



Artificial Intelligence

Agenda

AI Past and Future
AI Enabled Cyber-security
Research
Future
Q&A



Deepinder Chhabra

Experienced and trusted advisor in Governance, Risk, compliance and Cyber Security

Principal Consultant Verizon

Vice President (ISACA London Chapter)

Professional Doctorate Student (UEL)

Post Graduate Diploma in Management

Executive Education from Harvard Business School

PRINCE2, TOGAF, ITIL Foundation

CEH, CHFI, CGEIT, CISM, CRISC

Senior leadership roles in FTSE 500 companies

Finance, Services, Retail, Manufacturing, Defence and HMG experience.

dchhabra@isaca-london.org

The views presented here are solely my own personal views and not those of my employer (Verizon)

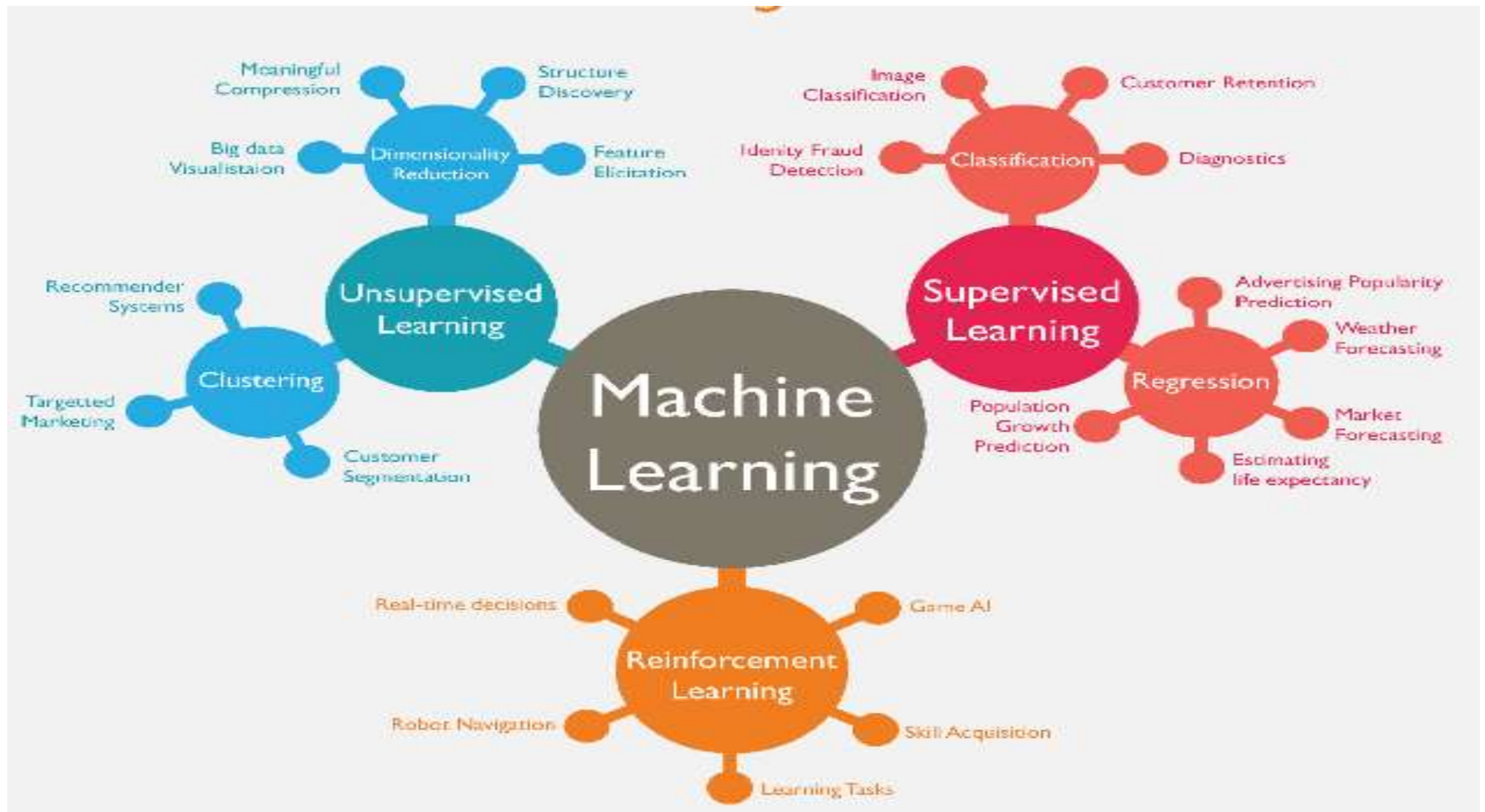




νοῦς

Understanding /Knowledge
/Intelligence

AI - Computer systems
able to perform tasks
normally requiring
human intelligence



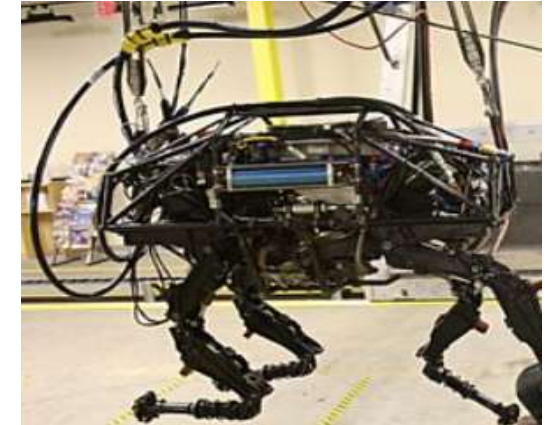
Current Applications of AI



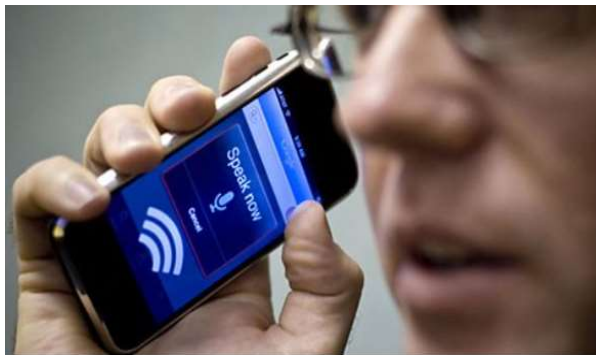
1997



2002



2005



According to Google, its speech recognition technology had an 8% word error rate as of 2015.



2011



2017







Drivers for AI Enabled Cyber Security

55
BILLION

by 2020

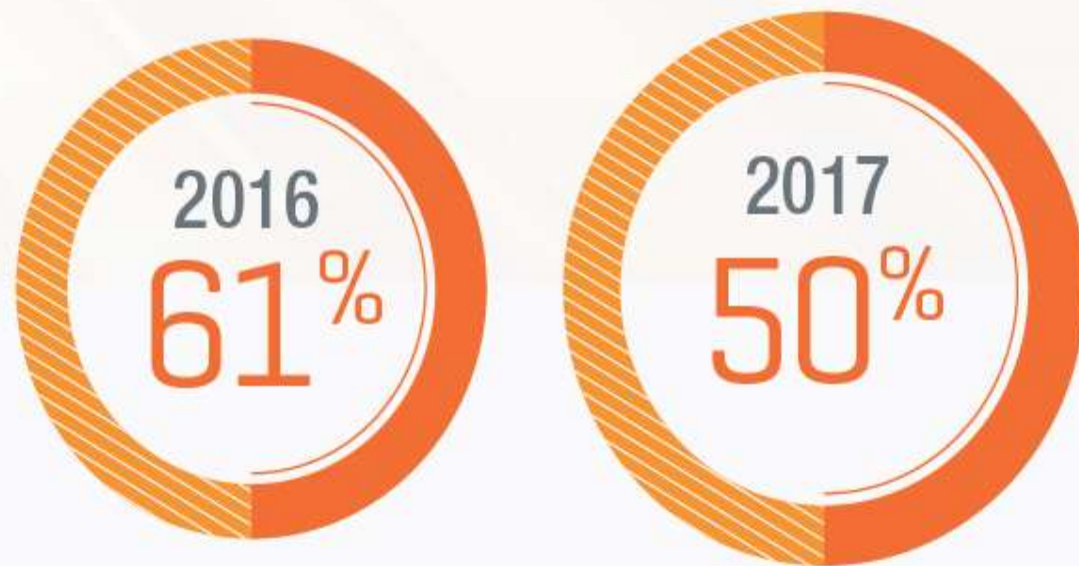


That's 5 per estimated
population of 2020

BUDGET



ORGANIZATIONS INCREASING SECURITY BUDGETS



Source: ISACA State of Security 2017

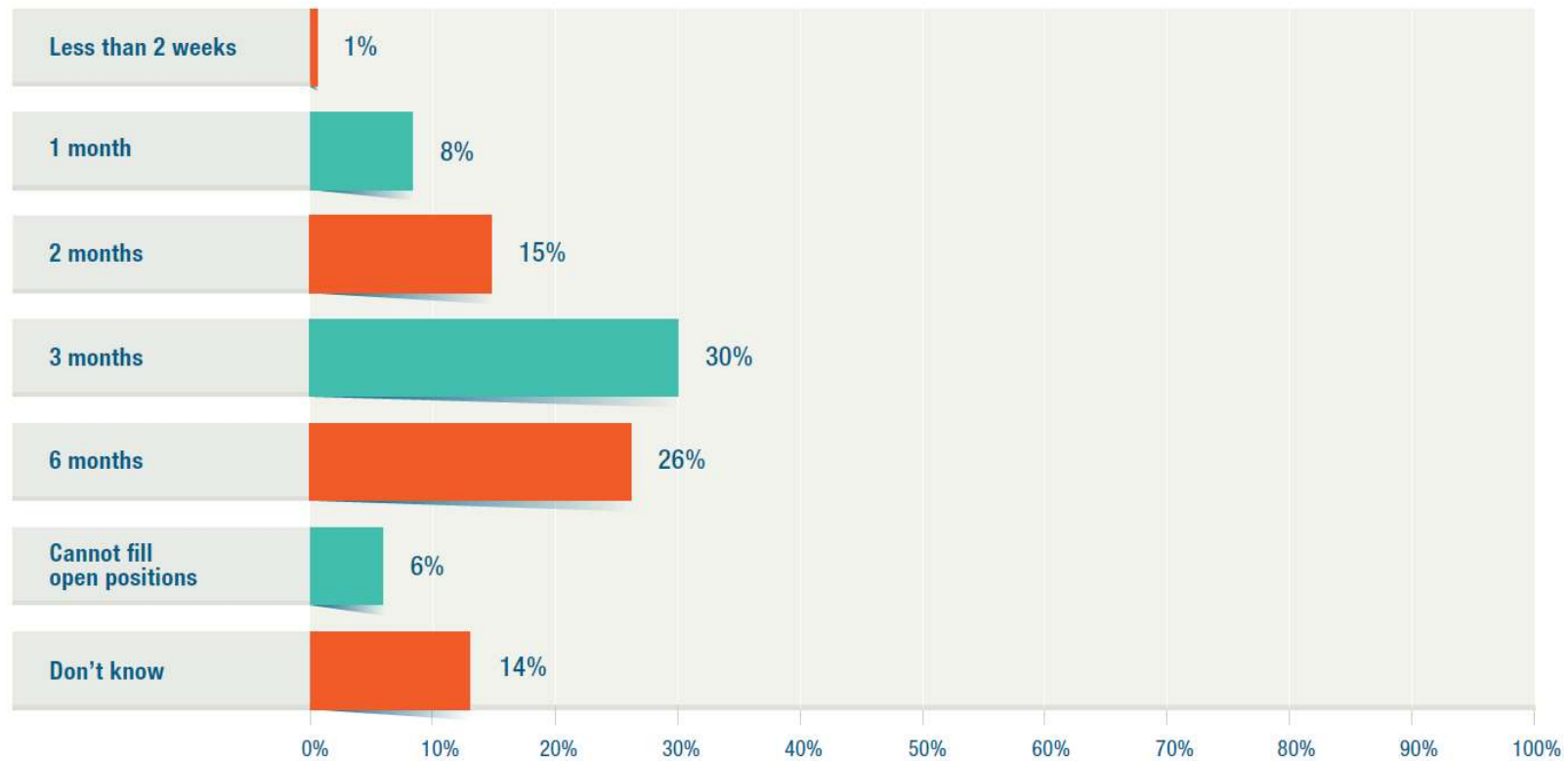


FEWER THAN HALF are
CONFIDENT in their team's
ability to handle anything
beyond simply cyber incidents

Source: ISACA State of Security 2017

FIGURE 4—TIME TO FILL AN OPEN CYBER SECURITY/INFORMATION SECURITY POSITION

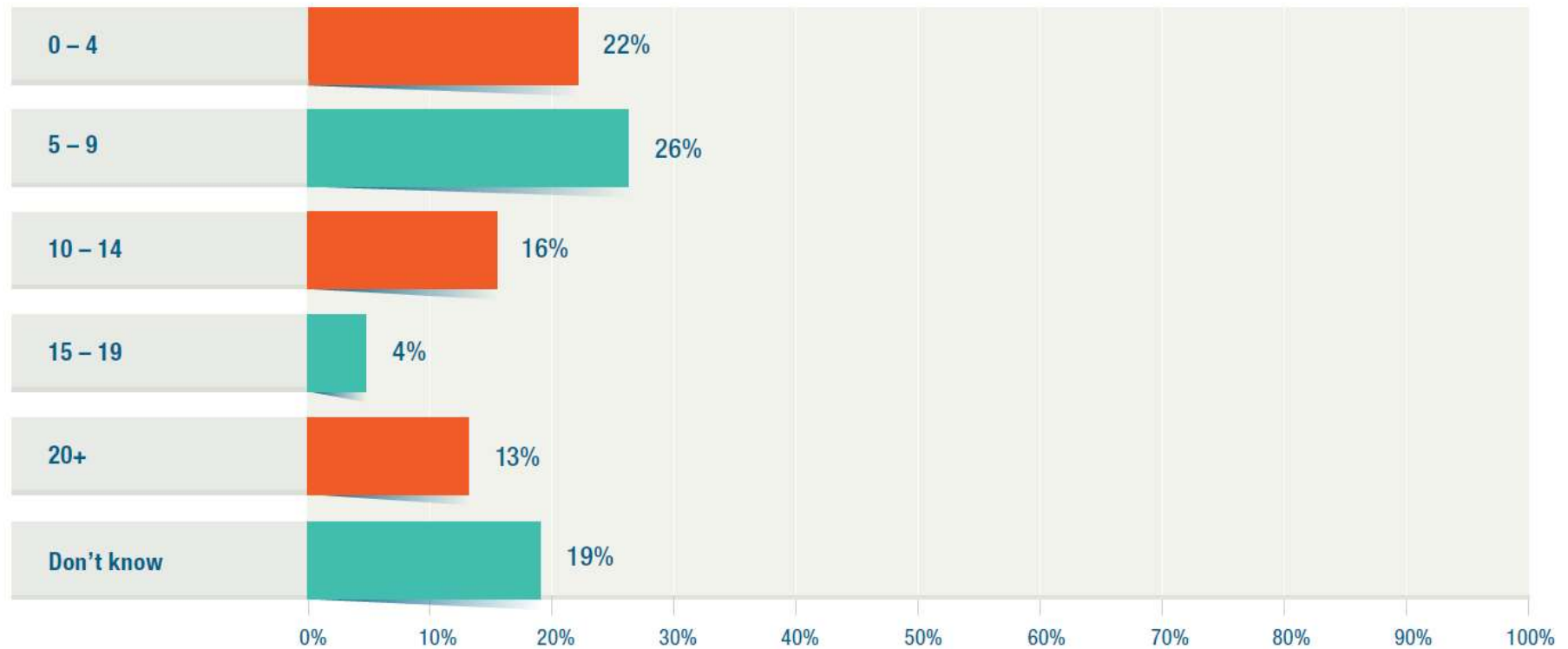
On average, how long does it take you to fill a cyber security/information security position?



Source: ISACA State of Security 2017

FIGURE 5—NUMBER OF APPLICANTS FOR OPEN SECURITY POSITIONS

On average, how many applicants do you get for open security positions?



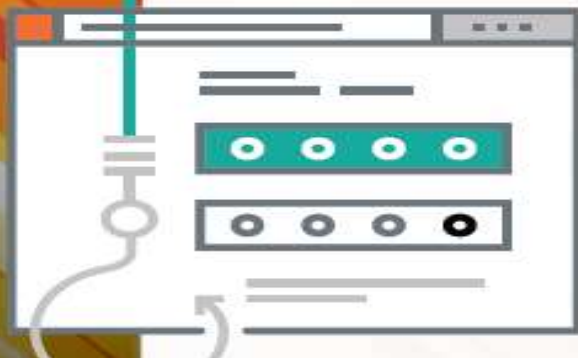
Source: ISACA State of Security 2017

IT Security				
Head of Information Security (10+ yrs' exp)	90 - 150k	95 - 155k	750 - 1100	800 - 1150
Information Security Manager (5 - 10 yrs' exp)	75 - 115k	80 - 120k	600 - 800	650 - 900
Information Security Analyst (5 - 10 yrs' exp)	60 - 95k	60 - 95k	500 - 750	550 - 800
Information Security Analyst (1 - 5 yrs' exp)	40 - 60k	45 - 70k	300 - 500	350 - 550
Information Security Risk Manager (5 - 10 yrs' exp)	75 - 110k	80 - 115k	600 - 800	650 - 900
Information Security Manager (1 - 5 yrs' exp)	55 - 75k	60 - 80k	450 - 600	500 - 650



4 IN 5

Think it is likely or very likely that their enterprise will experience a cyber attack this year



53%
OF ENTERPRISES
EXPERIENCED MORE ATTACKS
this year than in the year prior

SECURITY & PRIVACY

AI Is the Future of Cybersecurity, for Better and for Worse

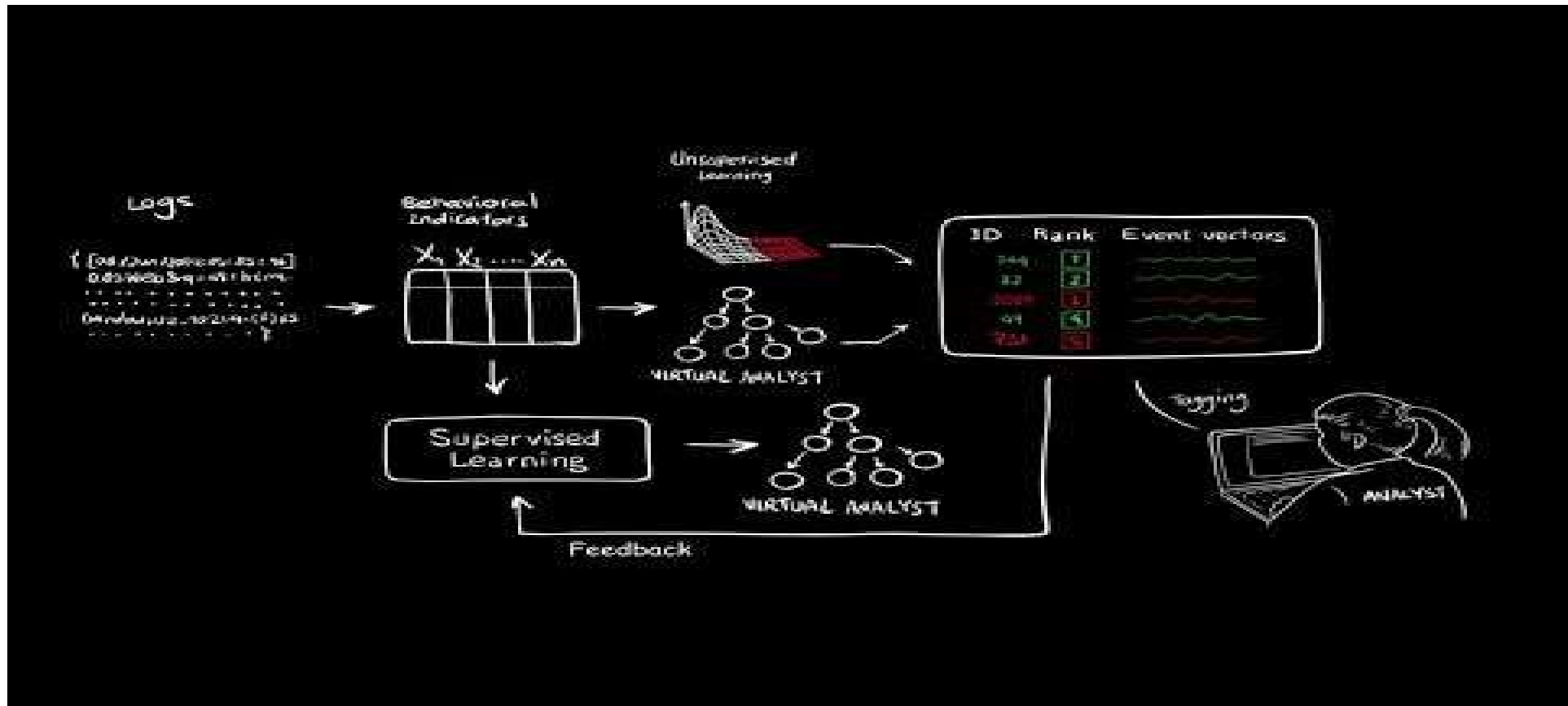
by **Roman V. Yampolskiy**

MAY 08, 2017

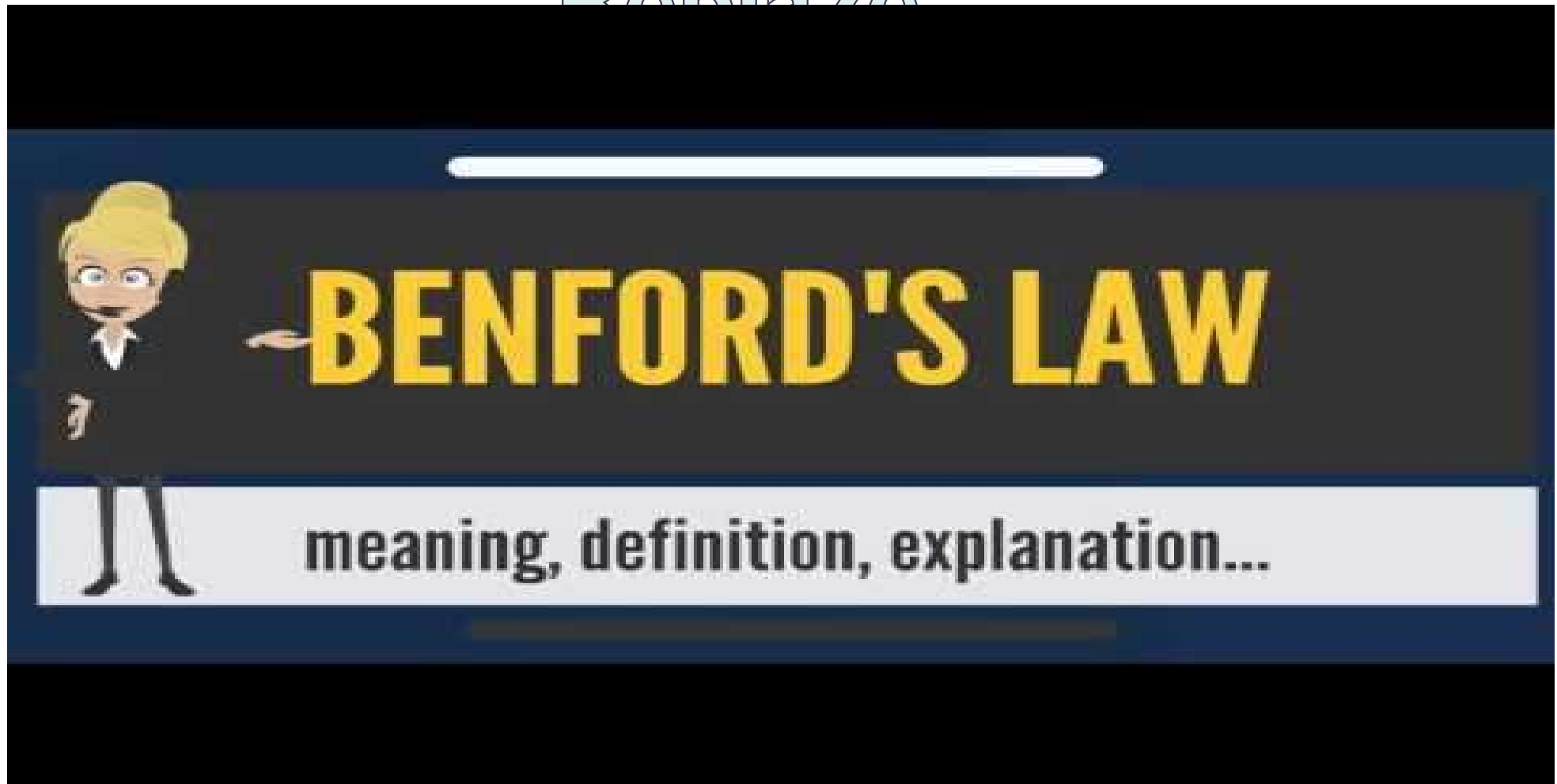


Current Landscape

AI2



https://youtu.be/b6HfIO_vpwQ

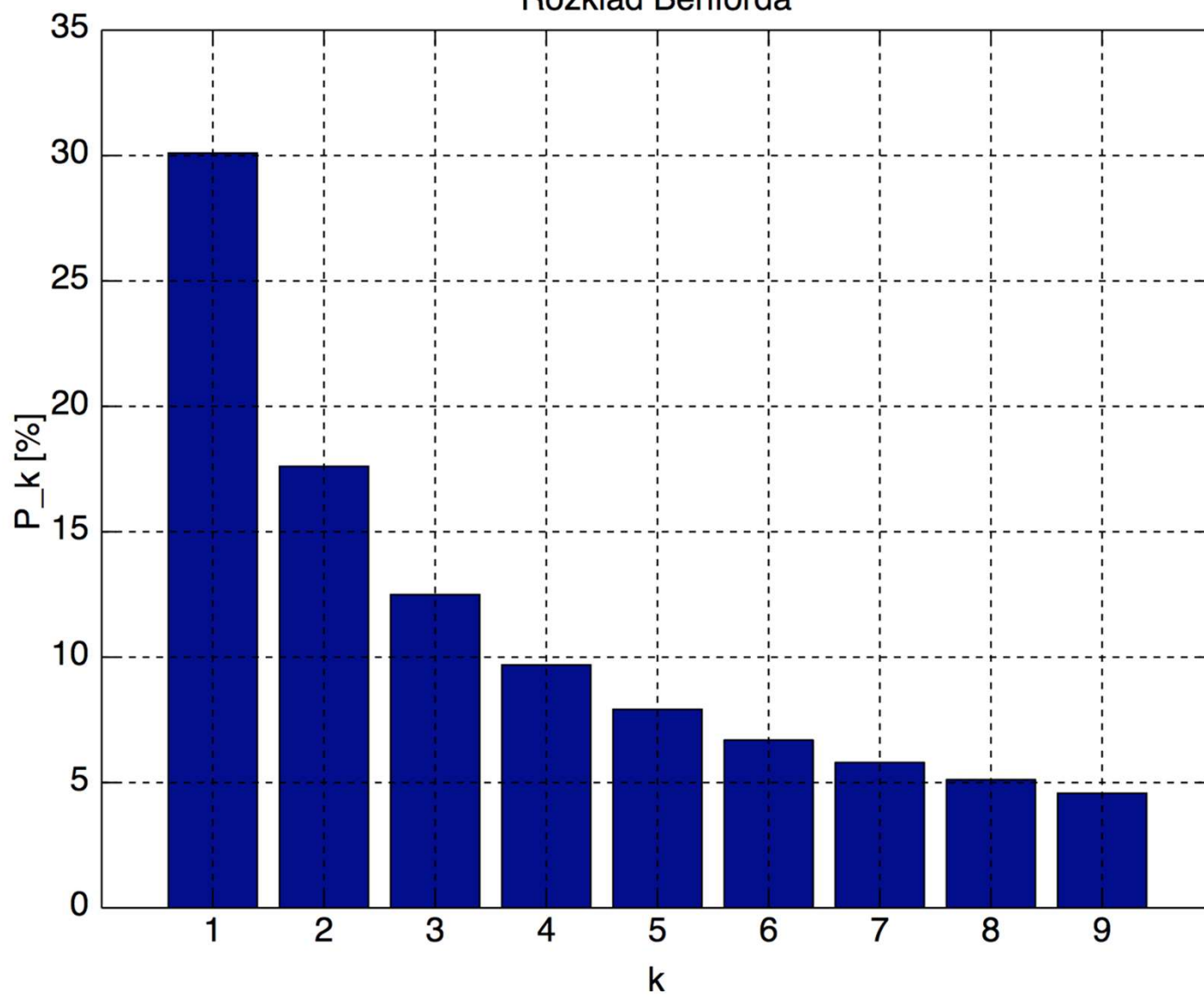


BENFORD'S LAW

meaning, definition, explanation...

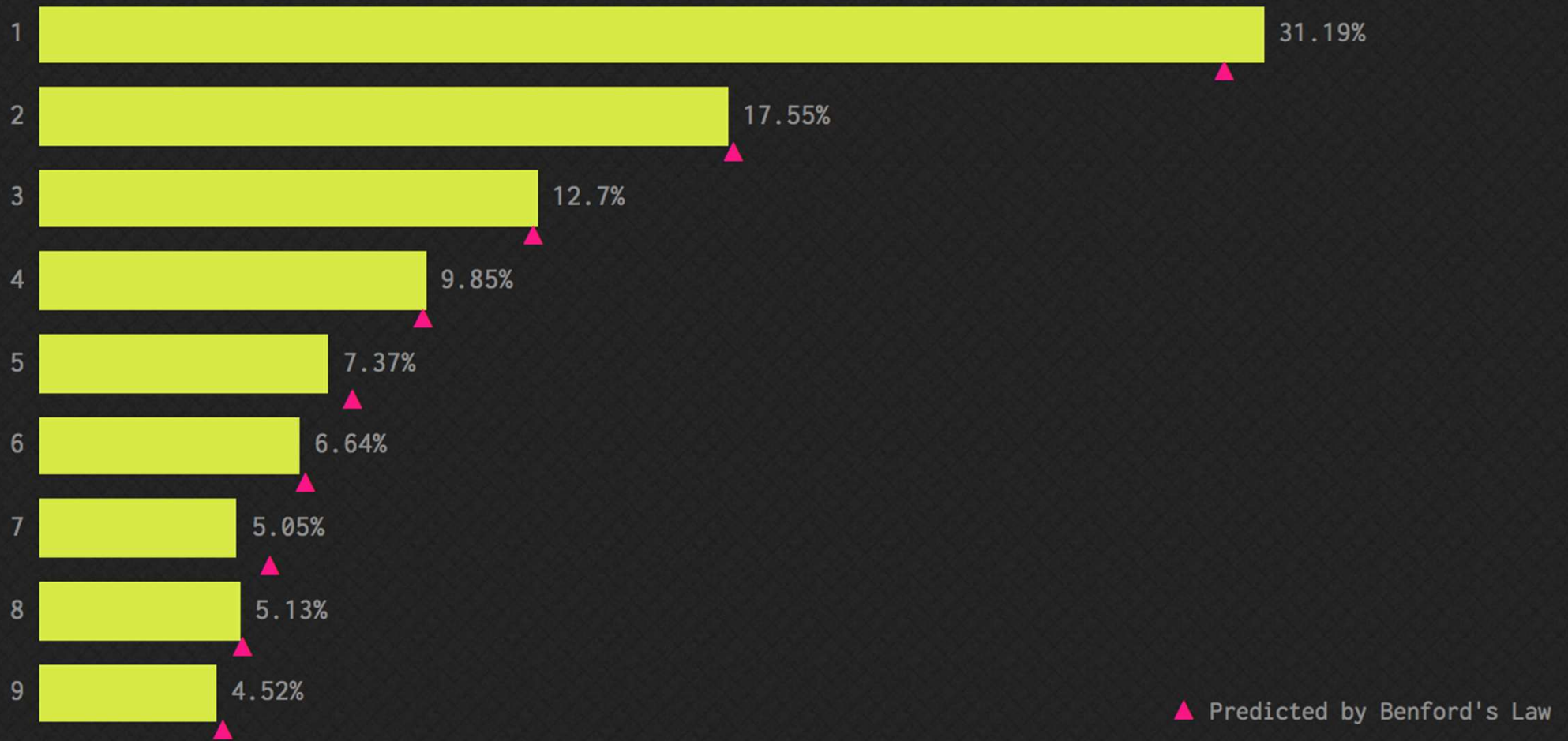
https://youtu.be/b6Hf1O_vpwQ

Rozklad Benforda



Population of Mexico's Counties (Municipios)

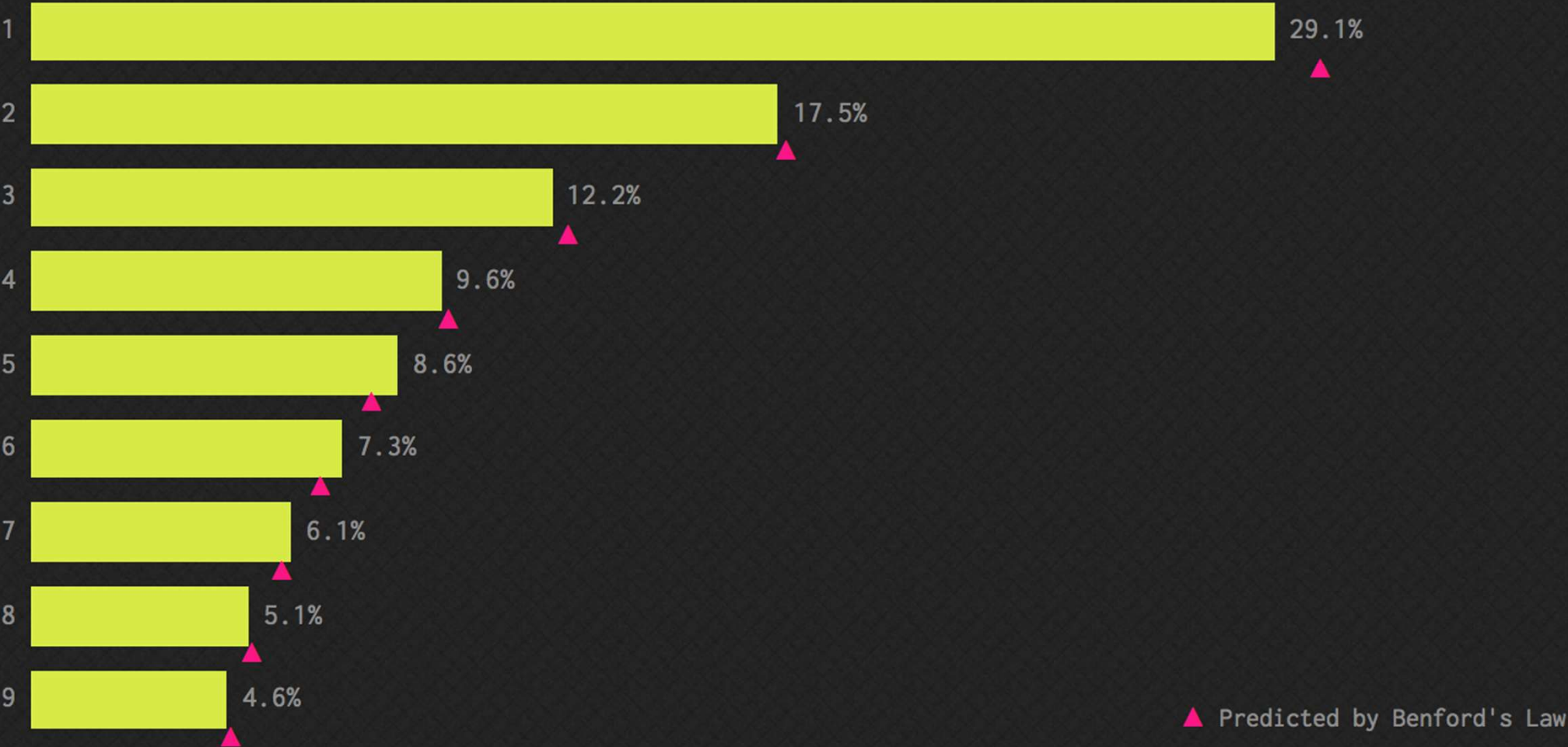
Leading digit frequency



Source: <http://testingbenfordslaw.com/population-of-turkish-boroughs>

UK government spending May–Sept 2010

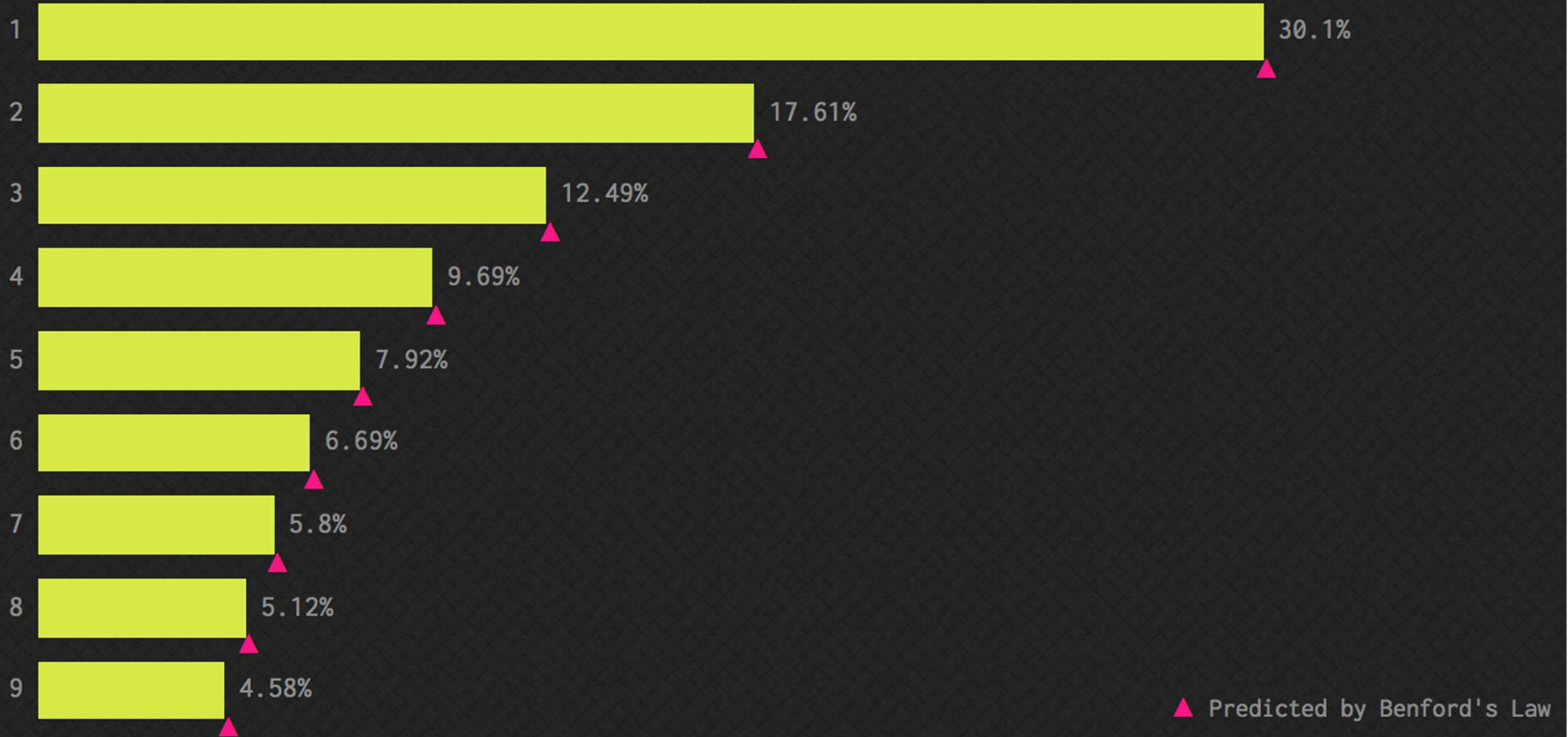
Leading digit frequency



Source: <http://testingbenfordslaw.com/population-of-turkish-boroughs>

First 652066 Fibonacci Numbers

Leading digit frequency



Source: <http://testingbenfordslaw.com/population-of-turkish-boroughs>

Colgate launches AI in app-enabled electric toothbrush



Confusion matrix for 2-class problems

		actual class	
		positive	negative
predicted class	positive	true positives (TP)	false positives (FP)
	negative	false negatives (FN)	true negatives (TN)

$$\text{accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}}$$

Other accuracy metrics

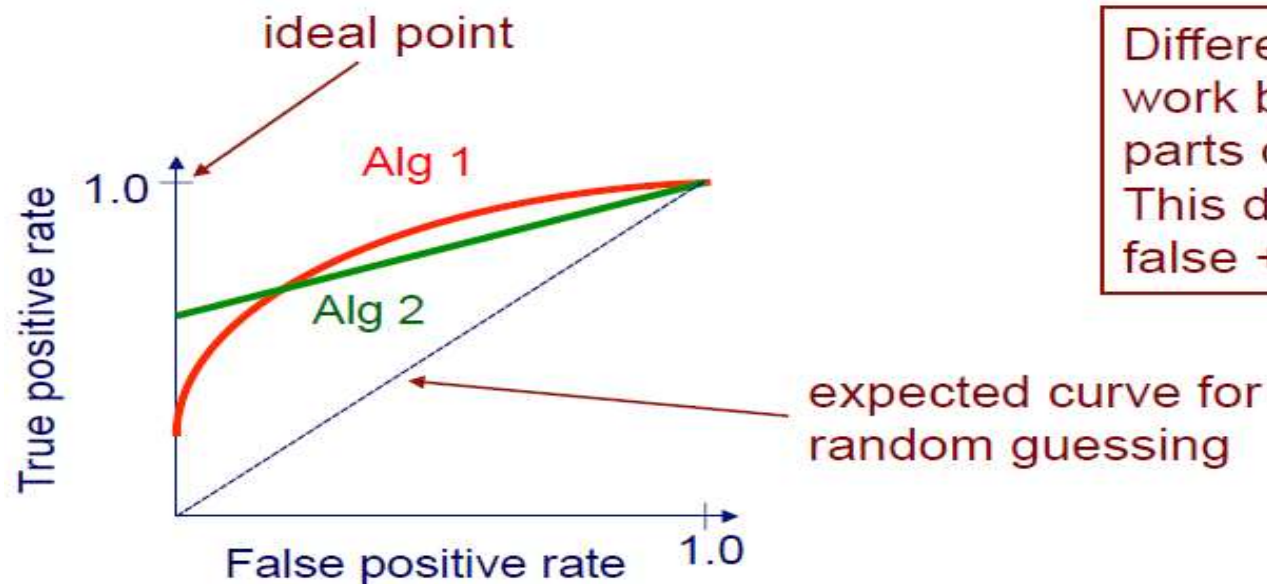
		actual class	
		positive	negative
predicted class	positive	true positives (TP)	false positives (FP)
	negative	false negatives (FN)	true negatives (TN)

$$\text{recall (TP rate)} = \frac{\text{TP}}{\text{actual pos}} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{precision} = \frac{\text{TP}}{\text{predicted pos}} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

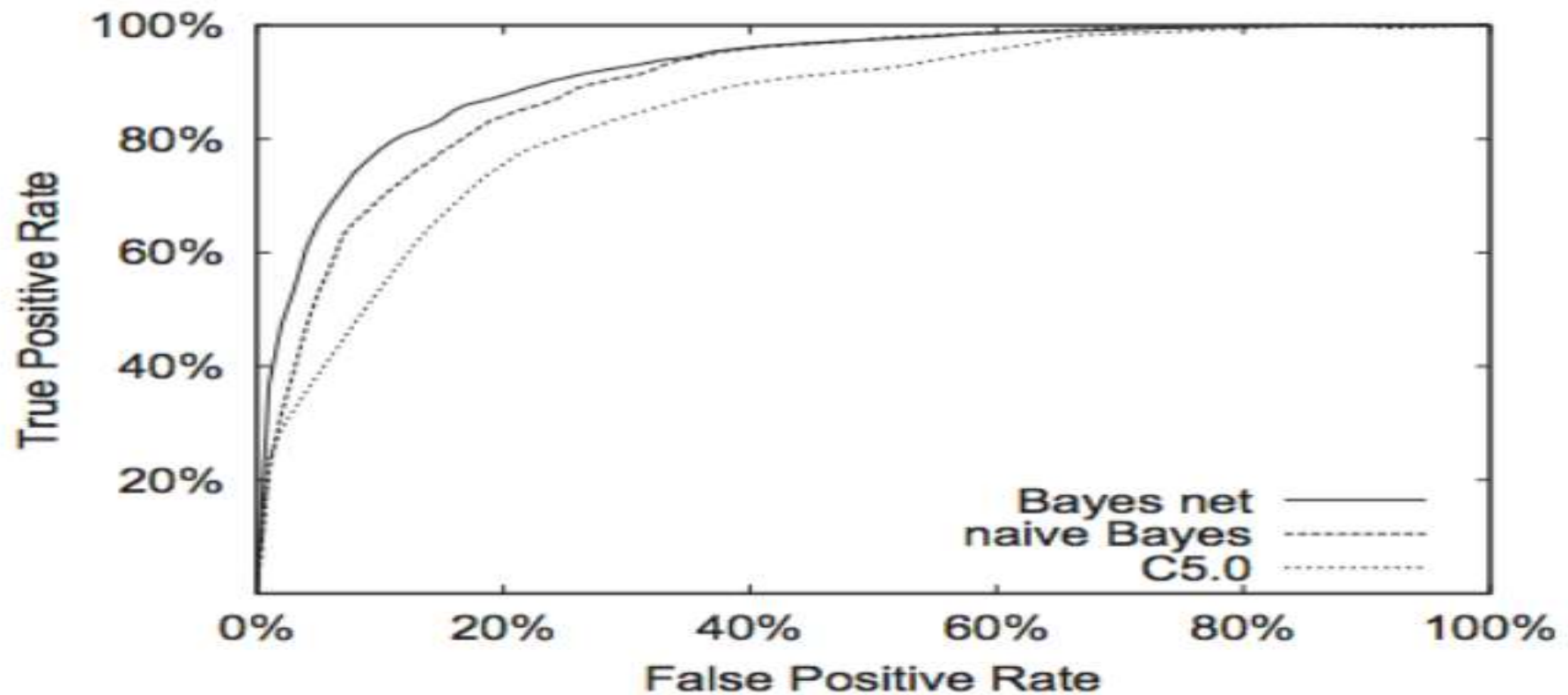
ROC curves

A Receiver Operating Characteristic (ROC) curve plots the TP-rate vs. the FP-rate as a threshold on the confidence of an instance being positive is varied



Different methods can work better in different parts of ROC space. This depends on cost of false + vs. false -

ROC curve example





Research in Cyber Security

Search String and Selection Criteria

Final Query (685 documents)

(TITLE-ABS-KEY ("Information Security" OR "Cyber Security" OR "Cyber Security" OR "CyberCrime" OR "Cyber Defense" OR "CyberDefence" OR "Cyber Crime" OR "Cyberdefence" OR "Cyberdefense" OR "Cyber Espionage" OR "CyberTerrorism" OR "Cyber War" OR "Cyberwar") AND TITLE-ABS-KEY ("Artificial Intelligence" OR "Machine Learning" OR "Computing Intelligence" OR "AI"))

Final Query (Limited)

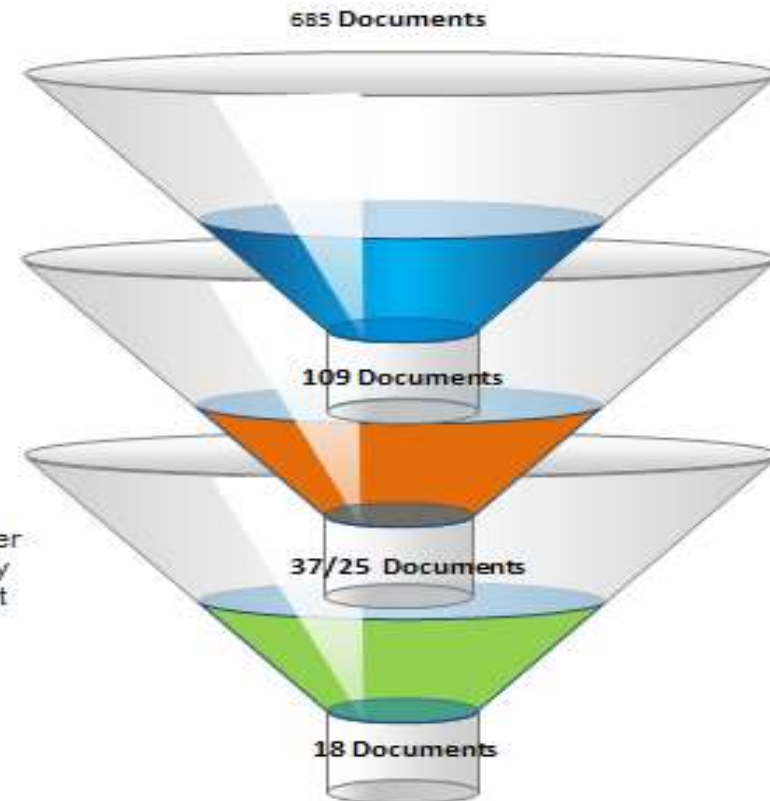
Same as above but limiting to Articles and Reviews – 109 Articles

Stage I Selection - 37/25 documents

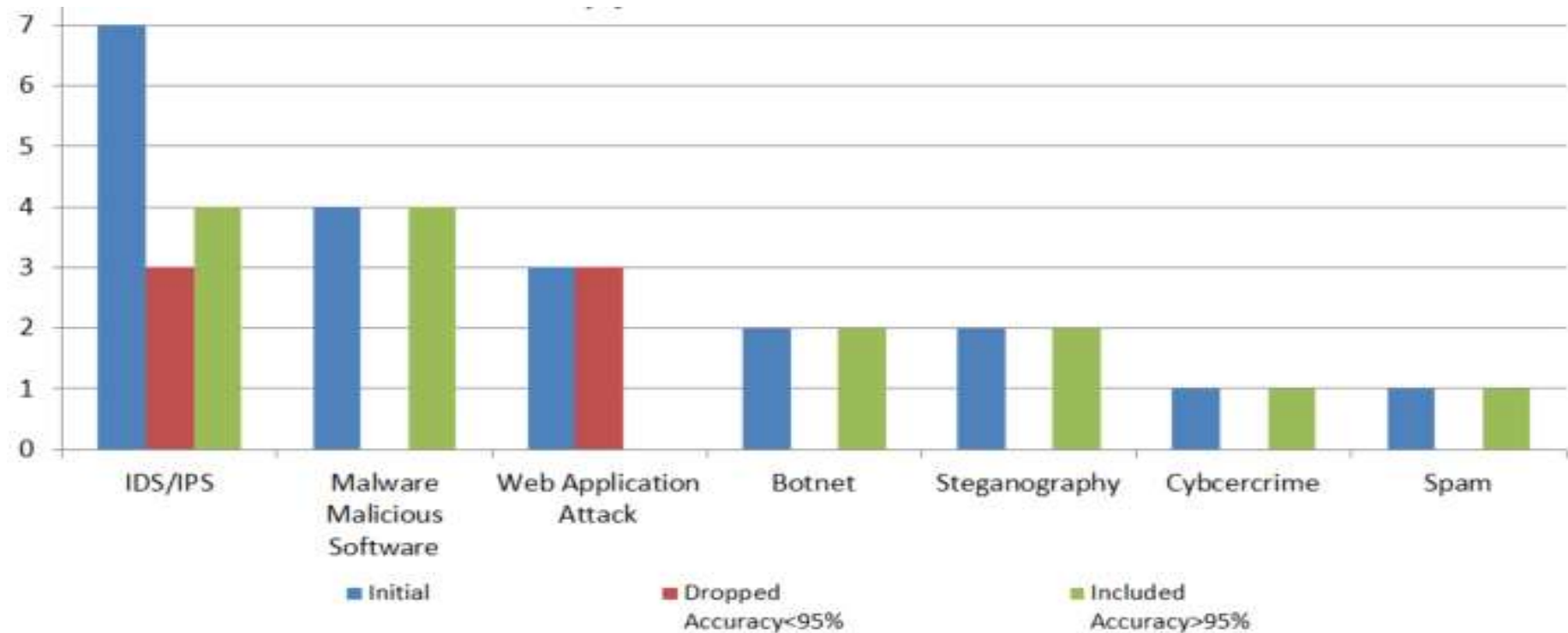
A review of Abstract was carried out and only those studies that refer to AI, ML or CI in the context of Cyber Security were selected. Any duplicates were also excluded. There were 12 articles that could not be downloaded

Final Selection

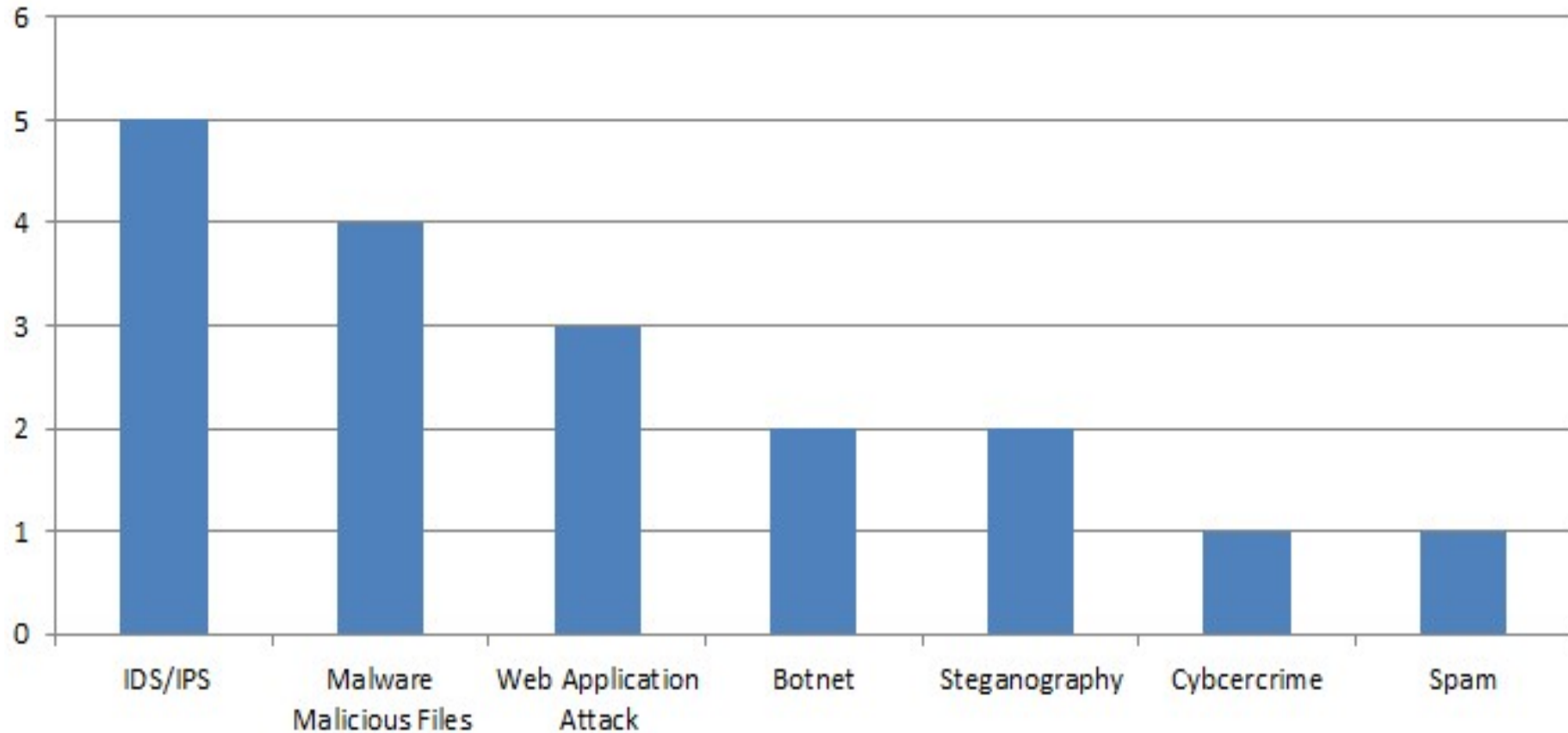
Full detailed review of the articles /papers were conducted and only those were selected in which the model has been tested with either simulated or real life data and their accuracy clearly stated.



Selected and Discarded



Research Papers by Topic



IDS/IPS

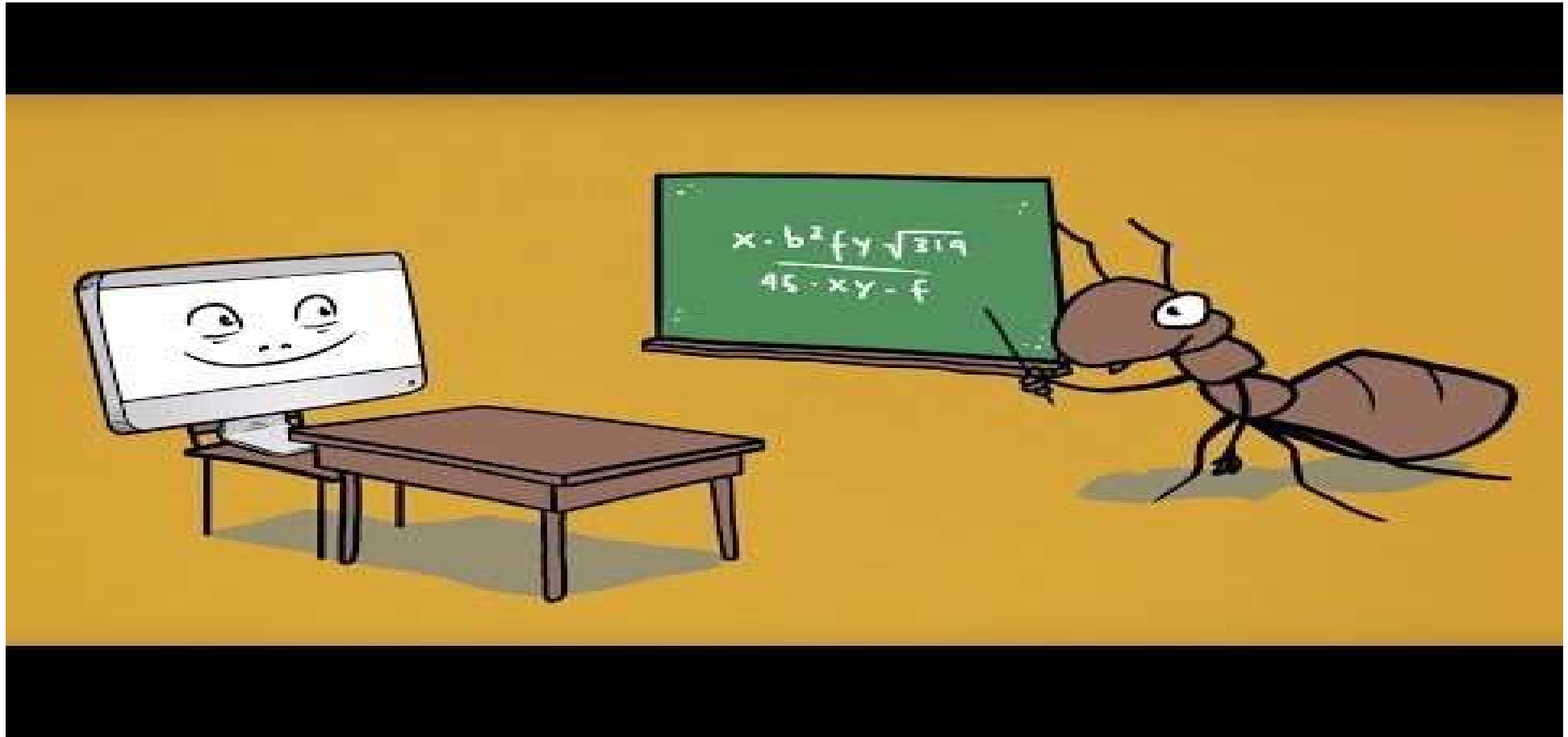
3 Papers were tested with the KDD99 data

MARKELM based model considered the well-published drawbacks and still achieved DR of 99.77% with KDD99 (FOSSACECA et al., 2015)

The model based on SVM and GMM with moving window; tested on real-life data from web servers and honey net is promising, but wider application to Mac and Windows OS is untested (MAMALAKIS et al., 2014).

Another SVM and Gaussian kernel based model Intrusion detection and prevention model have been only tested within Smart Grid context (PATEL et al., 2017).

Ant based Self



IDS/IPS

2017

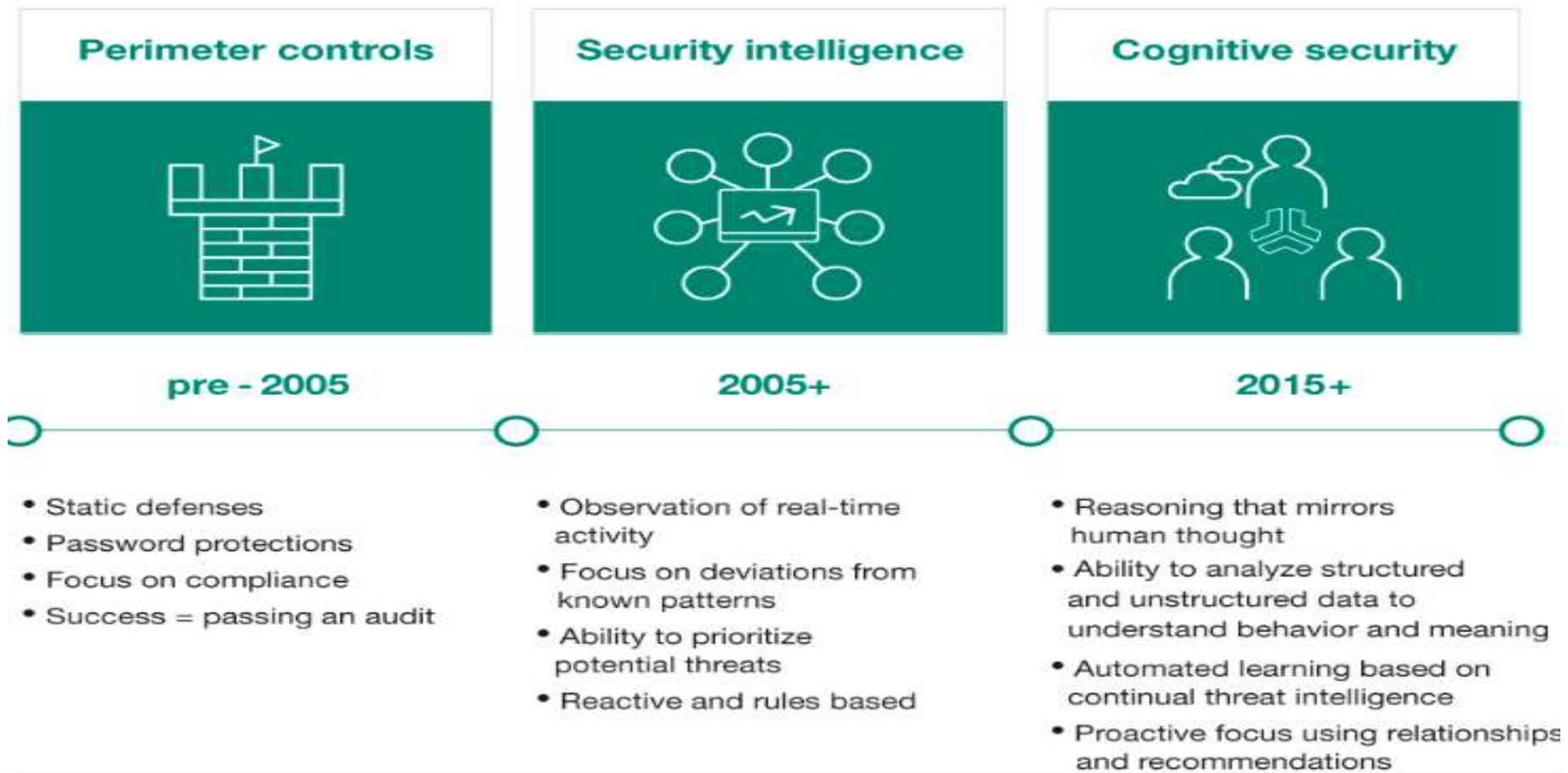
Combination of big data analysis with software security technologies such as feature extraction, machine learning, binary instrumentation and dynamic instruction flow analysis to achieve automated classification of malware algorithms. (Zhao et al.)

Combining intelligent cyber sensor agents which will detect, evaluate and respond to cyber-attacks in a timely manner and allow the groups of agents to make decisions.(Akila et al.)

The two-tier model : dimension reduction and feature selection; good detection rate against rare and complex attack
(Pajouh et al.)



History of security timeline



Thank You!

