

Technology Vectors

Insights and Expertise in Emerging
Technology Topics Most
Relevant to Senior Leaders



*An offering by the AFCEA International Technology Committee
with the support of The TechCast Project*



2021

About the Authors

The [AFCEA Technology Committee](#) is a standing committee of [AFCEA International](#). The purpose of the Technology Committee is to enhance AFCEA's outreach to the information technology (IT) communities; cultivate partnerships among government, industry, academic, and scientific leaders; and focus on finding solutions for the IT and related management problems facing government, military, industry, nonprofit sector leaders worldwide.

For more than two decades, [TechCast](#) has been providing guidance to decision-makers using one of the best strategic foresight systems in the world. It has been cited by the U.S. National Academies; won awards from AOL and Emerald; been featured in *The Washington Post*; and consulted by corporations and governments.

Technology Vectors *Concept and Background*

Concept of the Vectors Initiative

Leverage expertise and relationships to provide value to federal IT leaders, conference organizers and member firms by:

- Identifying the most relevant emerging technology topics
- Capturing key concepts for each topic in a concise knowledge base
- Identifying points of contacts (committee or external) for each topic

Mechanisms:

- Maintain a list of technology vectors, related sub-topics and subject matter experts
- Maintain a public version of distribution-ready material for use to present the vectors information

Note: This is a “living” document that will be updated frequently. The main Vectors as well as the material presented within each may be updated at any time.

Emerging Technology Vectors/Leads

Advanced Manufacturing

Cloud Computing

Big Data & Analytics

Advancing Cyber Security

Quantum Computing

Mobility/Wireless

Artificial Intelligence

Blockchain

Dr. Vicki Barbur, KeyLogic Systems

Bryan Ward, Unisys

Shaun Bierweiler, Cloudera

Dr. Gil Duvall, Data Security Strategies

Rene Copeland, D-Wave

Anitha Raj, ARAR Technology

Dr. William Halal, TechCast

Nikhil Shenoy, Colvin Run Networks

Advanced Manufacturing

Includes Additive Manufacturing/3D Printing/Printed Electronics/BioManufacturing

Key Points

Why This Matters New materials and manufacturing methods allow less expensive, better performing items, and also deliver resilience to the supply chain as well as allow customization to order.	Implications and Mission Benefits Missions can be carried out at less cost more effectively with higher performing manufactured items.
Adoption Approach and Challenges Find suppliers who work at the leading edge of manufacturing.	Additional Information and Resources See final section of this report.

Technology Vectors

Advanced Manufacturing

Executive Overview

- Manufacturing has traditionally been constructed by cutting materials and attaching them in various ways. This is starting to change as engineers experiment with new construction methods and materials. A White House report claimed, "Within a generation, you will have a hard time explaining to your children how you lived without a fabber."
- A major breakthrough has developed as 3D printing, and modular units are now able to ease construction, reduce costs, and allow better design of parts, homes, cars, and military equipment. China's Broad Group recently built the world's tallest skyscraper in only 90 days, mostly from factory-assembled parts. 3D printers are even being used to print customized tissues by creating a scaffold for nutrients and oxygen, then covering it with tissue cells.
- The greatest obstacles to the spread of these construction methods are not technological but practical and regulatory. Modular units are limited by the size of parts that can be transported over highways, and basic structures may still need wiring, plumbing, and other systems that buyers must arrange for on their own. The manufacturing industry and labor unions both frequently oppose regulatory changes that would make for better machines but also would eat into established markets.
- Although these methods only account for about 10 percent of manufacturing today, TechCast anticipates that hi-tech modular units made by 3D printing will make up 30 percent of new construction by the mid-2020s.

Additive Manufacturing

Why It Matters:

- Provides a means to transition traditional, labor intensive manufacturing technologies and solutions into the digital age.
- Delivers process capable of making 3D (and 4D) objects from a digital model or creating controlled 3D (or 4D) features into an existing object, typically layer by layer or point by point.

Implications and Mission Benefits:

- Just-In-Time Production.
- Obsolescence Management.
- Potential for Unique and Novel Parts.
- Value-Based Economics.
- Versatile, Adaptable, and Impacts SWaP.
- Functional Designs.

Adoption Approach/Challenges:

- Standards and Testing.
- Certification re: Airworthiness.
- Robustness and Integrity.
- 3D Printers and In-line QC/PC.
- Cyber Threat to Supply Chain.
- Progressed from Polymers, Metals, Hybrid, and now. Concrete

Additional Information and Resources:

- [The Emergence of Digital Manufacturing](#)
- [Cyber risk in advanced manufacturing](#)
- [Cybersecurity for Industry 4.0](#)
- [Locking down the factory Floor –Waurzyniak, P., \(2015\) SME](#)
- [Certification and Qualification in Additive Manufacturing Simplified](#)
- [Additive Manufacturing Review: Early Past to Current Practice](#)
- [A Framework for Designing End Use Products for Direct Manufacturing Using Additive Manufacturing Technologies](#)

Additive Manufacturing System Resilience

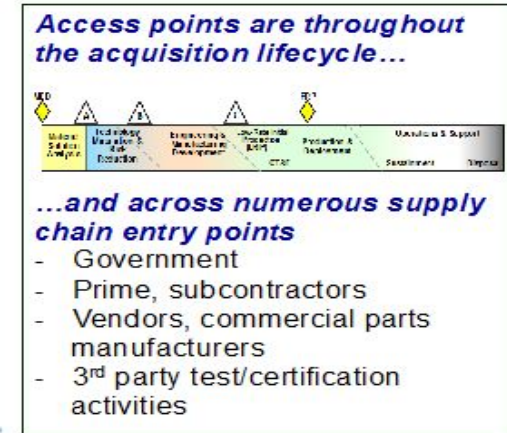
Why It Matters:

Threats and counterintelligence information can be used to determine what means are most effective to protect the system from intrusion.

Prerequisite throughout the life cycle of a process and adapts with time.

Insights:

- Cyber reports
- Threat reports and assessments
- Foreign collection methodologies
- Suspicious contact reports
- Insider threat assessments
- NISPOM related reporting
(National Industrial Security Program Operating Manual)



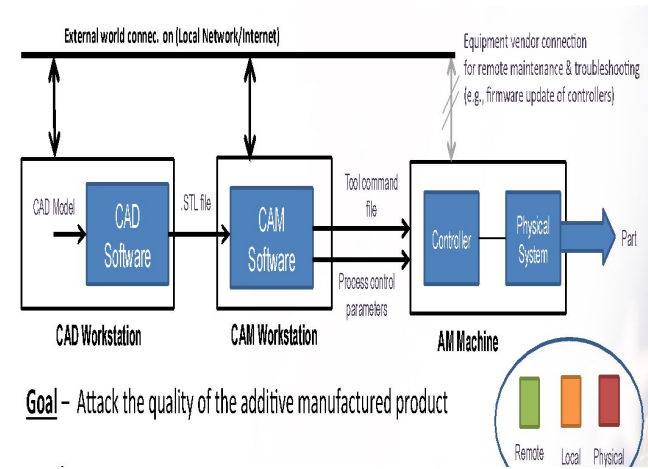
Additive Manufacturing Legacy Processes

Why It Matters:

Smart digital manufacturing needs to be integrated across the enterprise and the operational base, so product, production line, and business are linked to maximize the flow and the reuse of data throughout the entire enterprise.

Insights:

- Air gaps currently provide a means to isolate enterprise from operational floor will be eliminated in time
- Remote and other external connectivity necessary to support utilization and throughput opens up threats to internal process
- Attack vectors are documented in NDIA's CFAM efforts
- Breach closure approaches are being researched for deployment to prevent attacks



Additive Manufacturing

Digital Thread

Why It Matters:

Capabilities that contribute to the warfighters technological advantage may be compromised and copied, reducing the supremacy. Information about mission-critical functions and components can be lost.

Insights:

- Prevent compromise and loss of critical information
 - Anti-tamper and exportability features
- Deploy key protection measures
 - Software/Hardware/Trusted Systems
- Prevent Adversary Collection
 - Classification/Export Controls/Information Security



USS Sturgeon Class



Soviet Victor III

Additive Manufacturing Supply Chain Integrity

Why It Matters:

Vulnerabilities have been exposed for a fully digitized supply chain
Authenticity, performance, dimensions, quality of parts
Concern re: several points for breach and loss of integrity

Insights:

- NIST Cyber Infrastructure Standards in development
- NDIA's Cyber Security for AM Identifying gaps for closure
- Insider threats are often greatest
- Small-to-medium manufacturers are most at risk
- Loss of and/or manipulated design templates
- Contaminated materials impact performance
- Enterprise Suite to Operational Floor is a legacy gap to close
- AM advanced before implications fully understood



Additive Manufacturing Counterfeits/Authenticity

Why It Matters:

With counterfeits and lack of authenticity, both quality and performance can be compromised along with safety. In addition, lack of a trusted supply can lead to other embedded malware and active features detrimental to the mission at hand.

Insights:

- Wrong part, wrong material, wrong dimensions
- Ineffective part, substandard materials, misaligned fit
- Reliability, integrity, and robustness compromised
- Failure to perform, failure for mission
- Challenge to economics – lower cost/lower performance



Additive Manufacturing Measurement Standards

Why It Matters:

Edward Morris, director, America Makes, said: “Additive manufacturing needs to have an appropriate body of standards so that engineers can do their designs using materials with properties that the standards community has embraced.” The reasons are to:

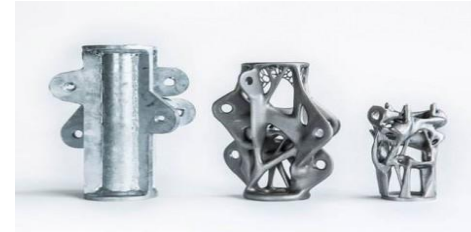
- Allow manufacturers to compare and contrast performance of different processes better
- Improve purchaser/supplier relationship by specifying parts requirements accurately
- Provide support for new adopters to appropriately use and implement AM technologies
- Enable researchers and process developers to provide repeatable results that can be independently verified



Additive Manufacturing Measurement Standards

Insights:

- ASTM's Committee F42 partnered with organizations to promote cohesive, broad adoption of additive manufacturing through standards
- 11 international standards covering several industry areas exist with more in progress, focused on mechanical properties, inter-laboratory collaboration, enhanced 3D printing etc.



Standards Available:

- **F2915** Standard Specification for Additive Manufacturing File Format (AMF)
- **F2924** Standard Specification for Additive Manufacturing Titanium-6 Aluminum-4 Vanadium with Powder Bed Fusion
- **F2971** Standard Practice for Reporting Data for Test Specimens Prepared by Additive Manufacturing
- **F3049** Standard Guide for Characterizing Properties of Metal Powders Used for Additive Manufacturing
- **F3091** Standard Specification for Powder Bed Fusion of Plastic Materials
- **F3122** Standard Guide for Evaluating Mechanical Properties of Metal Materials Made via Additive Manufacturing Processes

NOTE:

[Additive Manufacturing Technology Standards](#)

[The 5 Most Important Standards in Additive Manufacturing](#)

Additive Manufacturing

Airworthiness Demonstrations

Insights:

-
- The top image shows the Mars 2020 rover being lowered by a helicopter. The bottom image is a close-up of the rover's internal electronics, showing a person working on the wiring.
- Below the images is a detailed diagram of the rover's chassis with labels for various components:
- MBDA Electronics
 - SuperCam Calibration Target
 - MBDA AEROVIS
 - SuperCam Body Unit
 - MBDA Electronics & Pressure Sensor
 - MBDA Radiation & Dust Sensor
 - SuperCam Head Unit
 - 3 x Mastcam-2 Camera
 - 2 x MBDA Neural Sensors
 - P&L Scanner
 - SHIELDLOC Sensor
 - SHIELDLOC Calibration Target
 - P&L Electronics
 - SHIELDLOC Calibration Target
 - Maximum-2 Digital Electronics Assembly
 - 2 MBDA Air Temperature Sensors
 - MBDA Thermal Shielded Sensors
 - 3 x MBDA Air Temperature Sensors

Technology Vectors

Additive Manufacturing

Resources/SMEs

Resources:

- [The Emergence of Digital Manufacturing](#)
- [Cyber risk in advanced manufacturing](#)
- [Proceedings of the Cybersecurity for Direct Digital Manufacturing \(DDM\) Symposium](#)
- [Cybersecurity for Industry 4.0](#)
- [Locking down the factory Floor –Waurzyniak, P., \(2015\) SME](#)
- [Certification and Qualification in Additive Manufacturing Simplified](#)
- [Additive Manufacturing Review: Early Past to Current Practice](#)

SMEs:

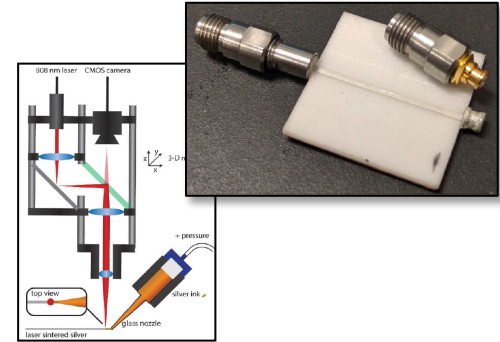
- [Melissa G. Dalton, Acting Assistant Secretary of Defense for Strategy, Plans and Capabilities](#)
- [Nanci Hardwick, CEO MELD Manufacturing](#)
- [John Barnes - The Barnes Global Advisors](#)
- [Peter Highnam - DARPA](#)
- [Dean L. Bartles – Manufacturing & Technology Deployment Group](#)
- [Vicki A.Barbur, Senior Advisor, KeyLogic Systems](#)
- [John Gronto – AM, Northrop Grumman](#)

Technology Vectors

Printed Electronics

What Is It:

- Printed electronics (PE) is one of the fastest growing technologies in the world. It is of significant interest to industries as diverse as consumer goods, healthcare, aerospace, electronics, and media. It allows electronics to be used in places where they have never existed previously, and it is enhancing capabilities in existing electronics and electrics.
- Flexible and printed electronics provide an opportunity for applications that can change the landscape. The interest in hybrid electronics, merging the advantages of silicon-based technologies with printing and other low-cost manufacturing processes, helps to bring these new products closer to the mainstream.
- PE is a set of printing methods used to create electrical devices on various substrates, including flexible substrates. Printing typically uses common printing equipment suitable for defining patterns on material, such as screen printing, flexography, gravure, offset lithography, inkjet, and 3D printing.



Open Questions:

- Improved Precision
- Graded Dielectrics
- Conformal Antenna
- 3D Printed RF Connectors

Relevant Subtopics:

- Functional Inks
- Design Capabilities
- Organic Electronics

Printed Electronics

Why It Matters:

- Successfully used to fabricate passive electrical components.
- Surpasses spin coating as an effective manufacturing method to fabricate organic or polymer light emitting devices (OLED/PLED).
- High-resolution patterning of polymer thin-film transistor (TFT) has been achieved.
- Devices currently restricted to low-end applications, e.g., radio frequency identification tags (RFID), as the active materials have low mobility.
- Switching speeds are low.

Implications and Mission Benefits:

- Non-contact process that selectively deposits a wide range of materials onto a wide range of substrates in a drop-by-drop manner.
- Suitable for a wide range of production scales, from prototyping to large-scale industrial production.
- Ink consumption and material waste are minimal.
- Flexible with regard to positioning within a process chain.
- Produces patterned thin films, a key requirement for organic electronics.
- Leads to integrated systems with low profile.

Adoption Approach/Challenges:

- Functional inks with relevant performance
- Process technology to meet resolution requirements
- Improved precision
- Graded dielectrics
- Conformal antenna
- 3D-printed RF connectors

Additional Information and Resources:

- *Next Flex*, A 2015 cooperative agreement between the U.S. Department of Defense and FlexTech Alliance, is a consortium of companies, academic institutions, and nonprofits and state, local, and federal governments with a shared goal of advancing U.S. manufacturing of FHE.
<https://www.nextflex.us/>
- PARC, A Xerox Company, provides materials characterization and device design to application development and full-system prototyping
<https://www.parc.com/content/attachments/printed-electronics-technologies.pdf>

Printed Electronics

Functional Inks

Why It Matters:

Inks used for printed electronics are either dispersed (pigment-like) or dissolved (dye-like) in one or more solvents. The solvents provide a vehicle by means of which functional materials are carried through the print head and ejected via the nozzle. A functional material fulfills an electronic/electrical functionality, e.g., conductivity, semiconductivity, resistivity, and dielectricity. Many types of inks that fulfill these functionalities are commercially available.

Insights:

- [Sridhar, A. An Inkjet Printing-Based Process Chain for Conductive Structures on Printed Circuit Board Materials. Ph.D. Thesis, University of Twente, the Netherlands, 2010](#)
- [Printed Electronics: A Manufacturing Technology Analysis and Capability Forecast; NanoMarkets report: \[www.nanomarkets.net\]\(http://www.nanomarkets.net\), 2019](#)

Printed Electronics

Design Capabilities

Why It Matters:

Possibilities exist to add functionality with printed electronics on a substrate that already has electronic structures and devices, fabricated using any other technology. Its non-contact, mask-less, and master-less nature, along with the freedom to position the printhead directly on top of any 3D coordinate of the substrate, enables this feature.

Insights:

- Printed electronics have been successfully used to fabricate passive electrical components
- Surpasses spin coating as an effective manufacturing method to fabricate organic or polymer light emitting devices (OLED/PLED)
- High-resolution patterning of an all polymer thin-film transistor (TFT) has already been achieved
- Devices currently restricted to low-end applications, e.g., radio frequency identification tags (RFID), as the active materials they are made of have low mobility
- Switching speeds are low

Printed Electronics

Organic Electronics

Why It Matters:

Organic electronics is a field of materials science concerning the design, synthesis, characterization, and application of organic small molecules or polymers that show desirable electronic properties such as conductivity.

Insights:

- Organic Photovoltaics/Solar Cells
Fabrication Methodologies provide flexibility
- Continuous Production
 - Roll-to-Roll – lowers cost
- Transparency and Minimum Footprint
 - Create multifunctional structure and save space

Technology Vectors

Printed Electronics

Resources/SMEs

Resources:

- *Next Flex* formed in 2015 through a cooperative agreement between the U.S. Department of Defense and FlexTech Alliance. NextFlex is a consortium of companies, academic institutions, nonprofits, and state, local, and federal governments with a shared goal of advancing U.S. manufacturing of FHE.
 - <https://www.nextflex.us/>
- PARC, a Xerox Company, provides materials characterization and device design to application development and full-system prototyping.
 - <https://www.parc.com/content/attachments/printed-electronics-technologies.pdf>
- MITRE engineers have leveraged a variation of the FUSE technology realized by all-metal additive manufacturing (patent pending) to make a wideband, active electronically scanned array (AESA) capability for CubeSat and other small platform applications.

SMEs: ○ [MITRE'S Patented Technology Benefits Government and U.S. Economy.](#)

- [Wajih Elsallal - Principal RF Engineer, The MITRE Corporation](#)
- [Jamie \(Hood\) Hill - Senior Mechanical Engineer, The MITRE Corporation](#)
- [Steve Gonya, Research Scientist and Fellow at NEXTFLEX, Lockheed Martin](#)
- [Denis Cormier, Professor & Head of Multifunctional Printing Center, RIT](#)

Technology Vectors

BioManufacturing

Why It Matters:

- Defined as area of biology using biological systems, living organisms, or derivatives thereof, to develop or modify products and processes for specific use.
- Industrial biotechnology is ready for development and will contribute to impactful applications as described below:
- Biosensors, 3-D Bioprinting, Bioplastics, Bioenergy, Biofuels, Biomaterials as replacements for traditional ones where typical sources are off shore, Gene Editing and Virtual and Augmented Reality (VR and AR)

Implications and Mission Benefits:

- “The Department of Defense is committed to promoting U.S. biotechnology innovation and securing America’s bioindustrial base,” said Michael Kratsios, former Acting Under Secretary of Defense for Research and Engineering. “We are pleased to work with new partners to accelerate the department’s biotechnology modernization and the development of this field, which is so critical to our nation’s future security and prosperity,”
- The latest Manufacturing Innovation Institute (MII), and one of the 17, BioMADE’s internal efforts focus on scale-up and downstream processing of laboratory R&D to commercial production.

Adoption Approach/Challenges:

- Biomanufacturing at scale requires coordination of automation, computational sciences, process engineering, and material sciences.
- Capacity to train a domestic workforce for Biomanufacturing jobs
- Commitment to include ethical, legal, and social implications (ELSI) as the underlying fabric of BioManufacturing

Additional Information and Resources:

- Engineering Research Biology Consortium/ERBC - <https://ebrc.org/bioindustrial-manufacturing-and-design-ecosystem/>
- AFRL awards \$3.5 million to Biotechnology Grand Challenge winners - <https://www.afrl.af.mil/News/Article-Display/Article/2478918/afrl-awards-35-million-to-biotechnology-grand-challenge-winners/>
- WIKI <https://en.wikipedia.org/wiki/Biomanufacturing>

BioManufacturing

Air Force Sponsored MII - BioMADE

Bioindustrial Manufacturing and Design Ecosystem

“The Department of Defense is committed to promoting U.S. biotechnology innovation and securing America’s bioindustrial base. Through today’s award, we are pleased to work with new partners to accelerate the Department’s biotechnology modernization and the development of this field, which is so critical to our nation’s future security and prosperity,” said Michael Kratsios, former Acting Under Secretary of Defense for Research and Engineering.

Enhanced military systems



E.g., Growable Runways



E.g., Domestic supply chain of rare earth elements

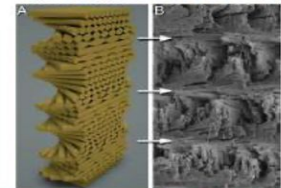
Optimized warfighter health and performance



E.g., Reduced contamination in locally sourced food and/or enhanced nutrition in food sources

Novel Materials

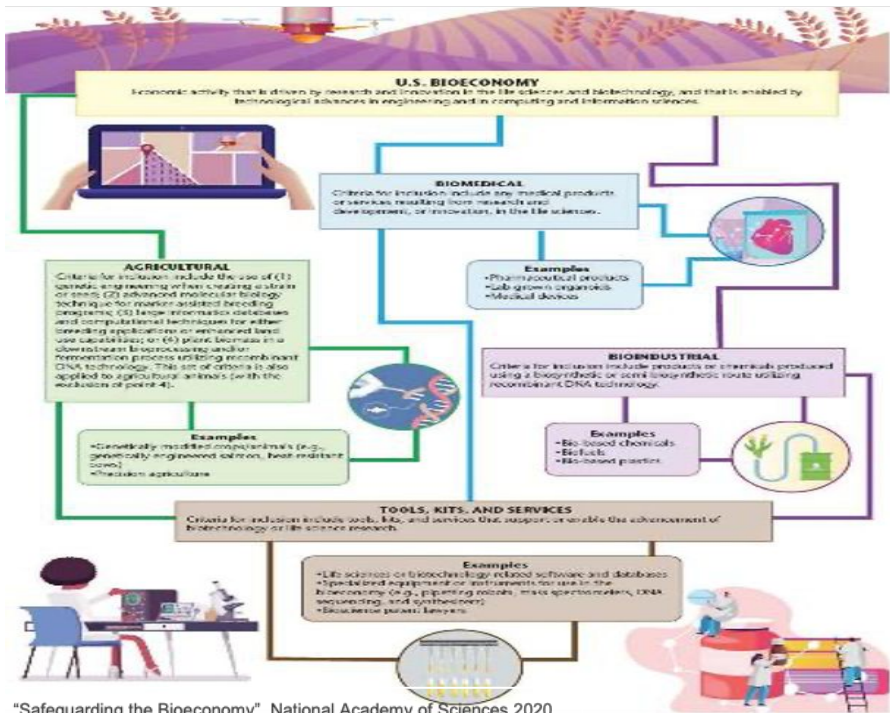
Helicoid structure found in the mantis shrimp.



E.g., Novel materials with unique structural properties

Technology Vectors BioManufacturing

Process Flow & Performance Expectations



"Safeguarding the Bioeconomy", National Academy of Sciences 2020

Opportunities for Superior Performance Materials				
Protection	Transportation	Infrastructure	Sensors	Upcycled High-Value Products
Active Decontamination	Domestic Rubber and Elastomers	Growable Pavements	Optical Sensors	Petroleum Oils and Lubricants
Active Barrier Materials	Lightweight Structural Materials	Spreadable Runways	Optical Coatings	Enhanced Nutrition
Lightweight Armor		Corrosion Repairs		Food preservation
		Self Healing Coatings		Food Flavors and Fragrances
Benefits - DoD				
Increased Protection	Decreased weight	Reduced logistics footprint	Increased lifetime	Reduced logistical burden
Increased Resistance	Increased mobility	Reduced Sustainment Costs	Sustained Communications	Increased endurance
	Increased mean time between failures	Increased operational availability	Increased system operational availability	Increased time on station for mission
Benefits - Industrial				
Production Efficiency Opportunities	Reduced dependence on non-domestic production	Increased Lifetime	Decreased production costs	Increased supply chain stability
Reduced Costs		Increased stress resistance	Fewer warranty claims	Increased shelf life

BioManufacturing

Bioindustrial Manufacturing and Design Ecosystem

Supply Chain Resilience

The Air Force's overarching objective by establishing a BioIndustrial MII as a public-private partnership between government, academia, non-profit organizations, and industry is to address manufacturing challenges associated with biomanufacturing of industrial products.

BioMADE will:

- Address design-for manufacturing, scale-up production (SUP), downstream processing (DSP), and test and evaluation (T&E).
- Build a resilient ecosystem, eliminating dependence on off shore sources for critical to mission materials, as well as allowing development of new novel materials enhanced in performance.

Initiatives already underway in this space are as follows:

- **Debut Biotechnology** - Dr. Davide Simone, AFRL's Leader for Biosynthesis of monomers for aerospace thermosets, stated Debut's effort "provides a path to a scalable, bio-and metal free synthesis of key aerospace polymer precursors, eliminating reliance on precious metal catalysts and corrosive reagents. Expected benefits for the Air Force include a significant savings in composite aerospace structural material costs and elimination of oxidation promoting metal catalysts from structural components, extending service lifetimes."
- **Amyris** targets biosynthesis of high-density endothermic fuels,
- **MIT-Tufts-Synlogic** supports human performance-enhancing probiotics, and
- **Tech Holding, LLC** directs efforts to biosynthesis of high-density endothermic fuels.

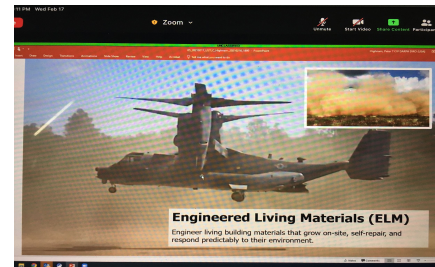
BioManufacturing

Solicitations:

- ARPA-E - Technologies that improve biomass characteristics, such as yield and sustainability, and decrease cost of production and/or water use. Technologies that utilize a biological agent in one or more principal step(s) of feedstock conversion to fuels.
<https://arpa-e-foa.energy.gov/Default.aspx#FoalId2b1605fb-a156-4d55-aa5b-b4c1a213c736>
- Department of Energy Announces \$35M for BioEnergy Research and Development -
<https://www.energy.gov/eere/articles/departments-energy-announces-35-million-bioenergy-research-and-development>
- FY21 Bioenergy Technologies Scale-Up and Conversion Building a clean energy economy and addressing climate crisis with a plan to lead the way, address climate change, and achieve net-zero emissions no later than 2050 to the benefit of all Americans.
<https://eere-exchange.energy.gov/Default.aspx#Foalde2bdb5c9-2b92-4b18-93c3-8f05383b9314>

Key Contacts w/SMEs:

- [Jason Kelly, Ginkgo Bioworks, Boston, MA](#)
- [John Cumbers, SynBioBeta, Pleasant Hill, CA](#)
- [Douglas Friedman, CEO, BioMADE & Engineering Biology Research Consortium - EBRC, CA](#)
- University of Minnesota - MN
- Stanford University, CA
- Northeastern University, MA
- [Zach Serber, CSO, Zymergen, Emeryville, CA](#)
- [Arunas Chesonis, CEO, Sweetwater, Rochester, NY](#)
- [Mark Randall, CEO, T2 Energy, CA](#)
- [David Nunn, VP R&D, Conagen](#)



Engineered Living Materials (ELM) Dr. Blake Bextine

Digital Twin Methodology

Generation or Collection of Digital Data Representing A Physical Object Value Add Applications

- Concept of digital twin has its base in engineering and the creation of engineering drawings/graphics. It is an outcome of continuous improvement in the creation of product design and engineering activities. Product drawings and engineering specifications progressed from handmade drafting to computer aided drafting/computer aided design (CAD) to model-based systems engineering (MBSE).
- Digital twin of a physical object is dependent on the digital thread—the lowest level design and specification for a digital twin—and the "twin" is dependent on the digital thread to maintain accuracy.
- Changes to product design are implemented using engineering change orders (ECO). ECO made to a component item will result in a new version of the item's digital thread, and correspondingly to the digital twin.
- Used for monitoring, diagnostics and prognostics to optimize performance and utilization.
- Sensory data can also be combined with historical data, human expertise and fleet and simulation learning to improve the outcome of prognostics.
- Digital twins of autonomous vehicles and their sensor suite embedded in a traffic and environment simulation can be used to overcome the significant development, testing and validation challenges for the automotive application, in particular when related algorithms are based on artificial intelligence approaches that require extensive training data and validation data sets.
- Further examples of industry applications: Aircraft Engines, Wind Turbines, Large Structures, aka offshore platforms and vessels, HVAC control systems, Locomotives, Buildings and Utilities (electric, gas, water, wastewater, networks)
- [Why Accenture lists 'digital twins' as top-five technology trend in 2021](#)
- [U.S. Air Force Embraces Digital Twin Technology](#)
- [Army Using Digital Twins to Breathe new Life into Aging Helicopter Fleet...](#)

Cloud Computing

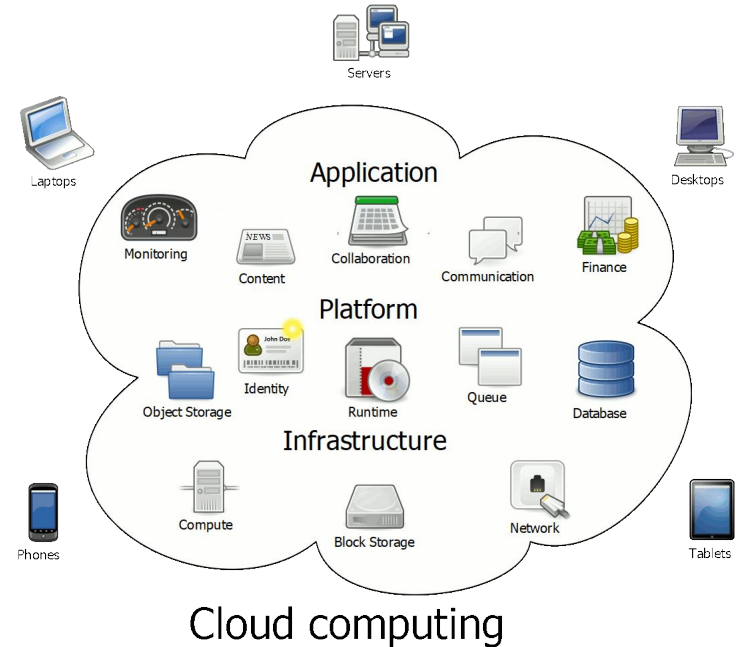
What Is It?*

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources:

- for example networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of:

- five essential characteristics,
- three service models, and
- four deployment models (and two premises models)



* NIST SP 800-145

Cloud Computing

Why It Matters

- Natural evolution of server virtualization and sysadmin automation
- Large commercial adoption created economies of scale and familiarity among leading IT professionals
- Federally mandated

Implications and Mission Benefits

- Cost savings
- Rapid scalability
- Transparent modernization
- Enables rapid innovation
- Familiar development environment
- Relieves DoD from low-value IT efforts, allowing focus on higher-value results

Adoption Approach/Challenges

Best Practices:

- Containers and microservices
- Risk management (impact levels)

Challenges

- Selecting a cloud service provider (vendor)
- Structuring cloud-related procurement contracts
- Migrating legacy apps to cloud
- Small business prime contracts

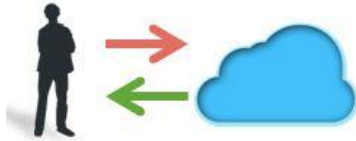
Additional Information and Resources

- NIST SP [800-145](#) & [500-293](#) (Foundational)
- [Federal Data Center Consolidation Initiative \(FDCCI\)](#)
- Foundation of Cloud Security - [FedRAMP](#)
- [DoD Secure Cloud Computing Architecture](#)
- [Cloud Security – DoD Impact Levels](#)
- [Air Force Cloud Migration Strategy](#)
- [Troubled USTC DIUx Cloud Contract to REAN using OTA](#)
- DoD Cloud - [JEDI](#)
- DISA IaaS Cloud – [MilCloud 2.0](#)
- DISA SaaS - [DEOS](#)
- [Cloud Security Alliance](#)

Technology Vectors

Cloud Computing

Technical Principle: 5 Essential Characteristics



On-demand self-service



Broad network access



Resource pooling



Rapid elasticity

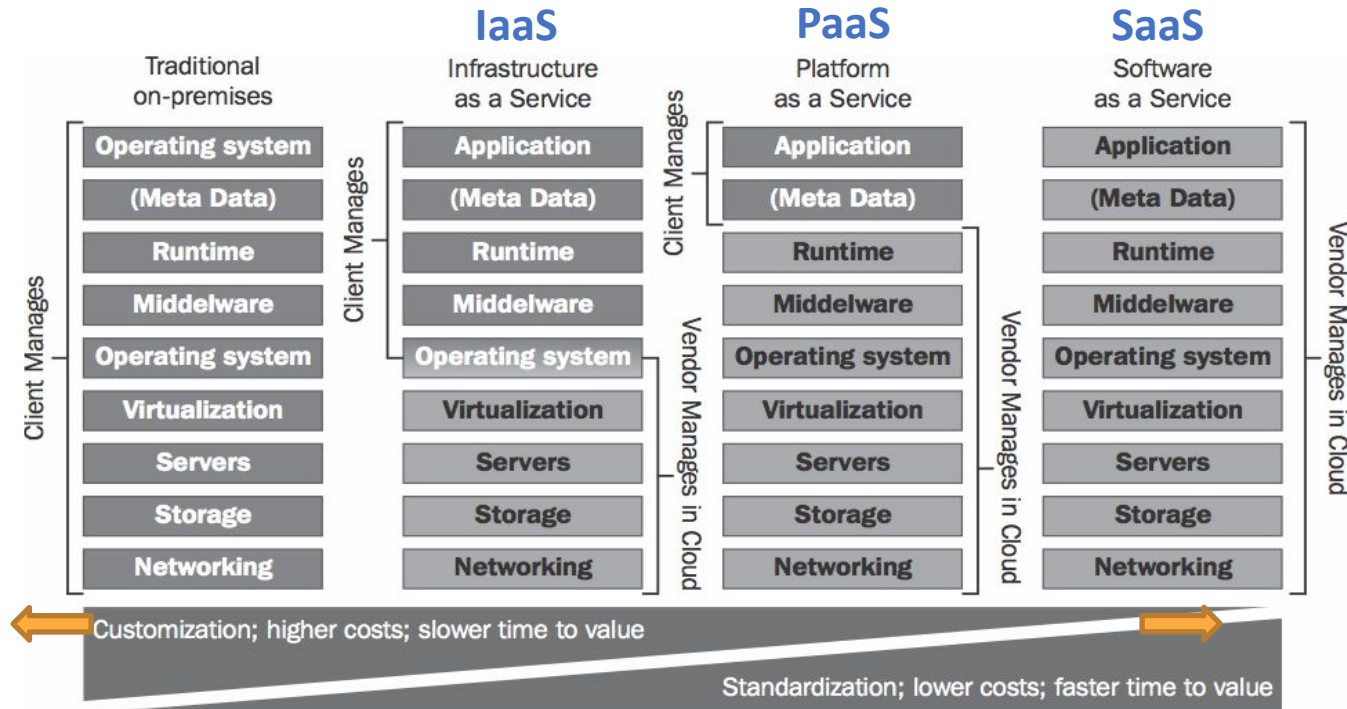


Measured service

Technology Vectors

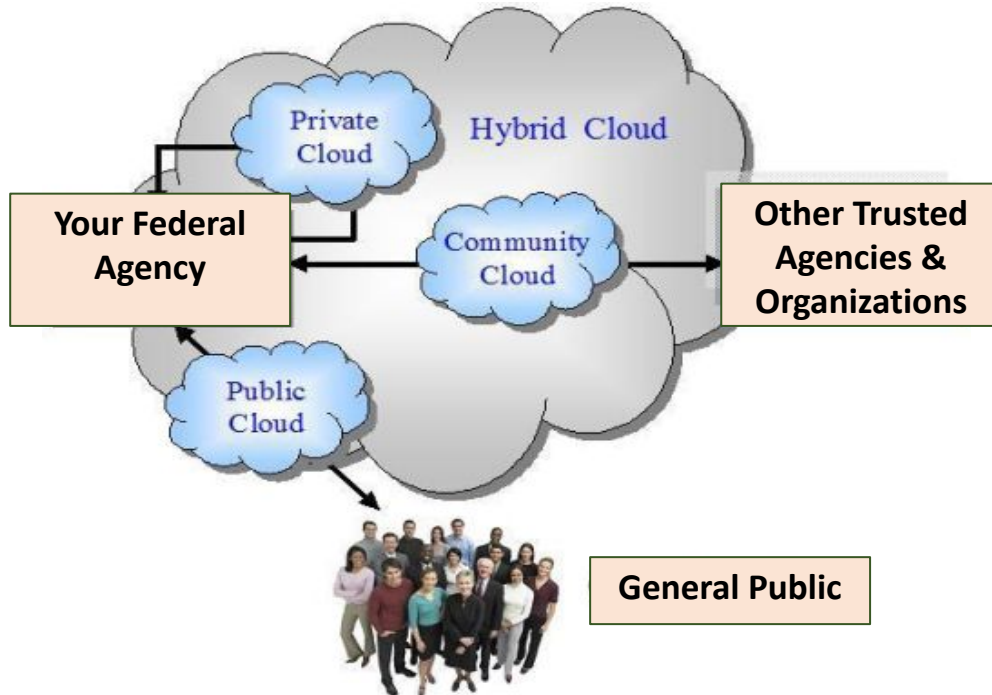
Cloud Computing

Technical Principle: 3 Delivery Models



Cloud Computing

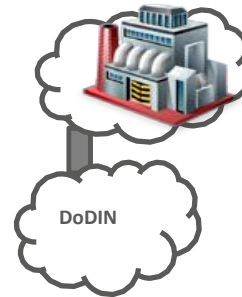
Technical Principle: 4 Deployment Models & 2 Premise Models



Adopted from NIH Cloud presentation



On Premise



Off
Premises

Adopted from DISA Cloud presentation

Cloud Computing

Technical Principle: Cloud Security

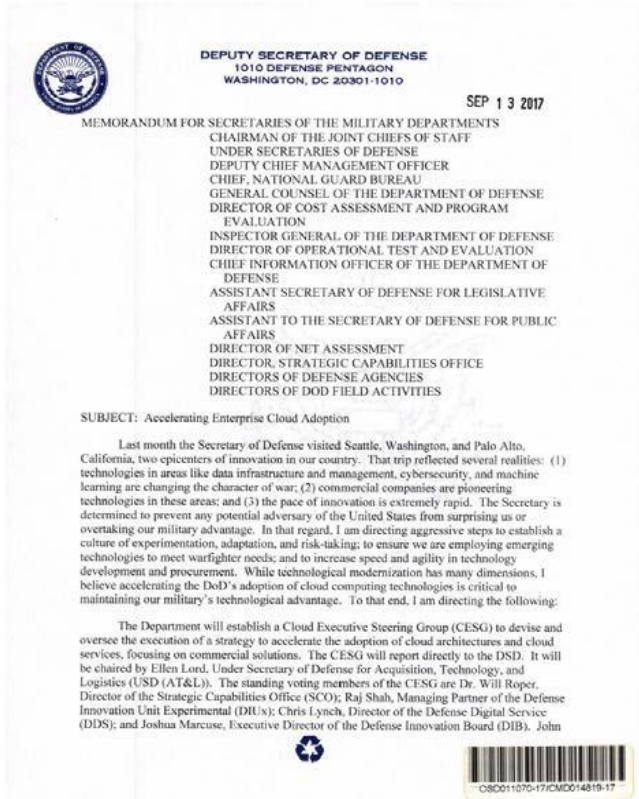
Federal Security Approach



DoD Security Extension

- Impact Level 2 (IL2) – Unclassified Data (public data) – requires shared or dedicated infrastructure
- Impact Level 4 (IL4) – Unclassified Sensitive Data (FOU, CUI, etc) – required shared or dedicated infrastructure with strong evidence of virtual separation controls and monitoring
- Impact Level 5 (IL5) – Unclassified Sensitive Data (NSS, PIAA, HIPAA) – required dedicated infrastructure
- Impact Level 6 (IL6) – Classified Data (Secret, etc) – required dedicated infrastructure approved for classified information

Cloud Computing



Secretary of Defense Guidance

- Sep 13th, 2017 Memo by Deputy Secretary of Defense
- Creates the Cloud Enterprise Steering Group (CESG)
- Two phase approach
 - Phase 1: Resolve acquisition issues around DoD consuming commercial cloud
 - Phase 2: "Rapidly transition" DoD Components and/or agencies to cloud
- Creates regular reporting process of status

Based on presentation by 

Cloud Computing

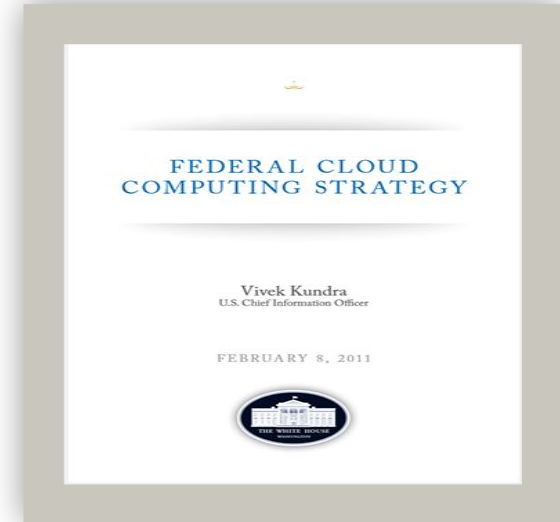
Decision Considerations for Adopting Cloud

Why It Matters:

Analysis of federal experience with cloud adoption provides insights into the factors a federal leader should consider about making a move to cloud

Insights:

- Former federal CIO published a set of decision factors
- Most actual decisions have involved:
 - Trade-off between benefits and cost
 - Assessment of security & other fed-unique constraints
- Actual cloud migration decisions indicate cost savings is often *not* the most significant factor
- Low-hanging fruit has been:
 - IaaS – For agency-unique applications
 - PaaS – For development and testing
 - SaaS – for common back-office applications (e.g. email)



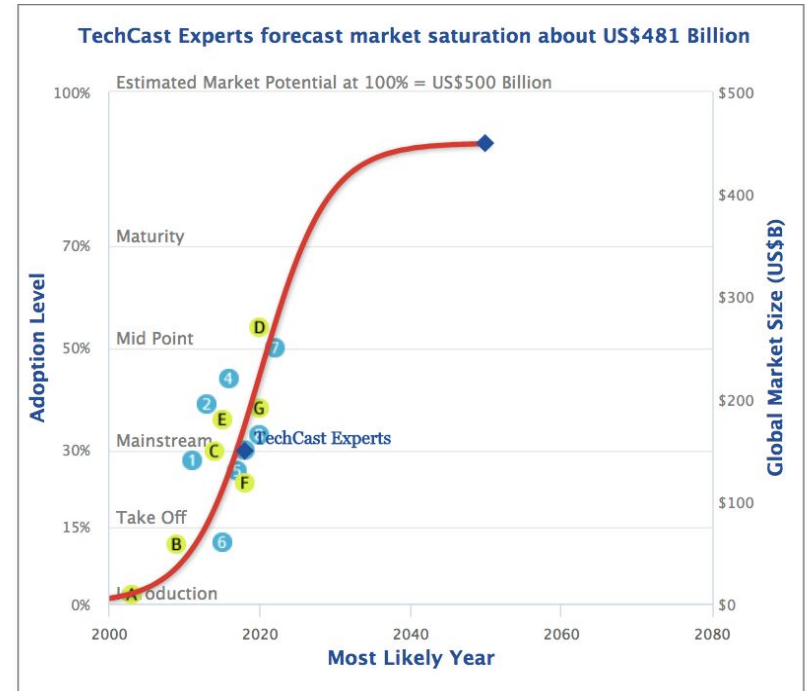
Cloud Computing

TechCast Life Cycle Graph (S-Curve)

The abundance of adoption data and forecasts lends confidence to this forecast.

The TechCast experts estimate of reaching 30 percent adoption by 2018 or so seems reliable, therefore.

There also is close agreement between the experts' estimate of \$481 billion for market saturation and the best fit S-curve estimate of about \$450 billion.



Cloud Computing Resources and References

- Foundation Cloud Documents
 - NIST SP 800-145, *Definition of Cloud Computing*
 - NIST SP 500-293, *USG Cloud Computing Technology Roadmap*
- Federal Cloud Guidance
 - Federal CIO Memo, *Cloud First*
 - NDAA Language
- DoD Cloud Guidance
 - SecDef Memo, *Accelerating Enterprise Cloud Adoption*
 - USAF CIO Memo, *Migrating to Cloud*
- Cloud Cyber Security
 - OMB Memo, *Security Authorization of Information Systems in Cloud Computing Environments*
 - Cloud Security Alliance
- DoD Cloud
 - MILCLOUD 2.0, DISA Partner Symposium Slides
- Decision Factors for Migrating to Cloud
 - Dr. Al Mink, *US Federal Agencies and Cloud: A Common Decision Framework for Determining Which Legacy IT Systems Should Migrate to Cloud*

Big Data and Analytics

Description (Vector/Trend):

Big data is a term applied to datasets whose size or type is beyond the ability of traditional relational databases to capture, manage, and process the data with low-latency.

Characteristics:

- High Volume of data
- High Variety of data (structured and unstructured) from various sources and formats
- High Velocity of data

Drivers:

- Exponential growth of Internet of Things (IoT)
- Social media analysis and insight
- Artificial intelligence (AI)
- Growing need to understand and gain insights/actionable intelligence from data holdings
- Availability of powerful open source products and cloud computing platforms



Big Data and Analytics

Why It Matters:

- Enables the capture, storage, analysis, search, transfer, visualization, query, and governance of ALL of data – both stored (“at rest”) and real-time (“in motion”)
- Allows for the storage of very large amounts of disparate and dissimilar data on commodity hardware
- Saves on operational costs and computational requirements by avoiding unnecessary movement and transformations of the data
- Provides true insight and intelligence from your data

Implications and Mission Benefits:

- Actionable intelligence from data
- Reduced operational costs
- Single view across previously disparate data sources
- Fraud + waste protection
- Predictive analytics and condition-based maintenance
- Cybersecurity
- IT modernization
- Enterprise data warehouse offload

Adoption Approach/Challenges:

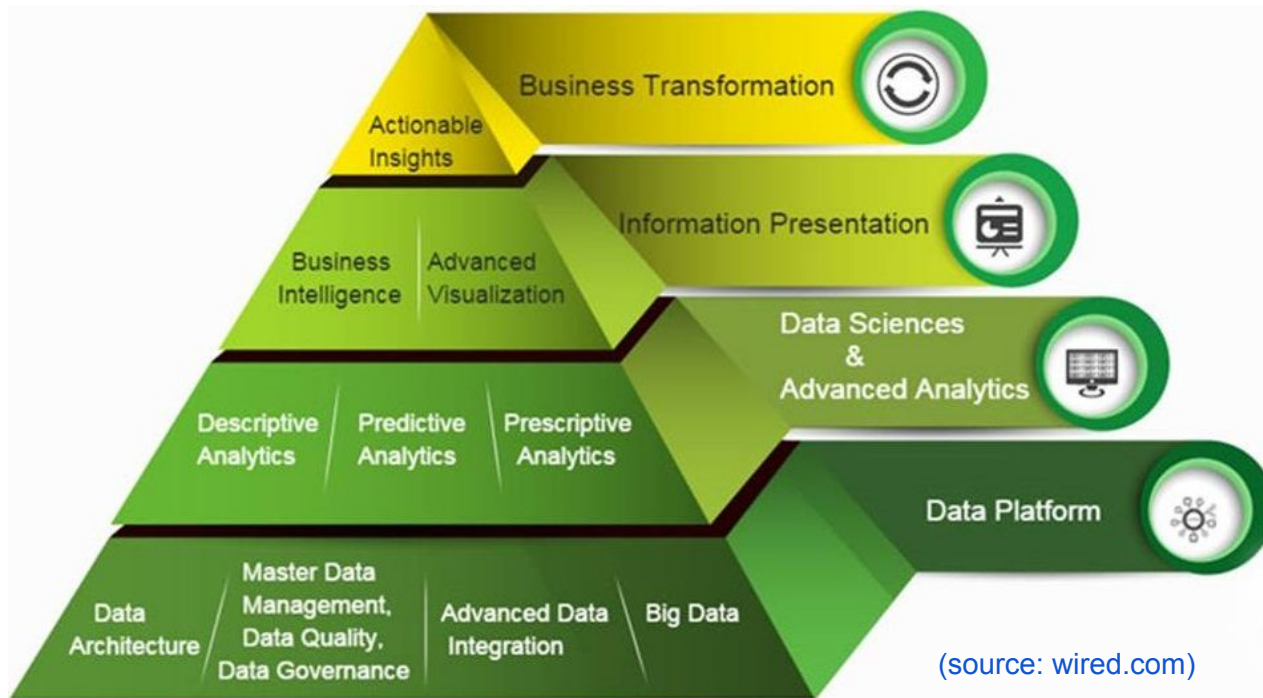
- Open source and open architecture
- Approach leveraging industry tools, capabilities, and interfaces
- Partner with enterprise providers and subject matter experts to overcome the complexity of the technology

Additional Information and Resources:

- https://en.wikipedia.org/wiki/Predictive_analytics
- <https://accumulo.apache.org/>
- <https://www.graphfoundation.org/projects/ongdb/>
- <https://hortonworks.com/solutions/public-sector/>
- <http://www.ibmbigdatahub.com/industry/government>
- <https://www.datamation.com/big-data/big-data-use-cases.html>
- <https://www.cloudera.com/products/cdf.html>
- <https://www.graphgrid.com/government/>
- <https://www.ibm.com/analytics/hadoop/big-data-analytics>

Big Data and Analytics

The 4 Layers of a Big Data Solution Architecture



Big Data & Analytics

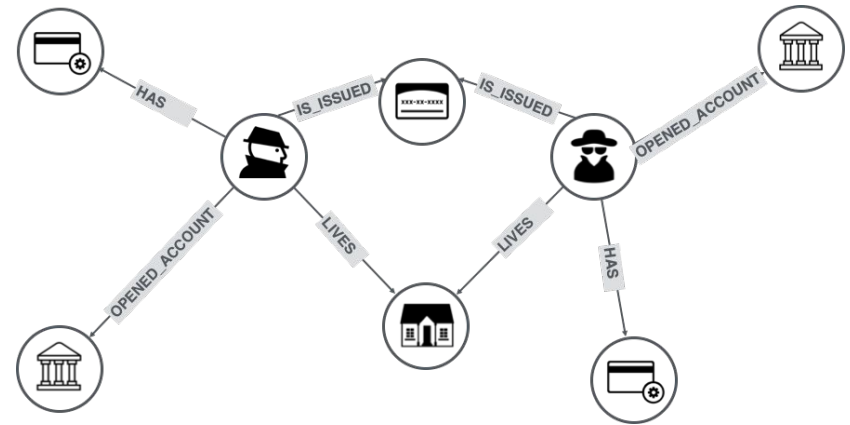
The Shift from Big Data to Smart Data

Why It Matters:

The world is increasingly connected and so is data. “Big Data” projects have led to data lakes that often fail to connect data in a meaningful way. More enterprises are turning to graph theory-backed data approaches to harness connected data.

Insights About Native Graphs:

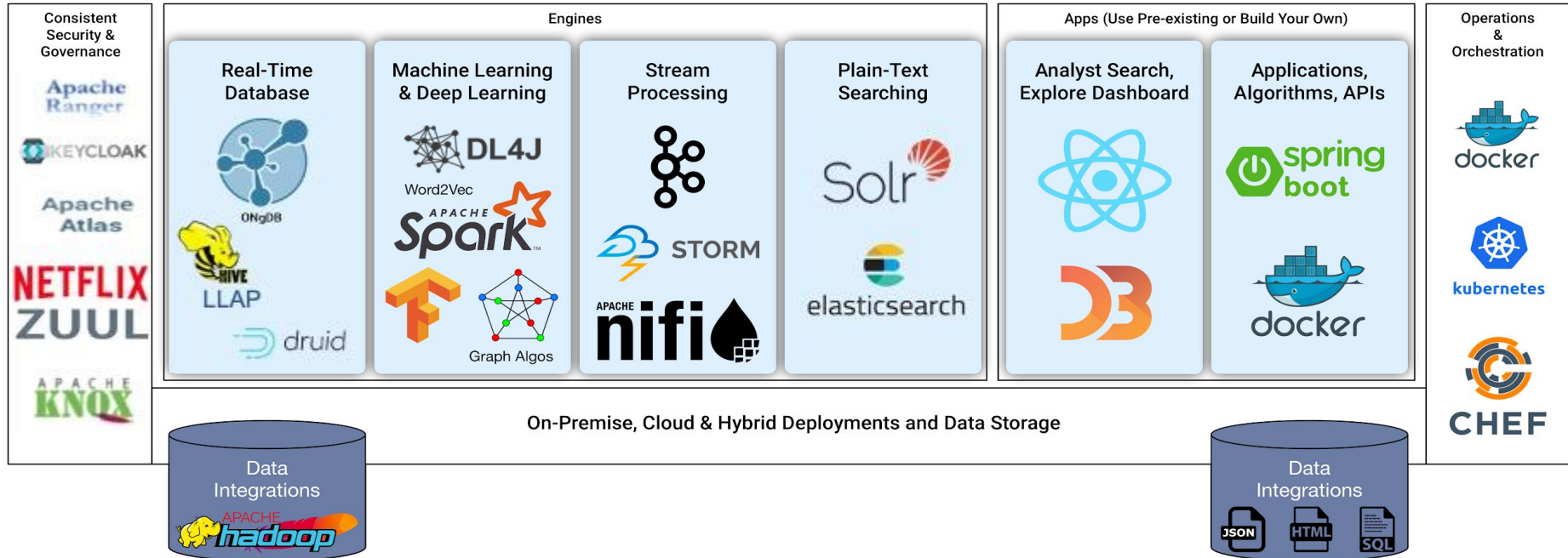
- Easy to model and store relationships about the real world because data is actually a graph
- Allows for fast traversal across billions of nodes
- Performance remains constant with data growth
- Queries are shortened and more readable
- Properties and relationships can be added on the fly
- Knowledge graphs are foundational for AI



Technology Vectors

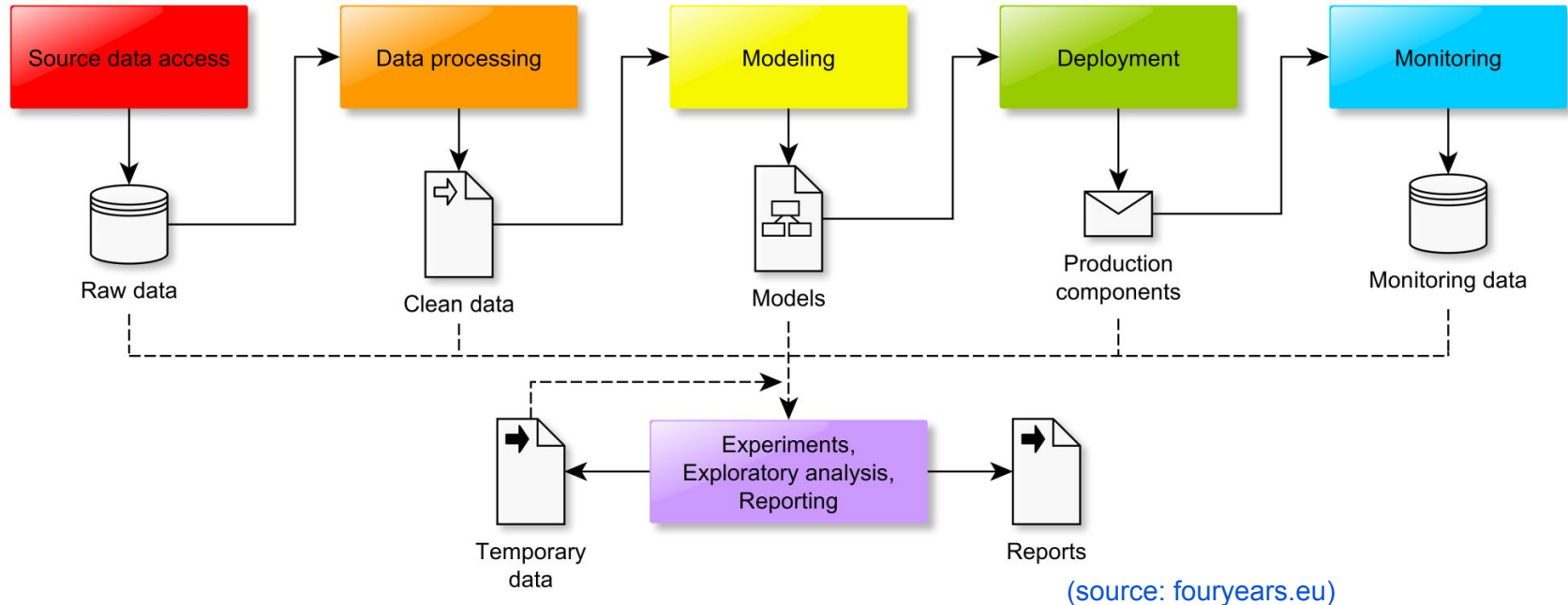
Big Data and Analytics

Notable Components in the Connected Data Ecosystem



Big Data and Analytics

Data Science Workflow Overview



Advancing Cyber Security

What Is It?

Concepts surrounding the effort of advancing cyber security involves examination of evolving threats to the use cyberspace and the technological solutions needed to ensure enterprise networks remain adaptive, resilient, and effective across a diverse range of business and mission areas.

At this point in time, four cyber security technologies stand out for their potential to counter a series of current and near-future high-impact threats that will happen at machine speed.



Technology Vectors

Advancing Cyber Security

Why It Matters:

- The ever increasing sophistication and destructiveness of cyber threats drives the need to understand technology.
- Weak cybersecurity features in commercial products threaten critical infrastructure security.
- Desire to drive down escalating costs of cybersecurity.
- Internet of Things (IoT) speed of deployment is exceeding the ability to defend it against the threat.
- Autonomous cyber defense systems are the future.

Implications and Mission Benefits:

- Cyber defense solutions must blend the strengths of both hardware and virtual machines.
- Improving attribution during cyber incidents (e.g., ransomware) can aid in determining appropriate responses.
- Determining the ROI for Zero Trust network adoption.
- Gaining control of the cyber supply chain.
- Using artificial intelligence (AI), machine learning (ML) & deep learning in contested cyberspace environments.

Adoption Approach/Challenges:

- Cyber threats must be addressed by public and private sector networks simultaneously.
- Cybersecurity must be “baked-into” commercial IT products as a prerequisite for acquisition.
- Cybersecurity solutions must be scalable.
- IoT inherits both IT and operational technology (OT) vulnerabilities and creates security seams (*IT + OT = IoT*).
- Trusting the use of autonomous AI cyber defense systems.

Additional Resources and Information:

- [NIST SP 800-161, Revision 1 \(Draft\): “Supply Chain Risk Management Practices for Systems and Organizations,” April 2021](#)
- [NSA Zero Trust Security Model, 2021](#)
- [NSA “Simon & Speck” encryption for the Internet of Things \(IoT\)](#)
- [ISO/IEC 29192: Lightweight Cryptography Standard](#)
- [AI as-a-service \(AIaaS\) ransomware defense - Cybraics Corp.](#)
- [Practical Machine Learning for Cloud Intrusion Detection - Microsoft](#)
- **See Resources/References/Links page for more listings.**

Advancing Cyber Security: *Executive Summary*

The threat of severe cyberattacks is growing exponentially as the digital world envelopes all facets of modern life. At least 15 countries have been shown to launch cyberattacks, with China, Russia, and North Korea posing the biggest risks, hitting Western governments and companies daily. The problem is expected to grow more menacing as new terrorist adversaries become involved.

The increased complexity of current and emerging cloud and hybrid network environments combined with the rapidly escalating and evolving nature of adversary threats has exposed the lack of effectiveness of traditional network cybersecurity defenses. Traditional perimeter-based network defenses with multiple layers of disjointed security technologies have proven themselves to be unable to meet the cybersecurity needs due to the current threat environment: cyber criminals and nation-state actors, have become more persistent, more stealthy, and demonstrate the ability to penetrate network perimeter defenses regularly.

More powerful cyber security tools are needed, including Zero Trust architectures, lightweight encryption, anti-ransomware, supply chain verification tools and anti-counterfeit technology techniques. Protective defenses are also being installed, and authorities think the possibility of a "Cyber Armageddon" is less likely than a continuing wave of smaller-scale assaults.

TechCast experts estimate advanced cyber security will reach the 30% adoption level about 2023 and produce a market saturation of about US\$ 600 billion in 2035. They also estimate a roughly 30% probability that a major attack could be launched over the next few years with devastating consequences.

Advancing Cyber Security: *Exploit Highlights*

- **Malicious compromise of the SolarWinds Orion platform** began as early as October 2019, with the first set of malicious code introduced in March 2020, through at least June 2020 in a variety of updates released by an unwitting vendor. The code penetrated the computer systems of critical federal agencies, including the Department of Homeland Security, the Treasury Department, the National Institutes of Health, the Department of Justice, as well as Fortune 500 corporations.
- In 2019, **Chinese cyber actors compromised and accessed the ASUS update infrastructure** and infected over a million users to advance targeted malicious updates to specific computers/users of interest.
- Announced publicly in 2017, but occurring in 2015, **Chinese APT-19 cyber actors** targeted system administrator accounts to steal credentials to replace legitimate application updates with a malware version containing an embedded backdoor.
- In 2017, Cisco Talos detected **Chinese APT cyber actors using download servers intended to distribute CCleaner**, a legitimate software package, to deliver malware to over 2.27 million endpoint users for over a month.
- For 17 days in August 2017, **Chinese APT 17 actors embedded ShadowPad malware** in the source code of a Windows server management product used by hundreds of organizations, including banks and energy companies,
- At least as far back as 2014, **Russian state-sponsored advanced persistent threat (APT)** actors trojanized update installers on a minimum of three industrial control systems (ICS) vendor web sites to advance Havex malware into industrial control systems.

Excerpts from "Deliver Uncompromised: Securing Critical Software Supply Chains, Proposal to Establish an End-to-End Framework for Software Supply Chains," by Charles Clancy, Joseph Ferraro, Robert Martin, Adam Pennington, Christopher Sledjeski, and Craig Wiener, The MITRE Corporation, 2021.

Advancing Cyber Security: *Impacts & Mission Implications*

- **Cyberattacks are Common:** A survey of 639 IT professionals in the U.S. found that 35% had been the target of a nation-state cyber attack ([Legal Tech News, Oct 27, 2015](#)).
- **Infrastructure Vulnerable:** Cyber attacks have been shown to bring down critical infrastructure, such as the malware that caused widespread electricity blackouts in Ukraine. A major cyber attack could target a country's vital military defenses, terrorizing the populace and making it much more vulnerable to conventional attack. A successful attack on the U.S. power grid has the potential to cause as much as US\$1 trillion of economic damage and significant loss of life ([Wired, June 12, 2017](#)).
- **Transportation Vulnerable:** Transportation devices from connected vehicles to airplanes have been shown to be vulnerable to hacking, even remotely ([Aviation Today, Nov 8, 2017](#)).
- **Small Attacks Most Likely:** Contrary to the common fear that cyber attacks would be devastating, James Clapper, the U.S. Director of National Intelligence, told the Senate, "Rather than a 'Cyber Armageddon' scenario that debilitates the entire U.S. infrastructure, an ongoing series of low-to-moderate level cyberattacks from a variety of sources will occur over time. ([Ars Technica, Feb 26, 2015](#)).
- **U.S. – China Cyberspace Agreement:** The United States and China agreed on the first arms control accord for cyberspace. The agreement says that each country will not be the first to use cyber weapons to cripple the other's critical infrastructure during peacetime. There is increasing doubt whether the agreement will have any practical effect on China's behavior ([Diplomat, Jan 19, 2017](#)).
- **Funding for U.S. Defenses Rising:** The cybersecurity spending of U.S. government is rising from U.S. \$7.5 billion in 2007 to U.S. \$28 billion in 2016. Budget blueprint proposes an additional billions for the Department of Homeland Security to protect federal networks and critical infrastructure from cyber attacks ([Hill, Mar 16, 2017](#))

Advancing Cyber Security

Cyber Supply Chain Risk Management

Component Verification & Anti-counterfeit Tools

Description (Vector/Trend):

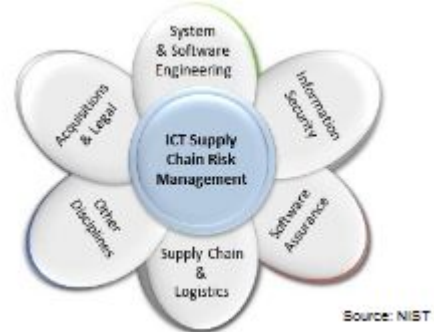
Counterfeit hardware, software and firmware threaten the cyber supply chain.

Implications (Drivers):

- Reduce the spread of malware
- Mitigate cyber espionage susceptibility
- Cost savings by eliminating substandard components
- Increased performance and reduced failure rates

Sub-Elements:

- Component marking and functionality testing
- CPU positive identification
- Invisible OR codes and digital signing with PKI
- NIST "Case Studies in Cyber Supply Chain Risk Management, Summary of Findings and Recommendations," February 4, 2020



Open Questions:

- Do policies require verification of manufacturers throughout the system life cycle?
- Do acquisition programs contain a program protection plan?
- Is a monitoring program in place to determine real-time use of safe components in assembly?

Advancing Cyber Security

Lightweight Encryption Modules

Description (Vector/Trend):

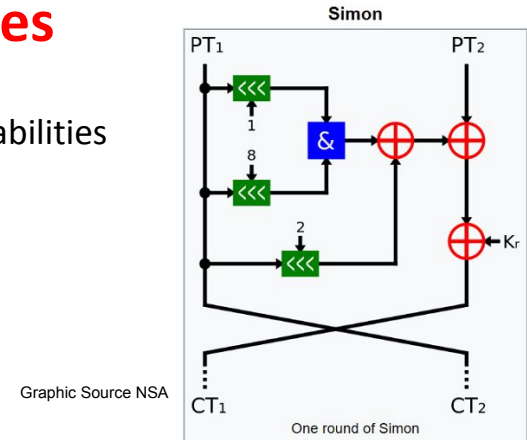
IoT devices lack self-protection features against cyber attack and inherit the vulnerabilities of both ICT and operational technology (OT) systems.

Implications (Drivers):

- IoT devices (sensors, actuators, network switches, CPUs) use is accelerating in critical infrastructure.
- Small size, short battery life, low computational capability prevents use of normal encryption methods for protecting data.

Sub-Elements:

- "Simon & Speck" publicly accessible lightweight encryption algorithm from NSA.
- ISO 29192 lightweight encryption standard.
- RFID, SCADA, WiFi sensors, implantable medical devices, cyber supply chain tracking



Open Questions:

- AES maturity and performance vs. lightweight encryption acceptance?
- Adoption of lightweight encryption by IoT manufactures as an industry standard?
- When and where to use lightweight encryption?
- Hardware vs. software encryption?

Technology Vectors

Advancing Cyber Security

Embracing an NSA Zero Trust Security Model

Description (Vector/Trend):

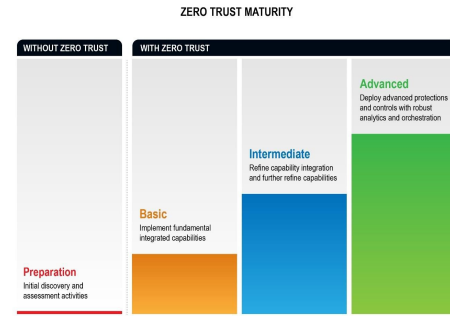
A security model with a set of system design principles and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries

Implications (Drivers):

- Increasingly sophisticated threats
- Cost savings and flexibility in using innovative technologies
- Federal regulations to protect sensitive information
- Multi-cloud computing environment advancement

Sub-Elements:

- Use of Zero Trust architecture & technology to prevent unauthorized users from seeing network endpoint nodes that process, store, and transmit large databases
- Prevent malware insertion on console machines that create backdoors



Open Questions:

- The future of software designed data centers?
- How to use Zero Trust principles in conjunction with traditional cybersecurity architectures?
- How to implement Zero Trust maturity?
- ROI of Zero Trust architecture adoption?

Advancing Cyber Security Machine-to-Machine Security

Description (Vector/Trend):

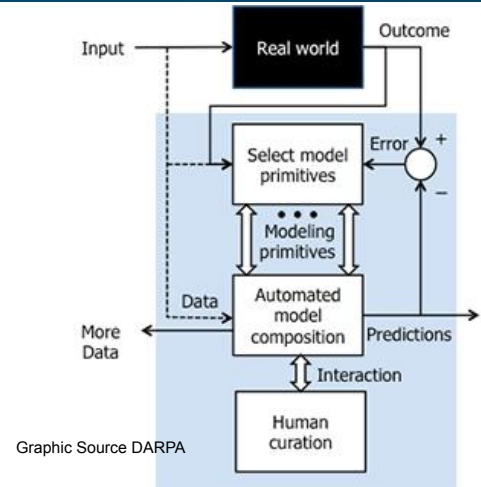
Ransomware use against high-stake enterprise networks is increasing.

Implications (Drivers):

- [Ransomware](#) use in 2021 spreads faster than current cybersecurity technologies can detect or prevent
- Malware signature-based defenses are time-late
- Loss of confidentiality (due to data exfiltration) or availability (because of malicious encryption)

Sub-Elements:

- Artificial intelligence (AI), machine learning (ML), and deep learning nesting
- Machine-to-machine communications
- Heuristic algorithms
- Predictive analytics to identify abnormal network behavior in contested environments
- DevSecOps, disruptive innovation, rapid integration



Open Questions:

- How to balance the risk and cost of false negatives vs. false positives?
- How to keep machine learning knowledge from decaying over time?
- When should AI be trusted over heuristics?
- Is sufficient attack-history data available to support autonomous cyber defense systems?

Technology Vectors

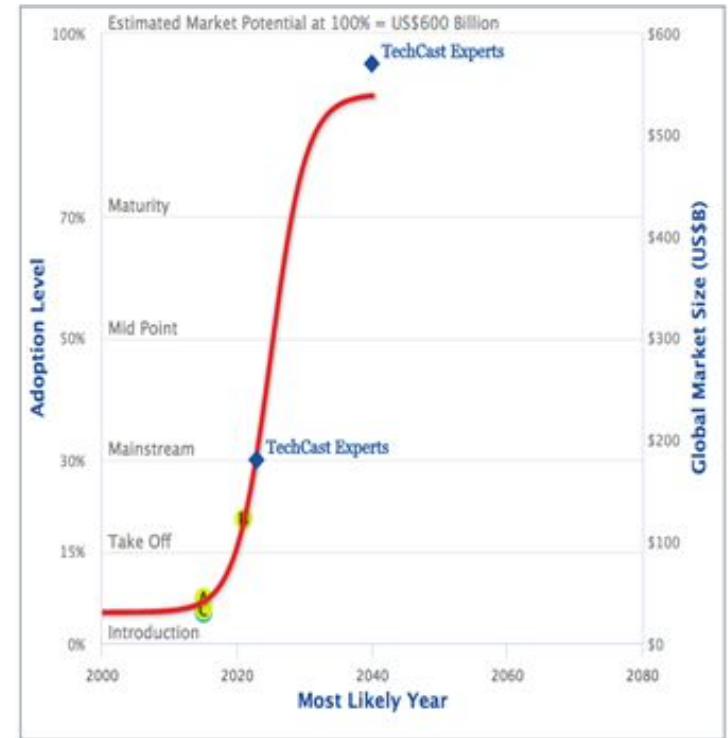
Advancing Cyber Security

Tech Cast Lifecycle/Adoption S-Curve

The company has good agreement between the best-fit S-curve and the TechCast experts, which is assuring.

This S-curve only has two adoption data points as shown, so it relies largely on the TechCast forecasts.

The best estimate is that advanced cybersecurity measures are likely to reach the 30% adoption level about 2023 years and produce a market saturation of about US\$ 600 billion in approximately 2035.



Technology Vectors

Advancing Cyber Security: *Resources & References*

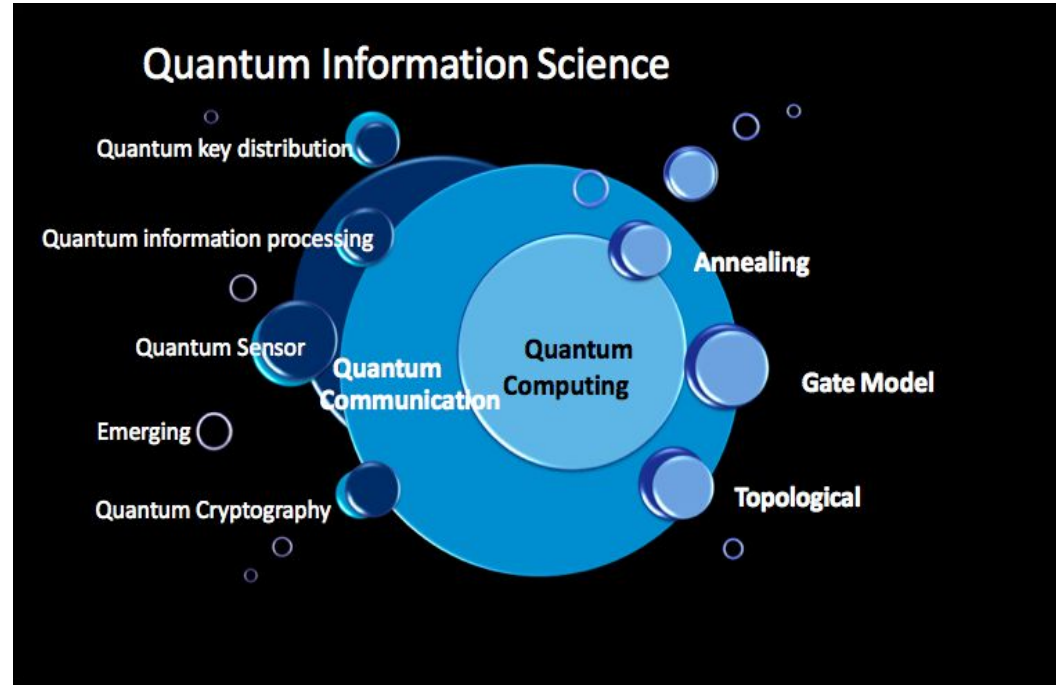
- National Institute of Standards and Technology (NIST) “Case Studies in Cyber Supply Chain Risk Management, Observations from Industry, Summary of Findings and Recommendations,” February 4, 2020 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-1.pdf>
- NIST Special Publication (SP) 800-161, Revision 1 (Draft): “Supply Chain Risk Management Practices for Systems and Organizations,” April 2021 <https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft>
- Embracing a Zero Trust Security Model, National Security Agency (NSA), 2021. Available at https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
- “Department of Defense (2019), DoD Digital Modernization Strategy. Available at: <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>
- National Institute of Standards and Technology (2020), Special Publication 800-207: Zero Trust Architecture. Available at: <https://csrc.nist.gov/publications/detail/sp/800-207/final>
- “Simon and Speck: Block Ciphers for the Internet of Things,” (publicly accessible lightweight encryption algorithm for constrained environments) by Ray Beaulieu, Doug Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks & Louis Wingers, NSA July 2015; <https://eprint.iacr.org/2015/585.pdf>
- ISO/IEC 29192: Lightweight Cryptography Standard; <https://www.iso.org/standard/56425.html>
- “Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process,” October 2019 <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8268.pdf>
- “Practical Machine Learning for Cloud Intrusion Detection - Challenges and the Way Forward,” Microsoft Azure Lessons Learned https://machine-learning-and-security.github.io/papers/mlsec17_paper_3.pdf
- “Ransomware in Health Care Case Study” (AI-based cyber defense) - Cybraics Inc., <https://https://cybraics.com/resources/#Solution-Briefs/>
- “Unwanted Software - P2P Software Attempting to Download Ransomware Case Study” (AI-based cyber defense) - Cybraics Inc., <https://https://cybraics.com/resources/#Solution-Briefs/>
- Institute for Defense Analysis (2015), In-Use and Emerging Disruptive Technology Trends. Available at: <https://apps.dtic.mil/sti/pdfs/AD1013834.pdf>

Technology Vectors

Quantum Computing -

Part of Quantum Information Science (QIS)

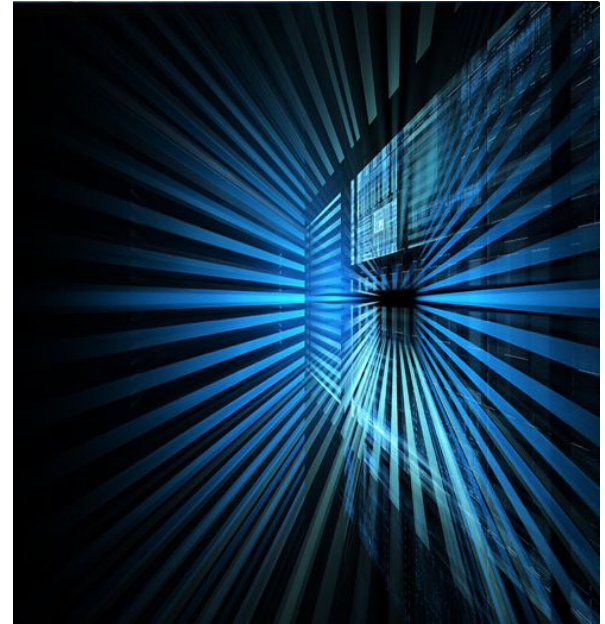
- **QIS Includes**
 - Quantum Cryptography
 - Quantum Communications
 - Quantum Key Distribution
 - *Quantum Computing*
 - Others
- **Types of Quantum Computing**
 - Gate Model
 - Topological
 - Ion Trap
 - Annealing



Quantum Computing

What Is It?

Quantum computing is a type of non-classical computing that is based on the laws of physics. Classical computers use bits that are binary, meaning they are either 0 or 1, true or false, positive or negative. In a quantum computer, the fundamental bit is called a quantum bit or qubit for short. They are macroscopic objects that obey the laws of quantum mechanics. A qubit can represent 0 or 1 or a ***superposition*** of both partly 0 and partly 1 at the same time. A quantum memory register of several qubits can hold all possible configurations of those qubits simultaneously until read (or observed). The act of reading or observing the object will cause the object to be limited to a single possibility or state.



Technology Vectors

Quantum Computing

Different Types of Quantum Computers

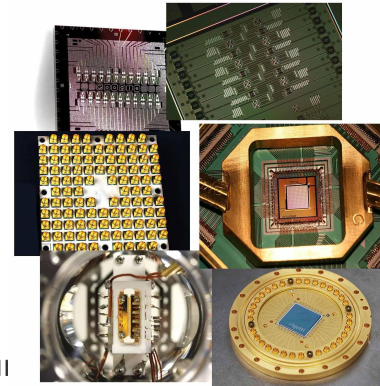
There are several different architectural models of QC being explored today. Each has its strengths and weaknesses. The most common approaches today are quantum annealer and universal quantum computing.

Quantum Annealer:

- Ideal for discrete combinatorial optimization and discrete sampling problems.
- The current D-Wave quantum annealers are not universal quantum computers and cannot therefore run Shor's algorithm to break public key cryptosystems such as RSA and ECC.
- Annealing-based QC models do not use any quantum logic gate operations and are resilient to noise and decoherence, even without active quantum error correction, compared to gate model QCs.

Universal Quantum Computing:

- Pursued by IBM, Google, Intel, Rigetti, and others
- Similar to a Boolean logic circuit Bits are replaced by qubits and the Boolean logic gates by quantum gates
- Relies on building reliable qubits to put together basic quantum circuit operations in any sequence
- Shor's algorithm is the best example for the universal gate use case
- Susceptible to decoherence and must be quantum error corrected to scale up beyond simple problems
- Error correction overhead is significant (requiring hundreds to thousands of physical qubits to achieve one logical qubit) making large-scale gate model quantum computers a challenge.

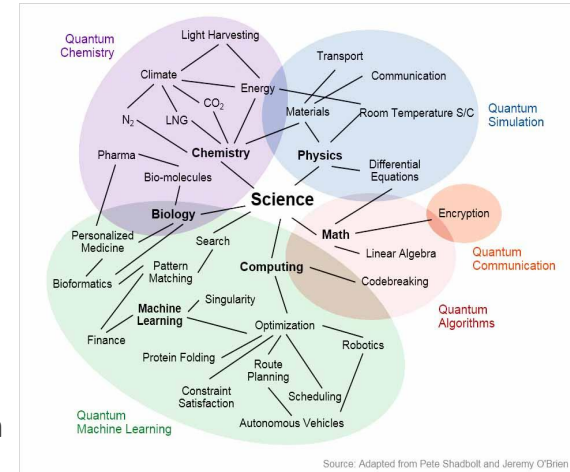


Quantum Computing

What Quantum Computers Are Good For

Quantum Computing is designed to address problems that are too complex and exponential in nature for classic computers to handle. QC has the potential to solve difficult problems, such as:

- **Machine Learning:** Improved ML through faster structured prediction. Examples include Boltzmann machines, quantum Boltzmann machines, semi-supervised learning, unsupervised learning. and deep learning.
- **Artificial Intelligence:** Faster calculations could improve perception, comprehension, self awareness, circuit fault diagnosis/binary classifiers.
- **Optimization:** QC could enable problems such as route optimization for vehicles, airplanes, satellites, and portfolio optimization.
- **Healthcare:** DNA gene sequencing, such as radiotherapy treatment optimization/brain tumor detection, could be performed in seconds instead of hours or weeks.
- **Computer science:** Faster multidimensional search functions. For example, query optimization, mathematics, and simulations.
- **Materials Science:** Research into the composition of structures.



Technology Vectors

Quantum Computing

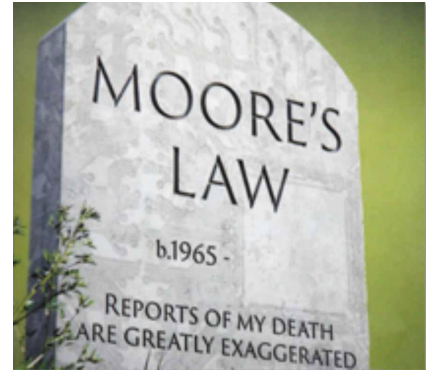
Why It Matters:

The End of Moore's Law:

- For more than 50 years, we have been able to depend on the number of transistors fitted on a chip being able to double every 18-24 months, effectively doubling the computing power.
- Much discussion occurs around the possibility of this increase no longer being able to continue, and as such, alternate architectures are thought to be needed to augment existing architectures.
- Neuromorphic computing and quantum computing are possible augmentation technologies.

International Investment

- **Europe**
 - UK: £400M Virtual Hubs - 17 universities; 130 companies
 - EU: Quantum Manifesto (2016) requesting €1B over 10 years;
 - Germany: Plans to invest €300M over 10 years via QUTEGA National Initiative for Quantum technologies
- **China**
 - Effort led by Chinese Academy of Science and the University of Science & Technology (UTSC)
 - \$10B National Laboratory for Quantum Information Science due to open in 2020
 - Spinoff companies such as QuantumCTek are seeking to commercialize current capabilities.



China building world's biggest quantum research facility

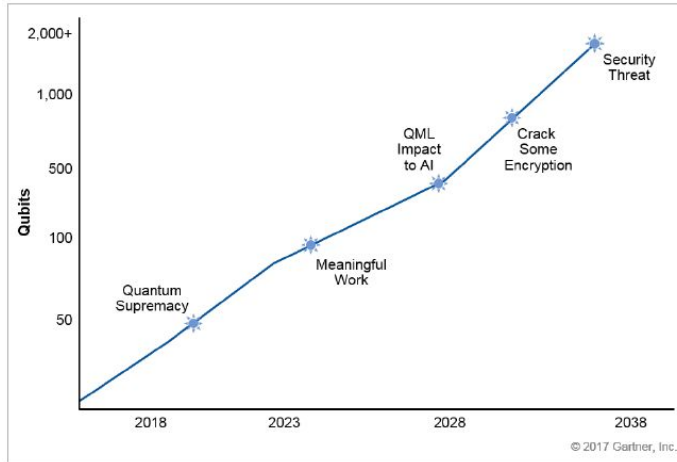
Centre could boost military's code-breaking ability and navigation of stealth submarines



Technology Vectors

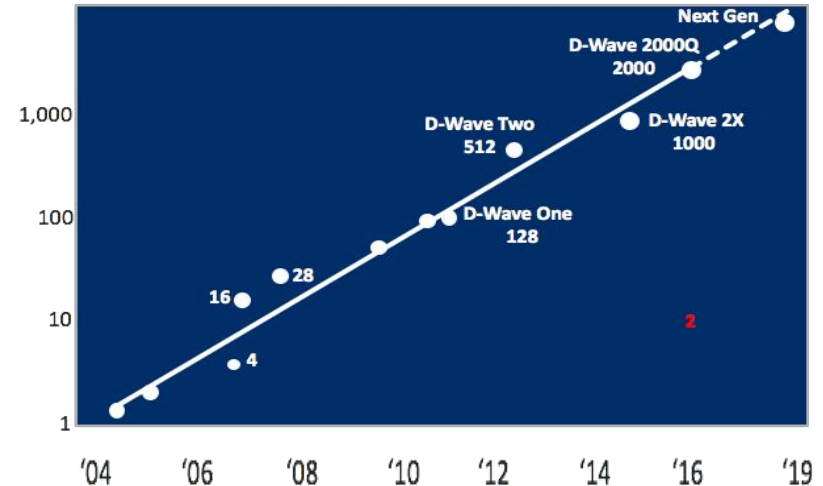
Quantum Computing

Adoption S-Curve



Gate Model

- Requires quantum error-correction schemes
- Requires 100s - 1000s physical qubits to achieve and control one robust logical qubit



Annealing Model

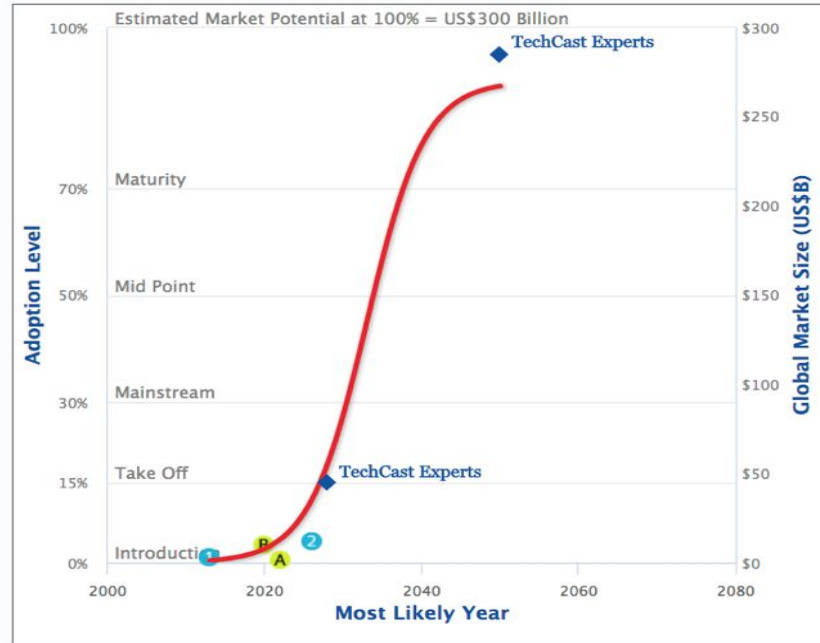
- History of growing qubit count; currently at 2048
- Approximately same growth rate expected to 5k -10k qubits

Quantum Computing

TechCast Adoption S-Curve

Life Cycle Graph (S-Curve)

Adoption data is available but very limited because quantum is just starting to become commercial as of 2018 so applications are rare. Good agreement between the best-fit S-curve and the TechCast experts leads to a best estimate that quantum computing is likely to take off at the 15 percent adoption level about 2025 +/- 3 years. Market saturation is expected to reach between US\$300 (S-curve) and US\$1000 Billion (experts) in 2050 or so.



Quantum Computing

Resources/References/Links

Quantum Computing Vendor Links

D-Wave Systems - <https://www.dwavesys.com/home>

IBM - <https://www.research.ibm.com/ibm-q/>

Google - <https://research.google.com/pubs/QuantumAI.htm>

Intel-https://iq.intel.com/readying-quantum-computing-lifes-biggest-mysteries/?_topic=tech-innovation&wapkw=quantum+chip

Microsoft - <https://www.microsoft.com/en-us/quantum/>

IonQ - <https://ionq.co/>

Further Reading

<https://www.gartner.com/doc/3791363/quantum-computing-research-project-practical>

<https://www.lightourfuture.org/getattachment/7ad9e04f-4d21-4d98-bd28-e1239977e262/NPI-Recommendations-to-HSC-for-National-Quantum-Initiative-062217.pdf>

Quantum Computing Applications

<https://dwavefederal.com/qubits-2016>

<https://dwavefederal.com/qubits-2017>

https://www.youtube.com/watch?v=Bx9GLH_GkIA

<https://www.youtube.com/watch?v=BkowVxTn6EU>

Government Activity

National Quantum Initiative Action Plan

<https://www.energy.gov/>

Mailing Lists

<https://elist.ornl.gov/mailman/listinfo/qci-external>

Mobile/Wireless

Description (Vector/Trend):

Mobile technology trends will allow employees to work outside a fixed location by using wireless untethered technology to optimize human and technical resources anywhere at anytime.

Implications (Drivers):

- Innovations in mobile devices, mobile apps, social networks, cloud computing, security, cost, global coverage and high-speed bandwidth, reciprocity, and governance



Sub-Elements:

- **Policy and Approval:** Evaluation through implementation of new mobile/wireless technologies, acquisition, regulations, and standards
- **Infrastructure:** Enterprise mobile management, devices, app store, Wi-Fi, security, cloud, architecture, carrier network, spectrum
- **Applications:** Development framework, component sharing, vetting/approval, deployment, updating, acquisition
- **Business Case:** Return on investment, mobilized workforce, telework, human machine interface, automation process
- **Future :** Private LTE, Internet of Things, Li-Fi, ubiquitous coverage, intelligent vehicles, 5G, geospatial, virtual reality, situation awareness, personalization, wearables

Open Questions:

- Governance
- Availability real-time of enterprise support systems
- Knowledge sharing and collaboration
- User experience and adoption
- Productivity and Efficiency
- Security and automation

Technology Vectors

Mobile/Wireless

Why It Matters:

Most important disruptor technology is rapidly connecting the world in a web of information on-demand communications that are fast, universal, and secure

- Enhances applications vetting with new security initiatives
- Efficient infrastructure and services with cloud management
- Enables enterprise systems integration with convergence of multiple devices (Internet of Things)
- Efficient customers, suppliers, workforce (military, emergency)
- Better business process, operation, and governance
- Define compliances, regulation & policies – maturity model

Technology Adoption & Integration Challenges:

- Location accuracy from autonomous vehicles/devices
- Big data for vehicles, smartphones, and the cloud
- Network - Private LTE, Li-Fi, Wi-Fi, 4G/LTE, & 5G
- New generation of batteries
- AI technologies – machine/deep learning, speech, virtual agents, decision management, optimized H/W, Biometrics, robotics, text/natural language

Implications and Mission Benefits:

Operations in mobility require constant, effective, reliable, and secure network for a connected ecosystem value

- Boosts productivity with an ‘always-on’ work environment
- On-demand mobility is accelerating shift in society, transport, health, and services
- Enhanced encryption for mobile data privacy
- Cuts long-term costs with positive ROI on business with EMM (Enterprise Mobility Management)
- Flexibility to input/access real-time data at any point and from anywhere via remote devices

Additional Information:

- Mobility enterprise vision and strategy is changing people’s culture, manner of service, and efficient use of technology
- Mobility as a Service is increasing visibility and control that intelligently secures, enables, and connects organizations
- Improved interoperability between public and private sector benefits consumers’ cost, time, and convenience
- Refer to final section for additional resources

Mobile/Wireless Policy and Approval

Why It Matters:

As with any new technology deployed in the DoD, policy and approval significantly impact which mobile technologies are evaluated and the pace in which they are tested and implemented.

Insights:

- Without a legacy approval roadmap to follow, the uncertainty of what approvals are needed and who should provide the approvals impacts agility in “mobilizing” the DoD.
- Security approvals are complex, take too long, and cost too much.
- Mobile technology and security standards compliance with unique requirements are issues and need to be incorporated with standards release of COTS apps and devices.
- Mobile devices continue to evolve offering new capabilities, services, battery technology, and form factors. Interoperability, connectivity, and usability are key factors to information sharing at all classification levels.

NT: NIAP PPs, DISA SRGs/STIGs

MT: Creation of a more flexible framework for mobile policy

LT: Synchronize Mobility as just another IT technology regarding policy



Mobile/Wireless Infrastructure

Why It Matters:

The unique nature of mobile technology and use cases require a re-thinking of traditional IT implementation and management.

Insights:

- Mobile devices operate primarily on commercial wireless infrastructures, but private LTE is emerging.
- Multiple hardware platforms, mobile operating systems, mobile management systems, and carriers must all be synchronized to provide a reasonable user experience.
- Enterprise network and cloud infrastructure and services must mature to integrate mobility capabilities to avoid duplicative, dedicated mobility infrastructure and services as the rapid pace of technology causes mobility infrastructure and services to be specialized and segmented from enterprise network and cloud infrastructure.
- Enterprise Wi-Fi is not widely adopted across DoD components limiting the value of inexpensive non-LTE devices.
- Mobility infrastructure continues to mature to mitigate vulnerabilities and allow deeper monitoring and inspection of work traffic.

Near Term (NT): Fragmented and non-strategic

Mid Term (MT): More sophisticated reliability and performance architectures

Long Term (LT): Fully integrated with IT assets/processes



Mobile/Wireless

Applications and Store (MAS)

Why It Matters:

The justifiable promise of mobility dictates federal agencies move aggressively beyond email and generic web browsing. Federated Mobile Application Store will avoid duplicative infrastructure and overhead.

Insights:

- Each department and agency has different app vetting criteria, processes, and tools, adding community risk.
- As each department and agency acquired its own MDM, each has its own MAS.
- Because of the complexity of mobile application development and deployment, these functions are ripe for standardization, thereby, eliminating a continual “recreation of the wheel” across the DoD.
- The federal CIO’s Mobile Technology Tiger Team (MTTT) is establishing federal app-vetting criteria and processes.
- DoD CIO has established baseline security requirements for the security evaluation of applications for use in the DoD.

NT: Standardize Application vetting process across agencies for quicker deployment

MT: COTS and vendor-driven application development

LT: Government-driven application development



Technology Vectors

Mobile/Wireless

Wireless Connectivity

Why It Matters:

Industry standards exist for seamless interconnecting between cellular and Wi-Fi networks, but they need to be matured for government enterprises.

Insights:

- Today, connectivity challenges still remain. Users must log off one network and log onto another once in range (i.e., hard handoff).
- Wi-Fi Alliance Passpoint standards were published in 2012 and are deployed by all four major wireless carriers, Wi-Fi aggregators, and cable TV networks to enable Wi-Fi Calling (i.e., soft handoff).
- Passpoint relies on WPA2 security standards and adds authentication pass-through to external service providers (e.g., government networks and PKI).
- Automated connectivity and aggregation of and cooperative multipoint among multiple wireless networks offer new performance levels.



NT: Hard handoffs (Break and remake)
MT: Soft handoffs (Make before break),
Wi-Fi Calling
LT: Seamless roaming (Aggregation,
Cooperative Multipoint)

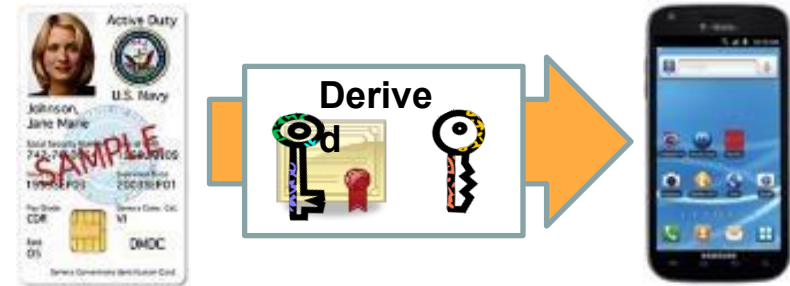
Mobile/Wireless Public Key Infrastructure (PKI) Credentials

Why It Matters:

Smart cards are cumbersome and expensive on mobile devices. PKI ecosystems must transition to hardware-backed software certificates, per NSA guidance.

Insights:

- NIST 800-63-3 (in draft)
- Authentication standards are maturing (e.g., Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST))
- Integration challenges for CAs, OSs, MDMs, 3rd-party apps, and enterprise services
- DoD Purebred pilot for iOS, IOC Oct 2016



NT: Mobile Security Credentials

MT: 3rd-party PKI services

LT: Automated provisioning

Mobile/Wireless Business Case



Why It Matters:

Overall, foundation work needs to be done around the business case for the mobilization of the DoD workforce in order to reduce the burden on mission owners looking to justify mobile expenditures and realize a ‘mobile first’ vision.

Insights:

- Although the mobile cost justification for the military is fundamentally different than the commercial world, there are some lessons learned that can reduce the ROI effort on the DoD.
- A high level but comprehensive mobile business case analysis will identify those cost areas within the DoD's mobile implementation that have to be addressed to allow the benefits of mobility to be justifiable to more DoD applications/use cases.
- The business case work for mobility can become a model for the DoD's analysis for deploying virtually all future non-weapon systems new technologies.

NT: Reliance on non-cost based justification

MT: Balance of mission and cost justification

LT: "Commercial" model for personnel productivity

Technology Vectors

Mobile/Wireless

Future

Why It Matters:

As with almost all technologies before it, mobility and the mobile infrastructure will move and morph from human interactive to being predominantly machine-to-machine and autonomous.

Insights:

- Mobile technology challenges are just beginning and will become more sophisticated as the numbers of manned and unmanned mobile devices dramatically increases.
- Risk assessment and justification will be the biggest challenges in leveraging new mobile and IOT technologies.
- New genres of technology will move far beyond mobilization of current applications and processes to allow for totally new approaches to mission organization and workflow.
- Other key areas: Private LTE, Classified Wireless Devices, Tactical Missions, Mobile Content Management.
- Enterprise Mobility Management (EMM) is mature, but some scaling challenges remain. Business processes that support mobility services add overhead and cause delays.

NT: Extensive Wi-Fi deployments

MT: Convergence of Technology, Internet of Things, Device2Device , Desktop

LT: Sophisticated mobile fabric and workflow models

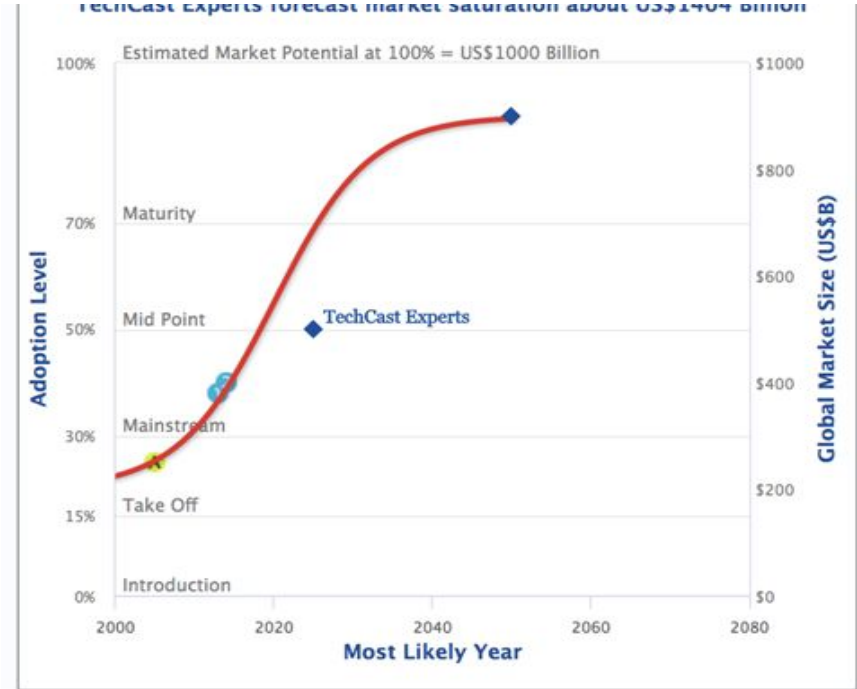


Technology Vectors

Mobile/Wireless TechCast Adoption S-Curve

Life-cycle Graph:

TechCast has some adoption data, so the S-curve is reasonably well-defined in this forecast of 50% adoption by 2019. But there is a sizable gap with the TechCast experts, who are more pessimistic. Both estimates have merit under the logic of collective intelligence, so a best forecast would be about 2023. TechCast also notes a sizable difference between the experts' estimate of \$1,400 billion for market saturation and the best fit S-curve estimate of about \$900 billion.



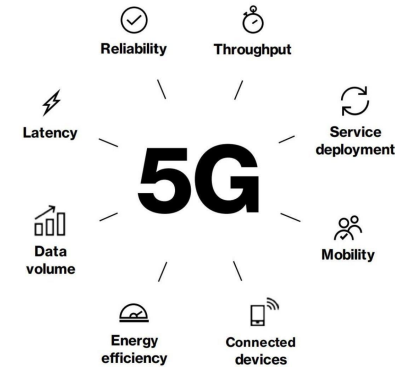
5th Generation Wireless

Description (Vector/Trend):

5th Generation mobile and fixed wireless performance targets high data rate, reduced latency, energy saving, cost reduction, higher system capacity, and massive device connectivity. It's imperative that the U.S. ensures its leadership in the 5G global economic ecosystem and the innovation that will drive new markets.

Implications (Drivers):

Innovations in spectrum access, private 5G, fixed wireless, industrial IoT, smart cities, robotics, edge computing, security, and governance.



Sub-Elements:

Policy & Approval: RDT&E new technologies, architectures, integration configuration, acquisition, regulations & standards, data ownership, and sharing

Security: Software-defined perimeter, zero trust, encryption entropy pools

Infrastructure: Dynamic Spectrum access, small cells, fiber, power, edge computing, security, cloud, fronthaul/backhaul, low Earth orbit/micro smart satellites

Applications: 4D Visualization, additive manufacturing, industrial IoT etc.

Business Case: Lower cost bits/Hz, Agile Edge configuration, network splicing, privatization

Future: Massive IoT, autonomous and semirobotic platforms, high-fidelity real-time geospatial intelligence, virtual/augmented reality

Open Questions:

- End-to-End Software Encryption
- 5G Core and Privatization
- Cross-Domain Interoperability
- User Experience and Adoption
- Economic Displacement
- Total Cost of Ownership
-

0

Technology Vectors

5G Fixed & Mobile

5G Technology Matters:

5G will usher in the 4th Industrial revolution by enabling massive capacity, high bandwidth, low latency, and new compute services to the edge.

- Speed - Peak data rates of 10 gigabits/second
- Throughput - Data volumes of 10 terabits/second/square mile
- Mobility - Mobile devices traveling up to 310 miles/hour
- Connected Devices – Est. 1/2 million devices/square mile
- Service Deployment - Specialized services in reduced delivery time
- Energy Efficiencies - Consume less than 10% energy than 4G
- Latency - < 5 millisecond from device to edge (blink of an eye)
- Reliability - 99.999%

Implications and Mission Benefits:

Leveraging \$60B global OEM R&D roadmap to unleash innovation across all sectors of the economy and will disrupt all elements of the ecosystem

- Design, build, operate, and maintain products and services
- Control, operation, and communications autonomous platforms
- Generation, dissemination, and disposal of micro-segmented digital certificates and encryption keys
- Additive manufacturing and 3D printing
- Intelligent video, low tolerance geofencing, logistics, and C2
- Telemedicine, remote surgery, multiple-domain operations
- Augmented reality/virtual reality training and operations

Technology Adoption, Integration Challenges:

- Spectrum trade-offs (low-band < 1 GHz, mid-band 1-6 GHz , high band > 24GHz)
- Artificial intelligence, cloud, and edge compute resources
- Software-defined perimeter/zero trust networking
- Infrastructure distribution
- Network slicing and privatization
- MIMO/3D beamforming/new active antenna arrays

Additional Information:

- Quantum information services
- Ultra wideband mmWave spectrum enables maximum speed, throughput, and latency based on > 100 MHz + channel width
- Supply chain/trusted manufacturing
- Refer to final section for additional resources

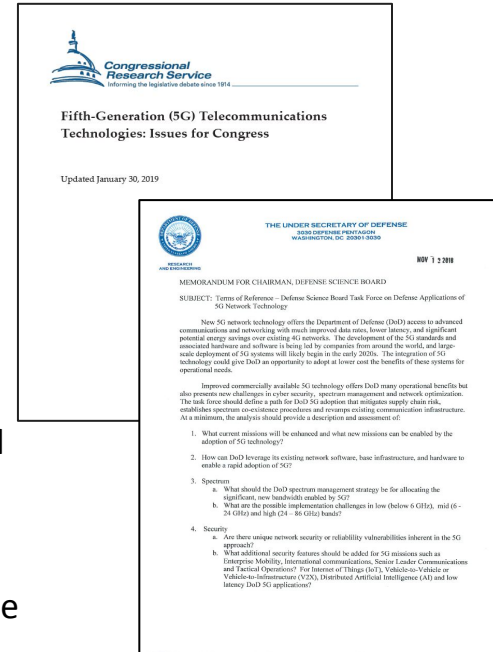
5th Generation Wireless Policy & Approval

Why It Matters:

Deploying 5G will require new and updated DoD policy and approval processes to enable the strategic, economic, and quality of life impacts to the mission and the warfighter.

Insights:

- Streamlining the site acquisition, real property, and spectrum policies and approval processes will be critical to incent commercial investment on federal lands.
- Identification and prioritization of DoD locations and their coverage and capacity requirements.
- Software-based end-to-end encryption methodologies and architectures need to be vetted and accredited.
- Software-based end-to-end encryption architectures approval process will need to be modernized.
- U.S. industrial base and government need to influence the 3GPP 5G standards as they continue to evolve.
- Standards-based interoperability across architectures, platforms, and features.

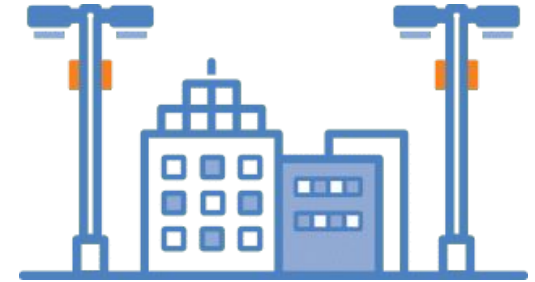


5th Generation Wireless

Small Cell Infrastructure

Why It Matters:

5G mmWave (> 24 GHz) radio frequencies maximize data and provide lowest latency, but these higher frequencies require a denser small cell infrastructure because of shorter travel distance of the RF signal.



Insights:

- Small cell infrastructure will need to be deployed for densification and areas requiring 5G performance advantages.
- Small cells require Joint Spectrum Office approvals, power, fiber, and real property upgrades.
- Private 5G networks will leveraging localized enhanced pack cores, dedicated spectrum, and specialized encryption architectures for classified mission areas.
- Localized cloud and edge compute infrastructure can be leveraged to provide additional security, control, isolation, and reduced latency.
- 3D beamforming antenna arrays will provide geographic control, LPI/LPD, and reduce SWaP requirements.
- Wireless backhaul can be an alternative to fiber for faster, less expensive, and less disruptive deployments, if engineering requirements are achieved.

5th Generation Wireless

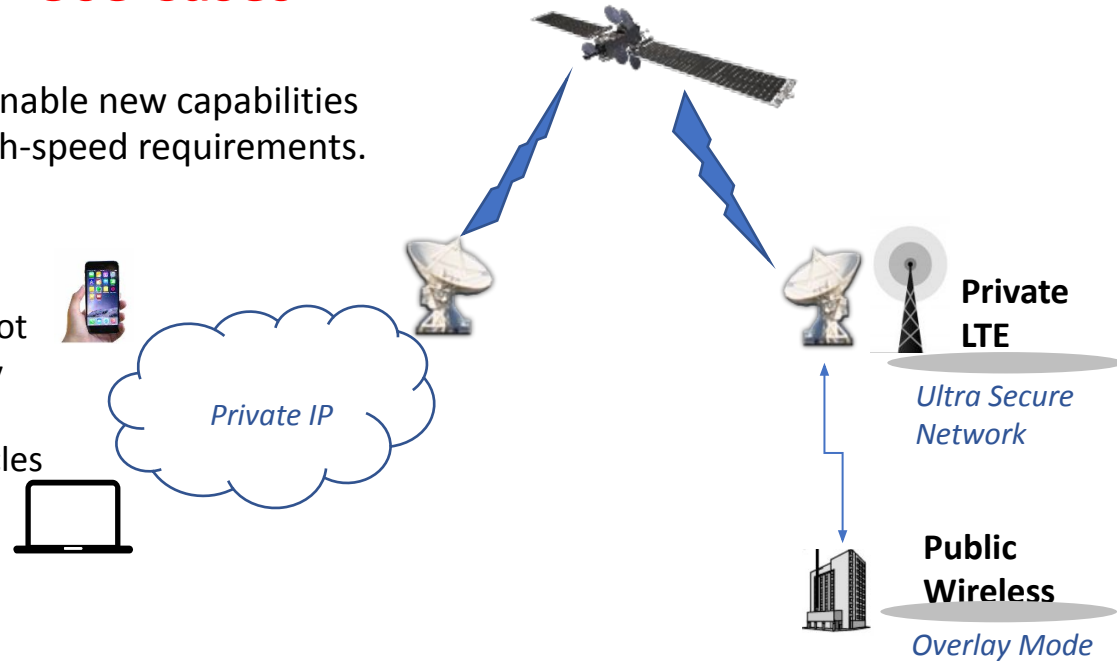
Use Cases

Why It Matters:

Emerging industrial/military 5G use cases enable new capabilities meeting high-capacity, low-latency, and high-speed requirements.

Insights:

- Agile Smart Base, Port, Flightline, and Depot
- Humanitarian Relief and Disaster Recovery
- VR/AR Training and Simulation
- Drone Communication/Autonomous Vehicles Robotics
- Telemedicine
- Industrial Massive IoT and Sensor Fusion
- Additive Manufacturing and 3D Printing



5th Generation Wireless Wireless Connectivity

Why It Matters:

Industry 3GPP 5G standards continue to evolve to enable the new economic benefits leveraging low-latency, high-bandwidth, reliable, and power-efficient wireless broadband connectivity. The federal government needs to understand the benefits to enable new enterprise and mission capabilities.

Insights:

- Secure, software-based end-to-end encryption across IP modalities is required to protect data over untrusted hardware.
- Private network substantiations will be enabled via network splicing, Private IP, Enhanced Packet Cores, and Dedicated RAN.
- Unlicensed and licensed shared spectrum can be aggregated to provide required bandwidth per use case.
- Supply chain risks need to be understood and mitigated.
- U.S. influence in global standards (3GPP) need to be organized.
- R&E funding via OTA needs to excellerate 5G mission capabilities.



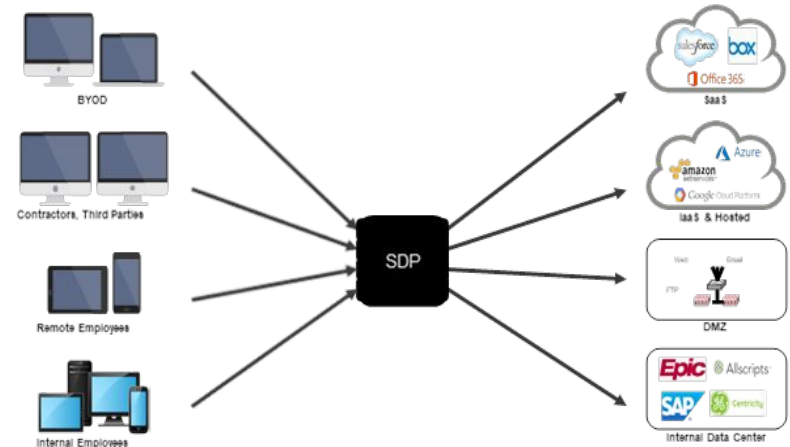
5th Generation Wireless Security

Why It Matters:

5G networks bring a new system architecture leveraging virtualization, cloud, edge compute, beamforming, etc. With global sourcing of electronic components untrusted hardware needs to be assumed and software-based zero trust and micro-segmentation methodologies need to be incorporated to reduce risk.

Insights:

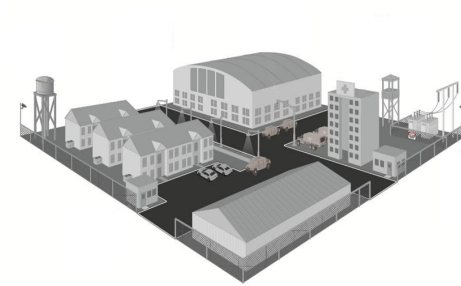
- NSA and NIST standards need to be evaluated
- Access, authentication, and credentialing need to leverage new quantum key technologies; e.g. true random number generation for each new digital certificate and encryption keys based in time
- DoD standards, policies, and guidance need to be updated to account for current and emerging technologies



5th Generation Wireless Business Case

Why It Matters:

Overall foundation work needs to be done around the business case for the mobilization of the DoD workforce in order to reduce the burden on mission owners looking to justify mobile expenditures and realize a 'mobile 5G first' vision.



Insights:

- Although the mobile cost justification for the military is fundamentally different than for the commercial world, “lessons learned” can provide best practices for DoD Total Cost of Ownership.
- A high-level but comprehensive 5G Business Case Analysis’ (BCA) will identify cost areas for fixed and mobile implementation and identify benefits to justify additional DoD applications/use cases.
- The existing mobility business case can serve as a baseline model for the DoD’s analysis for justifying and deploying future wireless systems and their enabling technologies.

5th Generation Wireless

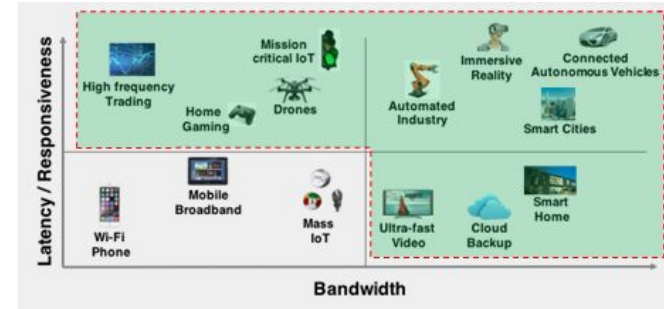
Future

Why It Matters:

As with almost all technologies before it, mobility and its infrastructure components will morph from being human interactive to being predominantly autonomously.

Insights:

- Mobile technology challenges are just beginning and will get more sophisticated as the numbers of manned and unmanned mobile devices dramatically increases.
- Risk assessment and justification will be the biggest challenges in leveraging new mobile and IoT technologies.
- New genres of technology will move far beyond mobilization of current applications and processes to allow for totally new approaches to mission organization and workflow.
- Other key areas: classified wireless devices, tactical missions, mobile content management, etc.
- Enterprise Mobility Management (EMM) is mature, but some scaling challenges remain. Business processes that support mobility services add overhead and cause delays.



Artificial Intelligence

Executive Overview

- **Historic Breakthrough:** AI is on the cusp of a revolution to become the most influential innovation in history, embedded in all devices and technologies.
- **Tip of the Spear:** China, Russia, and others consider AI the greatest strategic advantage. Putin said: “Whoever leads in AI will rule the world.”
- **Impacts, Issues, and Implications:** AI is likely to restructure and eliminate jobs, risk accidents, and make mistakes
- **Military/Intelligence Applications:** AI can improve intelligence analysis, strategic decisions, autonomous vehicles, logistics, weaponry, and more to come.
- **Big Advances in the Industry:** Strong capabilities now exist in predictive analytics, deep learning, and robotics. See the “Big Data and Analytics” Tech Vector for more.
- **Challenges Abound:** AI can be hacked, biased, hard to understand and control, and it can make dangerous mistakes.
- **Forecast Mainstream ~ 2025:** “Weak AI” able to automate routine tasks is taking off now and should enter mainstream about 2025. General AI is likely about 2040.
- **Recommendations** Combine AI and humans, use backup systems, involve all parties.

Technology Vectors

Artificial Intelligence

Key Points

Why It Matters

AI is ranked with fire and electricity in its power to transform the world. It is integrating appliances, homes, offices, cars and battlefields into a web of intelligence now essential for managing complexity.

Implications and Mission Benefits

Automating routine work allows leveraging resources and people to take on bigger and tougher challenges, beat the competition and improve preparedness.

Adoption Approach/Challenges

Develop a plan for implanting AI, starting with simple tasks and moving upward in complexity and strategic importance.

Additional Information and Resources

[IBM Watson | AI For Smarter Business](#)

See final section of this report for more.

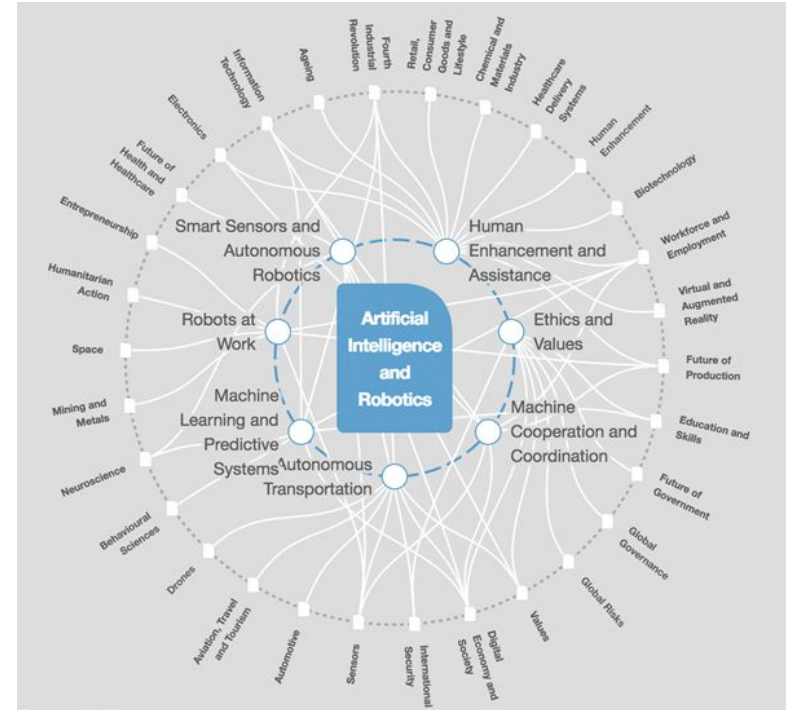
84

Artificial Intelligence

Technical Principles

Fields and Impacts of AI

There is always debate over the sub-fields of AI and their impacts, and this chart offers a useful framework. Note the profound expansion of AI throughout all sectors of society, suggesting the revolutionary power of this infant technology.



Artificial Intelligence Predictive Analytics

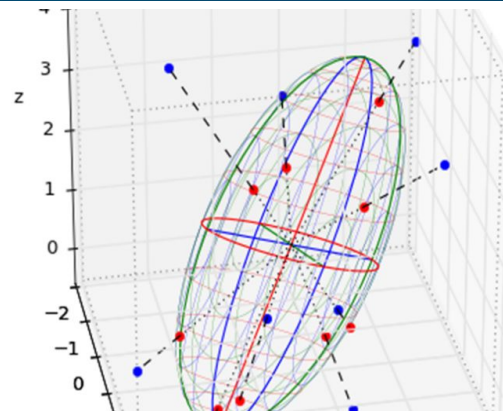
Predictive analytics uses statistical algorithms to help more accurately predict outcomes based on analysis of data.

Optimizing Planning: Statistical data is used to predict outcomes of a program so leaders can make better choices. Example: Predict types of cyber attacks and the best actions to combat them.

Optimize Cognitive Capabilities: Data from the mission and operations is used to inform better tactical decisions, information sharing, and integration of engineering, planning, and operations. Example: Identify patients that might be susceptible to cancers based on their genetic makeup.

Improving Operations: Maps key players, their roles, forecast outcomes, predict events, determine timing. **Example:** Commanders can predict the outcome of an attack or if a better measure is needed.

Reducing Risk: Uses data on the many variables of an operation's likelihood of success, allowing organizations to become proactive, anticipate outcomes, detect risks and opportunities. Example: Force engagements can use the right mix of assets and capabilities to achieve the desired outcome.



Technology Vectors

Artificial Intelligence Deep Learning

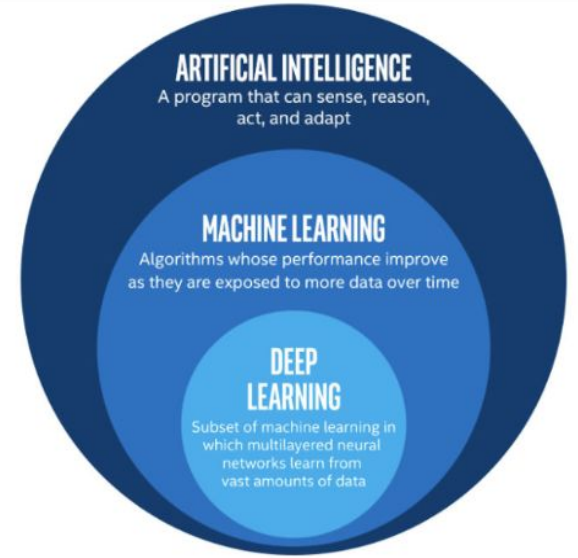
Definition: Deep learning is a sophisticated form of machine learning.

Technology: Both rely on large data sets to find patterns that effectively explain relationships.

Structure: Multiple layers of artificial neural networks, patterned after brain cells, are used to identify progressively deeper levels of information.

Example: Image identification uses the first layer to find the edges of an image; the second layer defines the large features; and the third layer maps out specific details.

Applications: IBM Watson, automatic speech recognition, facial identification



Technology Vectors

Artificial Intelligence

Robotics

Three Basic functions of Intelligent robots:

Perception using sensors – vision, sound, temperature, etc.

Decisions made by AI – programmed, semi-autonomous, autonomous;

Action through effectors – walk, grip, motion, speech, gestures, emotions, etc.

Interdisciplinary field: ME, EE, AI, etc.

Robotic Intelligence: Ability to understand the environment and make appropriate decisions to serve the robot's goals.

Degrees of autonomy: 10 level general scale, 5 levels for autonomous vehicles

Robot rules, ethics



Types of robots: Industrial, Domestic (vacuum cleaner, washer/dryer, etc), Military, Androids Telebots (drones, autonomous taxis), Smart Vehicles, Nanobots, Medicine, Farming, Games

Technology Vectors

Artificial Intelligence

General AI

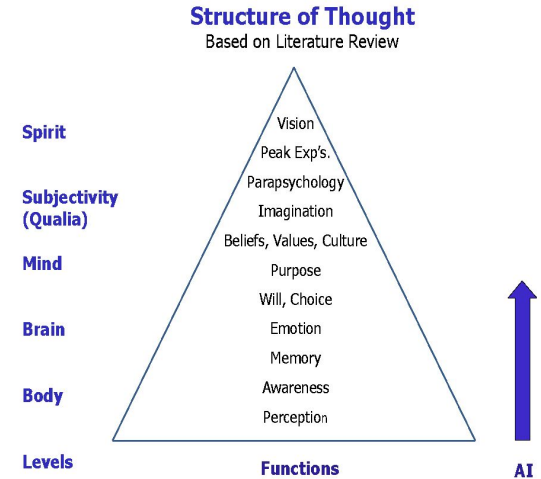
Goal of GAI: AI research is advancing beyond specific tasks ("narrow" or "weak AI") to create broader systems (GAI) that can emulate human thought generally

- **Perception** (video, speech, hearing, ambient sensors, touch)
- **Memory** (data storage and retrieval, big data)
- **Learning** (deep learning of new skills, predict behavior)
- **Problem Solving** (algorithms, data analytics)
- **Action** (robotics, speech)

Testing: Of the many tests for confirming GAI, the most famous is the Turing Test, which asks people to judge if an unseen voice is a computer or a human. It is thought this test may have been passed recently.

Forecast: Ray Kurzweil forecasts showing that a \$1,000 PC will have the computing power of the brain by about 2025. Estimates suggest that GAI is likely to arrive about 2040 or so. Some think AI will surpass human abilities to create a "super intelligence" or "super AI."

Beyond GAI: GAI may master cognitive human intelligence, but creative and interpersonal tasks are of a higher-order and not likely to be automated soon. This is the realm in which human skills are likely to dominate as automation eliminates routine work.



Technology Vectors

Artificial Intelligence

Impacts, Issues, and Implications

History of Over-Optimism: Herbert Simon predicted computer world chess champion by 1967 – three decades before IBM's Deep Blue beat Garry Kasparov.

Greater Efficiency: AI systems do not have the limitations of humans; they never get tired, never let their attention wander, etc. When AI replaces human workers, error rates often plummet while productivity soars.

AI Can Be Dangerous: Many warn that AI could lead to a dangerous new arms race. An open letter with hundreds of signatories claims "A global arms race is virtually inevitable, and there is a fear that autonomous weapons will become the Kalashnikovs of tomorrow."

Mass Unemployment: Studies suggest nearly half of jobs could be automated in the next 25 years, even the work of doctors, lawyers, and scientists. Humans will do work that requires creativity or good personal service.

Not Transparent: Machines cannot replace complex human skill and judgement; they often make dangerous mistakes; and they are not well understood. The two Boeing 737 crashes were caused by a confusing autopilot that failed and could not be controlled by the pilots.

Ethical Concerns: AI programs are often biased and cause social problems and other ethical concerns. Google has established an ethics board for its AI program.

Technology Vectors

Artificial Intelligence

Life Cycle Graph (S-Curve)

The plotted data are public estimates of adoption levels and market size that have been reached, as well as future forecasts. Note that the TechCast estimates closely follow the best fit S-curve for this data, steering a central path through the uncertainty. The result is our forecast of 30 percent adoption by about 2027 +/- 3 years.

Also note differences between the S-curve estimated market saturation of about US\$500 billion and the TechCast Experts estimate of US\$1055 billion. This type of uncertainty is a constant in forecasting, and collective intelligence suggests triangulating between the S-curve, experts, and any other source of useful knowledge. Our best estimate is about US\$700 billion.



Artificial Intelligence

Recommended Strategies

- **Combine AI and human intelligence:** Good AI can enhance human abilities and help people learn, while human intelligence can improve AI systems. Bill Gates expressed it well: “AI can be our friend.” “Collective intelligence” could integrate AI and human intelligence to create more powerful systems.
- **Provide Backup AI Systems and Ensure Human Oversight:** The dangers of AI failures and bias require redundant AI systems to take over from failures, and trained personnel should monitor performance and be prepared to take control.
- **Involve Stakeholders in Design and Operations:** McKinsey advocates engaging employees, customers, suppliers, governments, and other constituencies in designing better AI. It estimates this will outperform traditional approaches by roughly 100 percent.



Artificial Intelligence

References and Resources

Websites:

[McKinsey Global Institute | McKinsey & Company](#)

[The Future Of AI | Artificial Intelligence | accenture.com](#)

Publications

[Artificial intelligence - Wikipedia](#)

Authorities

[Google AI](#)

SME:

Predictive Analytics: Matthew Maher (CEO, Processus group)

Blockchain

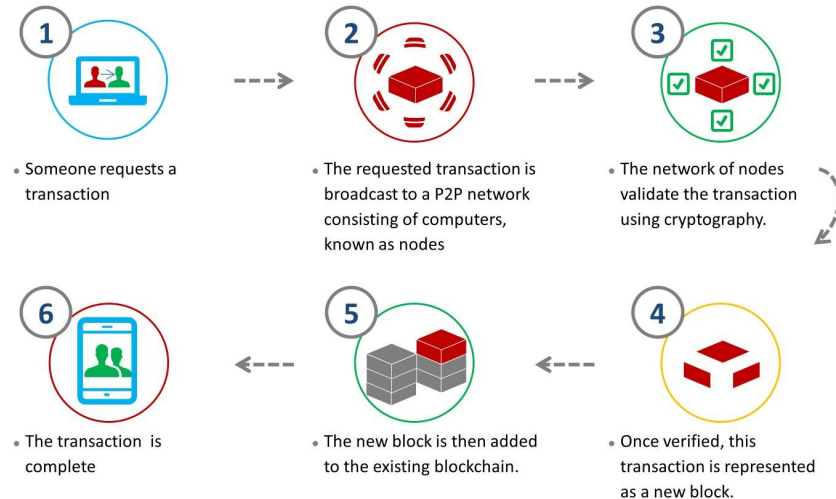
What Is Blockchain Technology?

A blockchain is a continuously growing list of records, called blocks, that are linked and secured. Each block contains a cryptographic hash of the previous block, destination, timestamp and transaction data. This technology allows efficient, reliable, and transparent peer-to-peer transfer of digital assets, and thus its potential impact on businesses is immense.

Depending on the decentralized governance, transaction is deemed valid. It is then added to the most recently verified block in the chain, creating a sequential ledger that is viewable by anyone and cannot be altered.

A distributed ledger is a database of transactions that is shared and synchronized across multiple computers and locations without centralized control. Each party owns an identical copy of the record, which is automatically updated as soon as any additions are made.

Blockchain technology



Technology Vectors

Blockchain

Why It Matters

- Blockchain can orchestrate and automate interactions with external parties.
- Streamline and integrate disparate systems, reducing data entry duplication, and reconciliation.
- Blockchain's verification methods enable near to or real-time processing and settlement of transactions without a central 3rd party.
- Combining with other emerging technologies become a force multiplier. e.g. combining blockchain, AI, ML, RPA for implementation in HHS applications.

Implications and Mission Benefits

- Enable secure, standardized data sharing in a trusted, assured, transparent ecosystem.
- Reduces the risks associated with traditional/stovepiped database models.
- Greater cost efficiencies and structural flexibility from continuous verification.
- Robustness from distributed data with a single shared version of the truth.
- Improved governance and visibility from shared ledgers and automation using programmatic "smart contracts."

Adoption Approach/Challenges

- Emerging standards (Note: NIST blockchain paper, along with Congress Promotion Act, both released October 2018)
- Blockchain is confused with cryptocurrency and hard to explain, with developers in short supply.
- Blockchain introduces lower immediate performance, higher complexity, and less privacy of traditional databases in return for increased disintermediation and robustness.

Additional Information and Resources

<https://www.ibm.com/blockchain/platform/>
<https://en.wikipedia.org/wiki/Blockchain>
<https://blockchain.ieee.org/>
<http://www.gbaglobal.org>
<https://www.gsa.gov/technology/government-it-initiatives/emergin-g-citizen-technology/blockchain>
<https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf>

Blockchain Drivers

Security: The distributed and encrypted nature of blockchain mean it is more resilient and difficult to hack, respectively.



Faster Processes & Scalability: Blockchain can speed up process execution in multi-party scenarios – and allow for faster transactions with and without humans in the loop.



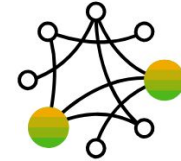
Automation: Blockchain is programmable – which will make it possible to automatically trigger actions, events, and payments once conditions are met.



Transparency: Information in blockchains is viewable by all participants and cannot be altered. This will reduce risk and fraud, and create trust.



Fewer Intermediaries: Blockchain reduces reliance on some types of third-party intermediaries – like clearinghouses, auditing contractors, and information brokers.









ROI: Distributed ledgers will provide quick but lasting ROI by helping agencies create leaner, more efficient, and more profitable processes



<https://www.sap.com/products/leonardo/blockchain/what-is-blockchain.html>

Blockchain Sub-Elements

PUBLIC	PUBLIC		
	 bitcoin	 ethereum	 ripple
	<ul style="list-style-type: none">• Digital Cryptocurrency• Mining Verification with specialized equipment• Up to 21 Million Coins• Decentralized; 23% “lost”• \$200Bn Market Cap	<ul style="list-style-type: none">• Cryptocurrency with a smart contract platform• Ether crypto is a platform component• Open-Source / Decentralized• \$113Bn Market Cap	<ul style="list-style-type: none">• Currency exchanges• Centralized model on a <i>permissioned</i> network• Ripple Labs owns 62%• 100 Billion coins minted• \$50Bn Market Cap
PERMISSIONED	PERMISSIONED		
	 HYPERLEDGER	 MultiChain	 c.rda
	<ul style="list-style-type: none">• Consortium hosted by the Linux Foundation, with IBM, Intel, Accenture, etc.• Several Open Source protocols purpose-built for enterprise applications	<ul style="list-style-type: none">• Designed for efficient indexing, storing, and retrieval of data on standalone basis• Backwards compatibility with Bitcoin Core & bitcoin network• Open Source Project	<ul style="list-style-type: none">• Specialized Blockchain/ DLT for financial services• Run by R3, a consortium of 70+ leading banks• In discussions to merge with Hyperledger project

- Public, decentralized blockchains are those most closely associated with tokens or cryptocurrency, where anyone can participate in the consensus-driven ecosystem.
- Private, or “Permissioned,” blockchains are access-controlled, so members must be invited to participate in the governed ecosystem, across multiple parties or systems within organizations.
- Private blockchains are more scalable and controlled and provide the greatest near-term opportunity for DoD stakeholders. Permission refers to read, write and/or verify.

Blockchain

Technical Principles: Distributed Consensus

Physical Transaction



Digital Transaction: Ledger



Decentralized Ledger



Insights:

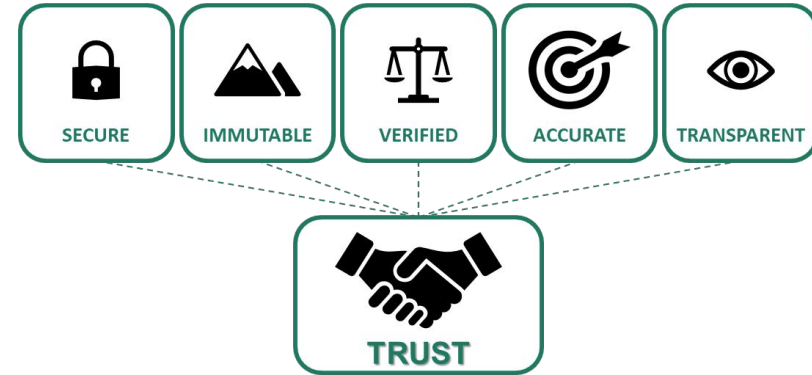
- Blockchain technology offers a way for untrusted parties to reach agreement (consensus) on a common digital history.
- A common digital history is important because digital assets and transactions are in theory easily faked and/or duplicated.
- Blockchain technology solves this problem without using a trusted intermediary.

Blockchain

Technical Principles: Trusted, Verified, Auditable Ledger

Blockchain Technical Characteristics of a Trustworthy System

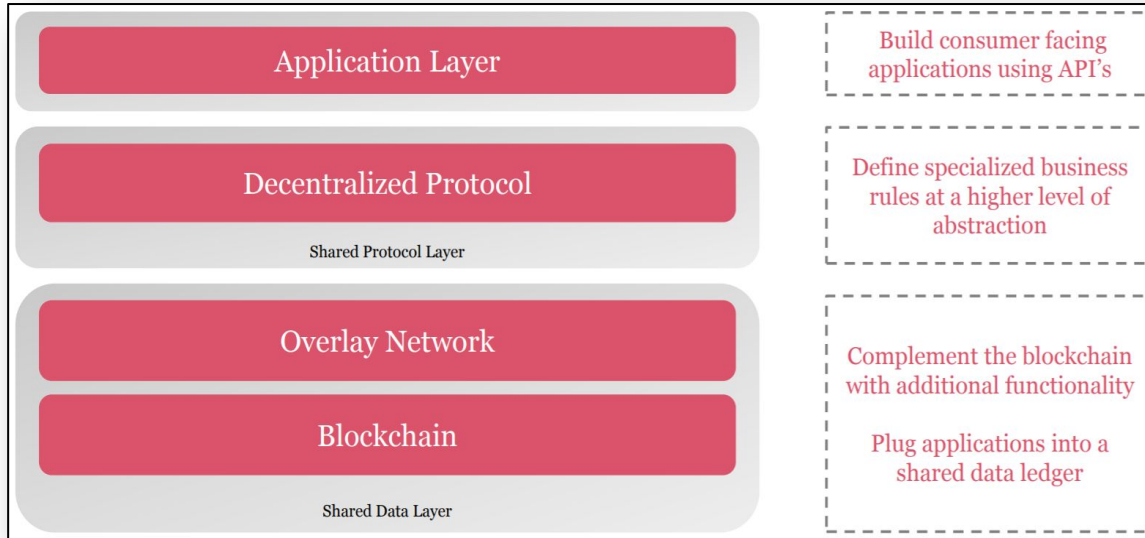
- **Secure:** Hashed (encrypted) records are easy to verify given some input, but it's impossible to find the input that produces a known or preexisting hash value.
- **Immutable:** Blockchain systems are significantly more robust and resilient than traditional systems because there is no single point of failure.
- **Verified:** Consensus mechanisms enable autonomous governance capabilities, so data write access is controlled.
- **Accurate:** Users have predetermined controls and data access rights, so data is complete, accurate, and consistent.
- **Transparent:** A single shared ledger to record transactions reduces the clutter and complications of multiple data sources.



Source: Colvin Run Networks

Blockchain

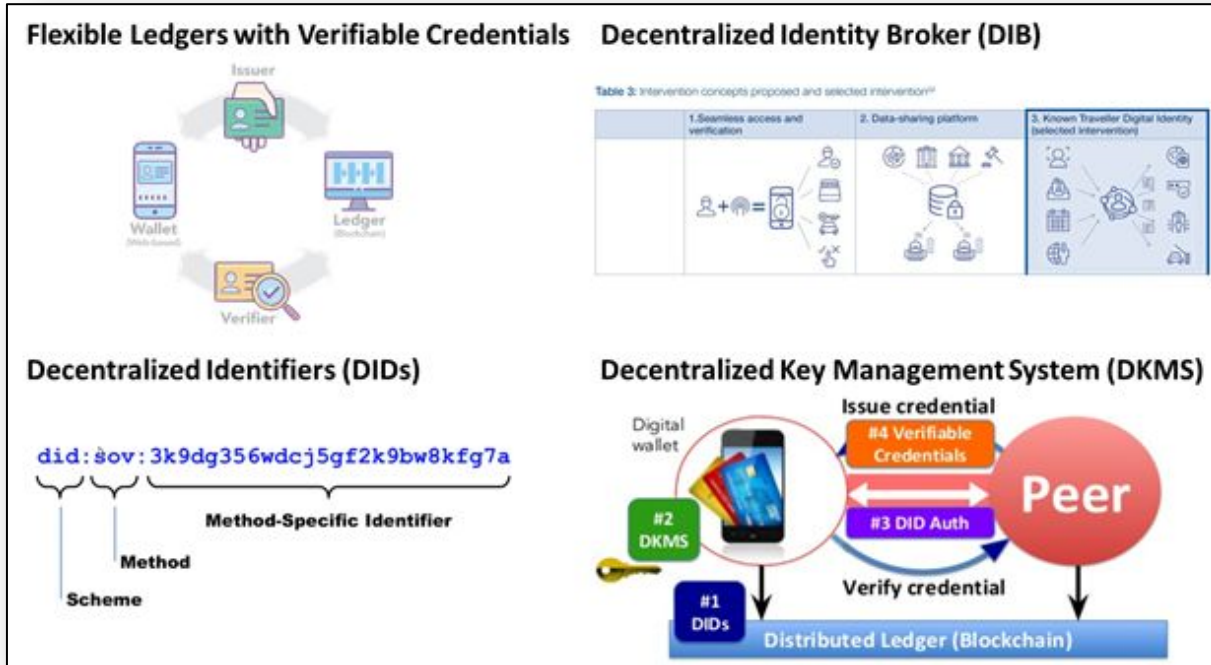
Technical Principles: Blockchain is a Foundational Technology



- Blockchain includes basic infrastructure, but many conceive of it as the entire “blockchain solution,” which includes the blockchain infrastructure, the smart contracts, the APIs, etc. baked into the blockchain layer as depicted.

Blockchain

Federal Scope: DHS Written Senate Testimony, May 2018

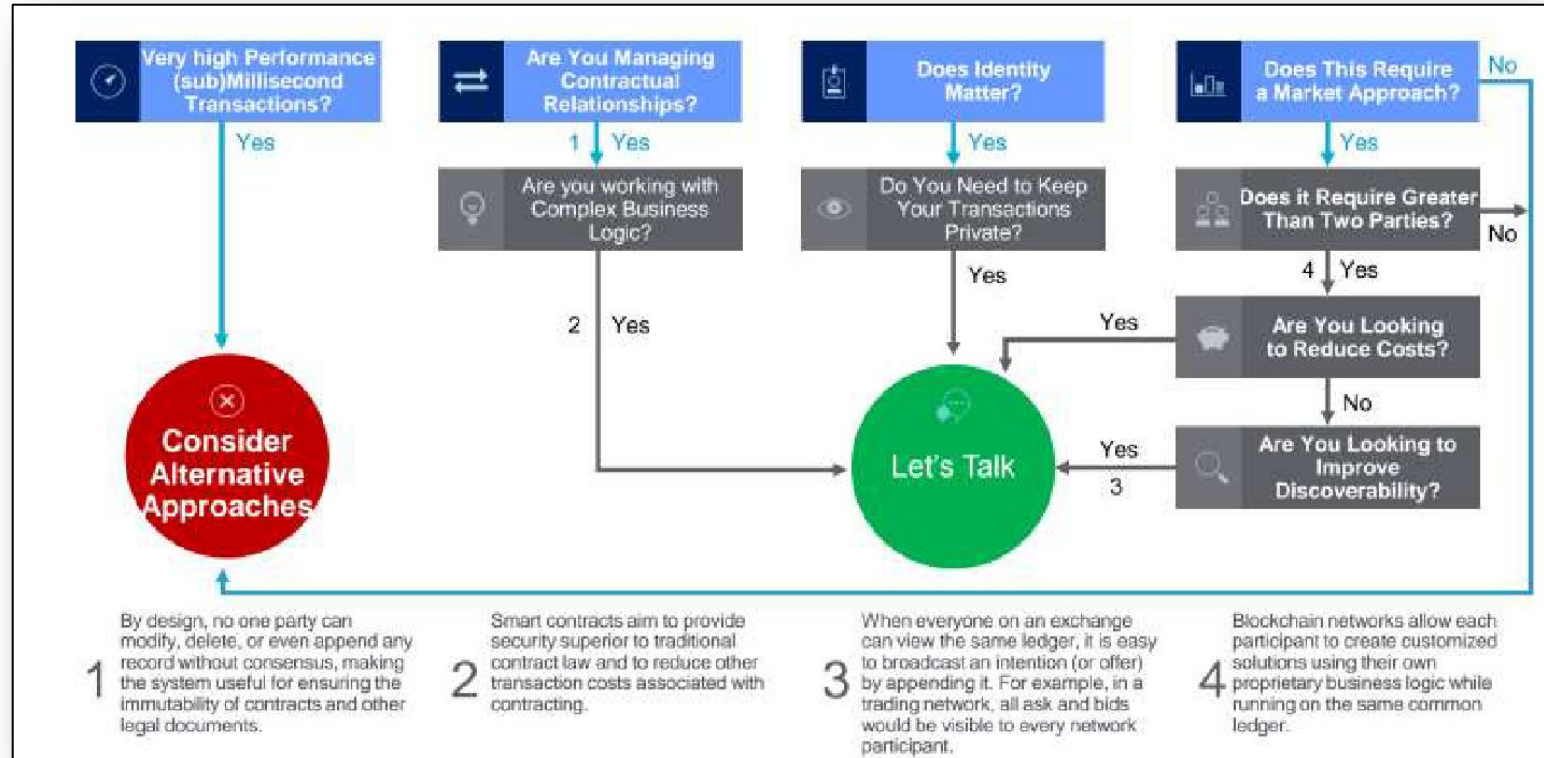


- Department of Homeland Security has extensively tested and piloted blockchain for a variety of use cases, including NAFTA trade enforcement in late 2018.
- DHS sponsored creation of fit-for-purpose blockchain platforms that utilize W3C web open standards.
- Most recent grant utilizes blockchain to secure IoT (Internet of Things) data with limited Internet connectivity.

Technology Vectors

Blockchain

Decision Framework: Do We Need a Blockchain?

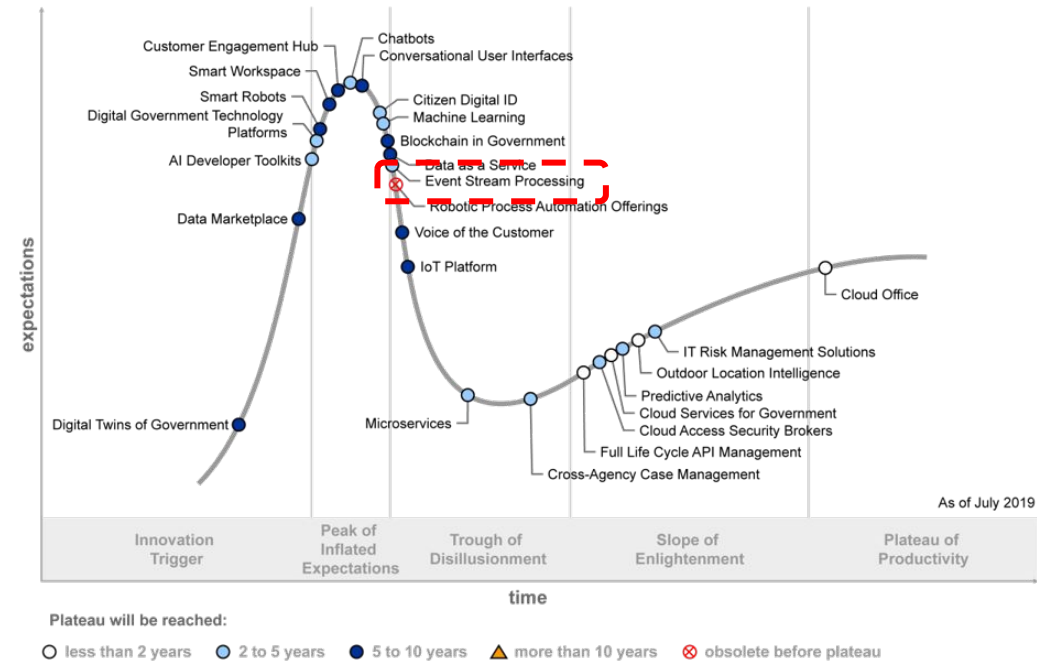


Technology Vectors

Blockchain

Gartner Hype Cycle: Entering the Trough

Hype Cycle for Digital Government Technology, 2019



Source: Gartner
ID: 370115

<https://whatsthebigdata.com/2019/09/06/gartner-hype-cycle-for-digital-government-technology/>

Blockchain

DoD Considering Applications for Armed Forces

Military Drone Technology & Communications



Blockchain can record and ensure the data collected by AI-powered drones immutably and in real time.

Blockchain Battleships



Despite its age, the Aegis is a highly sophisticated piece of military technology. However, Aegis is a centralized system with a single point of failure.

Decentralizing Weapon Control Systems



Blockchain allows decentralization of computing power across multiple nodes for supply chain risk management, software development, and systems engineering processes.

Additive Manufacturing

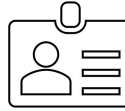
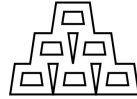


Blockchain could prove to be an enabler for widespread adoption of DoD AM into general manufacturing supply chains over the coming years.

<https://coincentral.com/blockchain-military-applications-the-future-tech-of-the-armed-forces/>

Blockchain

Five Predictions: By 2030...



Prediction #1 Government Crypto	Prediction #2 Trillion-Dollar Protocols	Prediction #3 Blockchain Identity for All	Prediction #4 World Trade on a Blockchain	Prediction #5 Blockchain4Good
Most governments around the world will create or adopt some form of virtual currency.	There will be more trillion-dollar tokens than there will be trillion-dollar companies.	A cross-border, blockchain-based, self-sovereign identity standard will emerge for individuals, as well as physical and virtual assets.	Most of world trade will be conducted leveraging blockchain technology.	Significant improvements in the world's standard of living will be attributable to the development of blockchain technology.

From An Op Ed piece by Ray Valdes (CTO @ ConsenSys) and Kate Mitselmakher (CEO @ Blockcelerate VC) on the future of blockchain technology:
<https://medium.com/the-future-of-blockchain-technology-top-five/the-future-of-blockchain-technology-top-five-predictions-for-2030-67df1d7c2391>

Need Additional Information?

If you have additional questions or inputs regarding this material, please send an email to:

TechVectors@afcea.org

To learn more about the AFCEA Technology Committee, visit:

<https://www.afcea.org/site/Technology-committee>

To learn more about TechCast, visit:

<http://techcastproject.com>

