

Moore's Law and its Implications for Information Warfare

by Carlo Kopp

CSSE, Monash University,
Melbourne, Australia

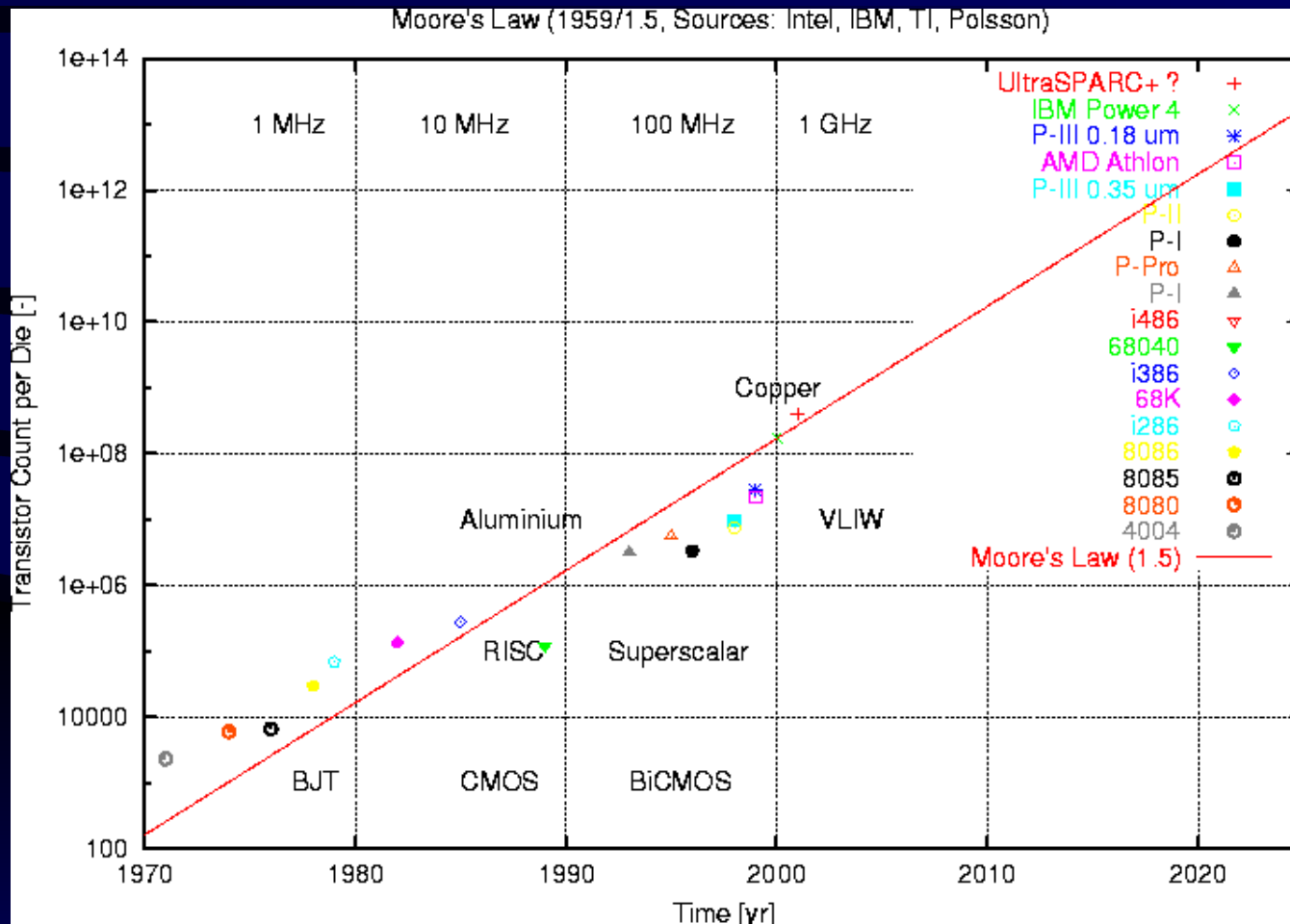
carlo@csse.monash.edu.au



Moore's Law

- Defined by Dr Gordon Moore during the sixties.
- Predicts an exponential increase in component density over time, with a doubling time of 18 months.
- Applicable to microprocessors, DRAMs , DSPs and other microelectronics.
- Monotonic increase in density observed since the 1960s.

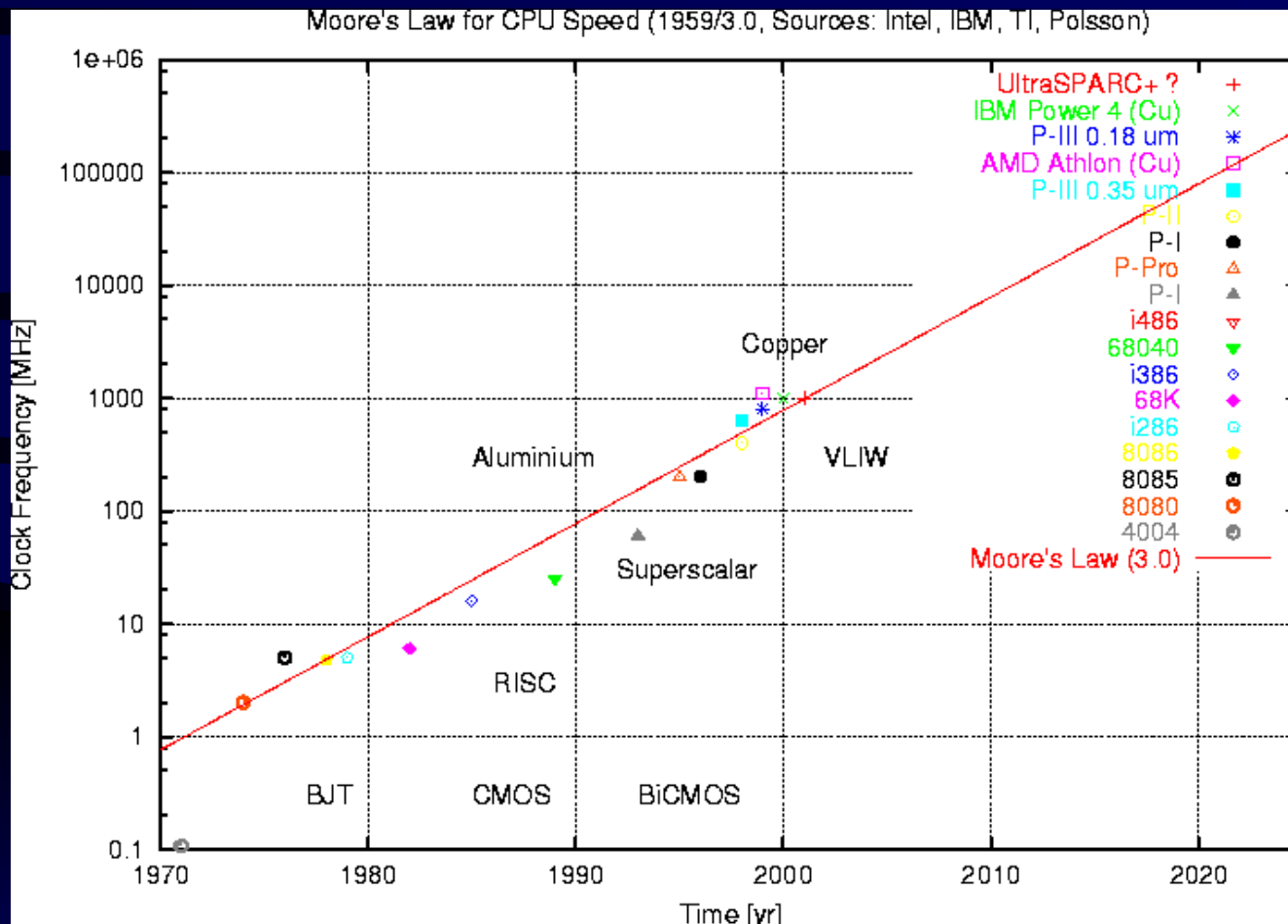
Moore's Law - Density



Moore's Law and Performance

- The performance of computers is determined by architecture and clock speed.
- Clock speed doubles over a 3 year period due to the scaling laws on chip.
- Processors using identical or similar architectures gain performance directly as a function of Moore's Law.
- Improvements in internal architecture can yield better gains of Moore's Law.

Moore's Law - Clock Speed



Limits to Moore's Law ?

- Scaling down the size of transistors will eventually limit density.
- If transistors become too small, quantum physical effects will prevent further gains.
- Scaling limit expected to be encountered ~2010.
- Clock speed limits - 60 GHz CPU ?
- *Is this the end of exponential growth ?*

Breaking the Quantum Barrier

- VLIW (Very Large Instruction Word) architectures.
- Highly parallel machine architectures.
- Neural computing techniques.
- Quantum Dot Transistor (QDT) devices.
- Optical techniques.
- Nanotechnology.
- Quantum computing techniques.

Future Outlook

- No evident barriers to Moore's Law until 2010 or beyond.
- Therefore we can expect exponential growth in performance until at least 2010.
- Future breakthroughs in architecture which allow performance growth with size, rather than clock speed, would extend Moore's Law beyond 2010.

IW 2000-2020

- Best current processors ~200 million transistors, clock speeds up to 1.1 GHz.
- Assume exponential Moore's Law for the foreseeable future.
- Commodity desktop computer in 2010:
CPU clock at several GHz frequency.
Gigabytes to tens of Gigabytes of DRAM.
Hundreds of Gigabytes of disk storage.

Data Mining

- Currently used mostly for marketing and consumer research.
- Potential for cheap analysis of large intelligence databases, including Imint, Elint, Sigint, DNA, fingerprints.
- Potential for real time automated analysis of video streams, eg TV and CCTV.
- Potential problems with proliferation of such technology to non-democratic regimes.

Information and Data Security



- The ability to sift huge volumes of open source information cheaply, means that it will become easy to monitor the activities of organisations and individuals.
- "Information leakages", even small, could compromise privacy and security.
- The only remedy may be "strategicheskaya maskirovka", i.e. tight control of all information leakages.

Cryptography

- Older ciphers such as DES will become insecure; the cost of encryption and brute force cracking will continue to decline.
- Variable length ciphers will be necessary, i.e. periodical increases in key sizes required to stay ahead of decryption hardware.
- Quantum computing techniques may defeat many ciphers which rely on factoring costs.

Propaganda

- High quality digital special effects as used in "Star Wars I", "Titanic", "Starship Troopers" will be computable on a desktop.
- Potential for forged video footage which is difficult to distinguish from real footage.
- Uncritical media acceptance of reports and video footage suggest that such forgeries will become an important propaganda tool for hostile govts and special interest groups.

Military Computing

- Applications which use COTS hardware directly will see ongoing benefits from exponential growth.
- Systems such as AWACS, JSTARS, Rivet Joint, LRMP will see major gains in processing capability as will ruggedised ground based and shipboard equipment.
- *What happens with classical Milspec harsh environments ?*

Embedded Computing

- There is a growing disparity between the operational life cycles of commercial computers (18 months) and military embedded computers (a decade or more).
- This effect will worsen due to the exponential growth behaviour in Moore's Law.
- *The gap will grow exponentially.*

Embedded Computing

- The production and support costs of low volume Milspec architectures (Mil-Std-1750A, AYK/UYK-14) will become prohibitive and unsustainable in the long term.
- Established Milspec architectures are no longer competitive regardless of clock speeds - 16-bit PDP-11 era technology with no growth potential.

Militarising Commodity Chips



- Established method relies on die modifications, selective screening and use of Milspec packages to increase reliability at elevated temperatures.
- The time to qualify the chip may now exceed its commercial life in the market.
- *Requirement: advanced Milspec packaging and cooling capable of supporting commercial dies directly.*

Embedded COTS

- "Bold Stroke" and "Oscar" programs aimed at replacing Milspec architectures with RISC PowerPC chips in VME hardware.
- Card level design is very close to Milspec - reliability requirements impose similar design rules.
- "Militarised" VME is a viable near term technology for retrofit of established in service systems.

Integrated Architectures

- USAF F-22/ATF and JSF model: large centralised multi-processors (CIP) perform all system and sensor computing tasks.
- Sensors are "dumbed down", signal processing in CIP.
- Capability upgrades in software and by replacing CPUs in CIPs.
- JSF objective to use commercial hardware standards.

ML Gains - Attack Radars

- Very high resolution Synthetic Aperture Modes, down to inches.
- 3D Interferometric SAR for terrain imaging, mapping and identification by shape.
- Ground Moving Target Indicator modes including signature analysis.
- Inverse SAR modes - moving target identification by shape.

ML Gains - Counter Air

- Space Time Adaptive Processing (STAP) for pulse Doppler look down clutter rejection.
- Mode interleaving with phased arrays, multi-mode antennas.
- Signature analysis and target identification.
- Increased track counts.
- Track fusion from multiple modes.

Other Sensors/Seekers

- Any sensor which uses digital signal processing and data processing will benefit from Moore's Law - FLIR, IRS&T, Lidar, DIAL Lidar, ESM.
- Currently "infeasible" algorithms become viable with increased computing power.
- Sensor Fusion becomes practical on every platform - commensurate improvements in missile seekers and jammers.

Sensors vs Signatures

- *The signatures of military platforms will become the decisive measure of their long term viability, since Moore's Law will result in sensors, fused sensors and networks of fused sensors capable of sifting targets from background, clutter, camouflage and jamming.*
- *Stealth will become a vital part of system survivability.*

Conclusions

- *The player who can evolve technology and doctrine faster, all other things being equal, will prevail.*
- Technology must be designed for "evolvability", and it should be a part of the initial system specification; doctrine and strategy must be developed around technological evolution, and its consequences in the operational environment.