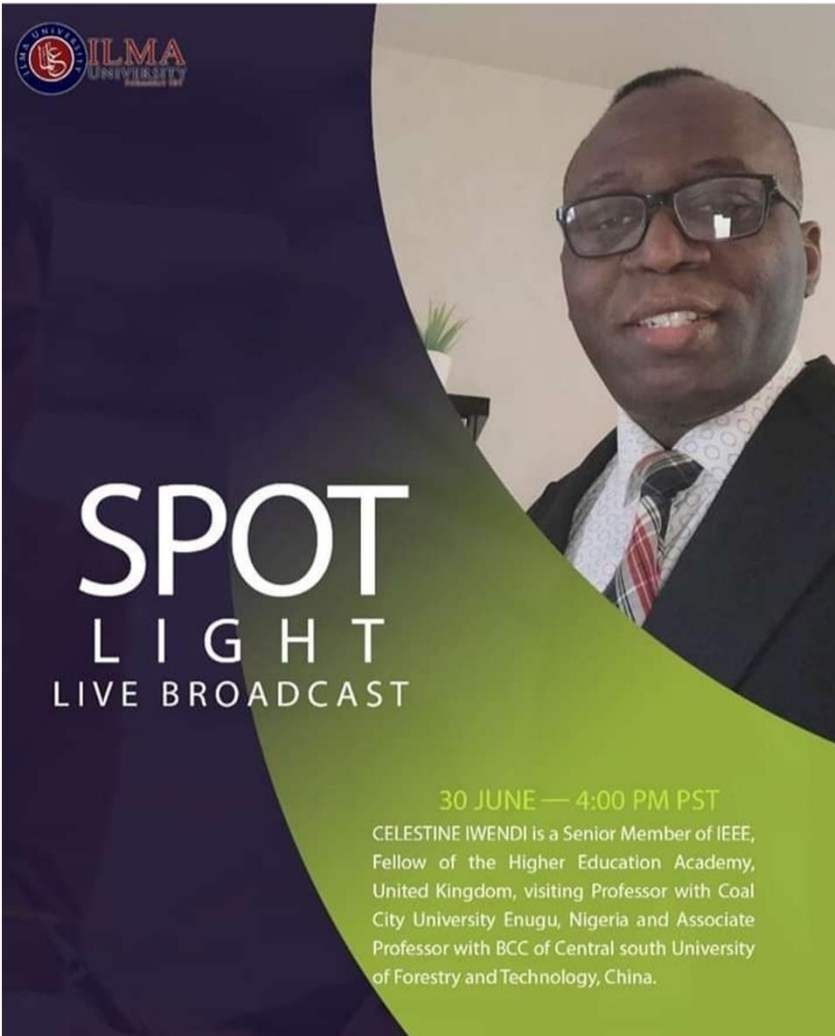




Ilma University

8 minutes ago ·

SPOT LIGHT
LIVE BROADCAST

30 JUNE — 4:00 PM PST

CELESTINE IWENDI is a Senior Member of IEEE, Fellow of the Higher Education Academy, United Kingdom, visiting Professor with Coal City University Enugu, Nigeria and Associate Professor with BCC of Central south University of Forestry and Technology, China.

Welcome

“Confidence is an Associate of Success” DrCI

ILMA Spot Light



“Spot Light”

“Exploring Opportunities in Covid-19: Artificial Intelligence & Security”

Celestine Iwendi

Senior Member IEEE

Fellow Higher Education Academy

Visiting Professor Coal City, Enugu

Assoc. Professor, Bangor College China

IEEE Sweden Section Board Member

ILMA University, Pk. 30th June
2020. 1pm CET

ILMA Spot Light

Disclaimer:

Some Part of this work has been done with many teams in Hewlett Packard Labs, HPE partners, universities, governments and Dejan Milojicic, Fellow IEEE

“Without intelligence, there is no value” Kiva Allgood, head of IoT and automotive at Ericsson

ILMA Spot Light

Key points

- Changing World – Chinese bank experience, AI Sustainable Future, Toilet sensors, Covid 19
 - Cybersecurity--a key concern to humanity, enterprise, consumer, virtual, cyberphysical,
 - Traditional solutions not sufficient anymore: AI enlarges the threat surface substantially
 - AI applied to cybersecurity and cybersecurity applied to AI, and 5G/6G Security Connectivity issues
- We need to, we ***have to*** react
 - Entirely new scenarios: mobility, IIoT, industrial IoT, gaming, deep learning
 - Traditional techniques– AI as a threat and AI as a solution to IIoT
- Call for action
 - Industry, governments, academia to eliminate noise and then focus on global challenges
 - AI 2.0 for Sustainable future for Pandemic Diseases
 - Cyber and AI apply to whole stack in eHealth

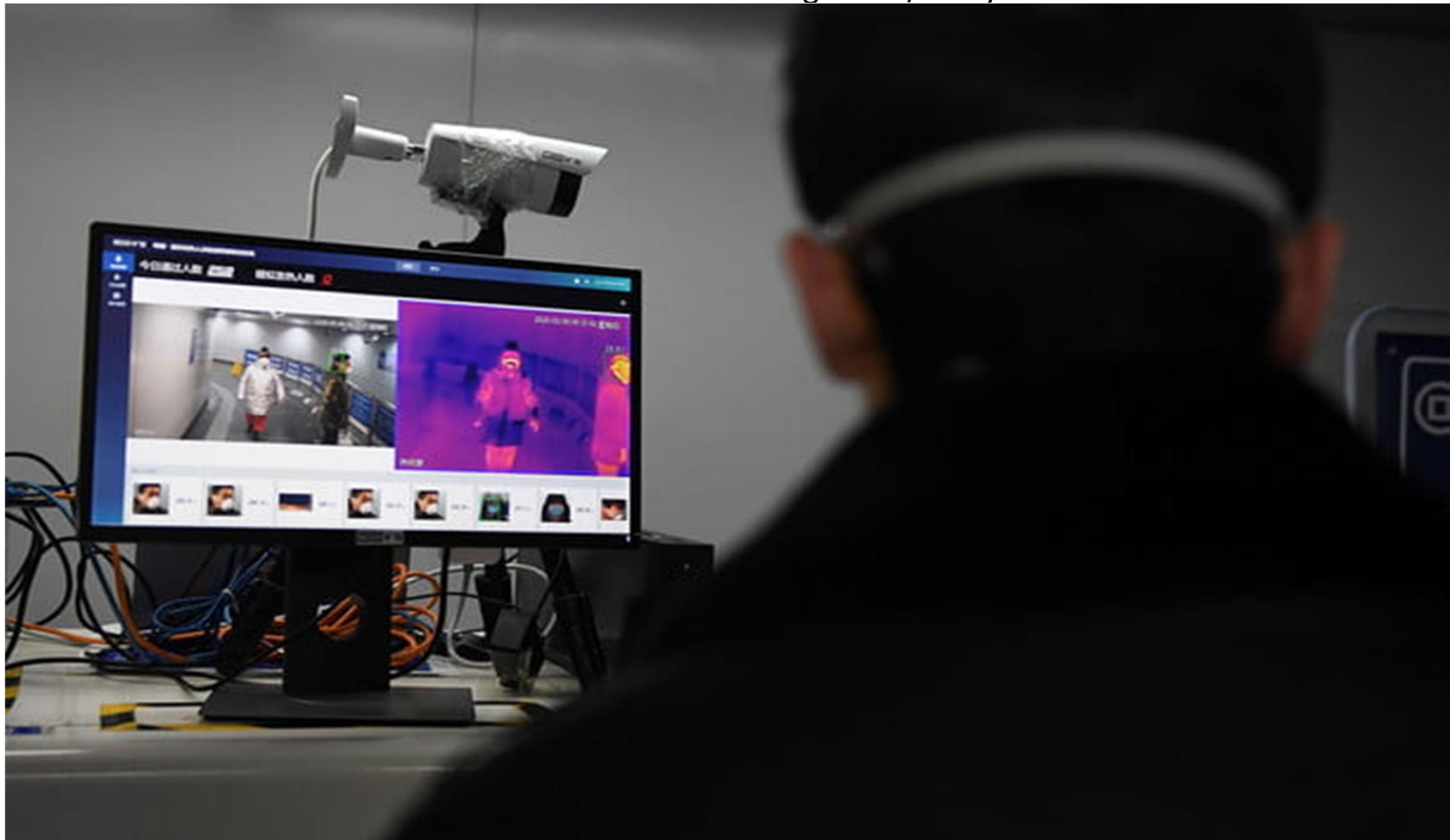
Changing World

- “The last decade was about connectivity, and we describe that dynamic with the Internet of Things,” Steve Koenig, vice president of research at the Consumer Technology Association, told Digital Trends.
- “This decade is really about adding intelligence to different devices, services, etc. We’re confronted with a new IoT: The intelligence of things.”

Changing World with Covid-19

- AI tools have been registering numerous successes in major disease areas such as cancer, neurology and now in new coronavirus SARS-CoV-2 (Covid-19) detection
- Covid-19 patients often experience several symptoms which include breathlessness, fever, cough, nausea, sore throat, blocked nose, runny nose, headache, muscle and joint pains.

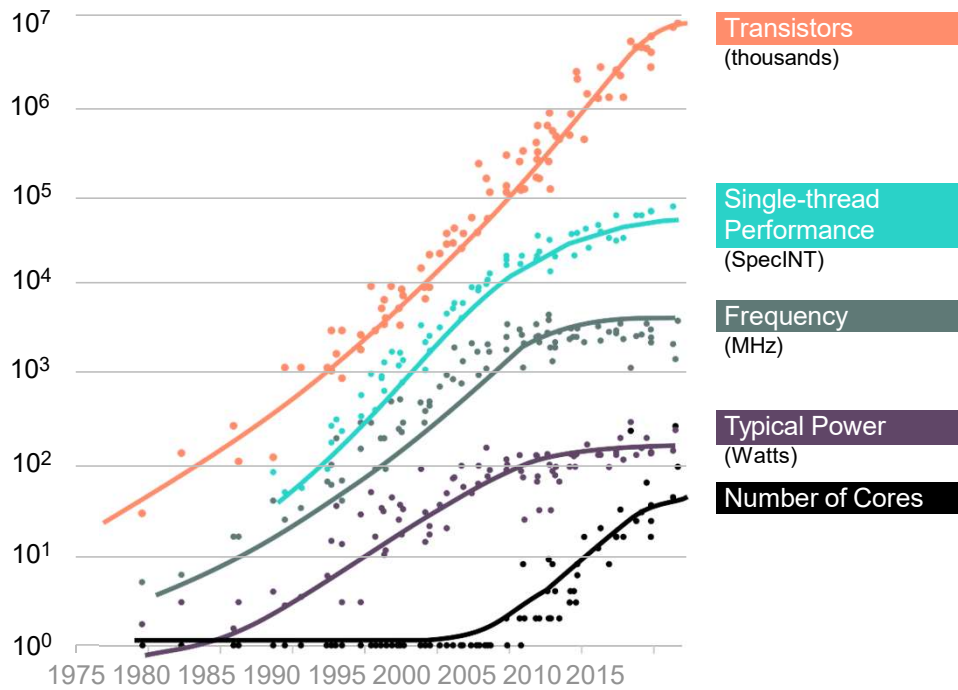
A security guard keeps watch as an A.I.-powered system developed by Chinese tech firm Megvii screens commuters for fevers as they enter the Mudanyuan metro station in Beijing, part of an effort to contain the spread of the new coronavirus in China. Greg Baker/Getty



ILMA Spot Light

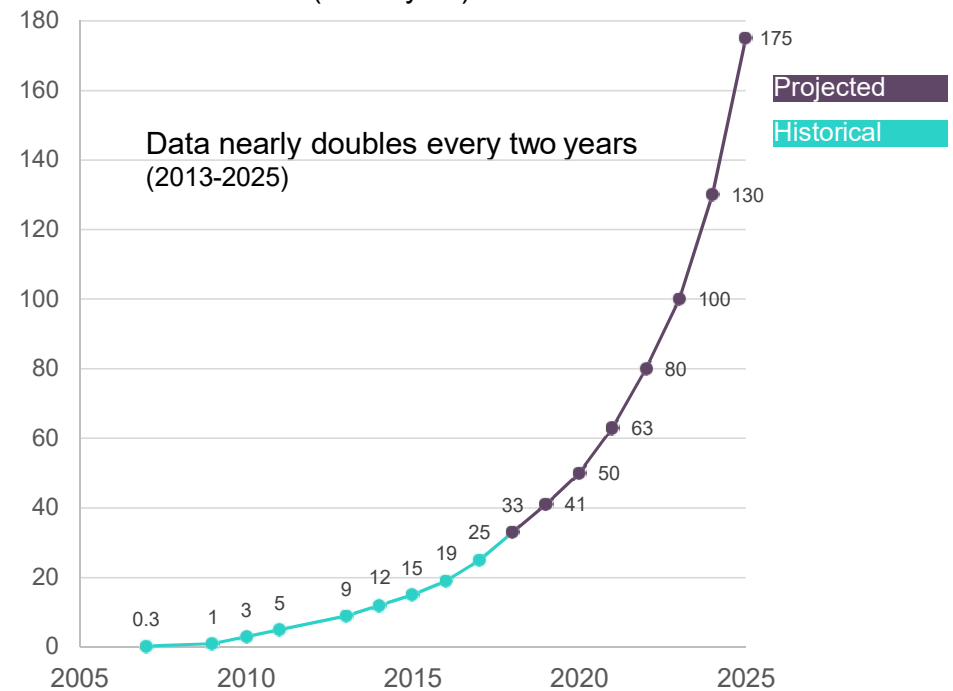
The New Normal: we are not keeping up

Microprocessors



Source: K. Rupp. 42 Years of Microprocessor Trend Data

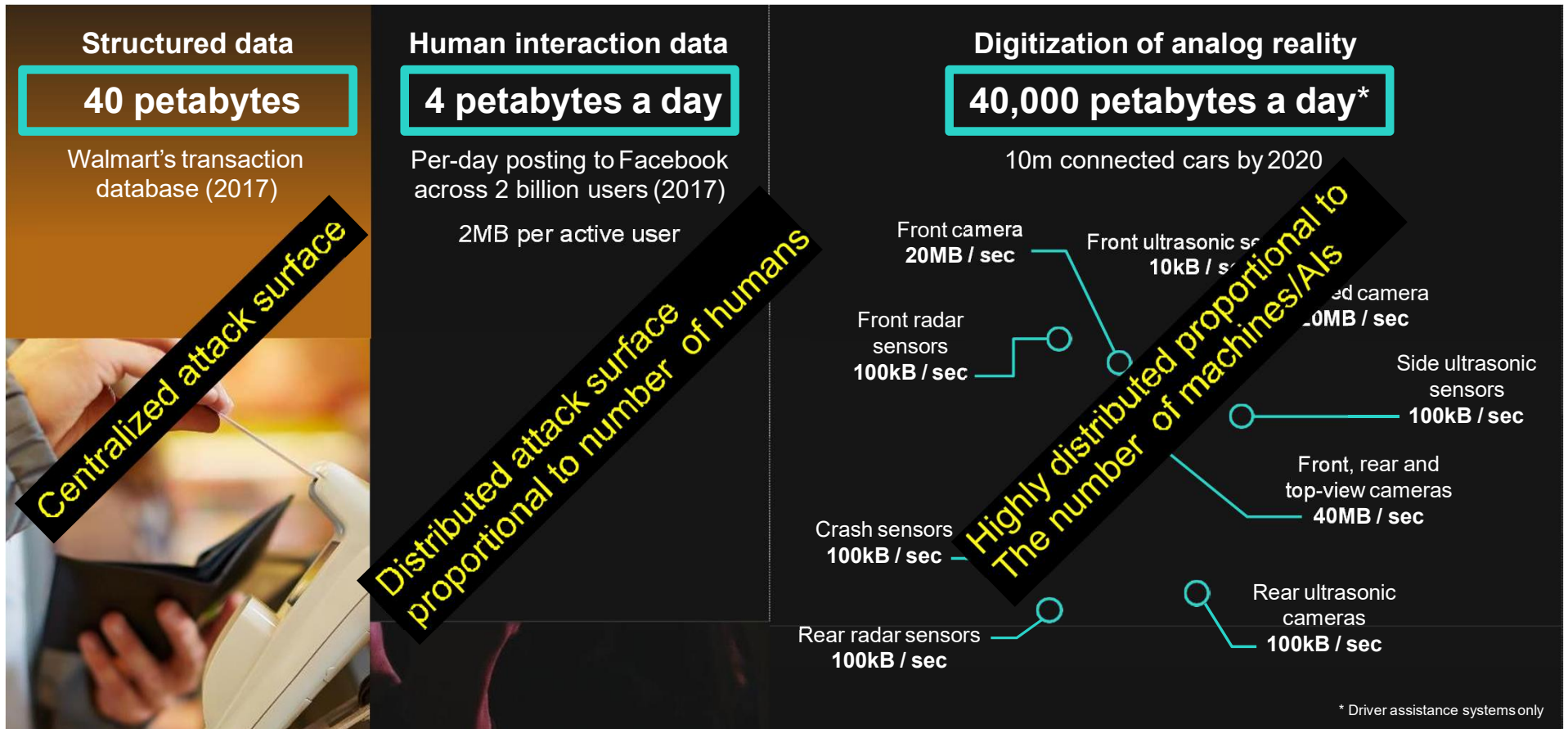
Global Datasphere (zettabytes)



Source: IDC Data Age 2025 study, sponsored by Seagate, Nov 2018

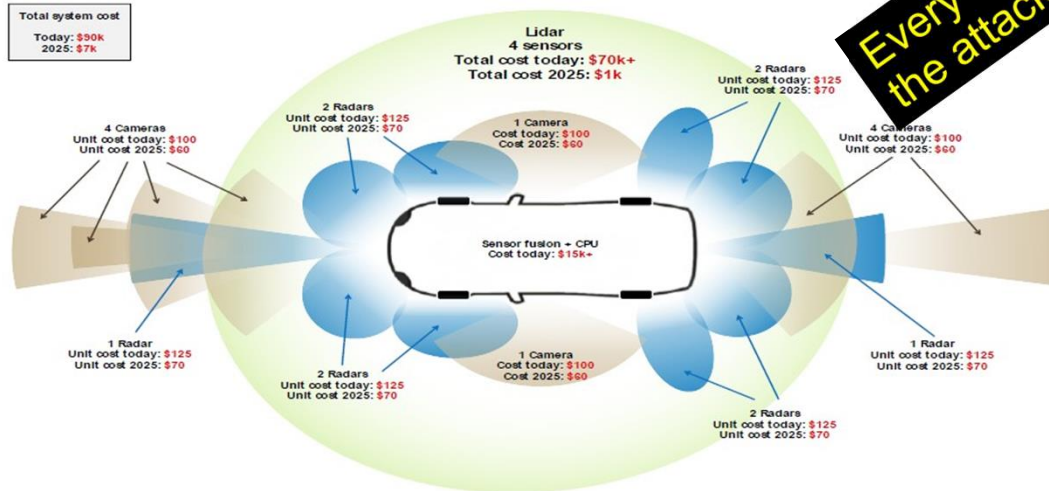
What's driving the data explosion?

How big is attack surface?



What is needed for an autonomous car?

LiDAR and HD map-based system (includes camera and radar as well)



Every single point is increasing the attack surface

We expect the prevailing sensor suite to include up to 12 cameras, 6 LiDARs and 6 radars ...

... and see the AV system cost below \$10,000 in 2025, versus \$100,000 today

Source: Infineon, UBS
Note: Excludes ultrasonic sensors for near-distance object detection (parking) – a minor cost item. Green = lidar, blue = radar, brown = camera.

The camera-only (and AI) AV system is cheaper, but has less redundancy. Regulators' approval could be an issue – potentially negative for Tesla



Intelligent Mobility – Spanning Edge/Cloud/Core

Every single interface is increasing the attack surface



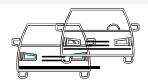
8. **Composable Memory-Driven Computing** enables fast processing of traffic and transportation data

7. **Edge-to-Core Resource & Data Management** through an integrated IoT platform that enables CICD deployment, aaS management of data & resources (compute, storage, stacks)

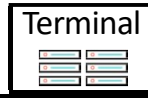
2. **Secure connectivity** with resilient platforms, services and data

4. **WiFi on-ramp to 5G Networks** allows seamless connectivity to LAN & WAN Network resources

Endpoint Devices



Edge IoT Platform



Cloud and/or Enterprise DC IoT Platform



1. **In-Vehicle Micro Data Center** with low power inference engines for safe, autonomous operations

3. **Mini Data Center** ingests vehicle data via WiFi as they return to Terminal during off-hours or maintenance

5. **SD-WAN** provides connectivity between Edge and Core Data Centers

6. **Composable Memory-Driven Computing** enables composable pools of memory & GPUs for big data training

AI: a solution and a Threat



Banks are evaluating AI-enabled real-time analysis of ATM use, including automated CCTV footage analysis enabling faster responses to fraudulent transactions.

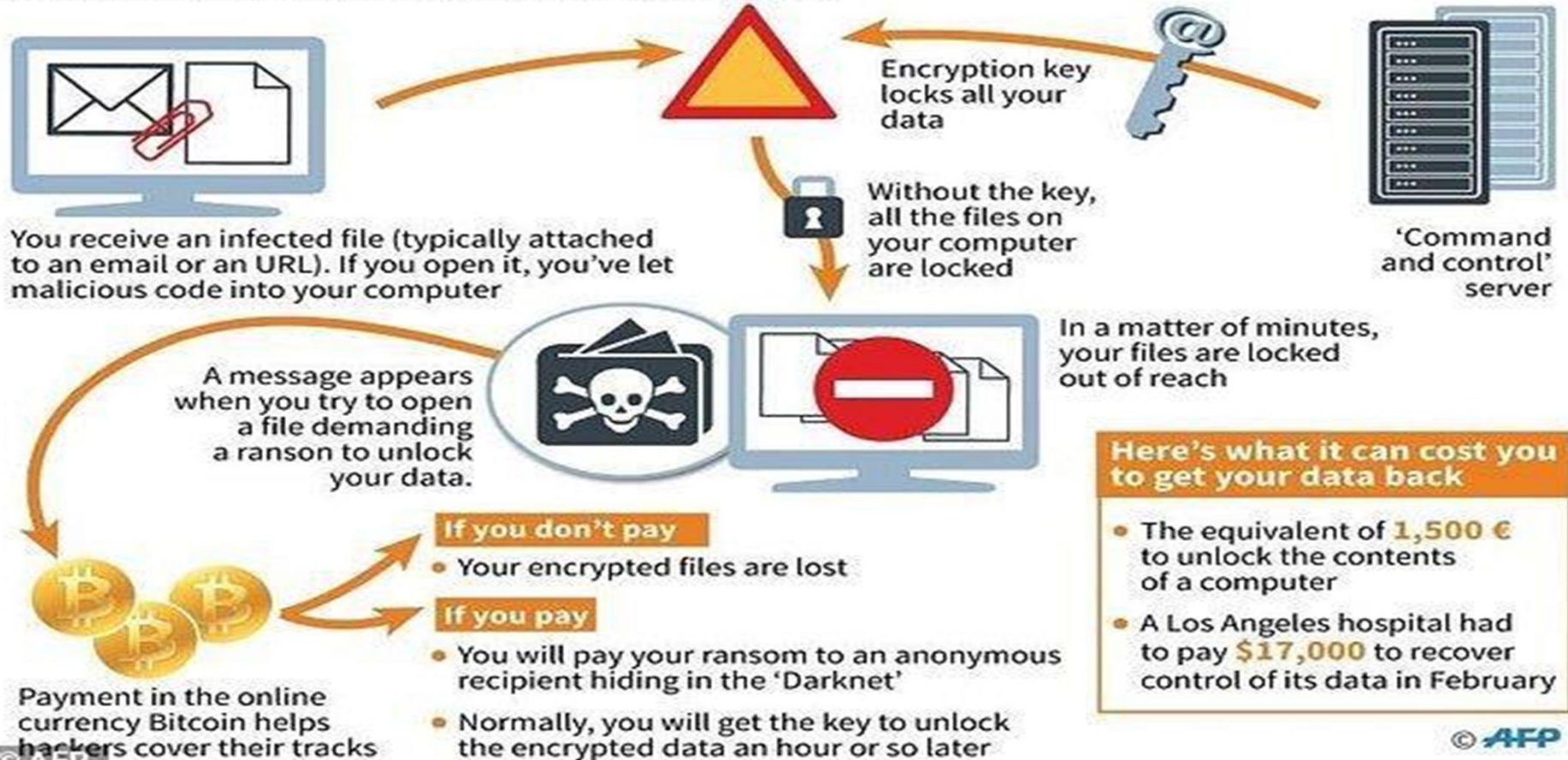
An Australian utility company is using predictive-based analytics drawing on IoT data streams to predict which conditions result in equipment failure. As a result, it can take preventative action in time, avoiding costly repairs

Rolls Royce is using AI-powered computing platforms to analyse the data generated by its aircraft engines. As a result, Rolls Royce can make design changes and operational recommendations that reduce airline fuel consumption.

Receiving Messages of fear of Covid-19 can affect your Computer

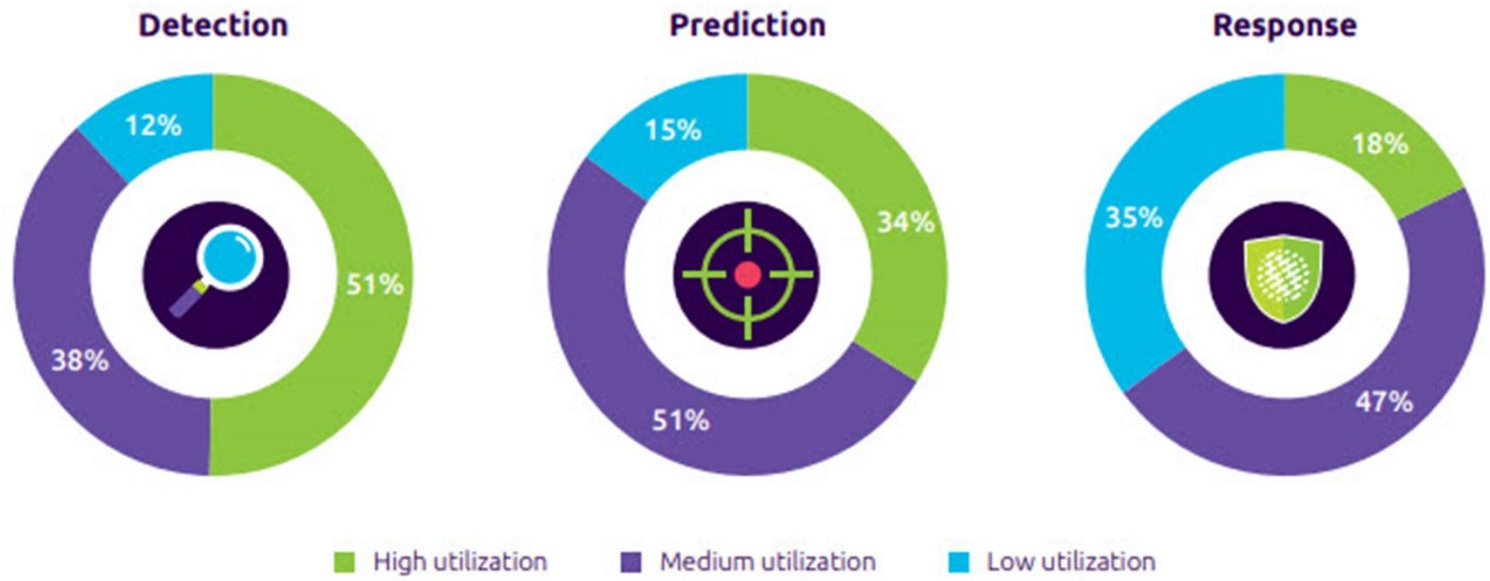
Ransomware: how hackers take your data hostage

Malicious code blocks access to the data in your computer



Higher utilization of AI for detection than prediction or response

Please rate your organization's utilization of AI in cybersecurity for the following areas



Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

IoT Vulnerabilities

- Weak, Guessable, or Hardcoded Passwords. ...
- Insecure Network Services. ...
- Insecure Ecosystem Interfaces. ...
- Lack of Secure Update Mechanism. ...
- Insufficient Privacy Protection. ...
- Insecure Data Transfer and Storage. ...
- Lack of Device Management.

<https://www.deviceauthority.com/blog/owasp-s-top-10-iot-vulnerabilities>

IOT real time data collection

- Generally, the devices are connected to a server via internet. ...
- The devices are connected to the server via various protocols like MQTT, XMPP, AMQP, or even http with a REST api or websockets.
- The data generated from the devices is stored in a database, and that is where you read the data. **IoT data** is mostly unstructured and so can easily be **stored** in public cloud infrastructure

AI as a solution: Deep Learning in Cyber Security

Example applications

- **Intrusion detection (IDS)**: Anomaly-based models that use autoencoders (fully-connected/CNN/CNN-RNN)
- **Malware detection**: Classification-based models that use fully-connected neural networks.
- **Spam and phishing detection**: Deep Learning methods for Natural Language Processing (unidirectional/bidirectional RNNs), URL classification with fully-connected models.
- **Traffic analysis (protocol identification)**: Classification-based fully-connected/RNN models.
- **Analysis of binary codes**: RNN-based sequence tagging with subsequent classification of suspicious code segments for identifying known classes of vulnerabilities.
- **DGA* names detection and categorization**: RNN/CNN+RNN models as binary classifiers.

*DGA – Domain Name Generation Algorithms, used by bot nets to generate domain names that are used as rendezvous points with their controllers.

IIoT - refers to the billions of internet-connected devices deployed around the world

AI as a solution: Deep Learning in Cyber Security

Method statistics

Number of papers

Application	Autoencoders	CNN	CNN RNN	DNN	RNN	RBM
Malware Detection/Classification	4	3	2	6	2	7
Intrusion Detection	11	2		3	8	6
Network Traffic Identification	2	1				
Spam Identification	1					1
DGA		1	2		4	

Numbers are from table 2 in A Survey of Deep Learning Methods for Cyber Security, Daniel S. Berman, Anna L. Buczak *, Jeffrey S. Chavis and Cherita L. Corbett

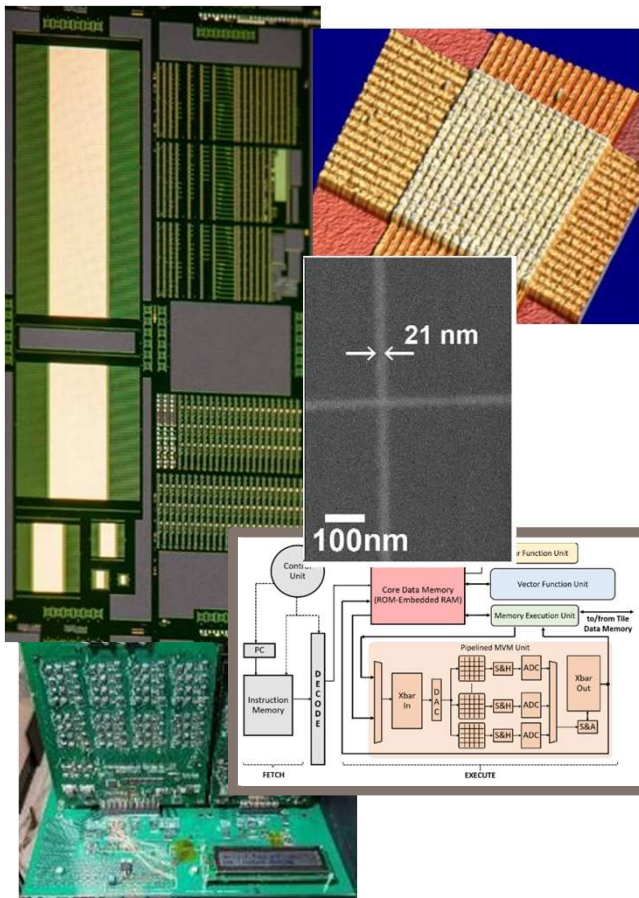
Artificial intelligence and machine learning can draw more advanced insights from data and draw these insights more rapidly. AI can identify unusual trends with greater accuracy and removes the need for human data review by using computer vision and speech recognition.

AI as a threat: Bias in deep learning

- Bias occurs when results are produced that are systematically prejudiced due to erroneous assumptions in the process.
- Algorithms can be designed by individuals with conscious or unconscious preferences
- Training data can introduce bias, etc.

- Or it can be result of a compromise
- Non trivial to discover

Hewlett Packard Lab's Efforts in Next Generation Accelerators



Hewlett Packard
Enterprise

Current computing workloads are predominantly limited by data movement (von Neumann bottleneck)

→ Develop novel non-von Neumann architectures

Combine existing CMOS + Non-volatile Analog technology

- In-memory processing
- Matrix operations in a single cycle
- Pattern matching (content addressable memories)

Some application areas for our accelerators

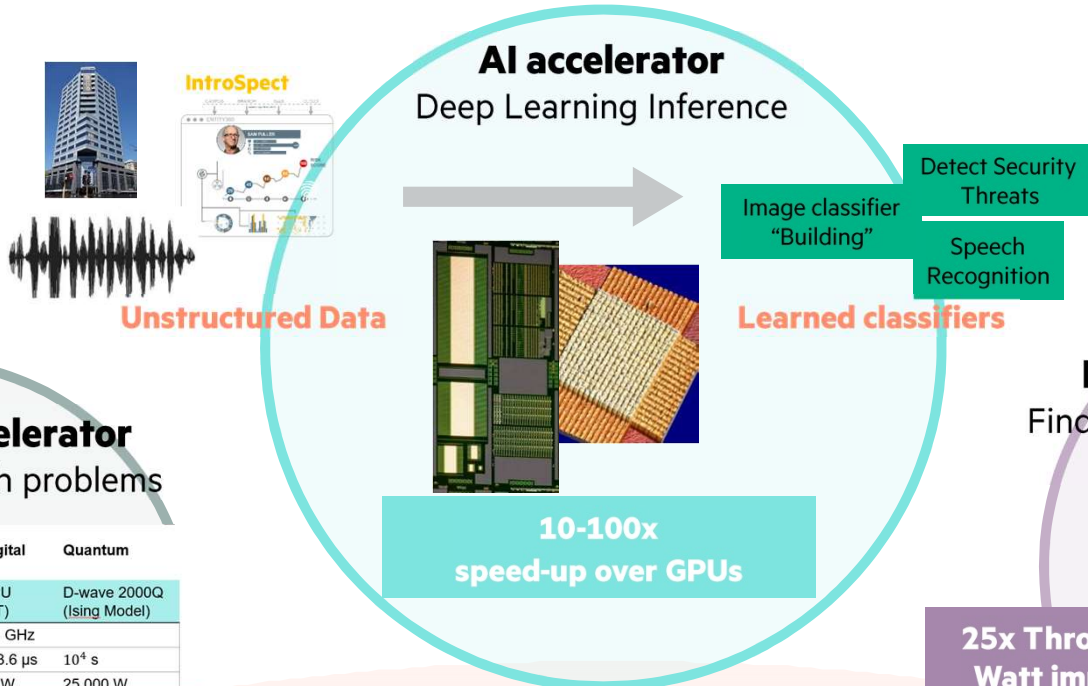
1) Neural Network inference: speed-up of >10x, with 10x lower area/cost over GPUs

2) Alternative to Quantum for solving NP-hard optimization problems – supply chain, scheduling, threat mitigation

3) Network Security – recognize attack signatures in packet data at wire speed ≥ 100 Gbps. 25x better than FPGAs

ILMA Spot Light

In-memory Analog-Digital approach enables 10-1000x gains across 3 challenging application areas



Optimization accelerator

Solve intractable graph problems

	HPE Analog/Digital	Digital	Digital	Quantum
	Dot Product Engine	GPU (NMFA)	CPU (PT)	D-wave 2000Q (Ising Model)
Clock frequency	1 GHz	1.5 GHz	2.6 GHz	
Time-to-solution	0.3 μ s	10 μ s	223.6 μ s	10 ⁴ s
Power	0.79 W	<250 W	20 W	25,000 W
Solutions/s/Watt	4.6 x 10 ⁶	>400	250	4 x 10 ⁻⁹

>100x vs Digital and Quantum today

Hewlett Packard Enterprise

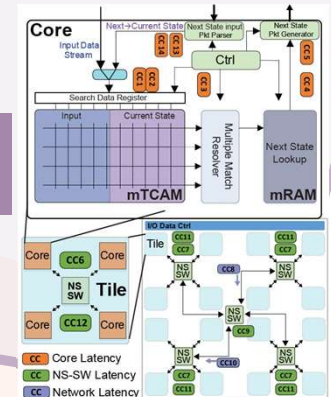
Combine CMOS + non-volatile analog technology for in-memory processing

ILMA Spot Light

Network Security accelerator

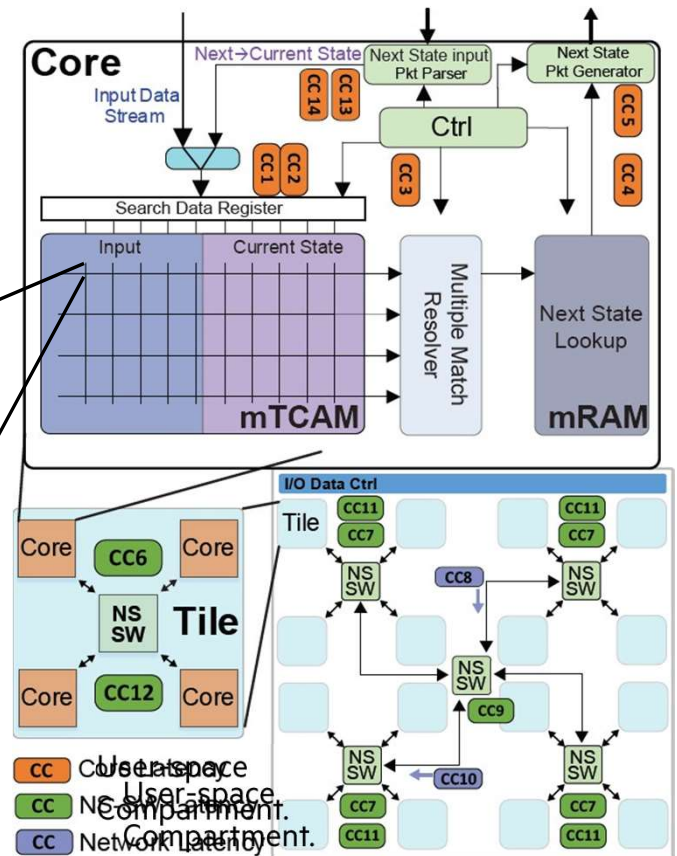
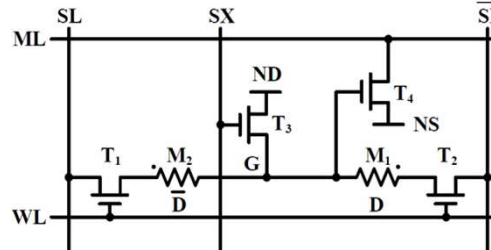
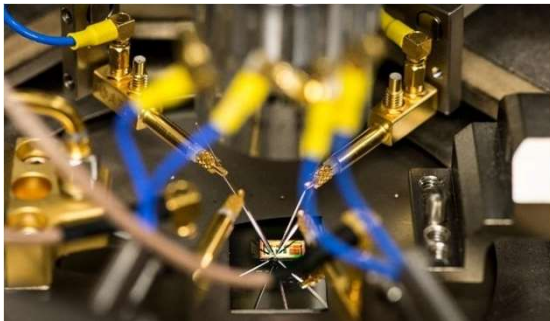
Finds attack signatures in data packets at wire speeds

25x Throughput per Watt improvement

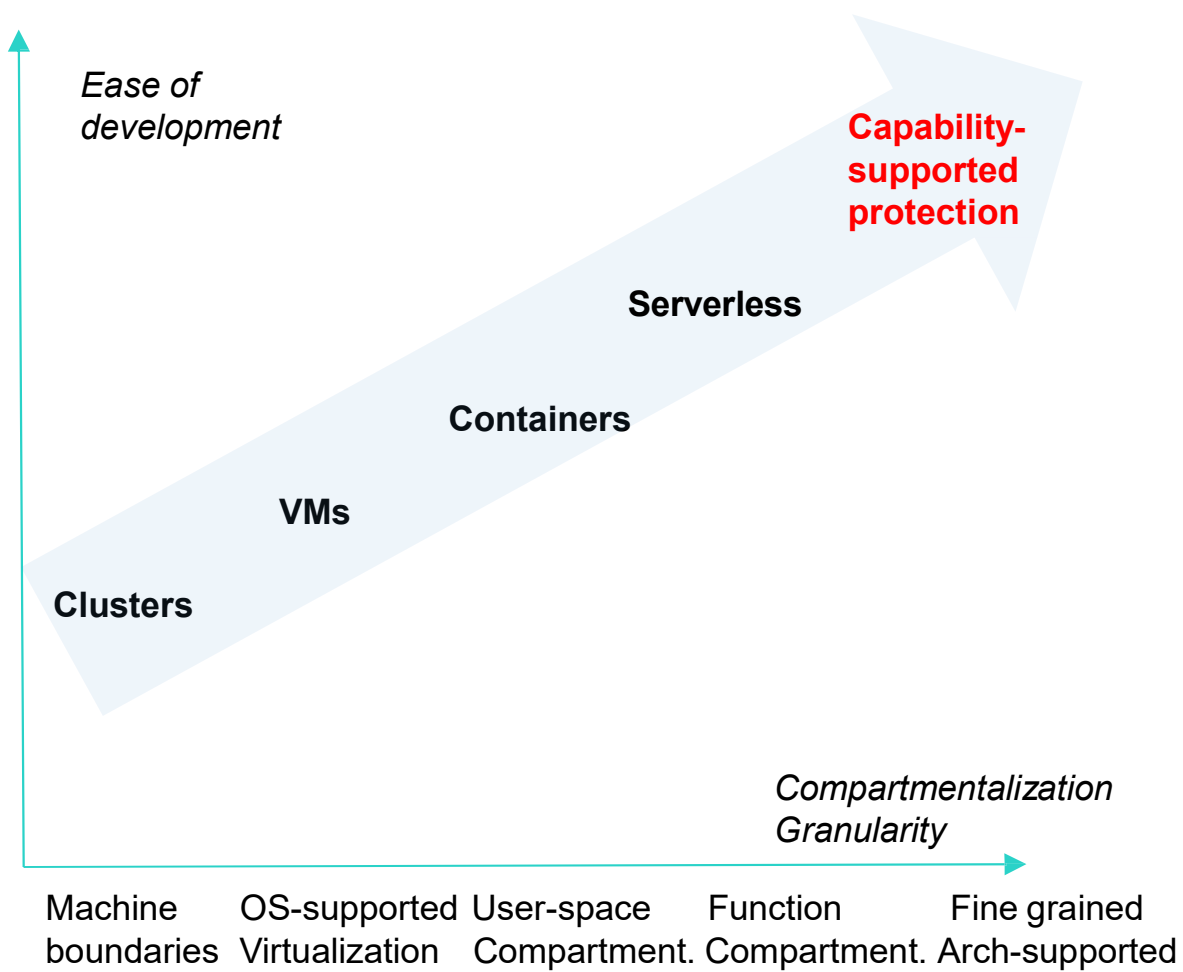
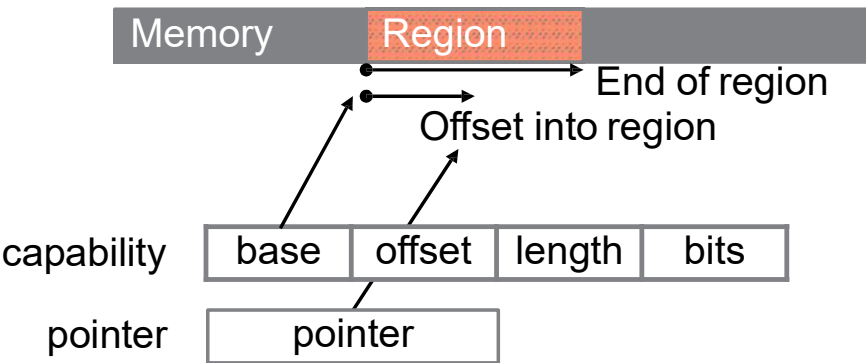


Network Security accelerator recognizes attack signatures in packet data at wire speed (≥ 100 Gbps) without error

- In-memory processing architecture encodes finite state machine in hardware to match patterns (RegEx) at $O(1)$
- Non-volatile analog technology reduces power and area
- 25x improvement in Throughput/Watt, **47 Gbps at 0.3W** on test
- set, target scaling to **100 Gbps** and beyond



Reducing Surface of Attack A Case for Capabilities



Transform performance with Memory-Driven programming

Modify existing frameworks

New algorithms

Completely rethink



In-memory analytics

15x
faster



Similarity search

40x
faster



Large-scale graph inference

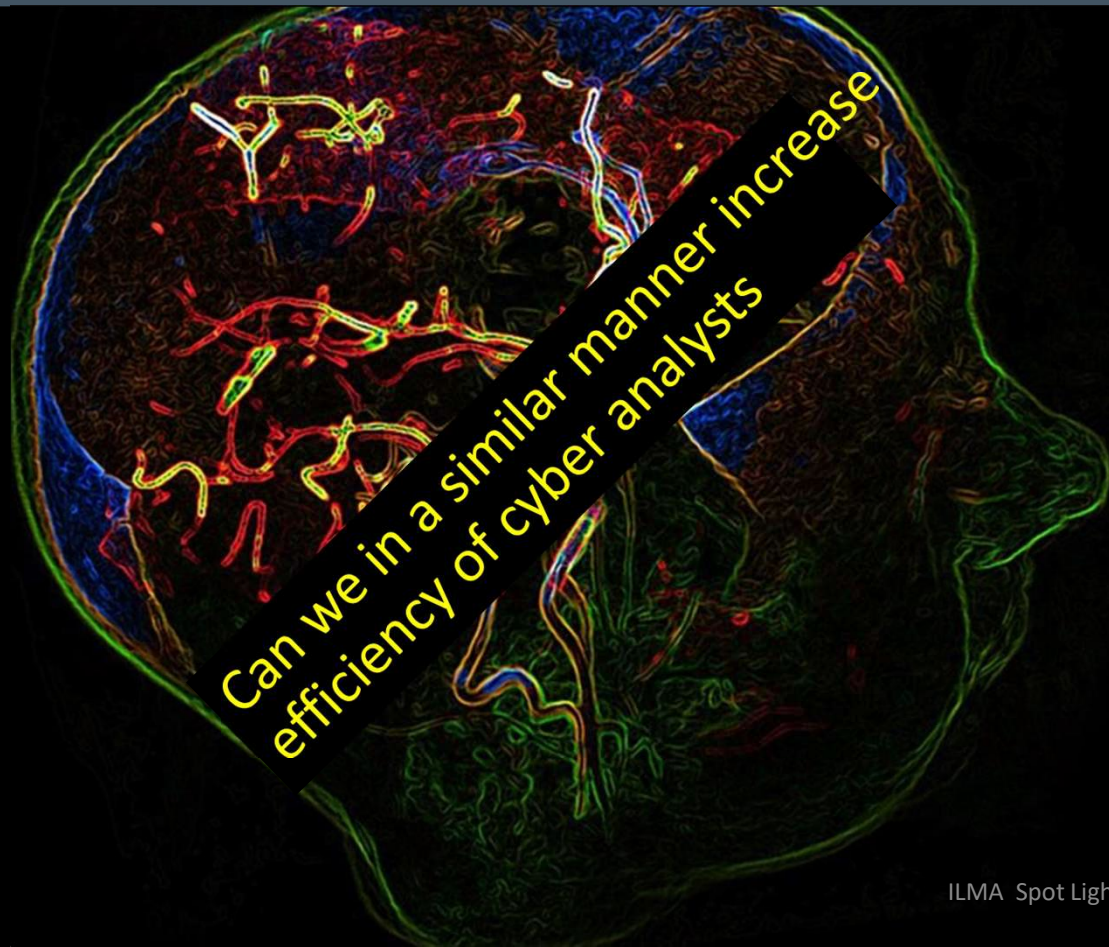
100x
faster



Financial models

10,000x
faster

Memory-Driven Computing helps outpace the global time bomb of neurodegenerative disease



Can we in a similar manner increase efficiency of cyber analysts



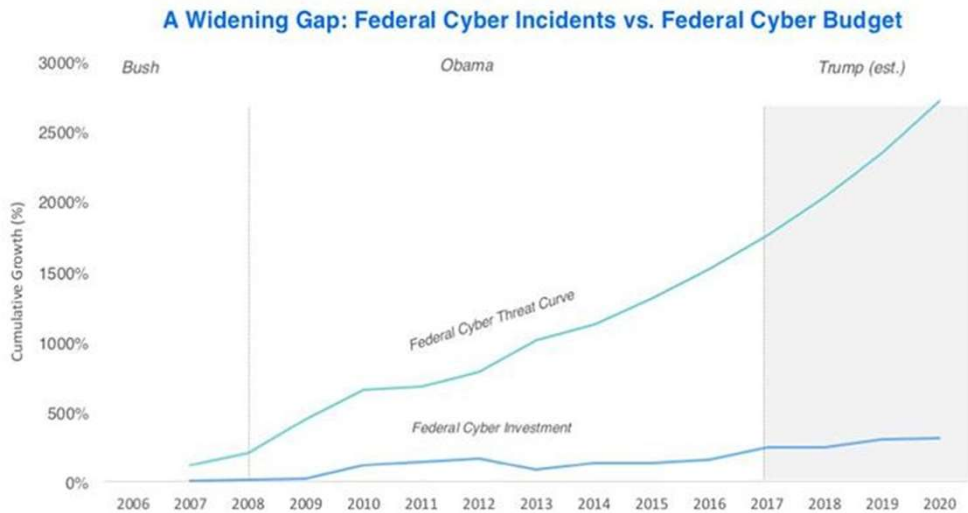
DZNE discovered HPE's Memory-Driven Computing — and saw unprecedented computational speed improvements that hold new promise in the race against Alzheimer's

60%
power reduction
cuts research costs

101x
increase in analytics speed
blasts research bottlenecks,
leading to shorter processing
time —
from 22 minutes to **13** seconds

Attacks are a Growing Problem

Government case, enterprises are similar



Prevention is nearly impossible

- Unless you're perfect
- Given enough time they will get in
 - Cost of attack is so low
 - Automated probing will find a weakness
- Advance Persistent Threats show hackers are patient

Why AI is the Future of IIoT

- 61% of enterprises say they cannot detect breach attempts today without the use of AI technologies.
- 48% say their budgets for AI in cybersecurity will increase by an average of 29% in Fiscal Year (FY) 2020.
- Breach attempts are proliferating with [Cisco reporting that in 2018, they blocked seven trillion threats on behalf of their customers.](#)

All Depends on the Analyst

Don't have the people

Cybersecurity Ventures estimates

3.5M unfilled cybersecurity jobs by 2021, up from **1M openings** last year

Don't have the right training

Enterprise Security Group and Information Systems Security Association

56% of respondents in 2016 survey said there was no training available

High turnover

Enterprise Security Group and Information Systems Security Association

46% of respondents were solicited to take a new job

It starts at the top

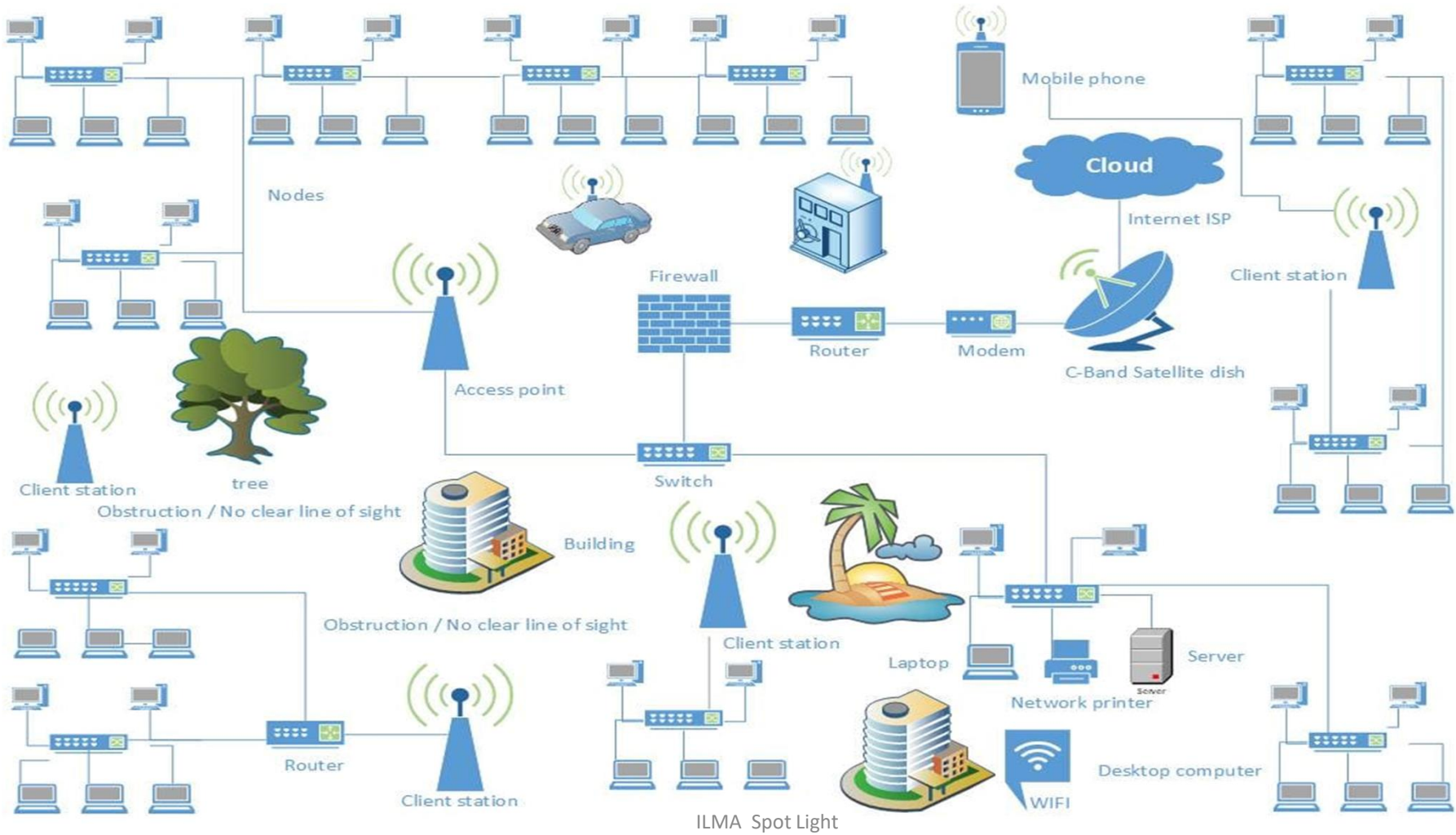
Enterprise Security Group and Information Systems Security Association

Average lifespan of a Chief Information Security Officer is 18 months

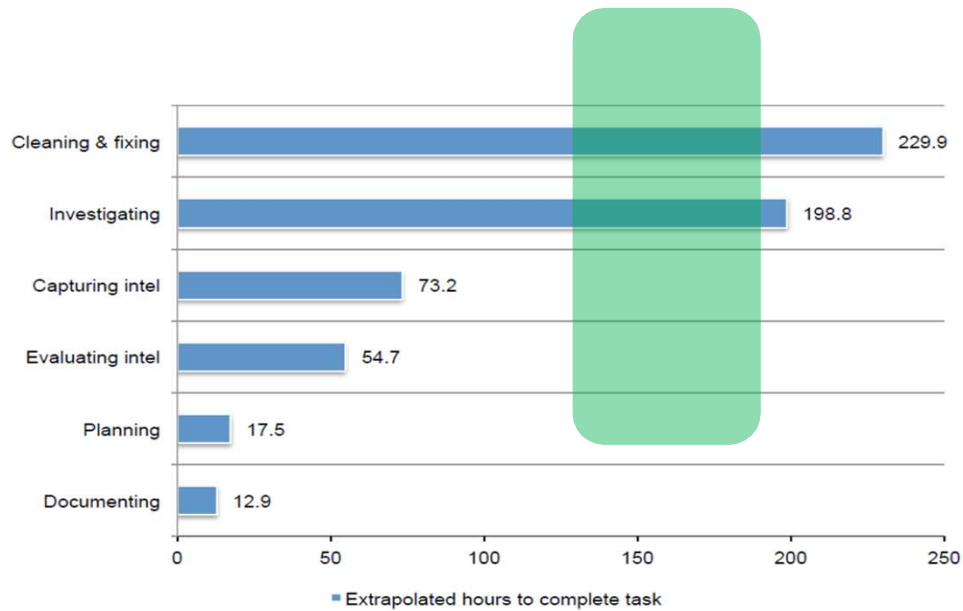
Enabling a sustainable future

- A new report co-authored by PwC and Microsoft, entitled '[How AI can enable a sustainable future](#)', argues that artificial intelligence technologies are among those that can enable real and effective change. Its claims are nothing short of bold; using AI for environmental applications in just four key industry sectors could contribute up to \$5.2tr USD to the global economy in 2030, reduce worldwide emissions by 4% in 2030, and create 38.2 million net new jobs.

Sustainable future



Automating Response with AI, Why?



- **Performance**: reduce response from 537 hours to seconds
- **Scale**: from 1 or 2 incidents to 1000s
- **Corporate knowledge**: transfer AI experience to new analysts

Barriers to implementing AI in Cyber (most related to standards)

- Lack of operational metrics to determine effectiveness
 - Preventing adversarial attacks
 - Ensuring AI is performing as expected
- Lack of realistic training data
- Lack of standardized workflows to enable integration of AI into current processes
- Lack of human-machine teaming model
 - How does the analyst use the AI
 - Who is responsible for training the AI

Partnering on Standards: Government, Industry, Academia, IEEE

- Governments can not do it alone (FIPS 192 for AES shows the flaws of Government only standards)
 - Limited participation (Most SSL systems not certified)
 - Expense of Government only certification expensive
- Industry standards are ubiquitous and well supported
 - UL is example of certification for fire safety seal of approval
 - Industry standards leverage worldwide technical expertise on the subject
 - Standards are more technical and touch more areas than regulations
 - Ensure minimum set of performance goals
- IEEE has 1300 active standards, 7,000 individual members in 90+ countries, 280 corporate members
 - IEEE 802.11 for wifi
 - IEEE 754 floating-point standard
 - And many others
- Academia brings out of box thinking

IEEE Standards Support

–Areas of potential standardization

- Format for network traffic capture
- Policy for AI/ML configuration
- Capture strategies
- Standard to define and capture execution environment
- Capture analyst steps

• –Process

- IEEE Standards Association offers a framework, processes, and structure
- Grand Challenge organizers will have to form the teams and create standards projects to actually execute on standards
- SA leadership will help in the process, advise on practical aspects and what to standardize vs not and how

AI 2.0 for Sustainable future

- Launch of the next generation AI (AI 2.0) in China soon. By 2030, the State Council of targets **China** to be the global leader in the development of **artificial intelligence** theory and technology

Focus will be on

- **Big-data intelligence:** transforms **big data** into insights and then renders an optimized engagement capability involving the active agents including BI strategists, **intelligent BI** analysts, **data intelligence** warehouse architects, **data** scientists, implementation and development experts.
- **Crowd intelligence:** essentially Internet-based **collective intelligence**
- **Cross-media intelligence:** Integrating data-driven machine learning with human knowledge. Using cross media data and make prediction, recognition, analysis and reasoning of these data
- **Hybrid-augmented intelligence:** Creating a hybrid collaboration between humans and machines. Long term goal to make machine think like human. Powerful more than machine or human intelligence
- **Unmanned autonomous systems:** are the next big step in the fusion of mechanical systems, computing technologies, sensors and software to create intelligent systems capable of interacting with the complexities of the real world.

AI/ML Practical application in Covid-19

- What you need to build an Intrusion Detection System or recommender system
- Python development Environment- download Anaconda and launch it or Natural Language Toolkit — NLTK 3.5
- Depending on the system you are creating. You get other packages needed for your work. For recommender, you install for recommender. I will need surprise, and for NLTK used for IOMT, I need numpy, panda, and for plot matplotlib. pyplot, seaborn

COVID-19 Patient Health Prediction Using Boosted Random Forest Algorithm

This paper aims to fill the voids of the traditional healthcare system by using machine learning (ML) algorithms to simultaneously process the healthcare and travel data along with other parameters of COVID-19 positive patients, in Wuhan, to predict the most likely outcome of a patient based on their symptoms, travel history and the delay in reporting the case; by identifying patterns from the previous patient data. Our contribution in the work include:

- Processing of healthcare and travel data using machine learning algorithms in place of traditional healthcare system to identify COVID infected person.
- This work compared multiple algorithms that are available for processing the patient data and identified Boosted Random Forest as the best method for processing data. Further, it executed a grid search to fine tune the hyper parameters of Boosted Random Forest algorithm to improve the performances.
- Our work obliterates the need to re-compare the existing algorithms for processing COVID-19 patient data.
- This work will enable the researchers to further work on developing a solution that combines the processing of patient demographic, travel and subjective health data with the image data (scans) for better prediction of COVID-19 patient health outcome.

Iwendi et al., COVID-19 Patient Health Prediction Using Boosted Random Forest Algorithm” Journal, Front. Public Health. 2020 doi: 10.3389/fpubh.2020.00357 Impact Factor. 2.031. SI Index . Main author.

COVID-19 Patient Health Prediction Using Boosted Random Forest Algorithm

- <https://www.youtube.com/watch?v=fTIYOJYyLaQ&feature=youtu.be>

PASMAI: Tackling Pandemic in Smart City using Artificial Intelligence

- This research proposes an artificial intelligence (AI) algorithms for predication on the quantiles of the distribution of a life table survivorship function of Covid-19 suspected patients. Four algorithms (Naive bayes, Logistic regression, Decision tree and K — Nearest Neighbors (kNN)) were used to determine which is better for this predication. The results show that Naïve bayes has 91.70% true positive rate for negative test. While logistic regression, kNN and decision tree have 99.20%, 99.20% and 99.30% true positive rate respectively for negative test. The analysis addressed in this research is significant for the study of the longevity risk in Covid-19 infected patients and their survival rate

Iwendi, Celestine.; Ebuka Ibeke; Cresantus Biamba; Gautam Srivastava. " PASMAI: Tackling Pandemic in Smart City using Artificial Intelligence". Journal of Sustainable Cities and Society. Main author. Impact factor: 4.624

Conclusion

- IoT and AI might help prevent future outbreaks of disease:
Imagine a global network of sensors and systems that provide an early warning system when infectious diseases threaten to become pandemics. Building one would be an enormous undertaking for governments around the world, but the potential is unquestionable
Therefore, Securing the Intelligence of Things will become vital to prevent hackers from gaining access to this beautiful idea.

Opportunities

Funding Available for Top Papers in top venues

Collaboration Available for Top Venue



Ilma University

8 minutes ago ·



**SPOT
LIGHT**
LIVE BROADCAST

30 JUNE — 4:00 PM PST

CELESTINE IWENDI is a Senior Member of IEEE, Fellow of the Higher Education Academy, United Kingdom, visiting Professor with Coal City University Enugu, Nigeria and Associate Professor with BCC of Central south University of Forestry and Technology, China.

QUESTIONS

Thank You

ILMA Spot Light