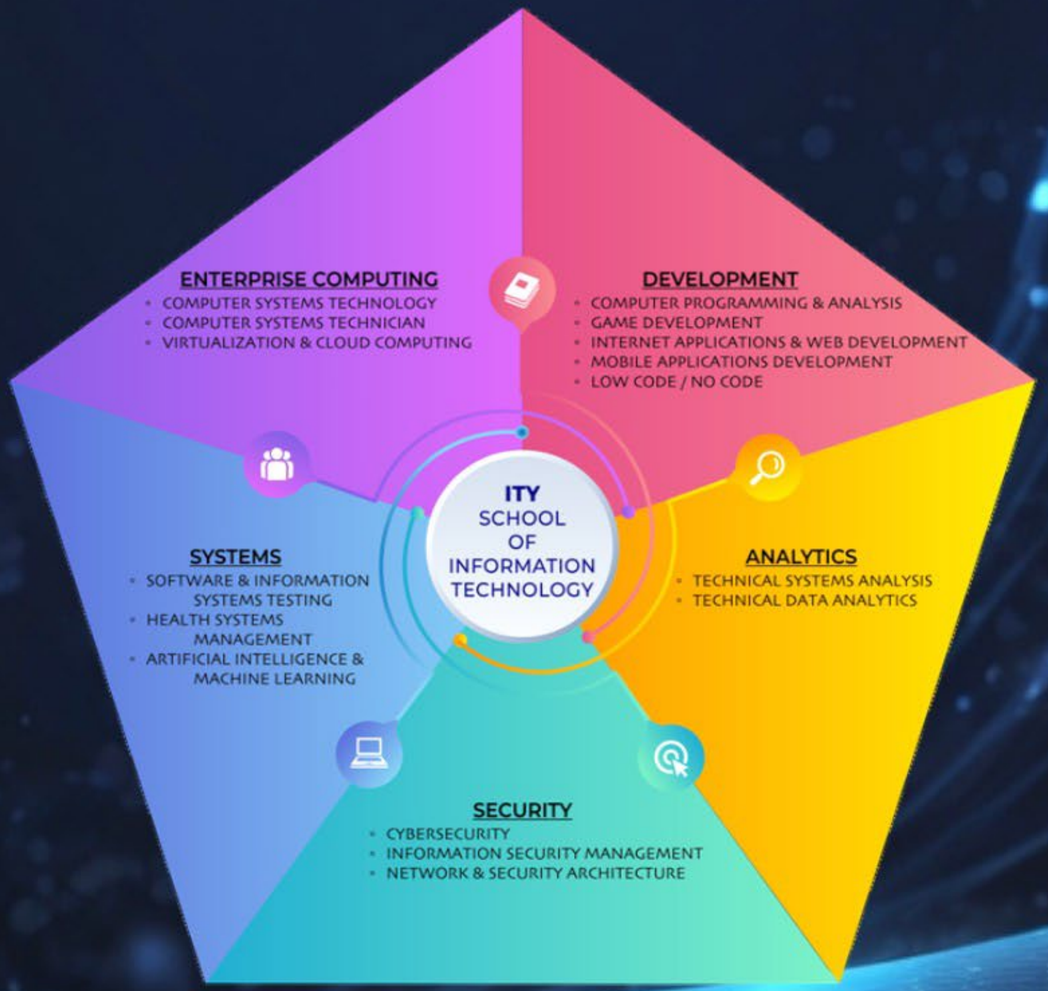
The opportunities that AI presents

04

In Summary

Cautionary Tales…

The School of Information Technology



F.O.B. Data Center

ITY CyberRange

High Performance Computing Cluster

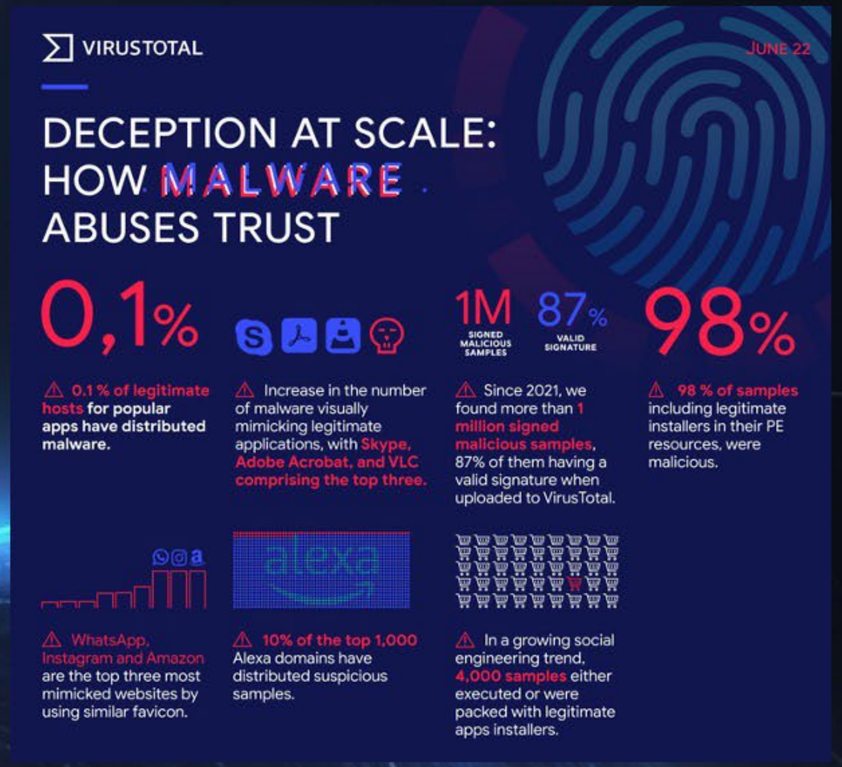
CyberSecurity – Reactive ➡ Proactive

- Attackers will target anyone they can, and the easier the target, the higher the likelihood that they will be attacked. Nothing in Cybersecurity is 100%, and so protection needs to be layered.
- Increasingly complex tactics powered by sophisticated technologies, targeting broader targets and higher stakes are the rules of the game
- The attack surface has increased exponentially from the domain of enterprise computing and data centers, to SMB IT installs, to an ever increasing segment of personal and edge devices
- Contextual threat intelligence will be central to proactive cybersecurity and international cooperation will be critical to countering the myriad of threats
- This is where Artificial Intelligence plays a crucial role in prediction, defense, mitigation and remediation

Some CyberSecurity Stats to keep you on edge at night, or day, or constantly…

- 300k new pieces of malware are created daily and ~180B spam emails sent every day
- >46M signals of cyberattacks every day worldwide
- ~530 signals of potential attacks per second
- ~30k websites are hacked daily
- 2200 actual cyber attacks per day ~ every 39 sec
- ~$8 Trillion in costs in 2023 rising to ~$15 Trillion in costs by 2025
- Ransomeware alone will cost the world upwards of $300B annually by 2030
- An average of 30,000 malicious mobile apps are blocked daily on various mobile app stores

- Browser Exploitations; Office Applications; 3rd party apps; Phishing emails; Redirects; Master boot record overwrites; Targeted file attacks; Ever-increasing sets of complex cascade attacks; Nation state sponsored actions; Ransomware, and so forth, and so on



Sources: Packetlabs CyberSecurity Statistics 2023; British Telecom; Cybersixgill Corporation; Embroker Insurance Services LLC; MSP Threat Report from Connectwise

Some CyberSecurity Stats to keep us on edge at night, or day, or constantly…

The Education Sector

- In 2023, it took organizations on average 49 days to identify a cyberattack…
- 40% of universities and colleges took over a month to recover from a data breach
- 1/3 of school districts do not utilize cloud security
- Educational records can go for upwards of $300 each on the dark web
- Almost 80% of post secondary institutions have experienced reputational damage as a result of a cyberattack
- >40% of higher education security incidents were triggered by successful social engineering attacks
- Education typically ranks the last in terms of preparedness for identifying and remediating cybersecurity threats

Fanshawe CyberRange

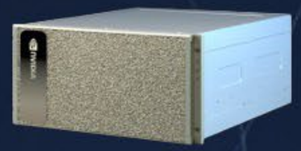
- We have acquired a CyberRange as an education / research / tool to complement our CyberSecurity Adv. Diploma, plus…
- A 24/7/365 fully sandboxed realistic global cyber environment
- A simulation and data generation platform that replicates the full functionality of the real Internet including:
  - Offence and Defence with multiple threat actor capability
  - Realistic ISP functionality and organizational networks
  - Globally routed networks with realistic IP addresses
  - Search & Social Media and Video Channels
  - Transaction Processing, Order & Delivery
  - Automated user traffic and background noise
  - Long time series data generation for real time analysis
  - Specifically constructed industry business models

Fanshawe CyberRange

- It provides a CybSec testing, education and development environment enabling real threat and defence capabilities
- It allows our students to practice and test their knowledge with cybersecurity exercises (Red Team : Blue Team, etc.)
- The cyberrange permits the comparison and evaluation of CybSec products and services
- The Fanshawe CyberRange provides our students with unparalleled capabilities in:
  - Cyber Security Education and Training
  - Skills Development
  - Security Operations Centre (SOC) development, management and operations

High Performance Computing Cluster

Artificial Intelligence and Machine Learning focused High Performance Computing Servers >20 Petaflops of computing



- The School of Information Technology hosts high performance computing infrastructure and capabilities that support all of our diploma, advanced diploma and certificate programs.
- The core Infrastructure includes some 3000 processors and graphics processing units, and multi terabytes of storage, high speed networking gear

High Performance Computing Cluster

Artificial Intelligence and Machine Learning focused High Performance Computing Servers >20 Petaflops of computing

Our Use Cases:

- Artificial Intelligence
  - LLM's, Algorithm Development, Simulation & Modelling
- Deep Learning / Machine Learning Applications
  - LLM's, Neural Networks, Training Models
- Cyber Security
  - Risk Analysis, Threat Identification, Decision Support, Risk and Threat Mitigation, Remediation, Learning
- Big Data, Data Analytics
  - Non-Linear Dynamical Time Series Analysis
  - Forecasting, Predictive Analytics, Chaos Theory

Artificial Intelligence

- Artificial intelligence (AI) refers to the simulation of human intelligence processes by machines, especially computer systems.
- These tasks include learning from experience, understanding and generating natural language, recognizing patterns in data, solving problems, and making decisions.
- These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), and self-correction, all without explicit programming.
- AI encompasses a broad range of technologies and applications, from simple rules-based systems to complex, self-learning neural network algorithms, to natural language processing routines capable of performing tasks traditionally requiring human intelligence.
- One of the goals of AI is to create systems that can perceive their environment, learn from it, adapt to new situations, reason and solve problems, ultimately advancing the capabilities of technology to interact intelligently with humans in the world.
- Ultimately, Artificial Intelligence aims to successfully mimick or even surpass human cognitive abilities in various domains.

SAMPLE PROMPTS: Give me a good definition of Artificial Intelligence; What is A.I.; Define A.I. ; Tell me about Artificial Intelligence

Artificial Intelligence – being extra…

- Artificial Intelligence epitomizes the apotheosis of computational prowess, embodying the quintessence of intellect distilled into algorithmic elegance.
- It transcends the confines of conventional programming, ascending to a realm where systems possess the sagacity to perceive, reason, learn, and adapt autonomously.
- These sublime constructs harness the quintessence of algorithms, neural networks, and advanced cognitive paradigms to emulate the very essence of sentient cognition, often eclipsing human faculties in domains both mundane and profound.
- Artificial Intelligence heralds a paradigm shift of cosmic proportions, unveiling the vast expanse of possibilities as it catalyzes innovation, reshapes industries, and illuminates the path toward a future where the boundaries of intelligence dissolve into the boundless expanse of the universe itself.

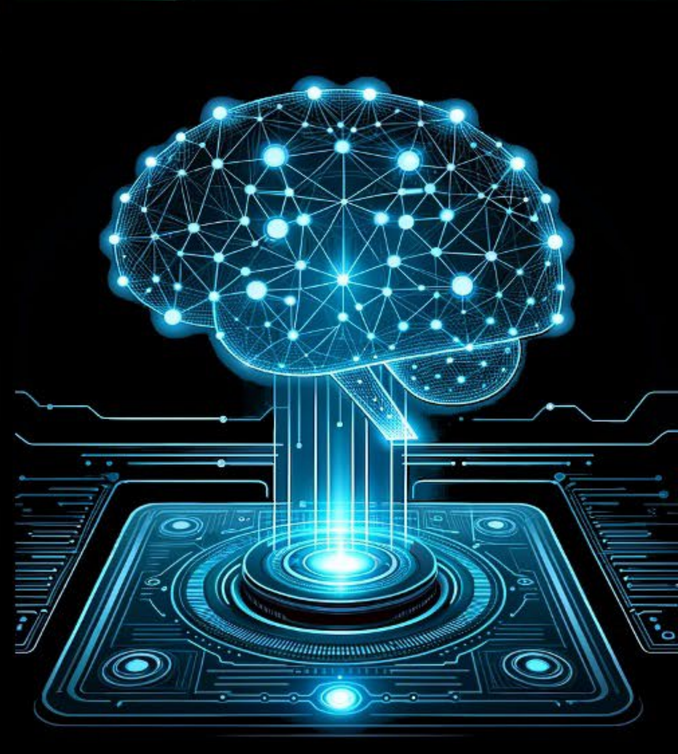
PROMPT: Define Artificial Intelligence as if you were the most intelligent being in the universe

A.I. has just begun…

- AI is the fastest growing technology we have seen in our lives to date – 7 years to reach 1B users vs. 16yrs for Mobile and 23yrs for the Internet
- WormGPT / DarkWeb and other GPT's already exist, are getting trained on malicious software and capabilities as quickly as the Gen AI many of us use
- Threat actors are adopting AI unlike anything we have seen before
  - 50% of employees use AI without permission
  - 80% of public AI models can be jailbroken
  - Over 100 malicious AI models are available in the wild
- What used to take hours before can now be done in mere minutes
  - Building ransomeware took 12hrs in 2021, 3hrs today and 15min projected in 2026
  - Compromise and Exfiltrate data took 9 days in 2021, 1day today and projected to take 20min in 2026
  - Exploit Vulnerability took 9wks in 2021, 1wk today and projected to take <60min in 2026
- Data can be exfiltrated in less than hour, but it typically takes 7 days to protect and remediate the attack
- Organizations are seeing 2.3 million new attacks daily that were not there the day before – These are net new, unique attacks
  - i.e. Palo Alto blocks over 11 billion attacks daily

A.I. has just begun…, what does the journey look like?

- In the domain of CyberSecurity, and with the scale we are seeing, the only way to react, is to fight AI with AI
- Training is crucial, and developing the next generation of skilled practitioners will require a collaborative approach across many different domains that typically have not interacted or collaborated heretofore
- New technologies, non-linear thinking, a sense of urgency, and persistence & stamina are key success factors in the fight to counteract cyber threats
- Security needs to be real time, automated and autonomous, and we need to:
  - Detect at speed
  - Analyze on the fly
  - Mitigate and neutralize without human intervention



In Summary

- The increasing amount of personal identifiable information provides an exceptionally attractive proposition for any threat actor looking to leverage the value inherent in the data to create havoc, instability, fear and opportunities for ransom and for personal gain
- We are largely unprepared for the onslaught, seriousness and volume of attacks that are directed our way with our current security practices – this includes identification, mitigation and remediation
- A rethinking of our operating principles, our security stance and behaviour, and our business continuity strategies including data, devices and policies is in order
- The use of Artificial Intelligence is a new and capable tool that presents a valuable countermeasure, capable of dealing with a new generation of threats and threat actors

Thank You