Market Outlook

February 2022

AIOps in Telecom Operations

Exploiting a $3.3 Billion Global Market

Author: Patrick Kelly

www.appledoreresearch.com

Appledore RESEARCH

Published by Appledore Research LLC • 44 Summer Street Dover, NH. 03820

Tel: +1 603 969 2125 • Email: Patrick.kelly@appledorerg.com• www.appledoreresearch.com

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Appledore Research LLC independently of any client-specific work within Appledore Research LLC. The opinions expressed are those of the stated authors only.

Publish date: 2/21/2022

Cover image: Patrick Kelly

Contents

EXECUTIVE SUMMARY

> ***"AIOps is the green shoot that leads to self-healing, hyper scaling of resources, and maximum automation."- Patrick Kelly***

AIOps is the foundation of telecom operations innovation platform to improve network availability, capital efficiency, and cyber-attacks in cloud networks.

AIOps is a critical system that dramatically reduces operational cost and improves the value of customer loyalty and brand equity. AI/ML is the green shoot that leads to self-healing, hyper scaling of resources, and maximum automation. In this new world CSPs can increase new services tenfold, turn up new edge services in minutes instead of months, and scale staff to customer ratios from 1:1K to 1:50K. These operational performance metrics are not theoretical but instead are real figures from the best run cloud hyperscaler, fintech, and e-commerce businesses.

Our thesis is that CSPs need to accelerate the adoption of ML faster and utilize the power of the technology across all areas of operations. The strategy must be unified in bringing different teams together that are isolated today, such as *Network operations, Customer operations* and *Security operations*. You can't deliver high network availability if a DDOS attack incident is being propagated and nobody outside of security silo is aware of it. A key part of realizing the promise of AI/ML requires the democratization of the data freeing it from the technology domain silo and organizational fiefdom. Open APIs will play a critical role with key suppliers to realize the promise of AI/ML.

However, the telecommunication market has been very slow to embrace the automation of operations relative to other industries. This unwillingness to restructure operations to take advantage of low-cost machine intelligence has had a direct impact on the financial performance of CSPs. The proven AI led business models applied by innovative providers in cloud infrastructure, fintech, and digital commerce have disrupted traditional businesses. In the telecom segment hyperscale cloud providers have captured market share in core areas of the communication sector including mobile content, cloud, and edge computing. Driven by the increasing disaggregation of network and the use of AI automation, cloud providers are able to outperform traditional telecom providers in terms of operational efficiency metrics. This is largely due to advances in the use of technology deployed to replace high input cost (labor) in business operations.

AI/ML brings with it high value use cases that span, operations, planning, capacity utilization, threat detection, and energy management. We forecast that the market will grow from USD 558 Million in 2021 to USD 3.3 Billion in 2026. The wider market for AI/ML is much greater. This report focuses specifically on the Network and Security AIOps (NSAIOps) in the telecommunication segment.

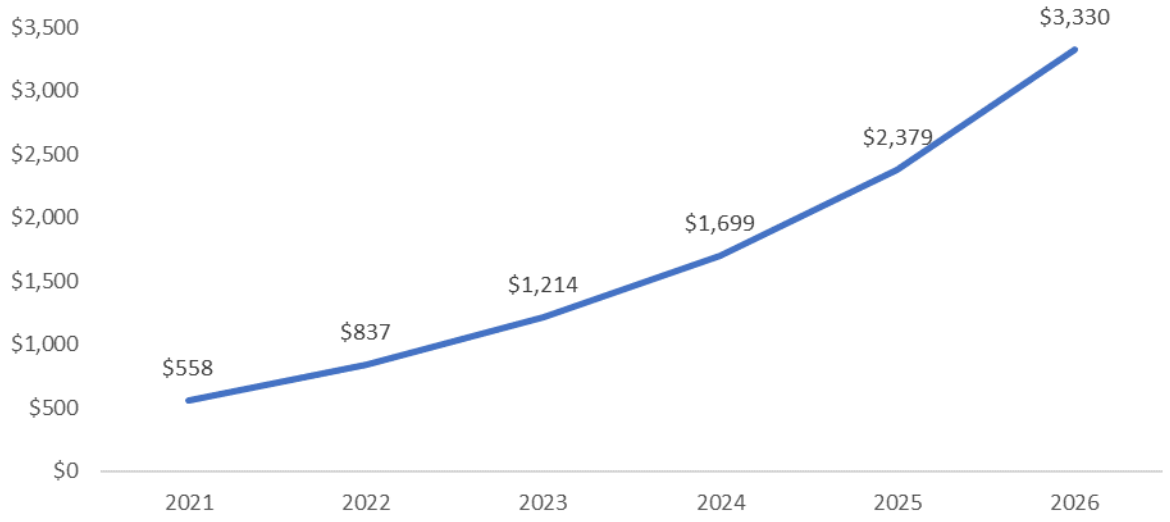
Today we have entered a market maturity cycle of crossing the chasm for telecom operations AIOps. The hype and bold promises, just a few years ago that suggested that AI and machine learning would lead to a fully autonomous network has moderated. Appledore expects more AI proof point wins that focus on value generation in targeted areas to include network optimization, problem-solving, operational efficiency, power management, and securing the infrastructure.

This report focuses on our findings in the most predominant use cases in the telecommunications industry. We evaluate the supply and demand side economic drivers. We also considered the broader secular trends impacting the market for AIOps investments including future labor force declines. As with most fast-growing early-stage market segments business models and the ecosystem will adapt quickly prior to maturation. We profile some of the leading suppliers and identify new entrants from the larger ecosystem.

AI SOFTWARE AND SERVICE 5 YEAR FORECAST

Appledore Research forecast that the Network and Security AIOps market will increase from USD 558 Million in 2021 to USD 3.3 Billion in 2026 (figure 1). We adjusted our forecast from our report in 2020 to adjust for changes in our market taxonomy. We exclude data curation platforms like Splunk from the forecast model. Representative supplier solutions include Nokia AVA, Ciena BPA, Palo Alto Networks Cortex, Symphony Innoeye, Spirent VisionWorks, IBM Cloud Pak, Google Anthos, Ericsson Intelligent Automation Platform, among others.

Figure 1: Network and Security AIOps Forecast 2021-2026



Source: Appledore Research

The use cases that we see the highest investment in AI over the next three years in the telco sector include:

1. A 20-fold improvement in isolating faults and service impacting events
2. Isolating and detecting cyber-attacks in near real time
3. Mitigating ransomware and data breaches against machine generated attacks
4. More accuracy in predicting demand of network capacity
5. Better asset allocation for capital investments
6. Increases in customer retention
7. Reducing fraudulent transactions
8. Improvements in personalized marketing campaigns
9. Predictive maintenance and avoidance of unnecessary truck rolls
10. Improvement in energy management

KEY DRIVERS FOR AI/ML IN SECURITY AND NETWORK OPERATIONS

NSAIOps is the term that we will use to define the submarket segment. It is focused on gathering log file data, telemetry data in the network, observing data in motion, and applying techniques and algorithms that yield insights and reliable predictions on the behavior and future state of the network.

Applying AI for improving prediction and business outcomes will transform decision making in most job functions of telecommunication operators in the next decade. AI tools used in the right context will improve subscriber experience, network operations & planning, energy management, and anomaly detection. Its application falls into a spectrum of potential uses including contextual insights, accurately predicting future events, and in the not-too-distant future full automation of workflow task.

Increased Sophistication of Cyber Attacks

Telecommunication providers face two broad security attack surfaces.

- The first attack surface is the internal network that delivers voice, video, and data services to millions of customers. Attack vectors facing the public network must be secured at each point of presence and must take a comprehensive zero trust architecture to secure the access networks and gateways that are vulnerable to state sponsored groups and criminal organizations.
- The second attack surface that could potentially become compromised is managed services that include PaaS, IaaS, and SaaS related offers which rely on a larger partner eco-system. Attacks can occur at the endpoint, application, and network layer. This is a more difficult zone to secure due to the nature of many trusted relationships and distributed nature of the infrastructure. The Solarwinds incident was propagated using a method known as supply

chain attack to insert malicious code into the Orion system. Its success was predicated on targeting a third party trusted relationship and using a backdoor to gain access to system files circumventing other malware and security technologies.

Bad actors are taking advantage of the larger attack surface, driven by the lift and shift of workloads on premise to the cloud and the distribution of remote workers. At the same time, nation states have increased cyber attacks focusing on critical assets in the telecom, energy, financial, transportation, and government sectors.

The most recent highest profile cyber-attack was targeted at Solarwinds. In early 2020, hackers secretly broke into SolarWind's network and added malicious code into the product Orion. Solarwinds has 33,000 customers. Beginning as early as March of 2020, SolarWinds unwittingly sent out software updates to its customers that included the hacked code. The code created a backdoor to customer's information technology systems, which hackers then used to install more malware. The hackers used a method known as a supply chain attack to insert malicious code into the Orion system. A supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly. The third-party software, in this case the SolarWinds Orion Platform, creates a backdoor through which hackers can access and impersonate users and accounts of victim organizations. The malware could also access system files and blend in with legitimate SolarWinds activity without detection, even by antivirus software. SolarWinds was a perfect target for this kind of supply chain attack. Because their Orion software is used by many multinational companies and government agencies, all the hackers had to do was install the malicious code into a new batch of software distributed by SolarWinds as an update or patch.

Microsoft reported cyberattacks and data breaches in January 2021 after four zero-day exploits were discovered in on-premises Microsoft Exchange Servers. The attackers obtained full access to user emails and passwords and administrator privileges on the server. It was estimated that 300,000 servers fell victim to the attacks.

In August 2021 T-Mobile USA confirmed that a data breach exposed almost 50 million customers' data, with the attacker accessing social security numbers, names, and dates of birth.

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline. The primary target of the attack was the billing infrastructure of the company. It paid $4.4 Million to criminal hacking group DarkSide to restore the systems.

Meatpacker JBS USA paid a ransom equivalent to $11 million following a cyberattack that disrupted its North American and Australian operations. JBS is the largest meat producer.

Figure 2: Notable Cyber-attacks in 2020 to 2021

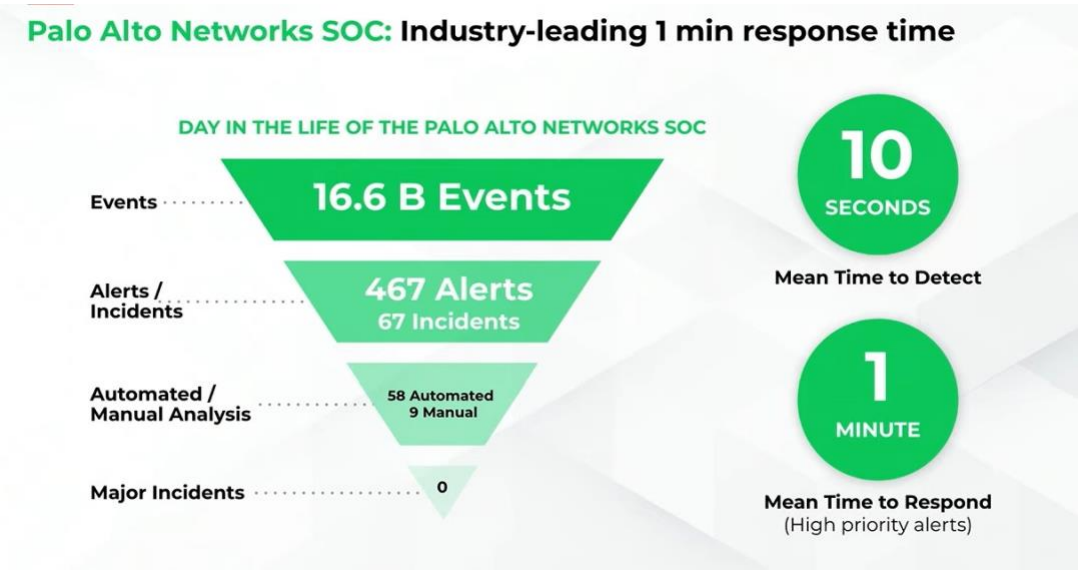
Sector	Cyber Attach Type
Federal, state, private companies (30K+)	Solarwinds Orion supply chain hack
Food	JBS ransomware
Energy	Colonial Pipeline ramsomware attack ($4.4 M)
Government	Belgium DDoS
Telecom / Cloud	Microsoft Exchange Server Zero Day hack
Government	Japan Olympics data leak
Transportation	South Africa port
Government	Russian Election hack
Telecom	T-Mobile 50Million account breach
Financial	Poly Network $600 Million cryptocurrency theft

Source: Appledore

Automation and security operations AI/ML, when fully deployed, provide the biggest threat mitigation to counter ransomware, financial theft, data theft, hijacking critical infrastructure, and brand destruction.

Zero trust security architecture requires a complete view of the attack surface. Data collection from the cloud, network, endpoints, and authentication identity management servers must be captured and correlated to scale security operations. Transferring the playbooks of experts in the security operations team to AI models accelerates detection of security attacks. This is achieved based on processing vast volumes of security events to focus on high vulnerability attacks in near real time. Figure 3 provides insights on security operations from Palo Alto Networks from data on their network. It reveals some spectacular results on event processing and the use of automation in the security theater to identify and isolate cyber threats in the detection to response time frames.

Figure 3: Palo Alto Security Threat Detection and Automation Outcomes



Source: Palo Alto Networks

5G Upgrade Supercycle

Almost 200 mobile operators have deployed 5G at the end of 2021. Between 2021 and 2026 capital spending for 5G radio and infrastructure is forecasted at $600 Billion on a global basis. Underneath this investment cycle is massive disruptions in the technology deployed and supplier ecosystem. The sheer complexity that comes with Open RAN, multi-vendor core networks, cloudification, edge computing, and 5GSA architecture will impact how mobile networks are managed to deliver reliable services.

If 5G is deployed with existing operational processes and tools, operational costs will rapidly inflate. This scenario on a long-term basis will become unsustainable and financially unattractive. An AIOps led approach to automation, is how this can be avoided

Previous generations of mobile network have fundamentally been about connecting handsets with centralized monolithic carrier grade applications and the internet, with the mobile network acting as an access technology between handsets and these central applications. 5G will be the first generation of mobile connectivity that is about connectivity to cloud applications and these cloud applications will be distributed within and beyond the mobile operators' network.

As an example, in the future 5G network it is possible that an operator may want to support a low latency application in a robotic manufacturing facility which demands recurring and rapid changes to factory production demands. The desired network state and associated KPIs must be captured in near real time to initiate new services, move workloads, or re-route network connections if service is impacted. AI is dependent on the ability to collect and process large

amounts of telemetry data to identify patterns and determine if the service is operationally "green" or an event trigger should be generated to the network service controller.

Scale and Skill Sets

In this future AIOps world, the workforce must be prepared for a different set of skills in the IT driven software centric world. Traditional workflow processes create bottlenecks and hinder operational efficiency. A NOC driven predominantly by a human-only workforce are not only expensive, but often cannot scale to meet the future consumer demand. The automation of high-volume tasks will require CSPs to think about alternative workflow processes. AI applied correctly in the service lifecycle will outperform and dramatically change the OPEX curve.

Harnessing the power of machines over human experts is necessary to deliver and maintain service availability. This is a huge cultural shift to how things have been done over the past 50 years. It's a leap of faith to achieve the moonshot of the self-learning autonomous network. We both understand and acknowledge that the cultural barriers are much greater than the technical barriers as this transformation proceeds over the next decade. We are in the AI crawl stage of the proverbial crawl, walk, run model. In the crawl stage that exist today we expect that machine learning "findings" may be checked and confirmed by human experts. Once they pass this review it will slowly be placed into semiautomated production with basic rules to drive well understood automation actions.

High Quality Data and Processing Power

The abundance of high-quality data, advances in computational processing, and sophisticated machine learning models, available in the open-source community, is reducing both the cost and accuracy of applying AI compared to conventional hard coded methods. Attempting to deploy AI even 5 years ago was not economically feasible because of limited data sets, higher cost computing, and inferior ML models to conventional statistical regression techniques. In short, it was difficult to justify the economic benefits. That has all changed and the technology is actively being deployed in many sectors. In the telecom market it is being applied in energy management, improving subscriber experience, optimizing network traffic, isolating faults, and identifying network threats, among other things.

The unique value of AI is that it uses massive amounts of high-quality data to discover patterns, and then predict outcomes more reliably than current methods. The power of AI is that it is constantly improving its learning algorithm, using a technique called back propagation that changes weights in the hidden layer, to achieve higher levels of accuracy.

Downward pressure on operator capital investments

Return on invested capital is a critical business metric and in today's telecom market capital investments are under pressure. Most CSPs are looking to improve their cost structure. One lever being used is cutting CAPEX budgets to reduce excessive debt on their balance sheet. The

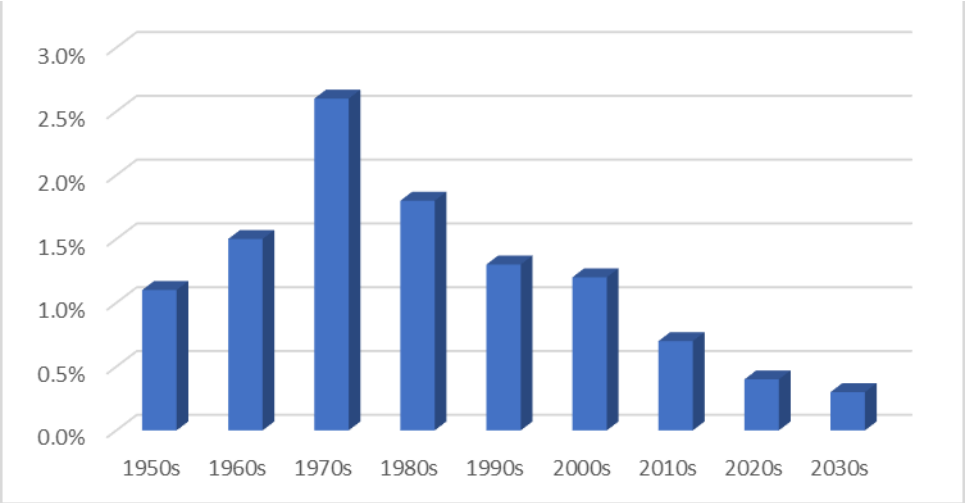
end goal for the C-Suite is to focus on improved earnings. Many in the C-Suite find their current capex process to be antiquated and deeply flawed. A recent study by PwC found that nearly two-thirds of executives say that capex is driven by technology with no clear business commercial objectives.

AI can be utilized to understand customer consumption patterns and predict capacity demand in shorter duration cycles. This helps drive a much more efficient capital allocation plan.

Workforce Declines

The workforce of many developed countries is aging rapidly including Japan, Germany, China, United States, and many other European countries. Figure 4 is specific to the United States but many other countries in developed economies would reveal a similar chart. The decline has been underway since the 1980's. Covid acted as a short-term accelerator to further declines in the labor pool as baby boomers opted for early retirement. This major demographic shift will bring an end to the abundance of labor that fueled economic growth post WWII.

Figure 4: United States Labor Growth Forecast 1950 to 2030



Source: US Department of Labor and Appledore.

The decline of available labor in the economy will drive most companies to evaluate investments in automation and robotics. In the telecommunication industry much of this operational leverage will substitute labor for capital efficiency in field force, customer care, operations, and engineering jobs. Faced with a rising scarcity of labor, businesses will leverage AI and automation to raise productivity.

NETWORK AND SECURITY OPERATIONS MARKET SEGMENT

NSAIOps will post process network data and log files to identify abnormalities. It also encodes logic imbued by domain experts to draw conclusions and then guide corrective action to reach

an outcome. This “expert playbook” is designed to maximize the power of the AI system to produce superior outcomes over human experts. It often follows a path that follows the proverbial crawl, walk, run as a natural progression. Right now, the industry is crawling, and basic techniques include:

- Build data lakes (system wide) and data pools (network edge)
- Focus on network observability which is data in motion (real time) to detect anomalies in near real time
- Blueprint normal data patterns and isolate outliers and therefore abnormalities
- Predict and prevent impending threshold crossings
- Adopt best practices to automate corrective actions, including guiding human actions – from CSRs to engineers who want more certainty, data, and guidance.

Existing service assurance systems in the telecommunication network were designed to manage a fixed set of resources and are inappropriate for monitoring dynamic distributed networks. Service Assurance code was written for known and well understood problems. Some advances were made to develop signature patterns to determine the root cause of a problem. But this approach won’t work in a dynamic, virtualized network, where autonomous changes will occur continuously.

SOLUTION APPROACHES APPLIED TO NSAIOPS

Applying AI for improving prediction and business outcomes will transform decision making in most job functions of telecommunication operators in the next decade. AI tools used in the right context will improve cybersecurity, network operations and planning, customer care, and energy management. AI enables the identification of unknown problems that coded solutions overlook.

The abundance of high-quality data, advances in computational processing, and sophisticated machine learning models, available in the open-source community, is reducing both the cost and accuracy of applying AI compared to conventional hard coded methods. Attempting to deploy AI even 5 years ago was not economically feasible because of limited data sets, higher cost computing, and inferior ML models to conventional statistical regression techniques. In short, it was difficult to justify the economic benefits. That has all changed and the technology is actively being deployed in many sectors outside of telecom for natural language translation, facial recognition, advance driver assistance systems, and industrial automation.

The value of AI is that it uses data to discover patterns, and then predict outcomes more reliably than current methods. The power of AI is that it is constantly improving its learning algorithm, using a technique called back propagation that changes weights in the hidden layer, to achieve higher levels of accuracy.

Figure 5 provides some of the most popular use cases of AI/ML in network and security operations centers.

Figure 5: Network and Security Operations AI Use Cases

	Network Operations		Network Planning			Customer Care		Security Operations			Energy Operations	
	Assurance	Fulfillment	Lab Test	Optimize	Deploy	Subscriber Experience	Call Resolution	Fraud	Trojan Code	DDOS Attack	Power Mgmt	Sustainability
5G site design				High								
Battery capacity prediction												Low
Cell site capacity planning					High							
Cell site energy management											High	
Device interoperability			High									
NOC Fast fault isolation	High											
NOC Faster MTTR							High					
Network Inventory		High										
Ransomware attack									High			
Data Breach attack								High				
Network threat detection										High		
Customer Care NPS prediction						High						
Order fallout		Medium										
Power failure prediction												Medium
Radio coverage					High							
Radio signal loss prediction	Medium											
Sleeping cells prediction	Medium											
Virtual drive test				Medium								
Work order volume prediction	Low											

Source: Appledore Research

We consider AI, in its current state, as having the potential to become a high value tool used for specific tasks to solve difficult business problems. It is important to look at AI in the context of the business problem and the results that you want to achieve that yield faster, cheaper, and more accurate results that current workflow tasks or traditional IT tools. The executives and implementers of AI must balance the long-term strategy, organizational impact of AI on existing jobs, data privacy laws, and the economics of AI in improving decision making for all aspects of its business.

It is critical to balance the cost of data acquisition with the accuracy and business outcome that you want to achieve. Organizations applying AI for specific functions will need training data to train the AI tool, input data to test and run the AI system, and feedback data for improving the accuracy of the AI tool. The context and type of data will determine the value and its relevance in solving specific use cases. Another consideration in the AI driven project is the use of data that may violate data privacy and regulatory laws on the use of personal data. AI will be useful for some tasks, but not relevant for other tasks. Applying AI for a limited data set or when the problem is not well defined should be avoided.

Secular Shift Towards Observability

To observe the networks behavior, CSPs must deploy distributed data collectors that provide sufficient output to understand the health of the network. A key input is the deployment of active testing and passive collection of data plane network flows. The data stream and collection of performance metrics and fault events become critical inputs of user activity to reach observability. Baselining performance metrics provides the basis for establishing network state.

Active testing provides a continuous proxy method for how the service is performing at any given time. It provides a low-cost option to simulating traffic, measuring performance, and yielding a reasonable benchmark as to the overall health of the network. Passive probing provides the data flow of real user activity across the entire service chain. It is more precise, higher cost, and very effective at isolating problems quickly.

Observability is necessary in the telecom cloud network to realize the automation of labor-intensive activities which cost the telecommunication industry half a trillion dollars every year. Automation is being deployed today in the 5G radio access (RIC), SON, and SD-WAN network domains. CSPs should be preparing now to implement network observability to realize the benefits of closed loop automation for orchestration driven processes. Logic follows that you can only control by observing the complete state of the network. Observability deployments must begin at each technology domain to accrue the benefits necessary to realize a fully autonomous network by 2030.

Many CSPs have been resistant to thrust forward most automation related projects outside of the domains we mentioned above. This is largely driven by the uncertainty of unleashing a rogue algorithm driven process engine that is perceived to create unforeseen and potentially catastrophic consequences. Self-driving cars with passengers sleeping in the back seat that crash reinforce the bias against fully autonomous systems. Similarly, the telco mindset is to push back on the telco autonomous network for now in favor of defending the Five 9's of reliability.

Our long-term thesis is that automation will come to the telecom vertical albeit slowly. It will be necessary as labor shortages persist and managing the network complexity increases with advanced technologies such as 5G, Edge, and private networks. Many developed countries which have a skilled labor shortage will face an increasing labor shortage in the latter years of this decade. Germany has a labor shortage of 2.5 million workers today which will grow to 10 million by 2030. Countries that have a surplus of labor such as the United States at 20 million workers will see a decline to 7 million workers by 2030. Observability is an effective strategy to improve operational efficiency, hedge against tight labor supplies, and is necessary to achieve closed loop automation.

The promise of the modern network is to provide highly valuable dynamic services which must become autonomous. Network observability provides the high value data inputs to gain insights and actions for telco operations.

Customer Churn

One of the most important business metrics in the telco industry, which is reported every quarter, is customer churn. Acquiring customers is expensive and the ability to predict customer churn is critical. The first step in reducing churn is the ability to identify customers most likely to leave. Many methods have been applied in the industry, including reporting on network KPI's, deploying subscriber analytics tools, and using 3rd party services to report on net promoter scores.

Regression methods have been the backbone of the industry up until now. Regression attempts to predict churn based on what has happened in the past. Regression can be improved for churn by considering multiple conditions. For a mobile user, conditions might be handset in use, coverage area, technology deployed in the RAN, pricing plans, usage patterns, bill shock, payment patterns, and so forth. This technique was known as multivariate regression, and it improved the error rate in predicting churn. The problem with regression is that it almost never accurately pinpoints which customers might leave. Instead, it predicts an average. Today machine learning based churn models are outperforming regression models. The reason for this is more variables are available on a larger data set of subscribers. Instead of hundreds of variables and thousands of customers, CSPs can now apply AI to thousands of variables and millions of subscribers, in near real time.

Anomaly Detection

Anomaly detection in the past was based on rules-based programming and root cause analysis. This technique is still applicable today and should continue to be used in classical root cause and problem resolution task found in the NOC, security, and fraud domains. AI based methods should be applied to the most difficult areas of anomaly detection. New services and technology deployments are a clear greenfield for AI. The variety of uses for applied AI in the telecom operational domain includes: 5G radio access planning, root cause analysis in SD-WAN deployments, and quality of service in edge cloud applications.

WHAT ARE THE RISKS TO ACCELERATING AND ADOPTING AIOPS?

Many factors are in play that create barriers to adopting AI/ML in operational domains. We see the key inhibitors to faster adoptions as:

1. Access to data
2. Skilled labor in the design, build, and deployment phase
3. Poor modelling

4. Regulatory and privacy laws

Access to Data

Data is the oxygen that powers the AI engine. To improve the prediction of any AI engine it must have large, diverse, high-quality data. The biggest challenge we see, in speaking to implementers of AI driven projects, is both finding the data and getting access to it. The data can be available but access to the data pipe could be restricted because of governance and lack of cooperation between departments.

The most important take away for AI projects is the availability and quality of data. Without it, machine learning is impossible. You can have the best team and a solid ROI, but without high quality data your entire AI project will fail.

Data is used for training the ML algorithms, validating that it works, and then testing the AI outcomes. The validation phase is used to refine and tune the model. Keep in mind that after identifying and gathering the data it must be classified and labeled.

A good rule of thumb on data acquisition and its use is that 60% of the data is used for training the model. This is often the case for adjusting weights in the model in a technique known as back propagation. More on that process later. The training data can't be used in the testing phase because the ML algorithm already knows the expected output. The goal is to get the ML algorithm to improve on its learning with new data and achieve better outcomes for anomaly detection than is possible with a human.

Probably worth emphasizing that this is not a one-off activity – training and adapting the model is an ongoing activity that moves with changes in the network and business.

Reference or maybe move observability section to here – AIOPs needs an observability platform.

Getting good quality large scale data is the biggest barrier to adopting AI. Specialty companies are emerging that assist humans to label data quickly. Future data labeling platforms will be embedded in the design of the application, so that the data created by using a product will be captured for training purposes. And there will be new service-based companies that will outsource labeling to semi-skilled staff. Finally labeling will be done using AI engines.

Owning data can give immense power and commercial opportunity in AI. However, in many cases the fragmentation of ownership of data can mean that no one has adequate access to enough data to truly solve complex problems. This is particularly a problem in telecommunications where we have a fragmented operator landscape and complex interactions of different vendor solutions. To date operators and vendors have tended to be commercially protective of "their" network data, preventing its use in supporting industry wide problems. The industry needs to find effective ways of beneficially sharing data, with appropriate protection or anonymization, to enable the greater prize of a cost-effective network.

Skill Sets

AI is fundamentally reliant on data scientists. The demand for data scientist exceeds the pool of available experts in the field. This supply/demand imbalance will remain supply constrained for the foreseeable future, based on both our growth assumptions for the market and more AI driven use cases in the telecom market. The data scientist role is to conceptualize, prototype, design, develop and implement large scale solutions in the cloud and on premises, in close collaboration with product teams, data engineers and cloud enterprise teams. Competencies in implementing established as well as new machine learning, text mining and other data science driven solutions on cloud-based technologies is required. The data scientist will be knowledgeable and skilled in the emerging data science trends and must be able to provide technical guidance to the other data scientists in implementing emerging and advanced techniques. The data scientist must also be able to work closely with the product and business teams to conceptualize appropriate data science models and methods that meet the requirements.

We see in many cases CSPs relying on SI's and primary suppliers to advance their AI projects. This approach will yield fast time to market and bring domain expertise that may not be available to smaller regional or CSPs that accept the skill sets don't exist in-house.

Poor models that generate bias

Beware of bias in the AI model and data sets, that can impact the prediction performance of the output. Models with a high bias are more rigid and less sensitive to variations in the data. At the opposite end of the spectrum are high variance models which are better suited to flex with data complexity, but the tradeoff is that the model is also more sensitive to noise.

- Sample bias is the result of using data to train the model which does not accurately depict the problem domain. In the telco domain utilizing data on a 4G radio access network to train a 5G network coverage and capacity model will not produce the expected results.
- Prejudicial bias occurs when humans apply stereotypes to the training data. The classic cases are racial profiling, gender, and credit worthiness. For example, using socio-economic data that contains only age, race, and zip code will produce outputs that do misclassify the credit worthiness of low-risk default consumers.
- Measurement bias will result from faulty devices. This is easy to identify but should be considered in any prediction output.

Regulation and Data Privacy

It should come as no surprise that data privacy and consumer data protection are two of the most significant issues in our industry. Data privacy revolves around consumer consent, how data is shared with 3rd parties, what data is collected, and where it is stored. All companies must be compliant with regulatory restrictions on the use of data imposed by governments. The most

familiar is the European Union General Data Protection Regulation (GDPR) that applies to the use of EU citizen data.

The challenge for policy makers is to make clear what is collected, opt-in/out consensus rules for the consumer, and how data is collected, stored, and transferred to 3rd party companies. This cannot be done at local levels but instead must be implemented at a national level. In the United States policy makers at the federal and state levels are wrestling for who should legislate into law the use of data. We do expect the FTC to legislate a federal privacy law. Doing it at the state level makes enforcement harder and leaves more interpretation of how it should be implemented given each state will most likely craft their own regulations. In my opinion if it is not done at a national level, implementation and enforcement will fail to achieve compliance in the commercial market.

It's not a question of if, but when, policy makers will impose tighter restrictions on the use of data and make services more transparent and easier for the consumer to opt in or out. Much of this is driven by large data sets generated by mobile and sensor-based devices and the algorithms behind it that policy experts argue benefits suppliers (data collectors) not the consumer.

LEADING SUPPLIERS

Appledore Research has completed primary research on the following suppliers in the market that have deployed AI software and services commercially in the market. Many suppliers exist in the market, and we will continue to add to our corpus of research as the market matures. The suppliers profiled were required to provide us with supporting documentation on deployments within the past six months, access to experts, and documentation of commercial software that has been released into the market. Suppliers that want to brief us on their solution are encouraged to contact us directly.

Ericsson AI

CSPs evaluating AI suppliers to improve operational efficiency in the mobile network must have Ericsson on the short list. The combination of a global top tier managed service business with deep technical domain knowledge of the RAN, core, and OSS domains is powerful. Ericsson has proven AI deployments with some of the largest operators in the world. Downside risk should be minimal for RAN optimization and in understanding subscriber experience. Ericsson has both proven products in its portfolio and thousands of network experts and hundreds of data scientist on the payroll.

Ericsson has a smaller sphere of partners in its eco-system, preferring to take more of a go it alone tactical approach. This will work in the current market but in the future, we think this strategy has some obvious weaknesses. It has no preferred AIOps SI partner. Ericsson has not

announced any meaningful AIOps related partnerships with cloud providers. The Google announcement in June was specific to 5G edge and this is in the very early stages of formation.

Nokia AVA

Nokia is a top-tier supplier for AI centric solutions. We think Nokia is executing very well in the AIOps market particularly for its mobile operators. Applying AI to business problems requires high value data, domain expertise, innovation in the use of ML algorithms, and massive scaling in the cloud compute infrastructure. Nokia delivers in all areas. It has relationships with all the cloud platform suppliers.

Not much attention is centered on Nokia's Bell Lab assets where it has a deep bench of PhDs and data scientists to tune and perfect the algorithms. Combining this with Nokia's field and development resources in both the mobile and fixed network domains brings credibility and relevance to solving RAN optimization, and network anomalies.

Nokia is also focused on fringe opportunities that help control cost outside of the operational domain. Energy consumption by mobile operators will increase with the deployment of 5G which results in densification of the RAN. Nokia has deployed an Energy Efficiency service via its managed service business that uses AI to reduce energy usage in 5G networks by up to 20%.

Nokia's ambition in the future is to implement a more tightly coupled orchestration and AI analytics feedback loop to reduce human touch points in the lifecycle service chain.

Near-term we expect Nokia AVA and its other analytics assets to grow faster than other parts of the software business. We believe the market opportunity for the use of machine learning and AI techniques in the telecom industry is in the early stages of growth. Nokia has first mover advantage here.

Google Anthos

Google has not yet announced any specific solutions for telco AI in network operations. However, we see any future fitting into Anthos for Telecom which extends Anthos' reach to telecom edge cloud locations. Google sees Anthos as the operating system that can support every kind of telecom application, from high-performance RF processing to core, OSS, BSS, and network analytics.

Anthos for Telecom enables the move from telco's traditional siloed build-out to a more hybrid multi-cloud, open approach. Traditionally, most telecom network software used to reside in on-premises data centers, but this is shifting towards a mix of private, public cloud and edge. Increasingly, CSPs are moving in this direction for their OSS/BSS. With increasing emphasis on advanced 5G use cases (especially for enterprises), operators are exploring new ways to manage distributed software applications across complex cloud infrastructures.

Managing these new applications can be very challenging, even for a single telecom function. For instance, a 5G core can have 40-50 different workloads, and sometimes can involve two or three vendors. This is where Google has an opening in positioning Anthos for Telecom helping operators.

Ciena Blue Planet Analytics

Ciena leadership in the optical network domain is being applied to AI to solve some of the most difficult problems in signal impairments in layers 0, 1, and 2 (optical and ethernet). Using it software assets, the company has much more ambitious plans to not only leverage its predictive analytics engine but also to drive closed loop automation. Ciena has orchestration, inventory, and route optimization software products under the Blue Planet portfolio to automate most manual task done today by highly skilled craft technicians. Replacing craft technicians' long term will dramatically lower OPEX cost and achieve higher levels of service availability. Ciena is also applying AI for predictive analytics to improve dynamic network allocation and workload scaling at the 5G edge.

Ciena is taking a practical approach to machine learning and automation. They are beginning with network events, where they can bring their domain expertise to bear. Most of the initial use cases relate to degradation or loss of either optical or ethernet signals. Blue Planet Analytics (BPA) collects data from many sources and performs correlations. Using the data, it can learn the root causes of events without supervision. For example, BPA can predict Ethernet LOS after learning over time. BPA's actions are supervised (in part due to complexity and in part to provide CSPs' confidence). BPA first suggests what it believes to be the best action or actions, and human experts either select from the list or confirm/deny the corrective action. At some point its accuracy is sufficient to allow actions to be implemented without human intervention. This threshold is left to the discretion of each operator. Currently, the high variability of vendors, technologies and operational processes between customers means that standardized analytic and machine learning approaches are not possible. Instead, Blue Planet analytics and machine learning learns over time with each solution specific to customer.

Spirent VisionWorks

Spirent VisionWorks is a leading assurance solution providing proactive insight of network and service performance based on a cloud-native architecture. Using machine learning and AI, VisionWorks continuously monitors and develops network-specific baselines, called signature analysis, allowing potential deviations to be identified and addressed before becoming major network disruptions. Once a problem is identified, automation-driven diagnostic testing and intuitive, guided workflows quickly lead VisionWorks users to issue domain isolation and root cause repair.

Spirent is uniquely positioned to support AIOps efforts based on decades leading the test and validation market. Customers that want to reduce network validation time to deployment cycles

must consider Spirent as a testing and assurance supplier. Spirent has the credentials to deliver a testing solution at scale in a multi-vendor network. It has deep relationships with almost every infrastructure supplier in the telecom supply chain. As the market is evolving, so is Spirent, by transforming its products to support new outcome-driven “testing as a service” offerings.

Innoeye Foresight

Rakuten Symphony acquired Innoeye in 2020. Innoeye provides workflow orchestration and intelligent automation solutions. Innoeye Foresight is a real time analytics platform, which leverages and correlates data from multiple sources. The platform enables proactive diagnosis and remediation. Foresight is multi-vendor, multi-technology, configuration management, performance management and optimization platform.

The Foresight platform is designed to handle massive data volumes and transactions. Using this multi-functional platform customers can gain insight of network behavior, operational insights, and optimize the overall network performance.

Netscout Omnis Analytics

Netscout automates root cause analysis for network, service, and device problems with Omnis Analytics. It calculates the business impact by identifying how many unique subscribers are being impacted for each issue.

Omnis goes beyond what humans can achieve by performing always on analytics with cross-correlations across multiple dimensions and multi-pass outlier logic to achieve scale at the lowest cost. It uses Impact Analytics and Behavioral Analytics to identify usage patterns (both abnormal and normal) that are not visible otherwise. Omnis Applications are built on top of the nGenius platform.

IBM Cloud Pak for Watson AIOps

IBM is combining AI/ML in network operations under its umbrella of IBM Cloud Pak for Network Automation. It is an open, cloud native, technology/vendor agnostic solution. This means it is applicable, to a wide range of applications, technologies old and new, and across industries.

IBM also offers an AIOps-driven network performance management solution, IBM SevOne Network Performance Management. It delivers a comprehensive view of what’s happening in the network and how that performance affects the applications driving the business. IBM SevOne NPM integrates multivendor performance data with modular flexibility, allowing users to apply data-driven AI to the ITOps toolchain, like IBM Cloud Pak for Watson AIOps.

The event manager component of the IBM Cloud Pak for Watson AIOps includes all Netcool Operations Insight (including Netcool/OMNIBUS and the Agile Service Manager topology

function). Netcool remains one of the most widely deployed Operations and event management solutions in the world, present at almost every major CSP.

Palo Alto Networks Cortex

Palo Alto Networks has developed a comprehensive security automation and response platform under its Cortex brand. XSOAR has been designed to improve the efficiency of security experts in the SOC to manage incidents and automate cyber-attack incidents. XPANSE understands the exposure to new attacks from the public facing internet and other cloud provider attacks. XDR is the central product to integrate and normalize all data sources to include both network and security infrastructure assets such as identity servers and firewalls.

XSOAR makes use of ML to support functions such as incident triage or to offer SOC experts' suggestions for next steps. XSOAR has improved its ML capabilities to enable customers to train their own models. SOAR is available as an on-premises solution, a hosted solution, and a multi-tenant solution for MSPs.

Subex Network Analytics

Subex's current network focus is capacity management in RAN and transport networks at higher layers. They have not focused at L1 and L2 issues and instead focused on the areas where there is a complex data management need.

Subex has focused on RAN investment planning as their first network-related use case. The tool tells operators which cell sites will require expansion (and by how much) – but within constraints of service experience. The tool can also run what-if simulations, for example, to simulate the launch of a new iPhone. In essence, Subex are seeking to effectively find solutions that reconcile competing pressures – cost, performance, and business value.

Subex is now achieving a final investment planning outcome in 3-4 simple steps, compared to current multi-step and manual statistical based processes. With an AI-led approach they are needing less effort to do work and are avoiding making wrong predictions on network growth. They emphasise that they make fully accurate predictions and avoid over-investment in network growth.

Amdocs

Amdocs is taking a 3-pronged strategy towards AI and machine learning across its offerings. It is expanding existing product lines, launching new products, and creating cross domain OSS/BSS AI/ML solutions. In the category of expanding existing products, it is using ML in the areas of network capacity management, optimization, and site survey. In the new product segment, it is focused on Open Ran automation and 5G Non-standalone orchestration management. Its focus in cross domain leverages NWDAF and common approaches to unify the datasets to reveal anomalies impacting subscribers.

HPE Intelligent Assurance

HPE applies ML/AI to network data and provides actionable insights for run-time engines. Early iterations of HPE solution originated from Expert Systems. EA is embedded in HPE Unified Correlation and Automation product which has a respectable install base.

HPE is addressing the most advanced use-cases in automation through HPE 5G Automated Assurance product.

CONCLUSION AND RECOMMENDATIONS

AI will outperform even the best human experts. AI is capable of processing more data in shorter cycle times, with higher degrees of accuracy. Machine learning is the enabler for automation in a technology led world. The modernization of the telco cloud network is becoming more complex and beyond the capabilities of the best human experts and specialists. It's not a question of will AI replace humans in the areas noted in this report – it's when! It's not even a question of replace some things are unscalable without AI.

Buyers of AI solutions will need to separate the contenders from the pretenders before committing to any trials, much less purchase orders. Ask suppliers for reference deployments, capability statistics, costing models, and total economic value from use cases that best match your targeted use case. Ask for ongoing access to data insights across industry!

Suppliers, in this early stage of the market, should be laser focused. Don't try to be all things to everyone. If you can't explain your value proposition on AI in 2 minutes you have failed. Build a strong business case that shows strong return on investment. Successful suppliers can benchmark the customer journey from traditional tools to AI powered solutions in specific technology domains and workflow processes.

For the product managers and field experts, be realistic about acquiring high quality data in large volumes. If you stumble here your business case falls apart quickly. Be aware of access to data pipes that may be off limits. And don't overlook data privacy issues. Data drives the ML engine so unless you can overcome this hurdle you should steer clear of the use case being proved out.

The vendors profiled in this report, stand out and continue to push the boundaries of AI because of their focus and helping customer achieve success today. At the root of their success is collecting and labeling the data sets to drive the machine learning models. Each has a compelling, concise business case that is defendable. Finally, each does not over rotate on their marketing. Their positioning is on point and probably, most importantly, has the customer endorsements to back it up.

ABOUT THE AUTHOR

Patrick has more than 25 years of experience in product management, business development, and technology consulting. He has advised executives and developed actionable business plans to help hundreds of technology companies profit in high growth software segments of the market. He is the leading authority and has published research in the areas of cloud economics, virtualization of the network, AI and machine learning, orchestration, analytics, service management, and customer experience management.

Patrick founded Appledore Research Group in 2014 to focus on the business impact of cloud and virtualization in the telecommunication market. Prior to Appledore, he was Research Director at Analysys Mason, co-founder of OSS Observer (acquired by Analysys Mason in 2008), Director of Product Management for Aprisma (acquired by CA) and held many technical roles in the field supporting both enterprise and service provider customers.

E: info@appledorerg.com

www.appledoreresearch.com

44 Summer Street Dover, NH. 03820, USA

Appledore
RESEARCH