wattnow

DIGITAL TRANSFORMATION: THE ECONOMIC ENABLER

RSA | R30.00 incl. VAT

CYBER

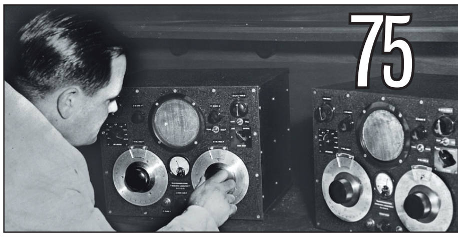
SAIEE THE OFFICIAL PUBLICATION OF THE SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS | FEBRUARY 2020

CONTENTS

FEATURES

GENERAL

REGULARS



SAIEE @saiee

wattnow

MANAGING EDITOR
M Avrabos | minx@saiee.org.za

TECHNICAL EDITOR
J Buisson-Street

CONTRIBUTORS
T Anscombe
J Moore
L Myers
C Pastorini
C Gutiérrez Amaya
U Exner
M Dlamini
N Moloi
M Soni
D Basson
J Buisson-Street
R Dismore
M Clarke

EVENTS
G Geyer | geyerg@saiee.org.za

CPD & COURSE ACCREDITATION
S Moseley | suem@saiee.org.za
www.trainingacademy.saiee.org.za

MEMBERSHIP & TECHNOLOGY LEADERSHIP
C Makhalemele Maseko | connie@saiee.org.za

ADVERTISING
Avenue Advertising
T 011 463 7940 | F 086 518 9936 | Barbara@avenue.co.za

SAIEE HEAD OFFICE
P.O. Box 751253 | Gardenview | 2047
T 011 487 3003
www.saiee.org.za
Office Hours: 8am - 4pm

SAIEE

SAIEE 2019 OFFICE BEARERS

President	George Debbo
Deputy President	Sy Gourrah
Senior Vice President	Sunil Maharaj
Junior Vice President	Prince Moyo
Immediate Past President	Hendri Geldenhuys
Honorary Treasurer	Viv Crone
Honorary Vice President	Marius van Rensburg
Chief Executive Officer	Sicelo Xulu

ISSN: 1991-0452

abc
2019 Q1 - 13457

Can you believe that it is the end of February 2020? Where did the month go?

This issue has a very apt (or advanced persistent threat) theme: Cyber - anything to do with cybersecurity, computer applications, etc.

In our first feature, we take a look at the Cybersecurity trends of 2020, which states that technology is getting smarter - are you? Read this on page 22.

The second feature article "The Human Factor" on page 36, explains how hackers exploit the human factor: the instincts of curiosity and trust that lead well-intentioned people to click, download, install, open and send money.

Our featured Opinion Piece, written by Ulandi Exner, Immediate Past President of the IITPSA, writes that message encryption goes far back as the 20th century and begs the question: "Why are we not protecting our personal and private information in 2020?" Read it on page 50.

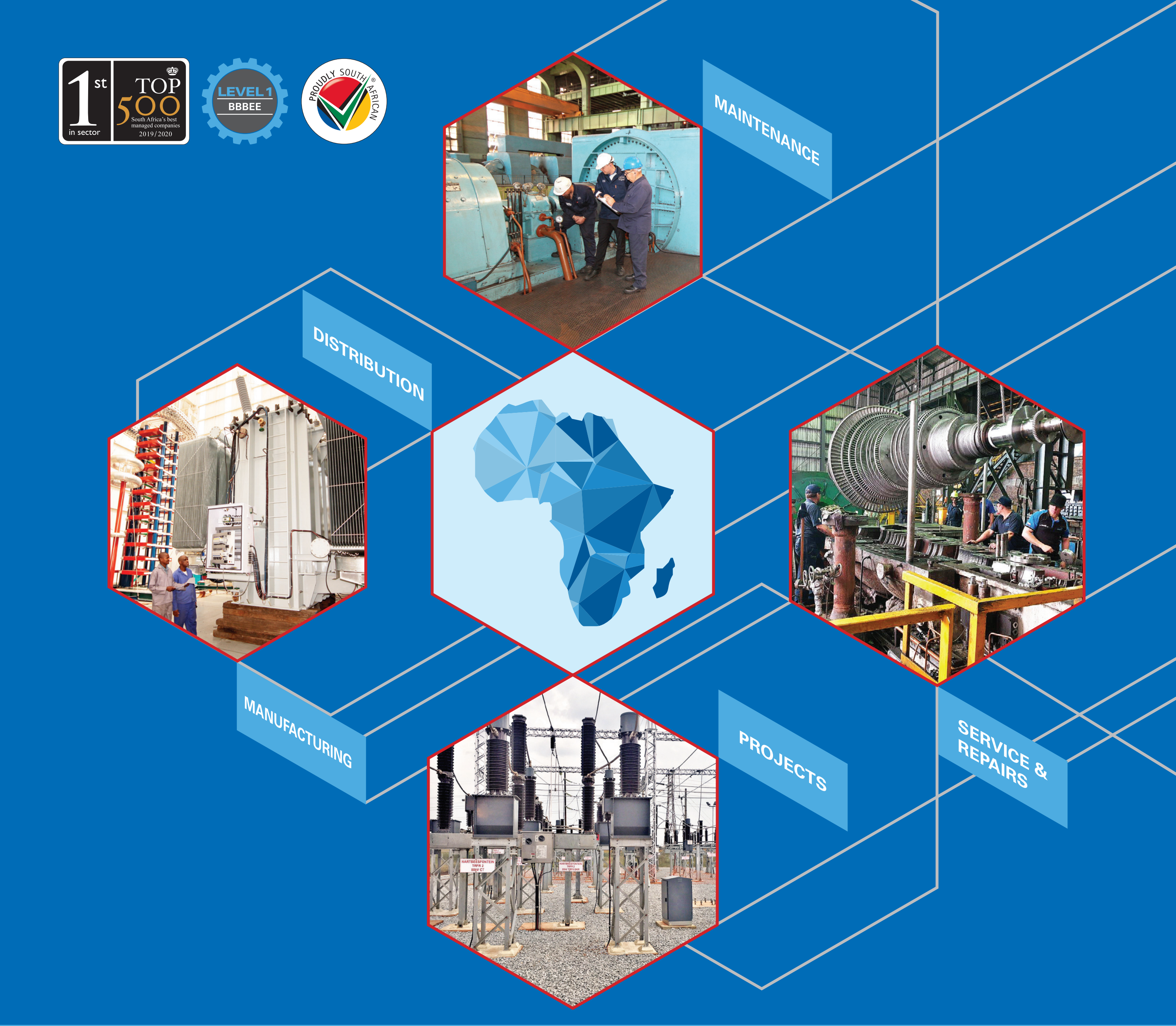
Page 54 showcases two essays from the IEC Young Professionals Essay Competition. The authors wrote about their take on the following question: *"Artificial Intelligence (AI) is becoming common in everyday application, from search engines to autonomous vehicles. Which areas of AI should the IEC prioritise standardising and why do you think these areas are essential?"*

On page 75, please find a historical booklet: "Wadley Masterpieces", compiled and written by Richard Dismore, a (remote) member of the Historical Section. Trevor Wadley would've celebrated his 100th birthday in February, and they took this opportunity to honour his memory and at the same time pay tribute to his unique talents and the effects his inventions had on society.

The March issue of **watt**now features Renewables - which is a hot topic at the moment. Please send your articles/contributions/leads to minx@saiee.org.za to reach me by no later than 16 March 2020.

Herewith the February issue, enjoy the read!

Minx



Key sectors served by ACTOM's equipment supply and solutions offering include:

Power Generation
Transmission
Distribution
Utilities
Construction
Energy
Environmental
Food & Beverage
Healthcare
Industrial Processing
Mining
Oil & Gas
Paper & Pulp
Petro-chemical
Rail Transport
Signalling
Renewable Energy
Sugar
Textile
Water & Sanitation

ACTOM, offering a winning and balanced combination of manufacturing, service, repairs, maintenance, projects and distribution of electro-mechanical equipment through its 35 outlets throughout Sub-Saharan Africa.

ACTOM

ACTOM (Pty) Ltd: 2 Magnet Road, Knights, 1413 | PO Box 13024, Knights, 1413
Tel: +27 (0) 11 820-5111 | Fax: +27 (0) 11 820-5044 | www.actom.co.za

Is 5G a Health and Environmental Hazard?

GEORGE DEBBO
2019 SAIEE PRESIDENT

During the President's Invitation Lecture last year, Professor Chrisna Du Plessis, Chair of Architecture at the University of Pretoria, mentioned 5G as possible health and environmental hazard.

There have been other individuals and organisations that have also expressed concern around the health risks associated with 5G technology. In June 2019 the Belgian Region that also includes the city of Brussels postponed the deployment of a 5G pilot network citing uncertainty about its effects on health.

The purpose of this short article is to identify and discuss the possible risks and to see if there is truth to the concern that 5G is a health and environmental risk.

Before we start, we need first to understand what 5G is. 5G is the next-generation cellular radio technology that is designed to provide several benefits over existing technology. These are:

- Faster connectivity speeds ultimately 1000 times faster than current LTE technology,
- Higher device connectivity density up to 1 million devices per square kilometre. This benefit is mainly intended to support the Internet of Things (IoT) which predictions indicate will result in some 50 billion devices being connected to the network by 2025.
- Lower latency of less than 10ms required by such applications as self-driving vehicles and augmented and virtual reality (AR/VR).

The characteristics of 5G that could lead to environmental and health risks include:

- 5G uses a broader range of frequencies than current cellular technologies, including spectrum in the mmWave (24 to 100 GHz) bands. These higher frequencies provide larger channel bandwidth, and this is how the higher connectivity speeds are reached. The use of higher frequencies also dictates the use of smaller cell sizes since radio propagation distances at a higher frequency are shorter.
- Due to the use of smaller cells, and therefore more sites, 5G is expected to consume up to three times the energy required to power current LTE networks. This will have CO2 emission implications, especially for countries that still rely heavily on the use of fossil fuels for electricity generation. Equipment vendors have taken note of this risk and designed energy-efficient solutions that rely on alternative renewable energy sources as

well as making use of software-defined architectures to make data storage and delivery more efficient through provisioning and dynamic routing.

There have been several myths about 5G doing the rounds, and I thought it would be appropriate to dispel some of these. The myths include:

- 5G is not radioactive! This myth was caused by a photo of a worker who was working on a 5G cellular tower wearing a hazardous materials suit. It has been proven that mobile towers do not emit enough radiation to cause risk to humans, and in fact, the suit in question was not graded to work with radioactive material.
- 5G does not cause cancer! Research has shown that human skin deflects nearly 50% of the power emitted by high-frequency waves used within 5G. Besides, these frequencies do not have enough energy to breakdown human DNA molecules.
- The Facebook post that appeared in 2018, claiming that 5G technology caused a flock of starlings to fall out of the sky dead was fake news. This myth was launched by a 5G conspiracy theorist and debunked by the Audubon Society. You can refer to their article "No 5G Radio Waves Do Not Kill Birds" on their website www.audubon.org.

In conclusion, to date, no significant detrimental effects on humans or animal health have been found as a result of the deployment of 5G technology. 5G technology will indeed consume three times more energy than LTE technology because of the number of additional base stations that will be deployed. Still, equipment vendors have countered the effect of this by designing the equipment to make use of alternative renewable energy sources and making use of software-defined architectures. Several myths around 5G technology have been dispelled in one way or another, including the myth that 5G is radioactive and causes cancer. In fact, a recent document from the SDXCentral website (www.sdxcentral.com) made the point that while cell towers and cell phones do emit a small amount of radiation, so do bananas!

G Debbo | SAIEE President 2019
Pr. Eng | FSAIEE

INDUSTRY AFFAIRS

SAIEE Council Partners Evening

The SAIEE recently treated their Council Members and partners to a cozy dinner evening at Bellgables Country Restaurant, nestled in the Cradle Moon Nature Reserve. This annual tradition, instituted about 30 years ago, is the SAIEE's way of giving back to the council members who volunteer their services to the cause of the SAIEE - to provide leadership to the electrical/electronic engineering discipline.

Anton & Gerda Geyer

Nicolas & Janet West

Tom & Barbara Eichbaum

Anlia & Jan-Harm Pretorius

Willie & Rika Cronjé

Elma & Jan de Kock

Prudence Msdiba & Sabelo Mchunu

Stan & Margaret Bridgens

Gladys & Jacob Machinjike

Patrick O'Halloran & Grace Horrocks.

Janet & Mike Barker

Fuluphelo Nelwamondo

Maryka & Clinton Carter-Brown

Dawie & Sy Gourrah

George Debbo & Sharron Stobia

Angus & Michèle Hay

Pascal Motsoasele

Mzwandile & Refilwe Buthelezi

Tshego Cornelius & Kgomotoso Sethlapelo

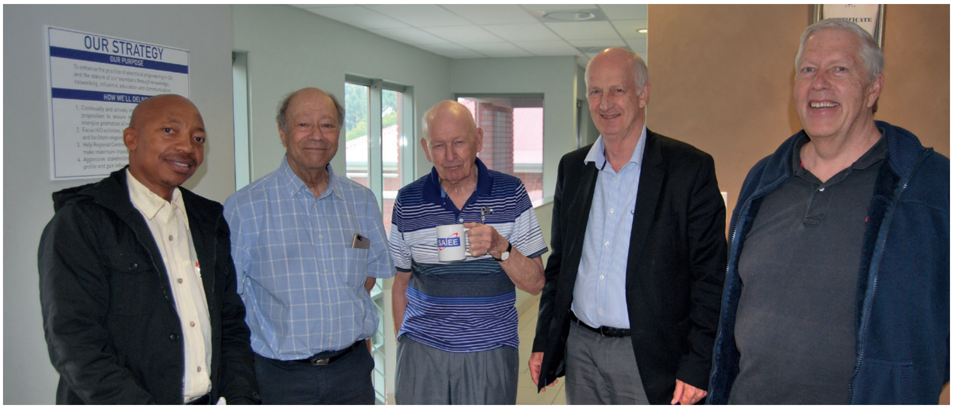
Selloane Matikane & Leanetse Matutoane

Kamogelo & Teboho Machabe

Max Clarke celebrated his 94th birthday at SAIEE Head Office

From left: Max Clarke, Gail Gordon, Mike Little and Neville Morrison.

From left: Sue Walker, Max Clarke and Androzette Muller.



From left: Leanetse Matutoane, Peter Heim, Max Clarke, John Gosling and Oliver Gerondeanos.

14th of February Max Clarke, Chairman of the Historical Section, celebrated his 94th birthday. This spritely young man decided to spoil the SAIEE office staff with cake to share in the celebratory milestone.

Max was joined by members of the Historical Section who shared with us anecdotes of his career which had us in stitches.

We wish to be entertained by Max for many years to come. Happy birthday uncle Max!

SAIEE welcome new Fellows

From left: George Debbo & Prof Simon Connell

From left: George Debbo & Claude Agostinetto

From left: George Debbo & Prof Jerry Walker

From left: George Debbo & Pascal Motsoasele

From left: George Debbo & Dr Dave Nichols

At the February 2019 SAIEE Council Meeting, President George Debbo inducted new SAIEE Fellows and handed each a Fellowship Certificate. They are Prof Simon Connell, Claude Agostinetto, Prof Jerry Walker, Pascal Motsoasele and Dr Dave Nichols.

Debbo also took this opportunity to welcome our newest SAIEE Member to the fraternity, Constance Nghonyama, who qualified with a National Diploma, Electrical in 2019 at the age of 65.

New range of game-changing electrical accessories by electricians, for electricians

In a world where products are moving from standardised to customised, today's consumers want high quality products that meet their specific requirements. Electrical accessories are no exception and Schneider Electric has risen to the challenge with the innovative Iconic™ range of modern electrical accessories set to turn the wiring devices market upside down.

With this range, Schneider Electric offers electricians and homeowners a host of sleek switches, dimmers, sockets, USB chargers, and motion sensors which are sure to shake things up. The new range is easy to customise, easy to install and pleasing to the eye, with a wide choice of stylish and elegant skins ready to fit into your environment.

Designed for electricians by electricians, Iconic electrical accessories raise the bar for extremely safe, long-lasting and reliable switching mechanisms. There are a variety of built-in features that are unique to the range, making it the obvious choice for a quality installation and unrivalled customer satisfaction.

"Iconic is truly next generation, loaded with clever features like a locking bar and in-line terminals", says John Raptakis, Offer Manager, Home and Distribution Division for Schneider Electric. *"With the Iconic range, we are helping contractors and electricians deliver the best to their clients now and into the future."*

Innovative features

This innovative new range features a locking bar which makes it easy to change the orientation of the mechanism, resulting in a fast and easy installation. It also makes the switch safer for the end-user. To prevent cases of users unintentionally pushing back the switch inside the wall, Schneider Electric engineers have invented the mech lock which allows electricians to secure every switch mechanism in the grid. *"This is another way we are helping electricians and homeowners. By adding this measure, electricians can be rest assured that their installations are reliable, and they won't be called back to site facing unhappy customers,"* says Raptakis.

Furthermore, when removing the mechanism, there is no risk of damage to the grid. The locking bar can be locked or unlocked with just one push of a screwdriver. The in-line terminals for easy screw access and faster termination, are yet another exciting innovation.

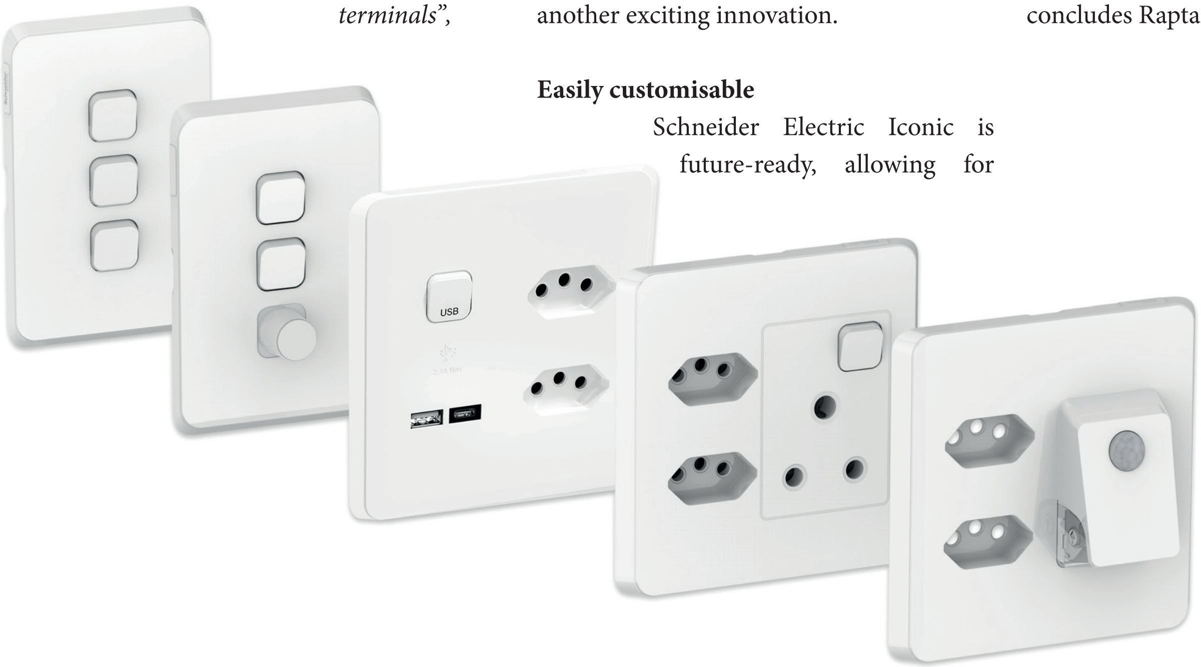
Easily customisable

Schneider Electric Iconic is future-ready, allowing for style and function updates in the coming years. The range offers game changing compatible modules and grids with changeable skins and dollies for unrivalled customisation. Whether it is a new installation or a retrofit, the aesthetics can be changed because the functional part of the switch is separated from the fascia. This future proofs your installation and allows it to be customised according to your customers' tastes, any time.

Easy to install

One of the slimmest ranges on the market with a 7 mm switch profile and 9 mm socket profile, your standard mounting accessories can still be used with Iconic accessories. Additionally, clear markings display instructions on the mech grid to facilitate installation for electricians such as strip length. The innovative safety flaps display warnings to advise customers against opening the unit or attempting to undo the screws.

"Schneider Electric engineers have really knocked this one out the park, ensuring that we continue to deliver a range of reliable, innovative and unrivalled electrical solutions. With the Iconic range, we are solving problems you didn't know you had," concludes Raptakis.



MICROSOFT LAUNCHES NEW COMPUTER LAB

In response to the serious need for greater student-centric IT facilities, Microsoft SA launched a new computer lab at the Afrika Tikkun Zolile Malindi Centre of Excellence in Cape Town recently.

As the Fourth Industrial Revolution looms and we head into an uncertain technologically driven future, it's essential that young people are exposed to as much as possible, and that learning evolves to include digital advancements.

As an organisation focussed on youth education, empowerment and leadership, Afrika Tikkun is committed to equipping their young people with employable skills for the changing careers of the future. And now, with the help of Microsoft SA, they are on a solid path to achieving just this.

The Zolile Malindi Centre of Excellence in Mfuleni, Cape Town has been using limited resources for some time, significantly affecting the learners in their Child and Youth Development (CYD) and Career Development Programmes (CDP).

Computers at the centre previously serviced over 3,500+ young people between 2011 and 2019.

"Until recently we had two computer labs that could only accommodate 44 learners at a time," says Lizo Madinga, the centre's General Manager. *"This wasn't sufficient for all the learners that the centre caters to daily and often we had learners pairing up at desks taking turns throughout lessons. In addition, the computers were outdated and the hard drives had started to fail. This is where Microsoft stepped in and generously outfitted a new computer lab at the centre."*

As a result, the centre is now able to accommodate 60 learners per class in a much larger and visually appealing space, giving meaning to the principle of *"leaving no-one behind"*.

As classes grow and eLearning and IT skills become more crucial these new PC's are expected to empower thousands more students over many years to come.

Compact infrared camera for laser machining processes

Temperature measurement in processes where lasers are used, provides major challenges for infrared measurement technology. For example, the camera needs to be insensitive to the laser's scattered light. INSTROTECH, local representative of Optris – leading manufacturers of non-contact temperature measurement devices – has launched Optris PI 08M, ideally suited to these kinds of applications. It has a very narrow-band spectral sensitivity of 800 nm. Most industrial machining lasers, such as for example NIR or CO2 lasers work outside this range, so that the detector is protected against scattered laser light, without additional filters.

Precise temperature measurement

With the wavelength range of 800 nm, the PI 08M has an additional advantage, as the measurement error is minimal with unknown or changing emissivity. At high temperatures it is only 1.5% of the measuring value; below 1,500 °C just 1%. The measuring range is from 575 °C to 1,900 °C. The interior of the IR camera

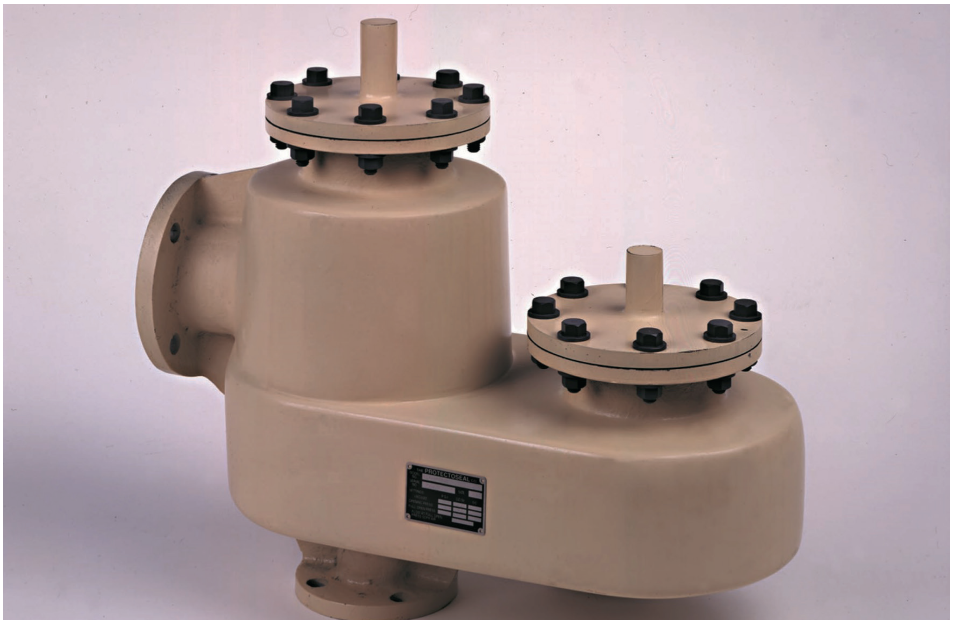
Understanding fibre-reinforced plastic vents

Liquid storage tanks are a crucial part of the chemical industry. With different types of chemicals having different characteristics and behaviours – it's important to find the right venting solution for each chemical.

Liquid storage tanks play a significant role as part of the plant in the chemical industry. The use of liquid storage tanks for the storage of flammable or combustible liquids is a common practice in the chemical industry. Liquid can be stored as a raw material, an intermediate product or a final product of the chemical process.

Lavenda Sekwadi, Process Engineer for Energas, says it is important to note that the different types of chemicals have different characteristics and behaviours when stored in these tanks. Therefore, breathing of liquid storage tanks is very significant as a safety measure against some of the common accidents – such as fire and explosions – associated with the storage of chemicals.

"Storage tanks have different sizes, liquids vaporising at different rates and liquid discharge rates and inflow rates. API 2000 standard is primarily used for determination of the suitable sizes of the safety equipment (mainly pressure-vacuum vents and emergency vents)," says Sekwadi.



COMPATIBILITY MATERIALS

The compatibility of the tank safety equipment and the medium stored is of paramount importance as it affects the service life and the performance of the equipment.

For hazardous vapours (for example, sulphuric acid), the typical materials such as carbon steel, aluminium, stainless are not compatible.

"Fibreglass Reinforced Plastics (FRP) are employed in applications of hazardous vapours due to their ability to withstand corrosion – this is due to their highest level of resistance to chemically hostile environments, yet extremely rugged and durable in construction," says Sekwadi.

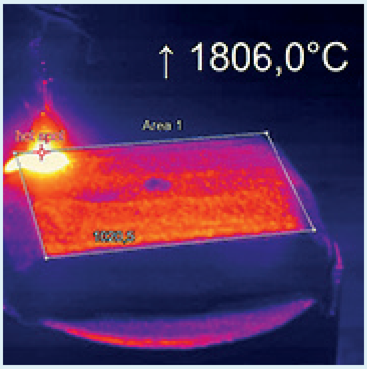
Such applications of hazardous liquids are typically found in petroleum, petrochemical, pulp and paper, waste treatments and food and beverage industries. FRP's eliminate the need for exotic metal construction.

holds a dynamic CMOS detector with an optical resolution of up to 764 x 480 pixels, which can be operated with a maximum frame rate of 1 kHz, making it highly suitable for very fast processes. A real-time analog output provides an output signal of 0 to 10 V. Here the temperature is averaged over an area of 8 x 8 pixels - the position of the area can be selected freely.

Optimum integration into the application

The new PI 08M can be integrated very easily into a wide range of applications, such as laser welding, laser soldering or laser hardening processes, where temperature plays a key role. The PI 08M comes with a Software-Development-Kit.

Contact INSTROTECH for more information on Optris PI 08M for laser machining processes, and for temps of up to 1900 °C, on 010 595 1831 or sales@instrotech.co.za



Cisco Forecasts on 5G

According to the new Cisco Annual Internet Report, 5G will support more than 10% of the world's mobile connections by 2023. The average 5G speed will be 575 megabits per second, or 13 times faster than the average mobile connection. With advanced performance capabilities, 5G will deliver more dynamic mobile infrastructures for AI and emerging IoT applications including autonomous cars, smart cities, connected health, immersive video and more.

For the past 50 years, each decade introduced a new mobile technology with cutting-edge innovations. Mobile bandwidth requirements have evolved from voice calls and texting to ultra-high-definition (UHD) video and a variety of augmented reality/virtual reality (AR/VR) applications. Consumers and business users worldwide continue to create new demands and expectations for mobile networking. This ongoing trend is clearly highlighted by the adoption and use of mobile applicatons. Social networking, video streaming and downloads, business productivity, e-commerce and gaming will drive the continued growth of mobile applications with nearly 300 billion downloaded by 2023.

"What we are seeing from our research is a continuous rise in internet users, devices, connections, and more demand on the network than we could have imagined," said Roland Acra, Senior Vice President and Chief Techonology Officer at Cisco. "The insights and knowledge gained by our Annual Internet Report are helping gobal businesses, governments and service providers prepare and secure networks for the ongoing growth in connections and applications. Strategic planning and partnerships will be essential for all organizations to capitalize on their technology innovations and investments."

Cisco Annual Internet Report Highlights (2018 – 2023)

The Cisco Annual Internet Report covers mobile, Wi-Fi and fixed broadband networking with quantitative projections on the growth of users, devices and connections as well as network performance and relevant trends over a five-year forecast period (2018 – 2023).

1. Global mobile and internet user projections by 2023

- More than 70 percent of the global population (5.7 billion people) will have mobile connectivity (2G, 3G, 4G or 5G).
- 66 percent of the global population (5.3 billion people) will be internet users.

2. Global devices and connections projections by 2023

- There will be 3.6 networked devices/connections per person and nearly 10 devices and connections per household.
- Nearly half (47%) of all devices and connections will be video capable.
- Machine-to-machine (M2M) connections that support a broad range of IoT applications will represent about 50% (14.7 billion) of total global devices and connections.

3. Global mobile projections by 2023
- 45% of all networked devices will be mobile-connected (3G and below, 4G, 5G or Low Power Wide Area [LPWA]) and 55% will be wired or connected over Wi-Fi.
- Global 5G connections will be 10.6% of total mobile connections, compared to 0.0% in 2018.
- By 2023, global LPWA connections will be 14.4% of total mobile connections, compared to 2.5% in 2018.

4. Global Wi-Fi projections by 2023
- Global Wi-Fi hotspots will grow four-fold from 2018 to 2023. There will be nearly 628 million global public Wi-Fi hotspots, up from 169 million in 2018.
- Global Wi-Fi6 hotspots will grow 13-fold from 2020 to 2023 and will be 11% of all public Wi-Fi hotspots.

5. Global network performance projections (mobile, Wi-Fi, and fixed broadband) by 2023
- Average global mobile connection speeds will more than triple from 13 Mbps (2018) to 44 Mbps (2023).
- Average global Wi-Fi connection speeds will more than triple from 30 Mbps (2018) to 92 Mbps (2023).
- Average global fixed broadband speeds will more than double from 46 Mbps (2018) to 110 Mbps (2023).

6. Global cybersecurity trends from 2018 to 2019
- Globally, the frequency of DDoS attacks increased by 39%.
- Globally, the peak attack size increased 63%.
- The average DDoS attack size is 1 Gbps (23% of attacks are greater than 1 Gbps); there has been 776% growth in attacks between 100 Gbps and 400 Gbps.

CISCO ANNUAL INTERNET REPORT FORECAST

The Cisco Annual Internet Report is a global, regional and country level forecast/analysis that assesses digital transformation and is developed by the same analyst team that created the Cisco Visual Networking Index (VNI) Forecast. The report covers fixed broadband, Wi-Fi, and mobile (3G and below, 4G, 5G) networking.

Quantitative projections are provided on the growth of internet users, devices and connections as well as network performance and new application requirements.

Qualitative analyses and assessments are also provided in four strategic areas: applications, security, infrastructure transformation, and empowering employees and teams.

Download the full report here.

The role of the cloud aggregator

– extracting more value out of your cloud environment

According to Andre Schwan, Deal Solutions Manager at T-Systems South Africa, many companies embark on their cloud journey, only to regret their early decisions and approaches further down the line.

“This is largely because the problem statement and the expectations that were created at the beginning of the cloud transition were incorrect. The result is that either the performance is not as expected, or the business case fails,” says Schwan.

Research by McKinsey shows that this is mainly due to the fact that companies fall into the trap of confusing simply moving IT systems to the cloud with the transformational strategy needed to get the full value of the cloud.

“It is important that enterprises understand their current baseline and how it all fits together, including data movement patterns and application use patterns. They must also understand which business processes their applications underpin,” says Schwan.

He advises that organisations start with a business strategy and design that supports these processes and applications. *“Just moving what you have into the cloud will not achieve the business value expected or opportunity. It is essential that we design for business outcomes and use all options available to realise these outcomes in the most effective manner,”* he says.

Enterprises must overcome two main obstacles. The first being legacy IT that was designed and built in the traditional IT paradigm, which is not suitable to the cloud. Simply moving legacy apps does not make them more dynamic.

“The second is that the skillsets required to design, build and run systems in the cloud is significantly different from that of traditional IT. In most cases, a re-design of the organisation is needed, and staff need to be reskilled,” says Schwan.

Sonja Weber, Lead Delivery Solution Manager at T-Systems South Africa, notes that the impact of a lack of organisational support and readiness has been widely underestimated when it comes to successful cloud migration.

"No business case will survive the resistance of the people meant to use it, which means that user adoption is a major driver for getting value out of your cloud environment," she says.

Furthermore, she says that the *"lift and shift"* approach only works for applications that are suited to it. For most legacy applications, enterprises will probably end up with more cost, less performance and a more complex environment to manage.

"The whole point of digital transformation is to evolve to a simpler state that is more agile and offers the business more opportunities by capitalising on modern automation and analytical capabilities and opening up new channels to market," says Weber.

"The business threat that we're countering is that if we don't grab an opportunity, someone else will and more often than not, it is small new companies, who are by nature of being new, are normally digitally native."

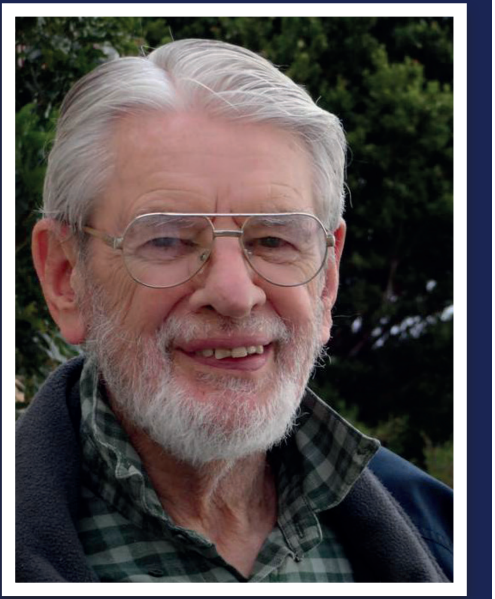
Weber says organisations also need to understand that they will probably have a hybrid solution for some time, so when selecting technology platforms, they need to consider interoperability, data transfer costs and a private cloud design.

"Be very selective when it comes to your cloud provider – multi-cloud providers with a track record of managing complex environments are your best ally in this journey, especially in the early stages when you're still adjusting your origination," she says.

In addition, organisations should avoid technology or platform lock-in, and rather adopt industry standards and platforms that use these standards.

"Do not make once-off decisions in isolation. Start with a sound digital transformation strategy and let that lead your decisions," Weber concludes. wn

OBITUARY - BRUCE JACKSON



BRUCE JACKSON
1930 - 2019

It is with great sadness that we recorded the passing of Wilfred Bruce Jackson in September 2019. He was a long-standing member of the South African Institute of Electrical Engineers and served as President for the 1988 term.

Bruce was born on 25th April 1930 in Durban. The family moved to Johannesburg, and he attended King Edward VII Junior and High Schools matriculating in 1947 with distinctions in Mathematics and English.

He attended Wits University and graduated with a BSc in Electrical Engineering in 1951. He received post-graduate practical training at BTH in Rugby, UK, in the 1952-53 period.

On his return to South Africa Bruce joined the Rhodesian-Congo Power Corporation and worked on the Copperbelt for some time. One of his projects was the Kariba line connection. In 1960 he was offered a position with Anglo American in their Salisbury office, and 1968 moved to their Lusaka operations.

In 1970 he was transferred to the Anglo American Corporation Head Office in Johannesburg and worked in their Consultants team, becoming a Senior Divisional Engineer in 1977. He travelled extensively for the company, including making visits to the UK, USA and South America. He was the co-presenter of an IEEE International lecture on the subject of "Electricity in the South African Mining Industry".

Bruce retired in 1990 but continued to consult in various countries including Chile where he spent many months on the Collahuasi mine working on the electricity systems with Chilean engineers, with whom he had developed a good rapport.

His membership of the SAIEE started in 1950 when he was admitted as a Student Member while still at Wits and then progressed through the membership ranks, finally becoming a "Fellow" in 1973. He was a long-standing member of the Historical Section and enjoyed working with the team up until his health prevented him from attending meetings.

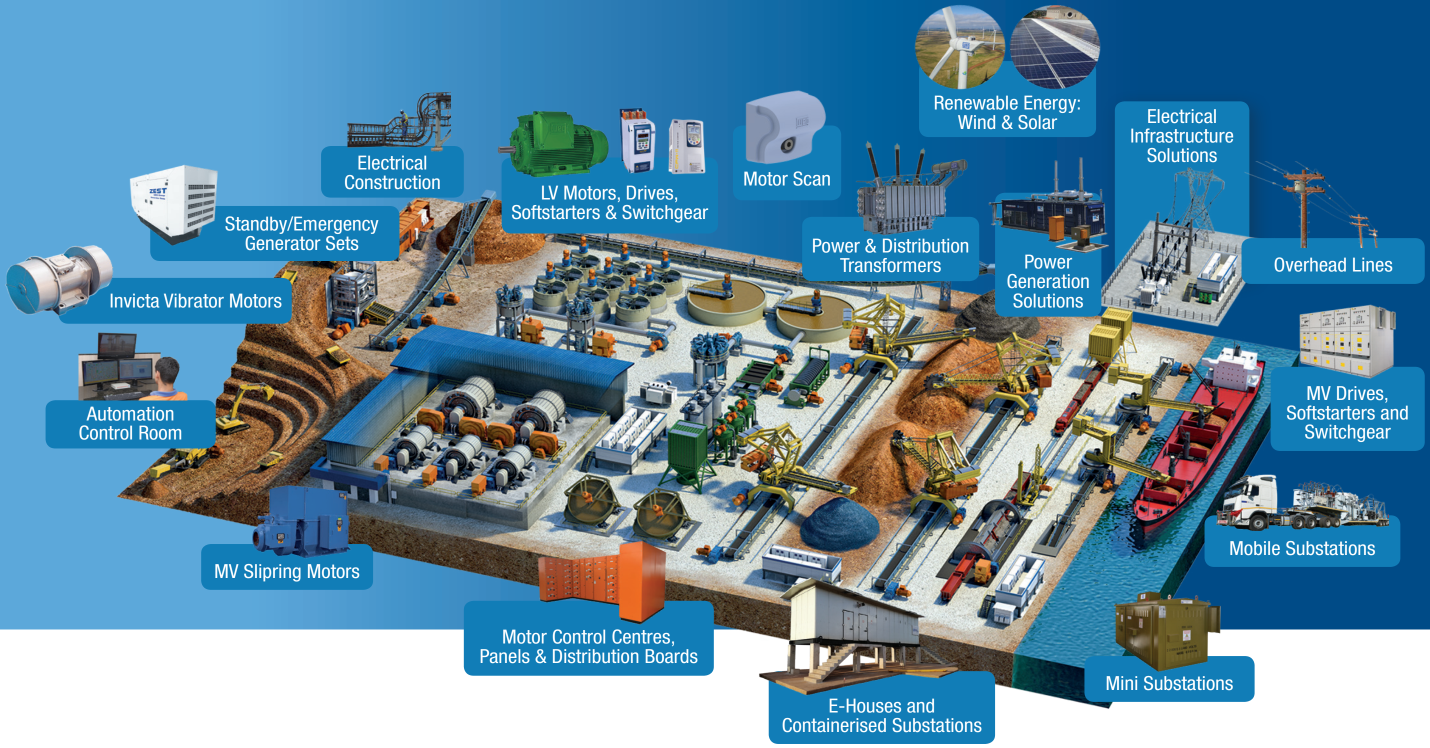
Bruce was passionate about steam engines and photography. Many family road trips were punctuated by stops to photograph substations and passing trains. He also designed and built the family holiday cottage in Kleinmond in the Western Cape.

He leaves his wife of 61 years, Heather, and their four children and six grandchildren, to all of whom we record sincere sympathy in their bereavement on behalf of the SAIEE Executive and all members who knew him as a friend. wn

BY I MAX CLARKE
CHAIRMAN I HISTORICAL SECTION
SAIEE

RELIABLE PRODUCTS & SOLUTIONS

for the entire mining sector.



Renewable Energy: Wind & Solar
Electrical Infrastructure Solutions
Electrical Construction
LV Motors, Drives, Softstarters & Switchgear
Motor Scan
Power & Distribution Transformers
Power Generation Solutions
Overhead Lines
Standby/Emergency Generator Sets
Invicta Vibrator Motors
Automation Control Room
MV Drives, Softstarters and Switchgear
Mobile Substations
MV Slipring Motors
Motor Control Centres, Panels & Distribution Boards
E-Houses and Containerised Substations
Mini Substations

Zest WEG Group is able to offer a range of standard off-the-shelf products as well as end-to-end energy solutions by leveraging innovative best practice engineering and manufacturing capabilities.

All products are engineered to facilitate a safe and reliable mine and plant with operational stability and the highest possible production levels as an objective. Reduced maintenance, energy efficiency and ease of serviceability assist in lowering the total cost of ownership for the mine.

Level 1 BBBEE

CIDB Grades 9EP & 6EB

ISO 9001:2015

African Distribution

ZEST WEG Group

www.zestweg.com
Tel: 0861 009378

Introducing:

SAIEE “Charged” Reward Programme

As an organization that is over 110 years old, the SAIEE has, in most cases, relied on its members volunteering their time to benefit the entire SAIEE membership. This has been in the form of technical talks, articles in the wattnow magazine or attending a Centre committee meeting, the list goes on. In return, members would be faced with an opportunity to avail themselves to these initiatives as part of their benefits. Attendance of these events has been the single most important selling point of the SAIEE as a voluntary association, viz. the ability to network with industry experts in any and every field of Electrical Engineering.

As the SAIEE, we have realised that we need to enhance our value proposition to our members, and we have been exploring a number of initiatives in order to achieve this objective:

- Membership base segmentation: Each and every member is at a certain stage of their career and has needs that are reflected by that stage. We have gone through the segmentation exercise and assigned each segment’s needs accordingly in order to service our members better. This means that each of the segments ought to have a value proposition that speaks to them. More details to follow in subsequent issues of wattnow.
- Introduction of SAIEE Technical Talks (ST-Talks): One of the value propositions of the SAIEE is continuous professional development. We have introduced ST-Talks as a vehicle to put emphasis on this important value proposition (CPD).
- SAIEE membership requirements: We have re-visited at the stringent requirements for becoming an SAIEE member and the results are shown in the revamped membership application forms that obviates the need for a professional seconder to provide their signature when applying for Student, Associate and Member grades of membership.
- Closer relationship with Centres: We have also decided to forge a closer working relationship with SAIEE centres in order to service our membership base better.

As part of our repositioning journey and enhancing our value proposition, we are proud to introduce a programme that incorporates all the above initiatives and incentivises you as a member. This is in the form of the “SAIEE Charged Reward Programme” which is aimed at rewarding members with points as they volunteer to participate in the day to day SAIEE activities. All SAIEE members will have the opportunity to gain “Charged” points through interacting with and being an active member of the SAIEE. A list of events that will enable members to accumulate points are listed in the table below.

Accumulated Charged points will be valid for 5 years and can be redeemed for activities listed in the table below. We are excited that, as a member of the SAIEE, your involvement and interaction with the SAIEE will finally be rewarded.

Herewith below are the “Charged” points accumulation and redemption events that members can look forward to:

Here’s looking forward to your participation in SAIEE and charging your points! wn

#	“CHARGED” POINTS ACCUMULATION EVENTS	“CHARGED” POINTS REDEMPTION EVENTS
1	Attend committee meeting	Receive 1-hour mentoring session
2	Attend section meeting	Attend 1-day CPD Course
3	Attend centre meeting	Attend 2-day CPD Course
4	Attend council meeting	Attend 3-day CPD Course
5	1/2 -day Technical talk	Membership fees
6	1-hour Technical talk	
7	Fees paid by 31 March	
8	Full article published in wattnow	
9	Successful referral of new member	
10	Conduct 1-hour mentoring session	

CHARGE REWARD PROGRAMME

MEMBER LOYALTY

We appreciate
our Member's
support
for 110 years

REWARD

A unique reward
programme
exclusive to
SAIEE Members

FEEDBACK

We received
your feedback
and we listened
to added benefits

LOYALTY CARD

Earn Charge Rewards
by attending events,
courses or writing
articles

SATISFACTION

We want you,
our Valued Member
to feel satisfied
when working with us

LOYALTY PROGRAM

Redeem your
Charge Points
towards
CPD credits

QUALITY

We guarantee
top quality events,
courses, and
services

SERVICE

We are here
to serve you,
our Valued Member
better

RESPECT

We respect you
and want to see
value for your
hard-earned money

SUPPORT

We are here
to answer any
queries you
might have

For more information:

Visit your Membership Porthole on the SAIEE Website:
www.saiee.org.za

Alternatively, call Connie on 011 487 3003.

SAIEE
CHARGE
rewards programme

As devices are undeniably getting smarter all the time, the question arises: Are we keeping pace with technological progress in terms of being "smart" enough to derive maximum benefit from these devices without suffering repercussions? The rise of smart devices, which until a few years ago seemed like nothing more than a hopeful vision of the future, has occurred so quickly that the technology has become part of our everyday lives almost without us noticing the change.

BY: TONY ANSCOMBE
JAKE MOORE
LYSA MYERS
CECILIA PASTORINO
CAMILO GUTIÉRREZ AMAYA

The gradual but persistent integration of technology into objects we use all the time is likely to change and impact social customs in ways that are yet to reveal themselves.

Every year experts decide which aspects of cybersecurity and privacy seem likely to present some of the critical challenges for the coming year. We review various cybersecurity issues with implications for people, governments and companies, as well as general concepts like privacy, democracy, digital transformation, and much more.

All these issues are intimately connected to user privacy. Lysa Myers looks at how attitudes have changed since the Cambridge Analytica scandal, the implementation of legislation at various levels, and the likely implications for companies and governments resulting from user disenchantment about data privacy.

The trend for all things "smart" has not only reached the objects people use every day but has begun to take importance on a larger scale. There are now many examples of smart buildings around the world, and there are expectations that

Cybersecurity Trends for 2020

more and more cities will soon become the latest in the long line to incorporate smart technology. However, could this lead to new types of attacks combining the digital and physical realms? Is cybersecurity advanced enough to ensure that these implementations can be carried out without putting users, citizens, and organisations at risk?

This paradigm shift is perhaps most visible in the digital transformation processes currently being implemented by many companies around the world, challenging IT teams to keep pace with all the technological change taking place. Camilo Gutiérrez Amaya dives deep into this issue, looking at the likely challenges for the corporate world soon.

One of the best tools to be prepared for the future is to stay informed, so why not read this article to find out what we can expect to see in 2020 and over the next few years?

2020: THE FOG THICKENS

”20/20” refers to perfect vision, but 2020 might just be another blurry year for the democratic process. What may stand in the way of our making informed decisions supported by facts?

As we head into 2020, there is one prediction from this entire Trends report that is probably guaranteed: there will be claims of meddling and manipulation in election processes during the year.

These issues are complex, and while it is easy to point the finger of suspicion that there was interference, it can be difficult to prove beyond a reasonable doubt. The complexity begins due to there being several types of intervention that can cause election results to be shepherded to a particular outcome or not actually to represent the vote cast by the electorate. When looking at online or cyber-issues, these range from fake news

Cyber Security Trends for 2020

continues from page 23

and voting machine rigging, all the way through to targeting parts of the swayable population with biased information.

The 2016 US presidential election was shrouded in post-election controversy with claims of fake news, interference from other nation-states and the potential hacking of the voting process itself. Further, there are claims that the Brexit referendum in the United Kingdom was biased due to meddling and that in South America disinformation spread through WhatsApp possibly affected the outcome of the Brazilian elections. How can we expect voters to have confidence in the democratic process when all this is clouding the issue?

FAKE NEWS

The Collins Dictionary awarded this term Word of the Year in 2017. Its rise to fame was mainly due to the 2016 US presidential election and the continual claims by candidates that articles appearing in the media and stories spreading on social networks were not factual. The meaning of the term is self-explanatory. It refers to the sensationalism of false information being disseminated under the guise of news reporting.

In the wake of the election, Pew Research surveyed perceptions about fake news. The outcome was startling, with 88% stating that Americans are significantly or somewhat confused about basic facts due to fake news.

Ofcom, the UK's media regulator, issued a report stating that half of UK adults receive news through social media sites, with 75% of these saying this includes Facebook as a source. This is although social media were not rated as impartial, trustworthy or accurate. The TV remained the most used, with 75% of adults polled listing it among their news sources, but the influence of social media should not be underestimated and is here to stay.

There are different types of fake news: for profit, for political gain, for crime, hoaxes, and viral pranks. The types may even be combined: creating a trick that puts a political candidate in a bad light may create a political gain, and with the "right" advertising being displayed around the fake news story it may also generate a nice profit. If the creators of such a campaign could be identified, they are likely to have committed a crime, but identifying the source is not always possible.

In the run-up to the 2019 UK general election a research organisation, Future Advocacy, and a UK artist, Bill Posters, created a fake social media video, or so-called "deep- fake". The video shows the leading candidates appearing to endorse each other for prime minister. This example of fake news was created in an attempt to demonstrate the difficulty in identifying real vs fake and that democracy is potentially being undermined.

But this issue is not new. I frequently stand at the check- out of the local supermarket and read the cover headlines of the magazines: celebrities splitting up, the UK Royal Family all getting divorced, or aliens landing in the car park.

The readers of such magazines hopefully know the stories are fake when they choose to purchase them, but when we switch to internet stories, which are spread quickly to much broader audiences, it's not so easy to tell the good from the bad.

Some social networks and search engine providers are responsibly attempting to combat the issue, under pressure from political and public outrage. For example, Twitter has recently announced a ban on all political advertisements about candidates, elections and hot policy issues ahead of the 2020 US presidential election. But this is a complex topic. It has even been referred to as freedom of speech infringement - if someone is denied the ability to post or place ads with a particular viewpoint. In reality: as fake news spreads, then page impressions increase and advertising revenue is gained, and not all actors displaying advertisements on websites are responsible.

The issue is the speed of dissemination of the disinformation – a story appearing in the next hour will spread quickly, primarily if the creator promotes it and spreads it from multiple accounts and networks at the same time. The companies responsible for the platforms have innovated detection methods and built reporting mechanisms to, when possible, automatically detect, or to allow users to report, fake news. Relying on reporting, though, is a flawed solution. As the disinformation has already been spread, many users will likely not take the extra step to report it. Those who have seen (and perhaps been influenced by) the disinformation are unlikely to become aware of its retraction.

As a cybersecurity professional, I consider fake news that damages democracy to be malicious – much like malware intrusions on your devices. There needs to be a more robust technological solution to stopping fake news from spreading when it first appears and killing it at the source in the same way that antimalware products detect

zero-day exploits. With the adoption of machine learning, some innovative solutions are likely to come to market that will detect and suppress fake news.

Education is also a longer-term solution to this issue, but the results are slower. In July 2019, the UK government published new safety guidance for schools; part of this updated policy states that every child will learn about confirmation bias and online risks as a compulsory part of the curriculum. This will help to enable pupils to spot techniques used for persuasion and to identify fake news and dangers, but it will take many years for an entire generation to understand what may be real or fake. However, understanding what is real or fake will give the next generation confidence in the democratic electoral system. More governments are likely to take this proactive stance and add this to their education policies. If they don't, then they should.

Targeted disinformation and propaganda
The Cambridge Analytica abuse of personal data shocked the world but did not surprise those of us who have always said – "if you aren't paying for it, then you are the product". For example, each Facebook user in the US and Canada generates more than US$130 for the company every year. The scandal eventually broke when three news organizations combined resources to cause enough traction for anyone to notice – after more than two years.

Fast forward a little in the story, and Facebook was fined US$5 billion by the US Federal Trade Commission (FTC) for its part in the data breach. I am not sure we can describe it as a breach, though, as documents now in the public domain show that Facebook knew what was going on – it was more abuse of trust for financial gain. On the day the FTC fine was announced Facebook's share price went up – it's clear the market either expected the penalty to be harsher or it understood that the deal struck with the FTC is actually in Facebook's favour.

The weaponisation of information, be it disinformation or propaganda, is set to continue and will take many different paths as the benefactors explore and adopt new methods to attack democracy or to make money. At the centre of this invasive and stealthy issue is - data mining - something we can't see and for many people, it is hard to comprehend. The data points available about individuals, given that the majority of people overshare on social media are extensive. The ability to adjust and manipulate the message sent to an individual is driven by technology, unlocking the power to individualise the messages sent to millions of people, all at the click of a mouse.

THE VOTING PROCESS

Whether the ballot is valid is not a new issue and relates to both pen-and-paper and electronic voting systems. Besides, it's an issue that's unlikely to be resolved anytime soon.

Many states in the US have spent millions of dollars on upgrading systems that will be used in the 2020 elections. One state, Pennsylvania, has benefited from US$14.5 million to update electoral systems, but even the new policies may be vulnerable. This is because the underlying operating system, Windows 7, which – unless a fee is paid – will no longer receive patches from Microsoft once this version of the operating system reaches its "end of life" in January 2020, 11 months before the 2020 US presidential election.

At the DEF CON 27 hacking conference in August 2019, there were real-time challenges to find vulnerabilities in election systems. One such experiment showed weaknesses in a ballot marking system. In this instance, the attacker had unrestricted physical access and direct connection to the devices, which should never to be the case in the real world. I hope someone might notice an attacker taking a terminal apart and connecting wires to it. This depends on devices being physically secured before the voting process, which, in some instances in previous elections, has not been the case. This may also lose relevance if the devices remain standalone and are never connected to a public network. While many devices theoretically could be vulnerable, it does not necessarily mean they can or will be exploited.

Technological solutions to both registration and voting will continue to have issues. We continually witness mass data breaches and system compromises in companies and government departments, so why would voting technology or processes be exempt from similar attacks? The good news is that the 2016 US presidential election heightened the awareness of possible vulnerabilities in the electoral systems being used, which directly resulted in the budget assignment as well as in the understanding of the need for the methods to be secure by design.

DE-MISTIFYING IT ALL?

For 2020, there will, of course, be numerous elections around the world and countless issues highlighted in their systems and

Cyber Security Trends for 2020

continues from page 25

processes, both technological and physical. The use of all the methods mentioned here is to be expected, but the question is: to what scale will they be used and will the interference change the outcome?

As voters and, hopefully, believers in democracy, we will pressure companies that distribute fake news and disinformation into detecting and ceasing the practice. However, large profits for allowing these practices, and lack of engagement by consumers, probably means that we will continue to see the flood of misinformation, be it mildly misleading or fantastically fabricated, keep flowing.

As with many questionable practices, such as the abuse of consumer privacy we have been subjected to over the last ten years, without government intervention and either regulation or legislation we will continue to a point where this practice can no longer be tolerated. Don't expect this to be in the next 12 months, though.

ML VS ML: CREATING SECURITY OR ATTACKING IT?

Advances in machine learning have brought considerable benefits to cybersecurity defenders. Still, the potential of the technology isn't lost on those who are looking to co-opt it for unsavoury ends.

Machine learning (ML) is, without a doubt, changing our lives. Increased computing power and the use of vast storehouses of data are rapidly enhancing our capabilities in multiple industries. Furthermore, if ML's distant cousin also known as true Artificial Intelligence (AI) takes off too and computers start "thinking for themselves", we're in for a wondrous future where a lot of what was once thought unimaginable could become possible. For now, though, self-sustainable AI still seems a long way off – whereas ML is making headway in one of the most exciting technological developments in history.

ML has also brought various benefits to cyber-defenders, including efficient scanning, faster detection, and improvements in the ability to spot anomalies. Cybersecurity companies have been taking advantage of the technology for years to enhance the detection capabilities of their products.

However, what if ML is misused to attack us and the systems we have made? It isn't hard to see why, and how, ML- or even AI-based malware might offer new and unique attack vectors – more potent than what we are currently used to. It's becoming clear, then, that ML will be an essential component in the future battle.

The technology has been advancing by leaps and bounds in other applications, too. In this Trends chapter, then, we will zero in on two ways in which ML algorithms could be weaponised to inflict harm.

FOOLING THE NAKED EYE

Surely you've seen one of the many convincing face-swapping videos that pop up, especially on social media. Such deep-fakes – doctored videos, audios or images that are designed to replicate the look and sound of real humans – can seem bafflingly legitimate and even shocking.

The deep-fakes may often involve celebrities or public figures apparently engaging in unexpected behaviour or saying something outrageous and not usually endorsed by them.

Deep-fakes are increasing in quality at an impressive rate, as seen in videos such as this one where a generated Barack Obama is made to say something the real one didn't answer. Moreover, when you take a look at Bill Hader being morphed effortlessly between Tom Cruise and Seth Rogan, it makes you realize that we may indeed have a significant problem on our hands unless this threat is addressed.

As with anything on the internet, the future could lead to this technology being used to damage public figures by making them appear to say whatever the creator wants, to damage society, or even to manipulate elections around the world.

Are we ready for the real impact of deep-fakes? With political scandals, pseudo nodes and almost unimaginable scenarios involving fake videos, we may be staring blankly at the beginning of an epidemic where the line between truth and lie may be impossible to determine.

What impact could deep-fakes have on society? In the light of the whole Cambridge Analytica scandal, in which data scientists were able to transform surveys and Facebook social graph data into a political messaging weapon via psychographic profiling, it seems that deep-fakes could speed up such transformations in influencing the public in elections. Will there come to the point where we don't even trust our own eyes and ears?

After FaceApp was literally plastered all over our faces and the groans and laughs rapidly died out, one question arose about the quality of such "wizardry" – might it one day create videos of people without their knowledge?

You need lots of data (many photos, videos and voice recordings) even to make a short deep-fake clip where the creator is in control of what is said. However, getting a significant amount of data on a non-public figure is quite a task in itself. But this is only thinking in a 2019 mindset, so what if we think next year or in a decade? Could it take just a short Instagram story or two for someone to produce a deep-fake that is believed by the majority of your friends online? This is very likely to happen, and there will be an app on our phones that will create such deep-fakes naturally and effortlessly.

Over the next decade, we will see some previously unimaginable fake videos appearing with public figures. Still, in time, these will include people closer to homes, such as our colleagues, our peers and our family members. No doubt porn sites will exploit celebrities in mysterious ways but, furthermore, cybercriminals will most definitely use such technology with great success to spear phish victims. Deepfakes could very quickly muddy the water between fact and fiction, which in turn could cause some of us not to trust anything – even when presented with what our senses are telling us to believe.

So, what can be done to prepare us for this threat? First, we need to educate people better that deep-fakes exist. People will need to learn to treat even the most realistic videos they see with a dash of scepticism. Also, and although painful, technology needs to develop better detection of deep-fakes. Although ML is at the heart of creating them in the first place, there needs to be something to act as the antidote, being able to detect them without relying on human intuition alone. Further, social media platforms need to recognize and address the potential threat as early as possible, as this is where deep-fake videos are most likely to spread and have a detrimental impact on society.

FOOLING THE ALGORITHM

Facial recognition is becoming more prevalent in current technology while also attracting some negative press. The implementation of facial recognition might not be 100% accurate yet, but again, it is only 2019, and things can only get better, right?

US cities have banned facial recognition being used by law enforcement after it wrongly identified 26 people as criminals who were law-abiding citizens. Research by the US Government Accountability Office found that FBI algorithms were inaccurate 14% of the time, as well as being more likely to misidentify people of colour and women. Furthermore, Microsoft has recently refused to install facial recognition technology for a US police force due to concerns about ML bias. This is where data have been input by humans, who tend to have various unintentional biases that influence the ML outcome.

There are arguments for facial recognition to be rolled out everywhere, with the millions of surveillance cameras already capturing our near-every move in public. For example, if you take facial recognition in its most basic form, it offers a way of collecting information on who has been where at a particular time. This is not a million miles away from a proper police officer who can recognize the local criminal on his or her patch (I know some police officers who can do this – they have incredible memories). So if facial recognition can become close to 100% accurate, then it may be watching our every move soon.

But if law enforcement knows the whereabouts of known criminals and suspects, what about criminals using the software to their advantage or stealing massive databases of confidential location data? It could be possible that the databases of people's faces could be compromised, meaning verification techniques such as facial or voice recognition could be fooled. Therefore, multi-layered security could be bypassed.

BOON OR BANE?

Complex ML-powered attacks are coming and let's not forget that some attacks are currently unfathomable due to the scale of the power they will use, so they have the potential to be bigger than we can anticipate. It is possible that attackers could weaponise ML, so we need to be ready for such attacks and be aware of how to combat them. ML-driven attacks will be able to learn what worked and what didn't work on the fly and then retrain themselves to bypass existing defences. As defenders, we need to understand how these ML-powered attacks will be created, what their capabilities might be and jointly tackle these future cyberattacks.

PRIVACY SEA CHANGE

Trust in our shared digital environment hasn't had a good run lately, and more and more people are on edge about safeguarding their digital data. What has been done and, even more importantly, what remains to be done for the tide to turn?

There's a particular "rite of passage" that happens when you've been talking about security and privacy for a while. You

Cyber Security Trends for 2020

continues from page 27

will make predictions about what the threatscape will look like in the future, and enough time will have passed that you can check to see how accurate your predictions were.

Mostly this happens on the near-future scale, such as this Trends chapter itself. Sometimes it's on the level of a decade or more. In my own experience with this phenomenon, I've noticed a few themes, most of which revolve around gaining or losing trust in our shared online environment.

As I was deciding what to write for this aritcle, I did an internet search for the phrase "year of privacy" plus a recent year, e.g. "year of privacy 2018". Headlines, including this phrase, can be a good indicator that the author thought a significant change was coming in regards to public perceptions of privacy, either positive or negative.

I think the first time I declared that about a year in review was in 2013, so I was curious how many times this had been reported. For every year from 2009 to 2015, those search terms returned more than a million results. After that, every year returned "only" eight-to-nine hundred thousand results.

Does this mean that 2016 was the year a lot of people collectively threw up their hands in disgust and abandoned all hopes of having control over their personal information? In some ways, this may have been the case; there seems to have been a certain sense of collective resignation. But it also looks as if we had reached a point where legislators and judges had started to catch up with the collective ire provoked by a constant barrage of privacy gaffes and breaches.

And that barrage has continued – in 2019 alone, we've seen quite a few countries and US states pass or implement new or expanded breach notification laws. We've also put forth data privacy legislation (though only in California has this legislation passed). Several notable fines have been levied on companies responsible for recent data breaches (though these are generally considered to have been merely slaps on the wrist). Executives from breached companies have had to testify before congressional hearings about these incidents.

Change has been slow, and arguably these efforts have not made much of a positive difference yet. The consensus among much of the US population is that they feel they cannot trust companies to protect their data, and this is the case in other countries as well. This situation, along with rampant fraud and other malignant traffic, has created a "low trust" environment in which we're increasingly interconnected but feel increasingly unsafe. When we have to approach everything on the internet with paranoia and scepticism, people feel understandably reluctant to engage with it.

In security, we often say it's best practice to "trust but verify": in the situation, we find ourselves now, distrust is rampant, and verification methods are full of holes. Until we remedy this, the internet will continue to be a scary place for most people.

So, what do we need to do to get out of this omnipresent sense of distrust?

DESIGN FOR PRIVACY AND SECURITY

One of the most important things that need to be done to improve customer trust is to create technology products and services that are designed with security and privacy in mind from the outset. The International Association of Privacy Professionals (IAPP) has created a document outlining its recommendations for the principles of Privacy by Design.

Much of what is covered is what one might expect: earn- ing trust through openness and transparency, enacting end-to-end security, creating policies that establish accountability for the business, and obtaining truly informed and ongoing consent from customers. But there is one more recommendation that is particularly notable, and which many people might find surprising: permitting full functionality while respecting privacy, in such a way that it benefits both the business and the user. Because the current model for so much of the internet is to use customer data as a product to be sold, this particular recommendation may require some genuinely innovative, "out of the box" thinking. Businesses that manage to accomplish this feat are likely to have a significant advantage in the marketplace.

IMPROVE AD TECH

While we're on the subject of selling customer data, we should also discuss the necessary improvements in advertising technology. In one survey, less than 20% of respondents found targeted ads to be ethical behaviour. Other reviews found that in some cases, targeted advertisements could backfire and cause less customer interaction.

Companies that use high-pressure sales tactics such as scarcity and social proof don't fare well either. A survey in the UK reported that almost half of respondents

MORE SPARKLING ACHIEVEMENTS

NEW BOOK TO BE PUBLISHED SOON!

Highlights of Electrical Engineering
Into the 21st Century from 2001

In October 2001 the **South African Institute of Electrical Engineers** published a coffee table book titled ***SPARKLING ACHIEVEMENTS.*** This highly successful volume was sponsored by **43** local companies and comprised **180** advertorial pages highlighting the achievements of these organisations from inception up to the year 2000.

The following list shows the number of pages sponsored by each organisation, in a range from 1 to 10 pages per sponsor: ***(In alphabetical order)***

ABB Holdings	**4**
ABB Powertech Transformers	**3**
ATC	**5**
Aberdare Cables	**4**
Alcatel Altech Telecoms	**5**
Allied Technologies	**1**
Alstom South Africa	**7**
Altech Card Solutions	**1**
Anglo Technical Division	**4**
Arrow Altech Distribution	**1**
CSIR	**5**
Circuit Breakers Industries	**1**
Conlog	**2**
Energy Measurements	**2**
Eskom	**3**
General Electric South Africa	**1**
Marconi Communications SA	**4**
Merlin Gerin SA	**2**
M-Net	**10**
MTN Mobile Telephone Nets	**10**
Multichoice Africa	**2**
National Data Systems	**4**
Orbicom	**3**
Potchefstroom University	**2**
Rand Afrikaans University	**2**
Reunert	**2**
Richards Bay Minerals	**2**
Rotek Engineering	**6**
SABC	**5**
Sentech	**3**
Siemens South Africa	**2**
Spescom	**2**
Spoornet	**8**
Stellenbosch University	**2**
Strike Technologies	**2**
Telkom	**3**
Transtel	**2**
UEC Technologies	**1**
University of Cape Town	**1**
University of Natal	**5**
University of Pretoria	**4**
University of the Witwatersrand	**4**
Vodacom Group	**8**

The second edition *MORE SPARKLING ACHIEVEMENTS* will include the following areas of electrical engineering activity:

Electrical Research Technology
Development and Standards
Telecommunications
Electrical Power and Distribution
Electrical Traction
Broadcasting
Information Technology
Mining
Radio Astronomy
RADAR
Medical electronics
Satellite technology

The cost of each page of advertorial will be R2000 and two books will be given free of charge, to each sponsoring company, for each group of four sponsored pages or part thereof. It is suggested that these books be placed in the company reception and CEO's office. The book will be advertised to the Institute's 6000 members and copies will be available at R350 each. The book is ideal to present to VIP visitors to this country who wish to learn about this country and what it has achieved.

We expect school and University libraries will value the book as an indication to students of what the profession of electrical engineering is all about. The new book will match the size of the first edition (240x320mm) and will consist of between 170 and 180 full colour high quality pages.

SAIEE

Cyber Security Trends for 2020

continues from page 28

said this behaviour would cause them to distrust the vendor. One third expressed an adverse emotional reaction (such as disgust or contempt). And 40% reported that these tactics would make them want to do the opposite of whatever action was being suggested.

The more often we're bombarded with high-pressure sales tactics and creepy surveillance tactics, the more quickly their (very limited) effectiveness declines. So many marketers have overused these strategies that they are likely limiting opportunities for other business- es as well. We need more effective ways to market that are honest, transparent, and respectful of our potential customers.

LEGISLATIVE CONSEQUENCES FOR BREACHES OF TRUST

Public sentiment about the trustworthiness of technology companies is unlikely to improve until it feels more likely they stand to lose at least as much as their customers do when privacy incidents occur. Although recent privacy-violation fines in the US and UK are breaking records, they represent a tiny drop in the bucket relative to the income that large businesses make from our data. Until these fines approach maximums that comprise a higher percentage of a company's revenue, they will continue to be more of a deterrent to small companies rather than to the mega-corporations.

Improve authentication and verification
Usernames and passwords simply aren't enough to keep people's identities safe anymore. This can decrease trust both for online account holders as well as that of people interacting with potentially hijacked accounts. Multifactor authentication significantly improves this situation, but very few people have adopted it yet. To change this, we'll need improved education about this technology, more companies offering incentives for using it, as well as continued improvements in its usability.

LET'S TURN THIS SHIP AROUND

I was first asked to predict the state of security on the internet a decade; hence, a little more than a decade ago. I said that I could see things going one of two ways: either we'd collectively wise up and things would be fine, or we'd continue to kick the can down the road, and the internet would be an "unusable slag heap". While no one would successfully argue that people are using the internet less than they did ten years ago, we also have to wade through a whole lot more internet detritus now than we did in the 2000s.

Those old-timers who have been working in cybersecurity since early days have been living in this state of distrust for decades. We saw the internet is built on shaky foundations that did little (if anything) to prevent misuse. Thankfully, we've also been thinking about – and talking about – what needs to be done to fix it. It's not too late to make meaningful moves to point privacy efforts back in the right direction. I hope that the appetite for necessary changes will continue to grow, so we can make those changes before my next decade in this business has elapsed.

SMART IS THE NEW SEXY:

From IoT devices to smart cities
With more and more towns dripping with intelligent technology that changes the way municipalities manage their basic operations and services, what do these developments mean for the security side of things?

Since 1994, when the very first smartphone appeared, the word "smart" has come to describe any kind of device gaining enhanced functionality through software and usually an internet connection. Then, in 1999, computer scientist Kevin Ashton became the first person to use the expression "Internet of Things" (IoT) - ever since expectations around the notion have been continually rising.

The 2010s have been notable for the revolution in the Internet of Things, and products such as watches, thermostats, lights, locks, cameras, toys, refrigerators, and other smart devices have now become a part of our smart homes, offices, buildings, and even cities.

Nowadays, the potential of IoT is not merely limited to the automation of tasks but includes analytical processes that can be carried out on the vast quantities of information generated. Smart structures make use of a variety of interdependent technologies, such as machine learning, various wireless networking protocols, cloud computing, and IoT sensors and devices. The vast amount of information generated by networked sensors and devices is stored in massive databases and processed using machine learning and big-data analytics for improving operational efficiency and developing a safe and productive environment.

Thanks to these kinds of features, such systems have come to be described as "smart" – but smart does not always mean safe. While technology keeps taking huge leaps forward, some of us wonder when, finally, security will be incorporated into these changes right from the design stage.

SMART BUILDINGS

Smart buildings use technology to control a wide range of variables within their environments, to provide more comfort and contribute to the health and productivity of the people working or living in them. To do so, they use Building Automation Systems (BAS). Using hardware, such as various kinds of sensors (light, temperature, air quality), cameras, access controls, etc.. A BAS can analyse, predict, run diagnostics, and maintain various environmental conditions, as well as automate processes and monitor many variables in real-time. Examples include optimizing power consumption for room temperature and lighting control, and automatic monitoring of security camera systems, elevators and parking facilities, among others.

The benefits of deploying smart devices are manifold. For instance, as ESET Global Security Evangelist Tony Anscombe relates, a well-known hotel in Las Vegas that automated A/C to operate only when rooms are occupied saved a cool US$2 million in the first year after the system was installed. According to the Smart Buildings Market 2019-2024 report, in countries such as the US, the smart buildings market – including warehouses, factories, office buildings, and other corporate, industrial, and government structures – is estimated to grow 16.6% by 2020 compared to 2014. As such, more than 80% of today's new buildings incorporate at least an element of IoT and technologies related to the smart buildings market.

SMART CITIES

In 2019, CES included an entire area devoted to smart city initiatives currently under implementation (or in planning) around the world. Some of them are aimed at improving transportation by using sensors to evaluate traffic flows and then controlling traffic signals based on these measurements. Others are for automating lighting through light sensors, measuring temperatures, incorporating monitoring systems consisting of networks of cameras and many other sensors to gather the information that is then analysed at a monitoring station to gain insights into everything going on in the city. Just as in smart buildings, but on a larger scale, it all revolves around sensors that gather information and where machine learning is used to analyze the data to automate a related service efficiently.

The problem is that many of these cities are not adequately prepared to safely manage the large volumes of information produced by these systems. An attacker could quickly gain access to sensors, adjust measurements, and make changes to services used in transportation, traffic, lighting, or other critical infrastructure. We have already seen proofs of concept of different types of attacks on smart cities and automated systems at conferences such as Black Hat and DEF CON.

Experts have expressed concerns that smart cities are experiencing rapid growth, but our ability to make them secure is not keeping up.

ATTACKS ON SMART INFRASTRUCTURE

On the one hand, it would appear that attacks on smart buildings and cities could only be carried out using detailed plans in which cybercriminals aim at a specific target. On the other hand, many BAS systems, as well as the sensors and devices used in smart cities, are directly exposed to the internet. Currently, searches on tools such as Shodan and Censys return results of more than 35,000 BAS systems, as well as hundreds of thousands of critical devices within public reach on the internet.

Many of these devices and systems do not have sufficiently strong authentication systems, have no kind of protection against brute-force attacks, are not updated, are not protected by any type of security solution, or simply have unsecured setups that could allow an attacker to take control of the equipment.

MALWARE

Although the systems used by smart buildings and cities do not browse the web or open email, they still need to protect themselves against malware, which could give cybercriminal access to critical information or cause damage to hardware. Malicious code can be propagated through the web access interface used to administer IoT devices, vulnerabilities in systems and even through physical access to USB ports that are unprotected or within reach of anyone passing by. It is also important not to neglect the protection of the network, especially in places where users will plug in personal devices, which could be compromised.

The systems used by smart buildings and cities could be attacked, for example, via botnets that aim smart devices. Is it far-fetched to imagine that, in the not-too-distant future, the IoT resources of an entire city could be hijacked by an attacker to generate millions of dollars through cryptocurrency mining? And cryptojacking is not the only threat. Three years ago in Trends 2017: Security held ransom, we presented the concept of

Cyber Security Trends for 2020

continues from page 31

jackware to describe malware that tries to take control of a device whose primary purpose is neither data processing nor digital communication. And immediately we derived from that the concept of Ransomware of Things, which refers to malware capable of blocking access to smart devices. That year, we discussed proof of concept involving the remote hacking of a moving car.

What would happen if an attacker managed to compromise the automation system of a smart building and threatened to cause havoc unless a ransom fee was paid? The types of systems that could be compromised include critical elements such as heating and air conditioning, fire detection and extinguishing systems, access controls, lighting, and the building's command and control centre. This scenario may sound like the plot of a science-fiction movie, but in fact, incidents that mix the concept of ransomware with BAS have already been reported – and we have dubbed it siegeware.

IDENTITY AND INFORMATION THEFT

Physical access to smart buildings tends to be controlled through IT systems whereby users identify themselves with biometric data or physical tokens. Such systems can be compromised through social engineering or shortcomings in their implementation, which could allow an unauthorized individual to gain physical access to restricted sectors.

Besides, digital identity theft can cause havoc if the attackers gain administrator privileges, which allow them to control the system(s) as they please. Once the attackers manage to make off with the victim's access credentials, they may go on to install malicious code, steal information, navigate through the system, and carry out any number of other damaging activities.
IoT sensors and devices used in most smart buildings and infrastructures can also act as an entry point to the network. This was the case for a casino that fell victim to an attack in which cybercriminals got into its network after exploiting a vulnerability in the smart thermostat of a fish tank in the lobby. They then accessed the casino's database, stealing information that included gamblers' data.

Smart buildings and cities are no longer the stuff of science fiction, but a reality of the world we inhabit. So far, the security incidents reported have been at an infrequent enough rate that they can be considered as isolated cases. Still, control systems for buildings and cities have become targets for cybercriminals.

The security measures to be taken to tackle these new threats are the same steps we always emphasize with each new wave of technological evolution: allocate sufficient budget for security, buy from vendors that have baked in the security at the time of purchase, implement programs for handling vulnerabilities, keep systems up to date, monitor the network and devices, and make sure you have security tools and the support of partners with knowledge in the field of security.

Additionally, there is a clear need to support legislation to mandate security right from the design of smart devices, and this is something likely to arise in the coming years, especially in the light of recent initiatives in the UK and California. Just as standards exist to regulate critical equipment, it is time to start analyzing what security norms and measures should be minimum requirements for the smart devices that interact with our information and privacy.

Many of us already live in cities with multitudes of sensors and cameras connected to the internet. In a not-too-distant future, we will spend a large part of our daily lives working and shopping in hyperconnected buildings packed with technology. And while all of this progress might seem exciting and impressive, we must not forget that behind it all, there have to be smart people.

SECURING THE DIGITAL TRANSFORMATION

As organizations set out on, or continue down, the path of digital transformation, they have to rethink all aspects of their operations. How can they reap the benefits of going digital without getting derailed along the way as a result of a failure to address underlying cybersecurity challenges?

Due to market dynamics, digital transformation has become a fundamental issue that affects all aspects of a company's affairs. The implementation of all these new technologies – a journey that many companies embarked on a few years back to deliver more value to their customers – requires cultural change at the organizational level. It is no wonder, then, that this represents a significant challenge for all involved businesses.

Naturally, information security should not be seen as something separate from these efforts. Instead, it as an essential part of the goals that companies need to plan for to avoid being left behind in the race due to lapses in cybersecurity.

Digital transformation tends to involve rethinking the processes and strategies of each company and, in so doing, allowing each to benefit from digital technology. On the other hand, this leads to new risks – and companies must not lose sight of these perils.

CHANGES IN CYBERSECURITY MANAGEMENT MUST SUPPORT CHANGES IN IT

Companies that are already undergoing changes that are part of their digital transformation have discovered that they are exposed to the development of business models that include a sizeable technological component. As a result, their IT teams have had to adjust to support the speed of this change.

All this change means that little by little, companies are moving from having the majority of their resources centralised to having to adopt a wide range of new services and assets to support their day-to-day activities, leading to an increase in the variety of technologies and platforms they need to monitor.

This complicated process of transformation – which, according to a survey by McKinsey, eight in ten organizations have decided to undertake over the last five years – has had direct implications for the organizations' cybersecurity posture. Companies need to work actively towards reducing the chances of falling victim to a cyberattack or data breach.

As a result, management teams have found themselves immersed in new paradigms that allow them to fulfil this mission – but without impacting their normal business operations. Organisations need to be able to secure their data during the transformation process of operating successfully in a digital ecosystem.

According to a study that the Ponemon Institute carried out in many countries in 2018, 72% of IT security professionals believe that a sense of urgency around achieving digital transformation increases the risk of a data breach. When coupled with the fact that 45% of organizations said that they do not have a strategy for dealing with the digital transformation, this is grounds for concern.

Security teams need to have a constant flow of information about all the changes going on inside their organizations. For this reason, smart technologies, including threat monitoring, are essential to provide a base on which other processes can be run securely, maintaining compliance with standards across the entire organization.

Technological variety as a driver of change
Companies need to see information security as a part of the digitalization process. As multiple technologies are now available for this process – including cloud computing, mobile platforms, 5G connectivity and machine learning, to name just a few – it is essential to understand that no single technology or application is going to be enough to guarantee data security and business continuity.

One of the main hurdles for companies that are embarking on the journey may be where to start. The starting point is understanding that all of this transformation is also radically and rapidly changing society as a whole – the way we work, socialize, buy things, and interact in the many aspects of our daily lives.

THE ROAD TO MOBILITY

From all these scenarios for change inside companies, there is one in particular that will be a significant factor in accelerating the process in 2020 – employee mobility. Undoubtedly, our ability to stay connected to networks, regardless of where we are, keeps increasing organizations' attack surfaces and exposure to risk.

All this change has been taking place slowly but surely over recent years, but companies' ever-increasing speed of adoption of mobile technology often occurs without due consideration of security. This is why companies need to stop traditionally thinking of security and instead consider adopting adaptive models that can respond to change.

And even more urgently, IT security teams need to dive headfirst into the use of monitoring technologies because detection technologies alone are not enough. Companies must develop processes for responding to incidents and then bring operations back to normal by resolving those incidents and applying suitable corrective measures.

CONCEPTS TO RETAIN IN THE DIGITAL TRANSFORMATION

Beyond these specific technologies, which in any case will keep evolving, we must not lose sight of critical concepts like privacy. We are living in a time when new, stricter laws on personal data protection are continually being adopted. As a result, people are gradually becoming more aware of their rights and are more concerned about how companies handle their data.

Over the coming months, we will see organizations implement significant

Cyber Security Trends for 2020

continues from page 33

changes in almost all areas of their businesses. The common thread running through all this will be how they handle information and the data involved in their operations. Therefore, business models that generate client trust will be a differentiating factor.

SO, WHAT SHOULD COMPANIES DO?

In terms of what companies are going to face over the next year, there are at least five key considerations they need to focus on to handle this transformation securely:

1. Find a balance between the implementation of new technology and cybersecurity. If they aren't balanced from the start and if security isn't seen as an enabler for the business, there are going to be more problems than solutions.
2. Develop projects that facilitate both the visibility and control of technologies. In doing so, the focus should not only be on preventing incidents but should also consider detecting and responding to an incident.
3. Security can't be focused solely on devices, because the quantity of equipment and technology is continuously growing, making it complicated to implement security on each component individually.
4. Foster greater collaboration between people and processes so they are aligned, and so that decision-making is based on shared data generated from the technology that has been implemented.
5. And of course, the human element cannot be neglected. Digital transformation is something almost all people are experiencing in their daily lives, but often with behaviour that involves risks for their personal information. As a result, it is essential to work on preventing the company's data from being vulnerable to social engineering attacks.

CONCLUSION

The challenges to come are undoubtedly significant, and we need to prepare ourselves, from the technological and educational perspectives alike. By doing so, both current and future generations will have better tools to tackle these challenges, and technology will be allowed to realize its true potential, translating into a better quality of life for humanity.

As this article has made abundantly clear, our world is set on continuing to evolve in its use of technology and becoming (even) "smarter" than it is at present. But only when advances in artificial intelligence have enabled machines to think for themselves, only when the transformation toward what we think of as smart cities has become a global phenomenon, and only when the process of digital transformation that many companies are currently undertaking has become history, will we be able to analyse with more precision what the actual costs of this process were.

What is clear is that considering the way things look at the moment, cybersecurity will continue to be viewed as an issue of secondary importance when it comes to technological development. This will have consequences in the short term.

On the one hand, there are encouraging signs that more and more people are coming to recognize the importance of cybersecurity, and the need for it to play more of a leading role as we head into the future. However, given that, in the last five years, eight in ten companies have started on the path of digital transformation, coupled with the growth in data breaches on a global scale and the predicted increase in costs for companies to deal with them, it seems impossible to avoid these types of incidents.

Additionally, if we stop to think about the growth anticipated for the construction of smart buildings and cities, and of the fact that many cities that are currently invested in the concept of "smart" have fallen victim to known threats like ransomware, what reason do we have to be optimistic and believe that the future will be any better in terms of information security practice?

Similarly, if we take as points of reference the current advances in the beneficial use of machine learning, the phenomenon of fake news, and what we can expect from a still distant future in which artificial intelligence has been developed, the challenge of being prepared for what is to come could provide us with the opportunity to take measures that give cybersecurity more of a leading role.

Deep-fakes have already given us a sense of their potential impact, creating confusion and sowing uncertainty about which pieces of information are true and which are false. In turn, this spreads mistrust among individuals, who, by being more interconnected, continue to expose their data and personal information due to a lack of knowledge – or implementation – of basic security practices. Many individuals vote in elections in countries that opted for electronic voting, despite the evidence of problems with such systems.

Returning to the question, we asked earlier; there have been some positive signs that give us cause for optimism.

Companies like Facebook, together with other big companies and universities, have demonstrated their willingness to fight against phenomena like deep-fakes by launching initiatives such as the Deep-fake Detection Challenge (DFDC), which is intended to promote the development of new technology capable of fighting back against deep-fakes.

Furthermore, recent times have seen changes to the legislative and regulatory landscape relating to data privacy. While these may have been slow to occur and have perhaps not yet generated a significant impact, they are at least developments in the right direction.

There is still a lot of work to do, and governments need to intervene and promote measures that provide a framework and a direction for the path forward. On the one hand, there is still a lack of awareness about many aspects of information security.

On the other hand, the distrust displayed by many people in that their data is being appropriately protected reflects the fact that they are continually less shielded from the impact of cybersecurity and privacy on their lives. This may be an indication that, across the range of issues discussed in this Trends report, further consumer education about cybersecurity issues is an essential factor for further consideration. wn

Each year, cybercriminals continue to refine their use of social engineering, relying on human interaction rather than automated exploits to install malware, initiate fraudulent transactions, steal data and engage in other malicious activities. Less than 1% of the attacks we observed made use of system vulnerabilities. The rest exploited "the human factor": the instincts of curiosity and trust that lead well-intentioned people to click, download, install, open and send money or data.

Instead of attacking computer systems and infrastructure, threat actors focused on people, their roles within an organisation, the data to which they had access, and their likelihood to "click here."

Whether attacking at a massive scale in large indiscriminate campaigns, going after specific industries or geographies with more targeted campaigns, or seeking out a single person within an organisation, attackers and their sponsors consistently found human beings to be the most effective vectors to infiltrate organisations and facilitate fraud and theft.

While ransomware was the most significant threat of 2017, the last 18 months have seen a marked shift towards information-stealing malware, with social engineering becoming ever more pervasive and effective at preying on people. Whether sending impostor messages that appear to come from a trusted colleague or installing increasingly robust malware that can silently profile individuals and steal data and credentials to make future attacks more effective, threat actors are following the money.

While cryptocurrency volatility and a growing ability to detect and mitigate ransomware may have driven this shift initially, the information provided by victims via malware and phishing attacks is fuelling revenue streams and facilitating future attacks.

Regardless of the means of attack—email, cloud applications, the web, social media, or other vectors—threat actors repeatedly demonstrated the effectiveness of the social engineering tactics that convinced victims to click malicious links, download unsafe files, install malware, transfer funds and disclose sensitive information at scale.

Whether financially motivated or state-sponsored, attackers all had one thing in common: an understanding of and a willingness to take advantage of the human factor.

KEY FINDINGS

Email remains the top attack vector. Threats range from malicious spam that clogs inboxes and wastes resources to impostor attacks that can cost organisations and people millions of pounds. Threat actors attack cloud applications, leverage increasingly robust multi-purpose malware, and seek out new ways to steal both money and data directly.

Here are the key findings from Proofpoint research over the 18 months of 2018 and the first half of 2019. The results, based on data collected across our global customer base and analysis of billions of messages per day and hundreds of millions of domains, highlight how actors are increasingly exploiting "the human factor."

Human Factor Report

ATTACKERS TARGET PEOPLE AND NOT NECESSARILY WHOM YOU MIGHT EXPECT

The modern threat landscape is increasingly "people-centric." Attacks focus on people and identities rather than infrastructure, making it more critical than ever to identify which users in an organisation represent the most significant sources of risk.

- "Very Attacked People" (VAPs) represent significant areas of risk for organisations. They tend to be either easily discovered identities or targets of opportunity like shared public accounts. Of the identified VAPs, 36% of the associated identities could be found online via corporate websites, social media, publications and more.
- VAPs are not necessarily high-profile individuals either (VIPs such as C-level executives). Only 7% of executive emails could be found online.
- For the VIPs who are also VAPs, almost 23% of their email identities could be discovered simply by a Google search.
- Education, finance, and advertising/marketing were the industries with the highest average Attack Index, an aggregated measure of attack severity and risk.

SOCIAL ENGINEERING REACHES CRITICAL MASS

Attackers are increasingly focused on obtaining credentials to feed further attacks and are improving the social engineering techniques with which they obtain them. Similarly, malware distribution is far more focused on establishing a silent foothold in organisations to commit fraud and steal data and credentials rather than merely smash-and-grab via ransomware attacks.

- Generic email harvesting accounted for almost 25% of all phishing schemes in 2018. In 2019, Microsoft Office 365 phishing was the top scheme, but the focus remains credential harvesting.
- The most effective phishing lures in 2018 were dominated by "Brain Food," a diet and brain enhancement affiliate scam that harvested credit cards. However, 2019 saw a shift in terms of effectiveness towards cloud storage, DocuSign and Microsoft cloud service phishing.
- Impostor attacks include schemes like business email compromise (BEC) and also include increasingly mainstream identity deception techniques used in a variety of scenarios supporting social engineering and more effective people-centred campaigns. 2018 saw impostor attacks at their highest levels in the engineering, automotive and education industries. This likely reflects easily exploited supply chain complexities in the first two and high-value targets and user vulnerabilities—especially among student populations— in the latter.
- Over 99% of emails distributing malware required human intervention—following links, opening documents,

Human Factor

continues from page 37

accepting security warnings and other behaviours—for them to be effective.

VECTORS MULTIPLY AS ATTACKERS REFINE TECHNIQUES AND LEVERAGE A RANGE OF PLATFORMS

How attackers select and target potential victims multiply as attackers refine techniques and leverage a range of platforms:

Themes vary widely by both actor and intended target. Food, shelter, love and money are perennial favourites, feeding everything from threats of lawsuits over food poisoning in attacks on restaurants to rampant sextortion schemes targeting individuals.

- BEC tactics—building rapport with attacked individuals, multiple points of contact and creating a sense of urgency, among others—began appearing more frequently in attacks involving commodity malware.
- Domain fraud and abuse ramped up even more, with attackers leveraging a range of techniques from look-alike domains to legitimate secure certificates to make malicious websites appear trustworthy.

INTRODUCTION

Malware-free attacks like business email compromise (BEC) and credential phishing continue to rapidly gain momentum as threat actors consistently attack individuals and business processes rather than specific systems and software. Similarly, attacks on Software-as-a-Service (SaaS) accounts and platforms create new risks for businesses that are increasingly reliant on the cloud. At the same time, malware-based attacks have shifted almost entirely to payloads that support long-term credential theft, information gathering, and the ability to flexibly load new malware in the future—all while evading detection. This pendulum swing toward persistent, non-destructive infection and information theft allow attackers to collect more and more data about us, all of which can be turned around in a feedback loop for a range of highly targeted attacks.

This year, we are uniquely positioned to examine four critical components of the attacks businesses and individuals face every day:

- Who within an organisation is being attacked?
- How are phishing and impostor attacks (including BEC) evolving?
- What malware is being used to attack individuals and organisations? And how is it being targeted and used?
- What kinds of attacks are increasingly targeting the SaaS platforms on which people and businesses rely? And how does the trend towards pervasive credential phishing (both socially engineered and malware-driven) feed into this?

BY THE NUMBERS

TOP 20 PHISHING LURES

Phishing lures leverage a range of brands and are set to resemble login portals from banks, online retailers, webmail and more. While some are phishing for credentials from specific services, it appears that many are only looking for the email logins used with various services to inform credential-stuffing attacks. By far, the most prevalent phishing campaigns in 2018 sought a variety of email login credentials, often offering to allow users to log in to fake services with any number of email accounts. This type of generic email harvesting accounted for almost 25% of all phishing schemes.

In the first half of 2019, the focus has remained on email credential phishing, although Microsoft Office 365 account phishing took the top spot from more generic efforts. So-called “Chalbhai phishing” took the third spot. CHALBHAI phishing targets credentials for several

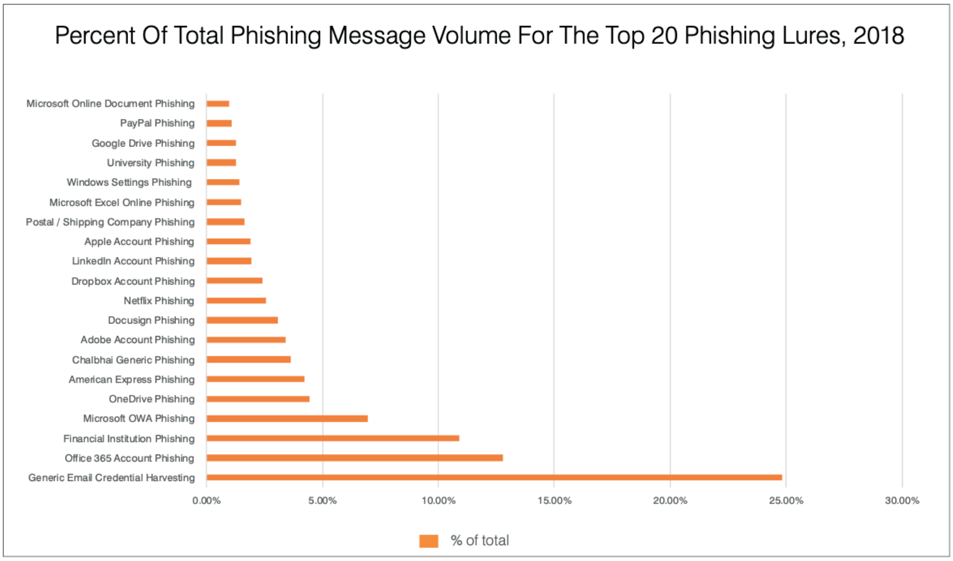
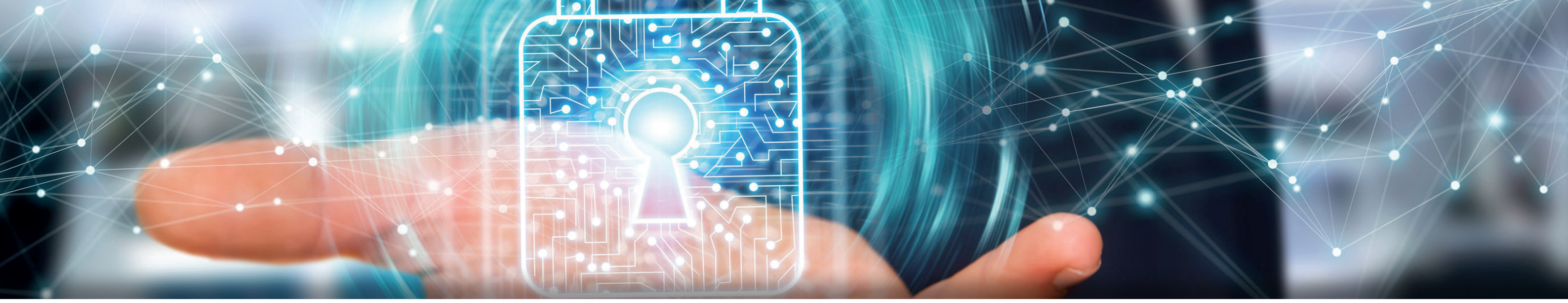


Figure 1: 2018 relative phishing campaign volumes1



top US and international banks, telecommunications companies and Microsoft services (among others), using a range of templates attributed to a single group but leveraged by multiple actors.

CLICK RATES FOR TOP 20 MOST-CLICKED PHISHING LURES

As we noted in previous years, the most-clicked lures are not necessarily the same as the most common phishing lures. In 2018, Brain Food phishing was by far the most clicked lure, with click rates over 1.6 CLICKS PER MESSAGE. This indicates that the messages themselves are shared and clicked through multiple times on many occasions.

Brain Food refers to a botnet that distributes diet and mental enhancement spam and routinely sends users to credit card harvesting pages, among others. Blackboard phishing, which collects credentials for the popular school management system, WeTransfer (a file-sharing service), and Zoominfo (a business contact database) all had click rates above 0.6 clicks per message.

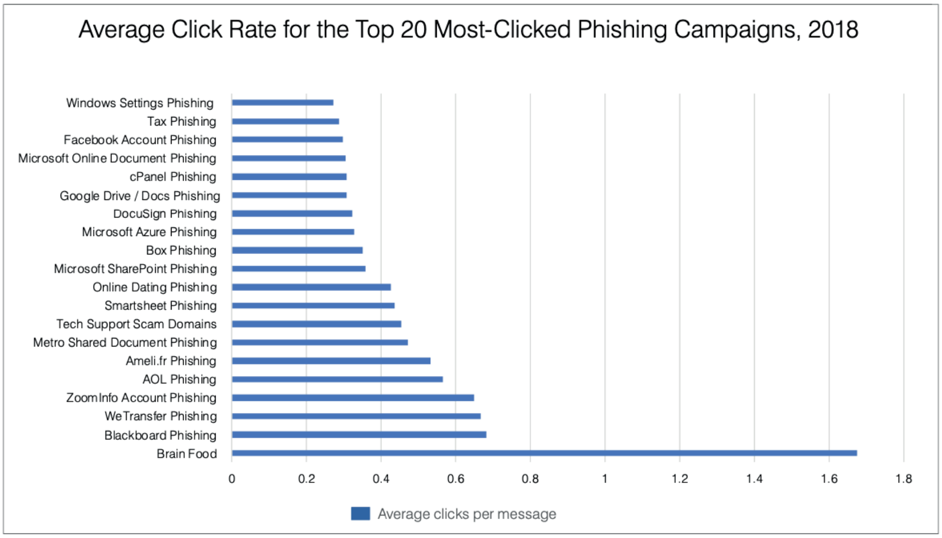


Figure 2: 2018 average click rates for phishing messages from the top 20 most-clicked lures

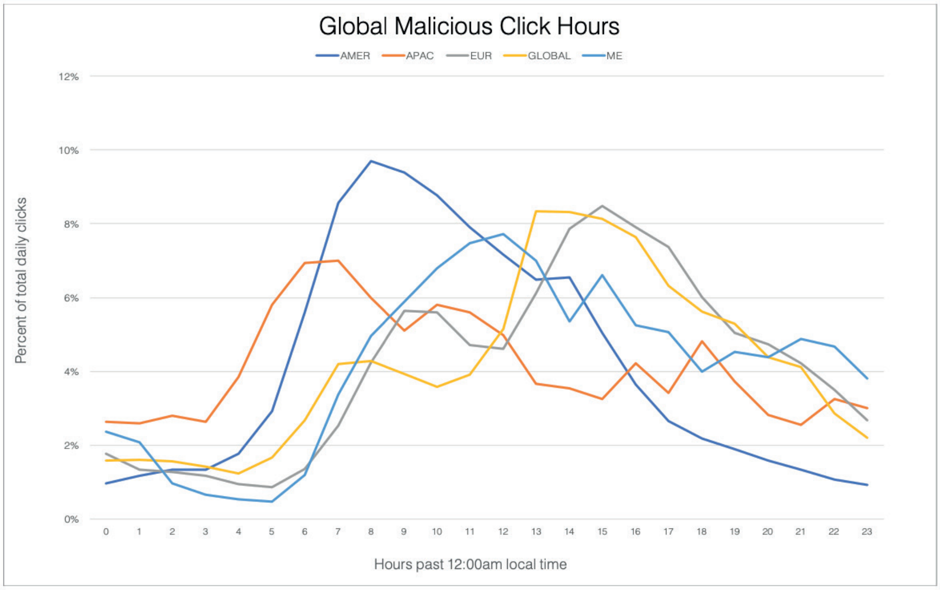


Figure 3: Relative click times by region, adjusted for local times, Q1 2018-Q1 2019

Click rates were nearly identical across industries, between 20% and 22% for all lures in aggregate.

However, in the first half of 2019, we have observed a shift towards cloud storage lures in terms of effectiveness—DocuSign, and Microsoft cloud service phishing in particular—with Brain Food activity dropping off and educational phishing often loaded towards the third quarter as school begins.

CLICK TIMES BY REGION

Click times have traditionally shown significant regional differences, reflecting differences in work culture and email habits among major global regions.

Figure 3 shows the percentage of phishing links clicked by the time of day, with Asia-Pacific and North American organisations far more likely to read and click early in the day and Middle Eastern and European users more likely to click midday and after lunch.

This is important for defenders in organisations looking to enhance training, mitigation and end-user outreach around phishing. Click times were averaged across five quarters, as they showed little quarter-to-quarter variation. These habits appear relatively fixed.

Human Factor

continues from page 39

THE AVERAGE NUMBER OF IMPOSTOR ATTACKS PER TARGETED COMPANY BY INDUSTRY

2018 saw IMPOSTOR ATTACKS at their highest levels in the engineering, automotive and education industries, likely reflecting easily exploited supply chain complexities in the first two and high-value targets and user vulnerabilities, especially among student populations, in the latter.

To date, in 2019, we have observed a shift in the most highly targeted industries, with financial services, manufacturing, education, healthcare and retail rounding out the top five. Regardless of industry, however, there continues to be no correlation between the size of targeted companies and the number of impostor attacks they receive. While larger organisations may be attractive for their deep pockets, smaller companies may be more vulnerable due to relative lack of controls and awareness, both of which create lucrative potential outcomes for threat actors.

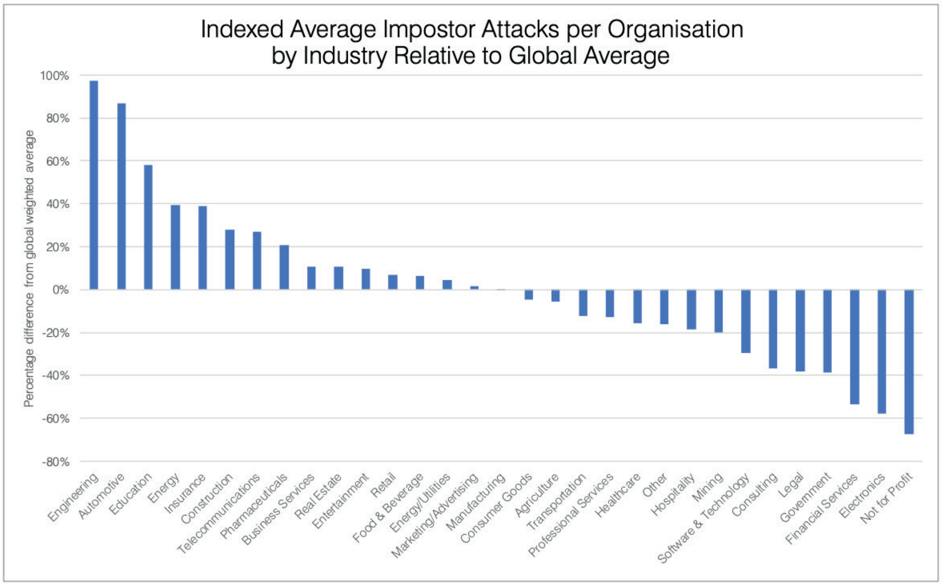


Figure 4: Impostor attacks by industry relative to the weighted global average impostor attacks per targeted organisation

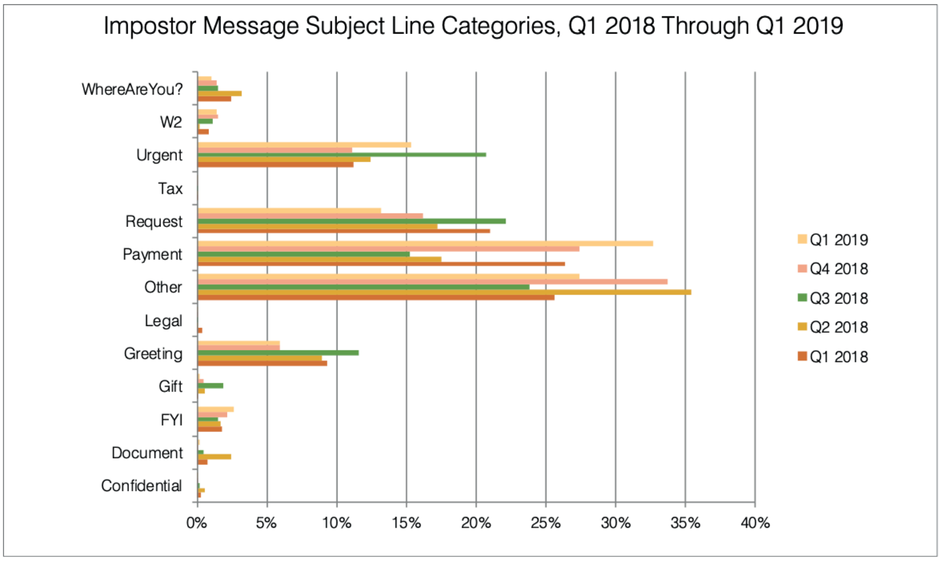


Figure 5: Most common subject line categories in impostor emails indexed by quarter, Q1 2018 to Q1 2019

TOP IMPOSTOR EMAIL SUBJECT LINES

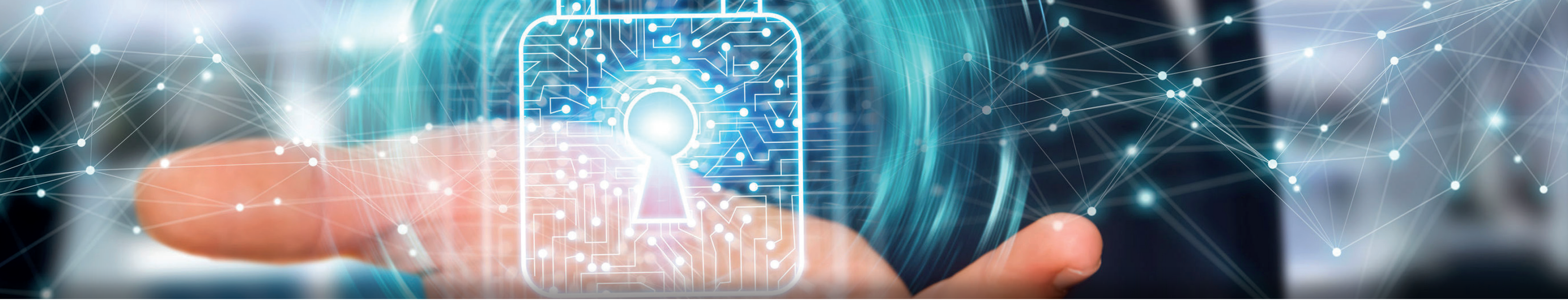
Simple subject lines in impostor emails continue to shift away from those related to a "Request" and towards "Payment" scams. Similarly, "Urgent" subjects are showing an upward trend while W2-related attacks maintained their expected seasonal upticks at the end of 2018 and the beginning of 2019, corresponding to tax processing seasons.

IMPOSTOR EMAIL SUBJECT LINES FOR THE TOP FIVE MOST TARGETED INDUSTRIES

Subject lines associated with impostor emails not only vary seasonally but also by industry. Looking more closely at the top five targeted industries, we see that education receives a disproportionate number of impostor emails related to "Request" and "Greeting" while attacks on engineering firms, for example, favour "Urgent" and "Request" messages. In any of these cases, the subject lines associated with impostor attacks are often tailored to the receiving industry in ways that more traditional AFFILIATE or malware-bearing spam is not.

IMPOSTOR MESSAGE VOLUME BY DAY OF WEEK

Impostor message delivery closely mirrors trends observed in previous years, with less than 5% of overall messages delivered on weekends and the most significant portion



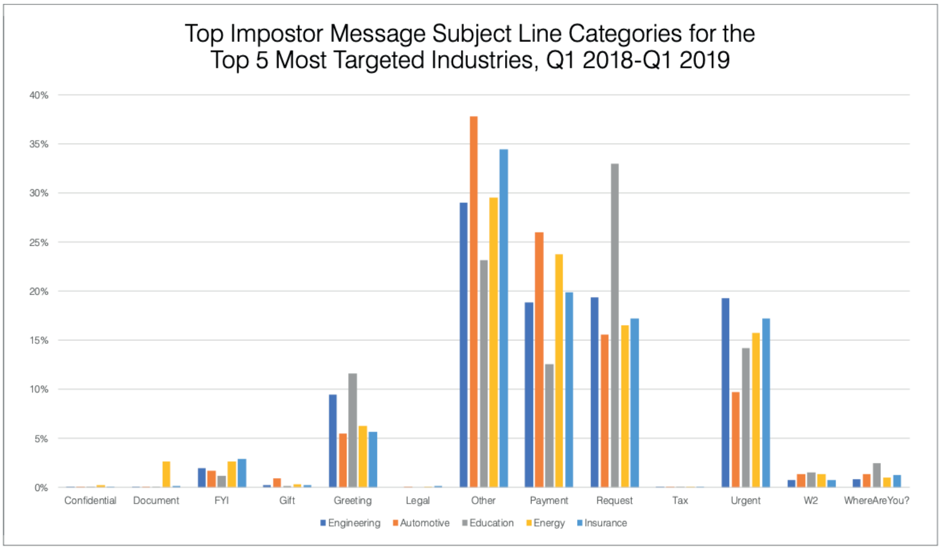


Figure 6: Top impostor email subject categories are broken out by the five most targeted industries

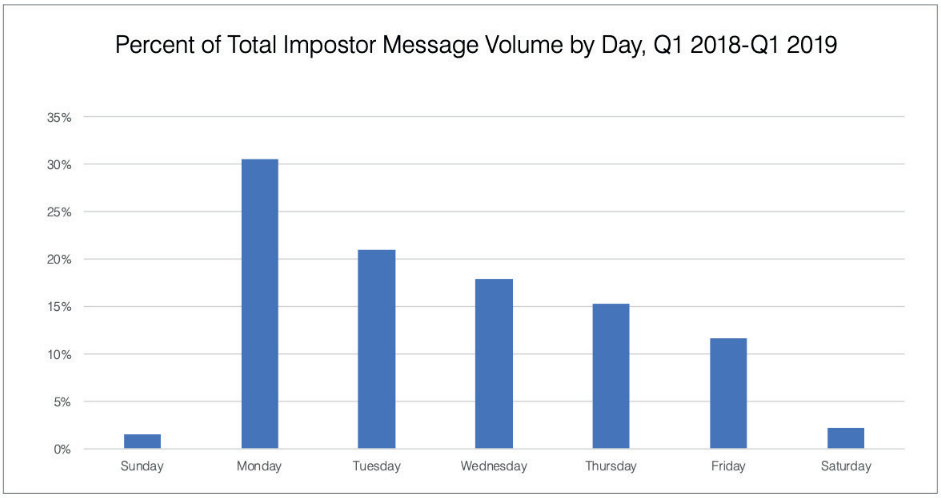


Figure 7: Relative volume of messages associated with impostor attacks by day of the week

- over 30% - delivered on Mondays. Threat actors capitalise on Monday morning backlogs and social jetlag to more easily fool people with impostor tactics and other social engineering elements.

Delivery rates steadily drop off through the week, and delivery rates are nominal when few employees are in the office.

By way of comparison, overall malicious message volumes sampled in the second quarter of 2019 were distributed more evenly over the first three days of the week.

They were also present in significant volumes in campaigns that began on Sundays, suggesting that malware actors, in general, are less concerned about timing than actors focusing on impostor techniques and the inherent social engineering approaches.

CHANGE IN IMPOSTOR ATTACK VECTOR BY QUARTER

In general, since the beginning of 2018, we have observed an ongoing and steady increase in the frequency with which multiple SPOOFED identities are used to target many individuals in organisations. For example, threat actors might spoof the identities of several executives or senior managers, sending a malicious document to a range of employees asking them to read the document. Alternatively, in a more traditional BEC-style attack, several spoofed identities might be used to ask all staff in the Human Resources department to forward W2 information for employees. While so-called one-to-one and one-to-many attacks were more common when impostor attacks first began to emerge—especially in the context of business email compromise—threat actors appear to be finding success in attacks using more than five identities against more than five individuals in targeted organisations. One point to note, however, is the relative increase, albeit at a smaller scale, in attacks over the last two quarters in which a single spoofed identity was used to target a single individual.

TOP 10 INDUSTRIES TARGETED BY MALWARE CAMPAIGNS

As with phishing, the top industries targeted by malware actors vary from year to year. However, financial services, manufacturing, technology, healthcare and retail frequently top the list, as they did in 2018.

RELATIVE DISTRIBUTION OF MALWARE STRAINS FOR THE TOP FIVE TARGETED INDUSTRIES, 2018

Banking Trojans, information stealers, downloaders and botnets regularly

Human Factor

continues from page 41

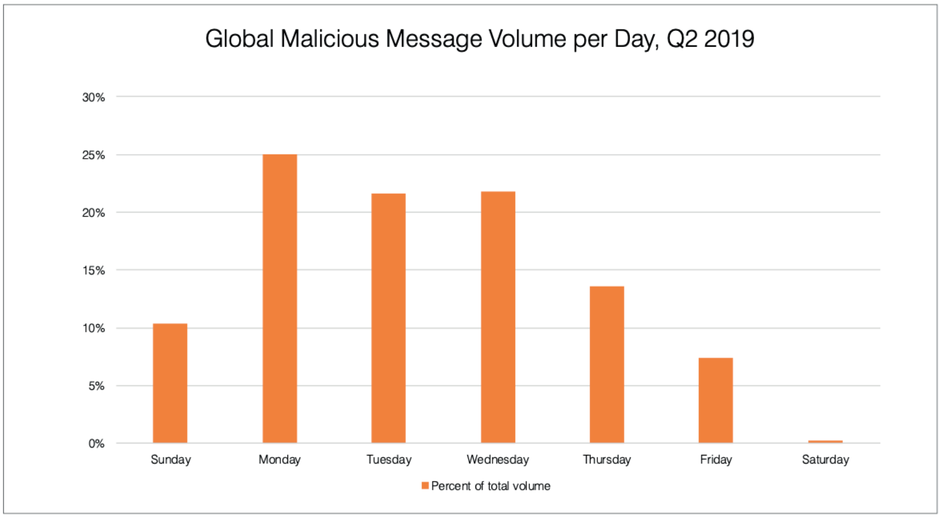


Figure 8: Relative volume of messages associated with all malware attacks by day of the week, Q2 2019

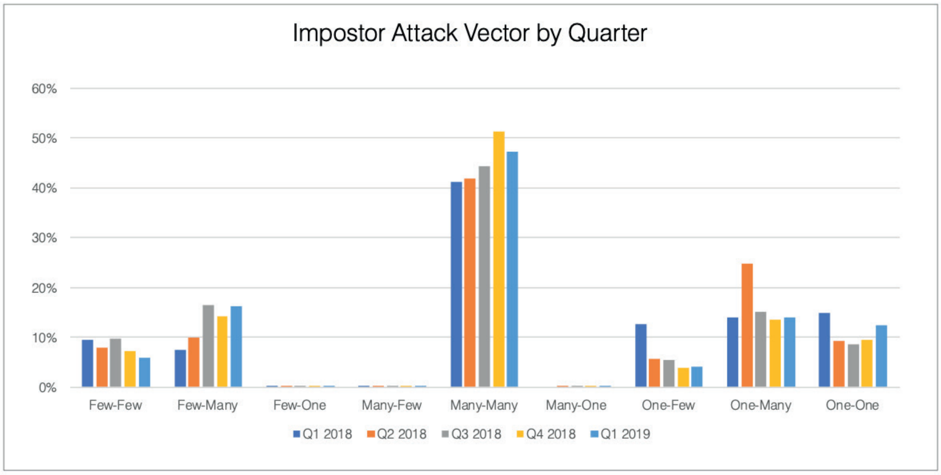


Figure 9: Relative volume of impostor attacks by type and quarter, Q1 2018 to Q1 2019

appeared in malware campaigns in 2018 as threat actors continue to favour longer-term information gathering and credential theft over the more damaging but short-term gains associated with ransomware that was endemic in 2016 and 2017.

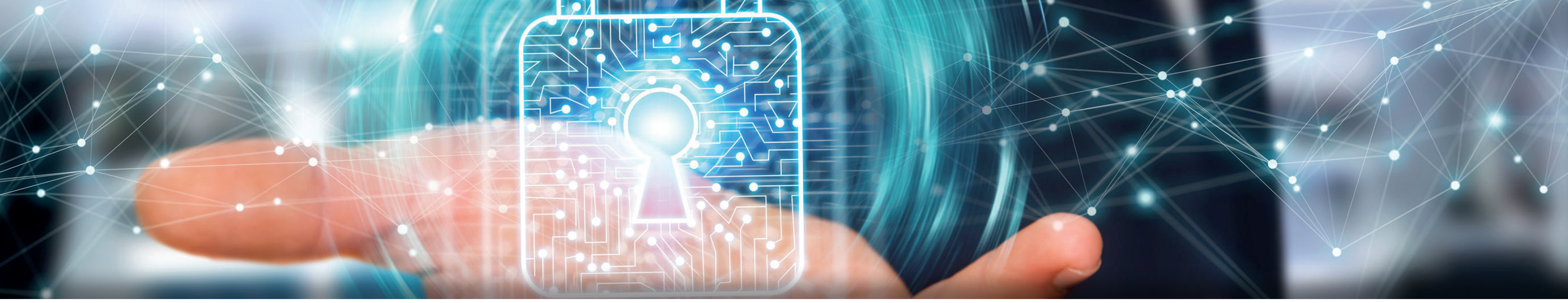
While the data presented are from 2018, we have observed similar trends in the first half of 2019.

Note that while the general distribution of malware in aggregate favours banking Trojans, REMOTE ACCESS TROJANS (RATS) and downloaders, individual industries experienced different proportions of malware families. In some cases, specific malware strains were only common in particular industries, based on the modus operandi of the actors targeting the verticals and specific vulnerabilities frequently associated with those industries. For example, the financial services sector tended to see higher volumes of FLAWEDAMMYY and SERVHELPER as the actor we track as TA505 turned their attention to finance. Technology companies, on the other hand, saw higher proportions of downloaders and banking Trojans, potentially for both financial gain and to load software for stealing intellectual property or launching further attacks. Again, the mail exchanger records (MX records) are noteworthy, as fraudulent domains appear to be coming in line with all domains, although it is not clear why threat actors are now more likely to create MX records for their domains.

We have continued to see robust targeting of these industries in 2019. Looking at the breakdowns for the top five gives a sense of how threat actors adapt techniques for various industries in some cases (such as the use of AZORULT in financial services). In other cases, threat actors still send broad-based campaigns (such as URSNIF) that affect organisations across a range of industries.

RELATIVE DISTRIBUTION OF ATTACK TECHNIQUES FOR THE TOP FIVE TARGETED INDUSTRIES, 2018

Regardless of the malware being distributed, 99% of the malware we observe requires at least some degree of human interaction to infect user devices. With exploit kits continuing to operate at a tiny fraction of their 2016 peak and many software vulnerabilities quickly addressed by more aggressive vendor patching, campaigns throughout 2018 and the first half of 2019 relied on users to click links, open documents, enable macros, bypass security alerts or unzip malicious executables. In the face of increasingly practical social engineering, people continue to do just that.



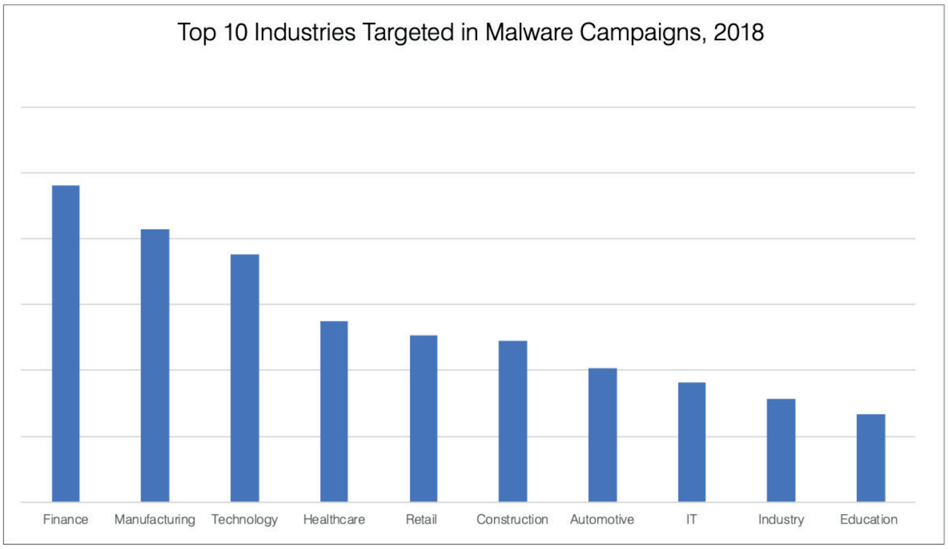


Figure 10: Relative total message volumes for malware campaigns in the top 10 most-targeted industries

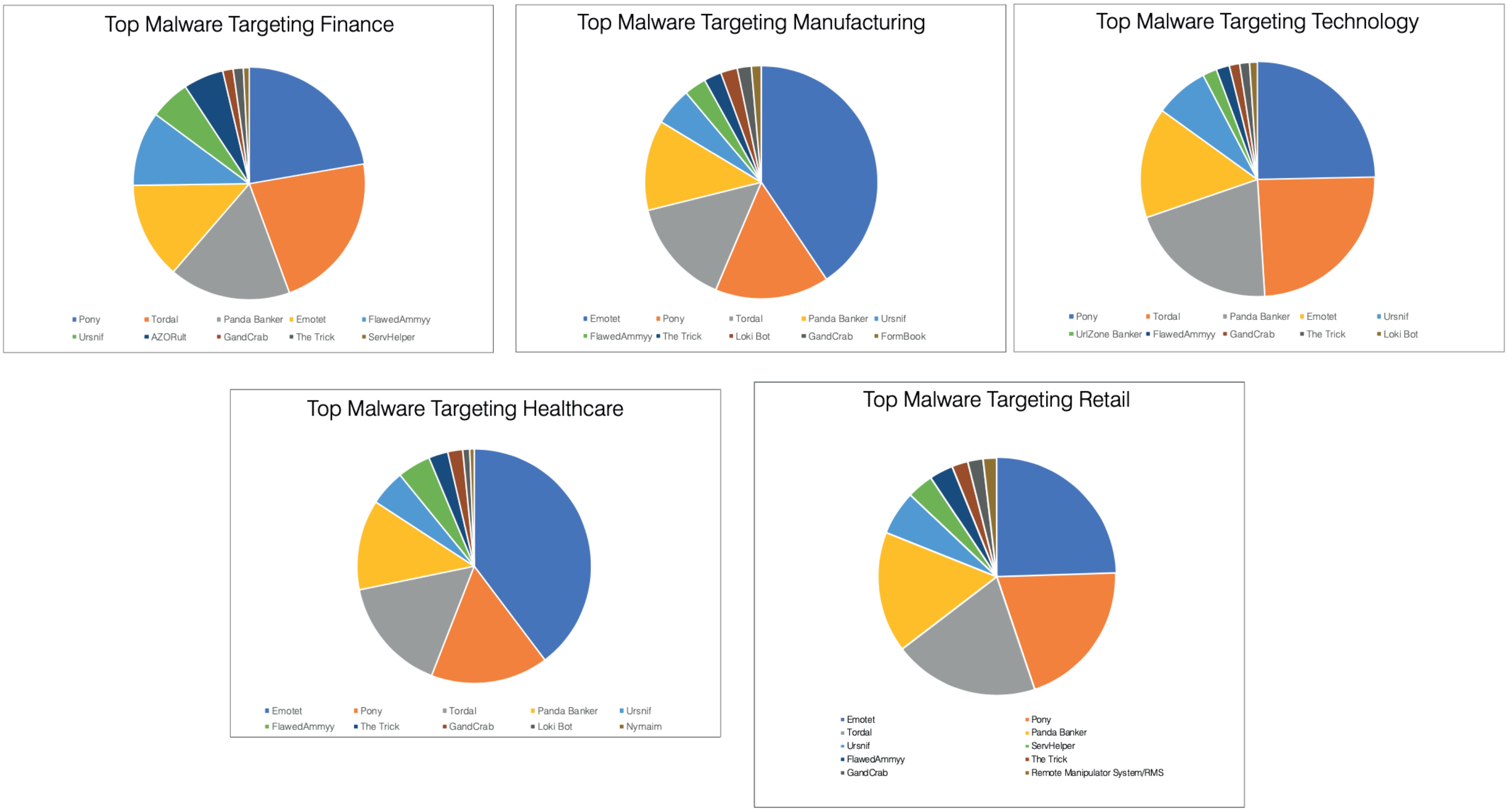


Figure 11: Relative malicious message volumes by payload for the top five most-targeted industries

Human Factor

continues from page 43

Figure 12 shows the most common attack techniques observed in the industries with the highest malware volumes in 2018. Microsoft Office Visual Basic for Applications (VBA) macros are the common thread. Malicious macro-laden documents are the most common vector we observe in aggregate when hosted and distributed with a link or attached to an email.

However, even the specific vulnerabilities noted below, like CVE-2017-11882, require humans to open the malicious document that leverages the exploit.

PEOPLE-CENTRED ATTACK METRICS

Attacker strategies go well beyond social engineering and convincing people to click. Threat actors are increasingly focused on getting the right people to click—those with sufficient access and privileges to best establish a beachhead on a network or with those most likely to move funds in a wire transfer scheme, for instance. Attackers also focus on "targets of opportunity," often going after shared accounts that are difficult to secure or accounts with broad public and social media footprints. The analyses below quantify the scale and targeting of these so-called "people-centred attacks."

ATTACK INDEX DEFINED

The Attack Index is an aggregate measure of cybersecurity risk for individuals in an organisation. Measuring it by person allows businesses to allocate security resources to individuals and departments with the most considerable risk of an active or damaging attack. Looking at summary measures of the index across industries provides a better understanding of the threat landscape, threat actor behaviour and the challenges faced by specific industries over time.

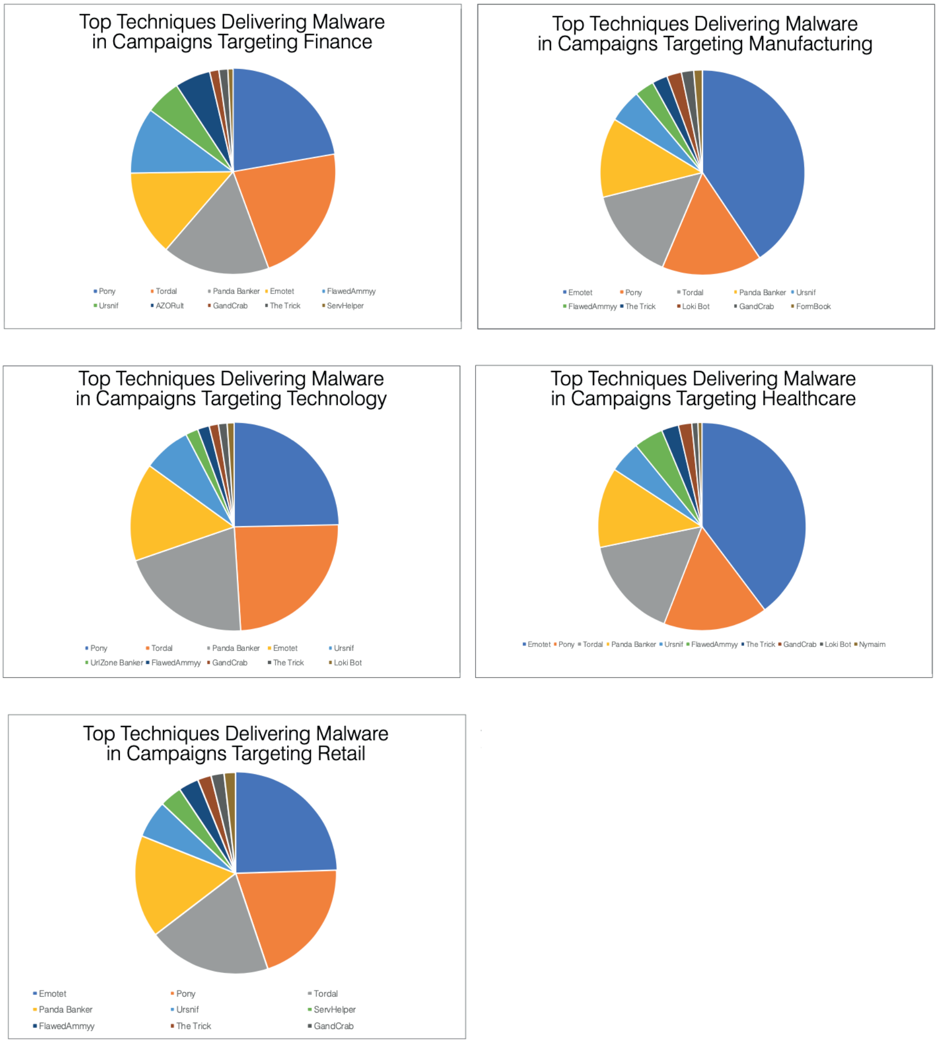
The Attack Index is based on three components:

- Actor type
- Targeting type
- Threat type

Actor type considers the attacker's level of sophistication. For example, an advanced persistent threat (APT) state actor will be given a higher score than a small-scale, financially motivated crimeware actor.

Targeting type speaks to the degree of targeting involved with the threat. Did the threat hit only a small number of global users? Was it focused on a particular user, company, industry or geography? Or was it a spray-and-pray campaign seen by half the globe? The former will receive a higher score than the latter.

Threat type addresses the type of malware involved in the attack. This considers how dangerous the threat is and how much effort went into the threat. In this case, a RAT or



Top Techniques Delivering Malware in Campaigns Targeting Finance

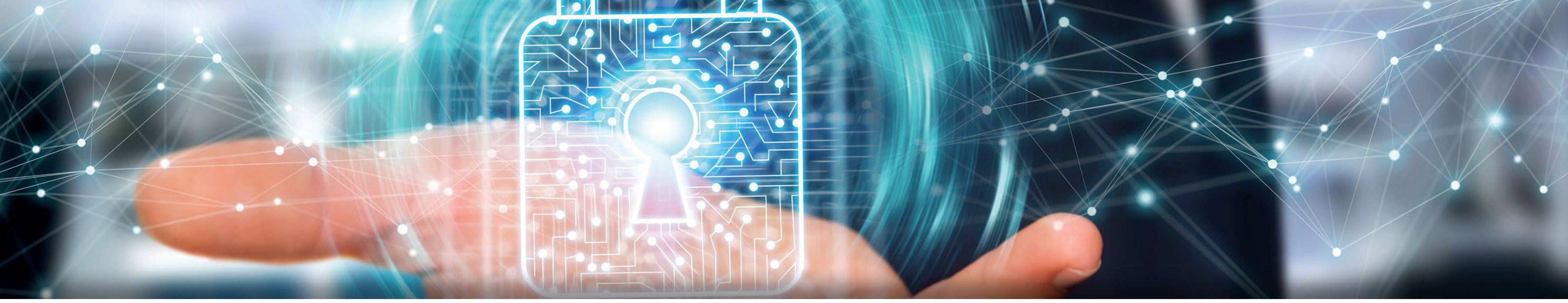
Top Techniques Delivering Malware in Campaigns Targeting Manufacturing

Top Techniques Delivering Malware in Campaigns Targeting Technology

Top Techniques Delivering Malware in Campaigns Targeting Healthcare

Top Techniques Delivering Malware in Campaigns Targeting Retail

Figure 12: Relative malicious message volumes by leveraged technique for the top five most-targeted industries



stealer is going to have a higher score than a generic consumer credential phish.

ATTACK INDEX BY INDUSTRY

As noted, attackers are increasingly focused on attacking the "right people" in an organisation rather than attacking every user and seeing which attacks are successful. These "right people," whether targets of opportunity or identified users with sufficient access and privilege, generally make up groups of VAPs in an organisation. Looking at average Attack Index and the average number of VAPs across industries provides a view of both the overall severity of the threats against organisations in a given industry and the number of accounts within industries that threat actors can identify for targeted attacks.

Figure 13 shows that education, for example, is frequently targeted with attacks of the highest severity and has one of the highest average numbers of VAPs across industries. Financial services, on the other hand, has a relatively high average Attack Index but appears to do a better job concealing individual identities and accounts from attackers, creating fewer VAPs to attack.

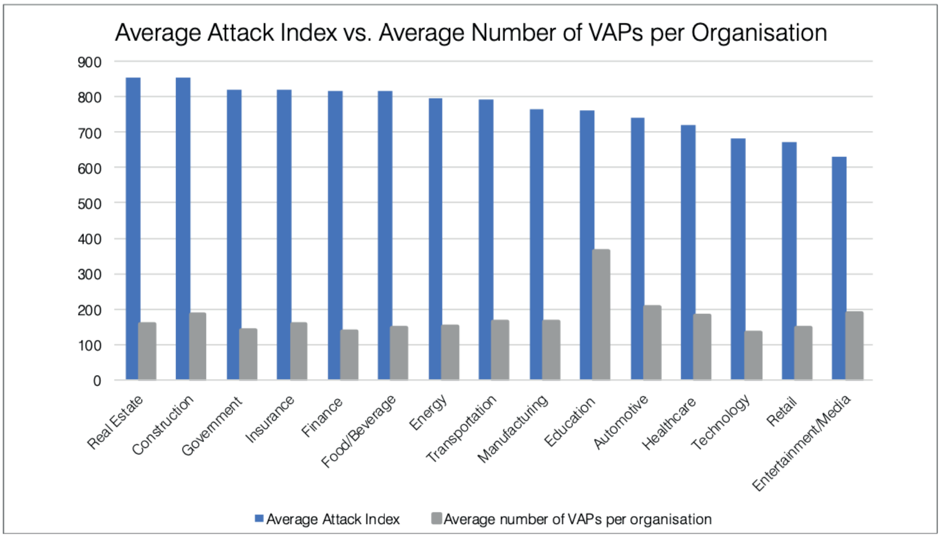


Figure 13: Average Attack Index associated with major industry groups versus the average number of VAPs per organisation in the industry

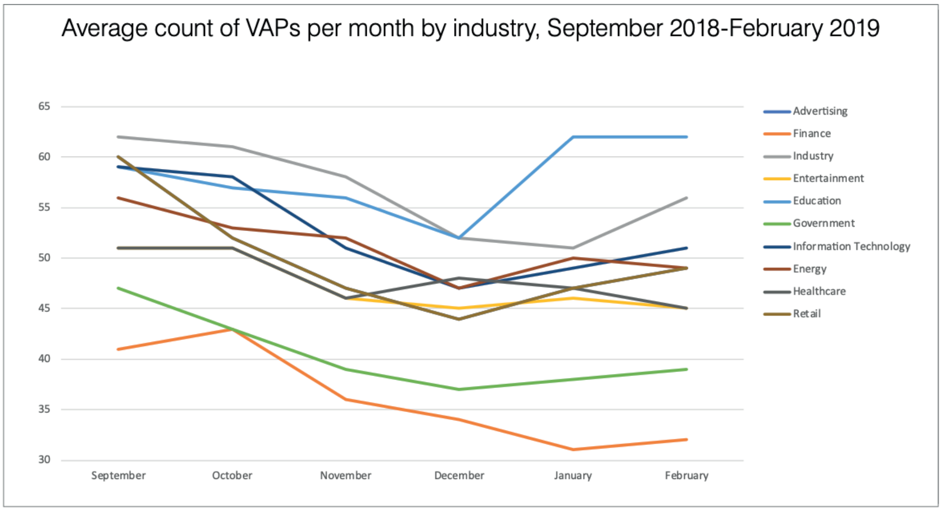


Figure 14: Average number of VAPs per organisation by industry

"VERY ATTACKED PEOPLE" BY INDUSTRY

Figure 14 provides a longitudinal view of the changing number of VAPs per month from September 2018 through February 2019. Seasonal dips around the holidays and the end of the year correspond to fewer targeted attacks overall during this period, while most industries showed an upward trend in the average number of VAPs targeted monthly coming into 2019. Education, heavy industry and healthcare consistently topped the list with the highest numbers of VAPs calculated monthly.

VAP SOURCES

Interestingly, VIPs, like C-level executives and board members are often not VAPs. Instead, email addresses for VAPs tend to be more easily identified online than those for VIPs, making it more straightforward for attackers to discover their contact information and role and target them with high-severity threats. Of the VAPs we examined in a sample across industries, 36% of them could be found online. Note that some VAPs may have been found in more than one place. For executives in our sample, only 7% of their email addresses could be discovered online.

However, for the VIPs who are also VAPs, almost 23% of their email identities could be discovered simply by a Google search. The intersection of VAP and VIP represents an area of particular risk for organisations.

FEATURE

Human Factor

continues from page 45

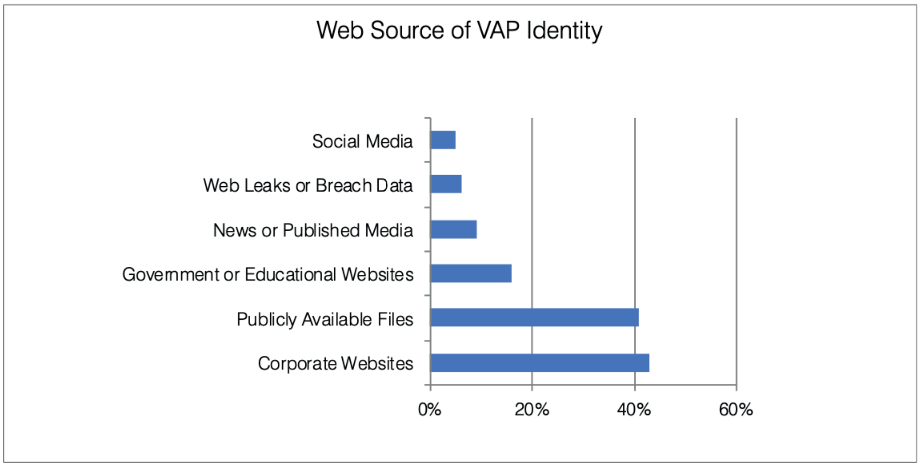


Figure 15: Common sources of VAP identities, 2018

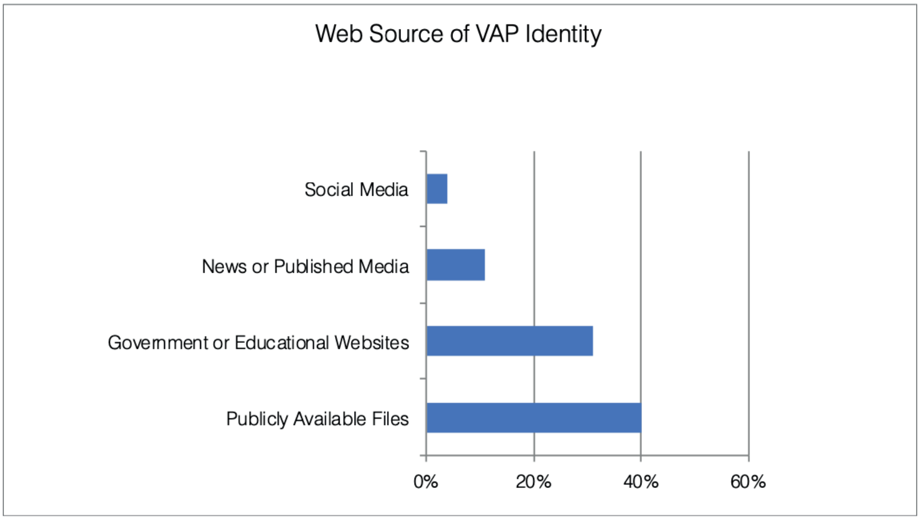


Figure 16: Common sources of VIP identities, 2018

TOOLS AND TECHNIQUES

Exploiting the human factor is the bread and butter of modern threat actors. Convincing people to take action—whether revealing credentials and sensitive information through phishing attacks or installing malware by following malicious links or opening macro-laden documents—relies on a range of tools and techniques. Each of these techniques builds rapport with individuals, creates believable situations, establishes credibility and creates a sense of urgency. Several categories of these techniques are outlined below.

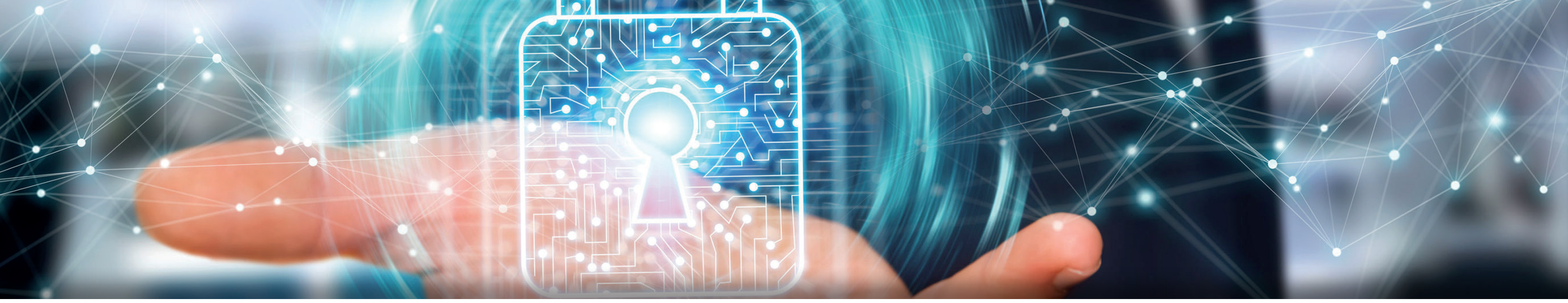
SOCIAL ENGINEERING BASICS

Social engineering is at the core of the majority of attacks we observe. Approaches range from simple lures designed to spark sufficient curiosity for victims to open a malicious document attachment—for example, a fake invoice sent to an accounts payable team or a résumé emailed to Human Resources staff—to much more elaborate schemes. These might include the threat of a lawsuit over a fabricated incident or threat through the exposure of potentially damaging online habits.

While themes vary widely by both actor and intended target, food, shelter, love and money are perennial favourites. Carbanak Group, for example, is a sophisticated, financially motivated actor who uses carefully crafted lures and professional-looking document attachments to distribute multiple strains of malware. For example, a Carbanak campaign in late 2018 featured a document attached to an email in which the sender claimed to have been double-charged and demanded resolution. The document used an increasingly common tactic among threat actors: stolen security vendor branding with claims that the vendor's technology protected the document. Embedded instructions to "decrypt" the document, however, were the steps to enable macros and allow the installation of malware. In the Carbanak example, these macros installed the GRIFFON backdoor. We have observed similar campaigns abusing a range of security company brands for social engineering.

This type of social engineering in a convincing lure and a realistic malicious document are typical of Carbanak and often carries into targeting as well. For example, Carbanak frequently targets restaurant chains with lures related to purported cases of food poisoning at a restaurant.

Real estate lures also provide noteworthy examples of social engineering. Because real estate transactions often involve contact with multiple parties, high degrees of urgency, the exchange of personal



information and digital signatures, they are frequent targets for criminals engaged in both phishing and malware attacks. Threat actors routinely abuse the DocuSign brand, a trusted source for electronic signatures, at all steps of a real estate transaction. In addition to the frequent abuse of trusted brands like DocuSign and various realty and bank portals, the stress and often unknown elements associated with buying a home or applying for a rental create compelling opportunities for threat actors to leverage the human factor.

Love and sex, on the other hand, prey on the lonely and general concerns about privacy. Dating scams, affiliate spam related to various products, and so-called "sextortion" scams are rampant in email. In sextortion schemes, threat actors send messages claiming to have evidence of the victim's potentially damaging online activities, often backing up their claims with passwords associated with the recipient's email account or publicly available personal information. While the passwords themselves may be guesses or old passwords gleaned from a data breach, the emails are designed to create panic and convince users to quickly pay the sender not to reveal browsing history, compromising webcam photos and more. In most cases, these are straight blackmail schemes, but we have also detected malware attacks delivered with the scams as well.

Regardless of the particular theme, some degree of social engineering appears in most campaigns. Given that over 99% of the threats we observe require human interaction to execute— enabling a macro, opening a file, following a link, or opening a document—the element of social engineering is key to successful attacks. More importantly, this technique is particularly useful, taking advantage of human vulnerabilities when software vulnerabilities are increasingly rare.

ACTOR SPOTLIGHT: TA557'S FAKE JOBS

An actor we track as TA557 uses multiple points of contact to complete their social engineering scheme and better establish a relationship with the victim. TA557 sends a LinkedIn invitation to the victim using a legitimate account and then follows up with a personalised email without any malicious content. It is not until a subsequent email that the actor sends a malware-bearing message.

This type of attack, with multiple touchpoints and in-depth social engineering, has previously been associated with BEC, a scenario where actors convince victims with access to corporate funds or sensitive information to initiate fraudulent wire transfers or send sensitive personal information to a threat actor posing as a business leader in a position of authority. In this case, however, TA557 uses the interactions to more effectively trick victims into installing malware. We are increasingly observing this cross-pollination of techniques and more effective targeting by malware actors who are capitalising on the human factor rather than the scale of their attacks.

Domain abuse: Brand theft and look-alikes Believable domains and web presence tangibly support social engineering efforts. Whether malicious and fraudulent websites use stolen branding to create legitimate-looking landing pages or threat actors register domains that resemble those of real brands, fraudulent domains are a critical piece of the cyber criminal's toolkit.

While the frequency with which particular brands are abused changes from month to month, the first half of 2019 bore perennial favourites. Threat actors stole branding and created lures and landing pages most often for

- Major US and international banks
- Amazon and other major retailers
- Cellular providers
- Shipping carriers
- Document signing and electronic faxing services

Hundreds of brands, however, frequently appeared in malicious emails.

Although many threats simply stole visual branding without regard to hosting domains, many others layered domain fraud techniques into their scams. Look-alike domains are increasingly sophisticated, sometimes making use of Unicode characters that render indistinguishably from the ASCII characters for which they are substituted.

In other cases, threat actors rely on more traditional approaches, substituting the number three for the letter "E", the number one for the letter "I", and so on. Regardless of the particular substitutions, at a glance, the domains are close enough to the originals to fool even savvy but hurried victims.

Beyond strict look-alikes, threat actors also register seemingly legitimate variations of brand-owned domains. For example, acmeanvilssupport[.]com would appear to be associated with acmeanvils[.]com but provides opportunities for social media support account fraud (also known as angler phishing), impostor email attacks and more.

Human Factor

continues from page 47

Notably, these domains feature secure certificates at much higher rates than domains across the web, creating a false sense of security and privacy for potential victims. Recent Proofpoint research demonstrated that fraudulent domains implemented SECURE SOCKETS LAYER (SSL) certificates at three times the rate of their legitimate counterparts.

At the same time, threat actors tended to register .com domains for these schemes, further adding to the sense of trust and familiarity that cannot be achieved with TOP-LEVEL DOMAINS (TLDs).

GOOD FOR BAD: LEVERAGING LEGITIMATE INFRASTRUCTURE

As we increasingly move infrastructure to SaaS platforms and rely on a variety of file-sharing, collaboration and communications tools, threat actors take advantage of their familiarity and frequent whitelisting to distribute malware, host phishing templates and more. Frequently abused platforms include:

- Document collaboration services like Google Drive and Microsoft Office 365
- File-sharing services like Box and Dropbox
- Mass mailing services like MailChimp and SendGrid
- Payment services that allow outbound mailing of invoices
- Social media platforms

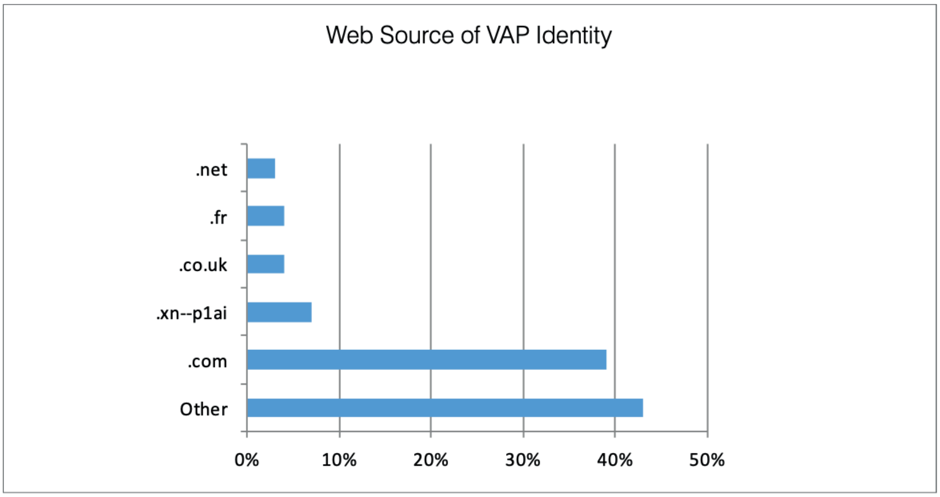


Figure 17: Top TLDs appearing in fraudulent domains 2018. Note that ".xn--p1ai" is the ASCII equivalent of the Cyrillic Unicode text representing the .ru TLD

Recently, we detected sophisticated phishing templates hosted on GitHub, a ubiquitous platform for code development that includes free hosting for projects.

In contrast, campaigns hosting malware on Google Drive, Microsoft SharePoint and other similar services are almost daily occurrences. Not only can these attacks bypass traditional defences because legitimate uses prevent organisations from blacklisting them, but they also leverage the human factor quite effectively.

Because we are conditioned to open links received in notification emails from these services, users often do not consider that the links may lead directly to malware or credential phishing.

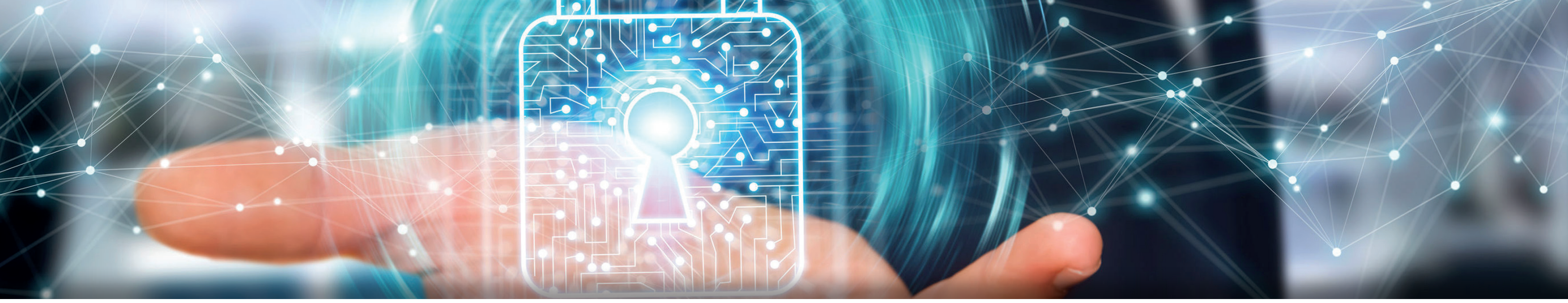
Although the human factor is focused on attacks against people rather than infrastructure, SaaS infrastructure is the exception that makes the rule.

If attackers can infiltrate SaaS platforms, they can launch a range of secondary attacks like those described above that are hard to detect algorithmically and even harder to spot by users. In addition to using the platforms to send spam or host malicious content, they can conduct internal phishing that requires sophisticated detection mechanisms to separate from legitimate emails from trusted colleagues. The widespread availability of credential dumps has also provided threat actors with deep data mining capabilities that inform credential-stuffing attacks and other intelligent brute-force attacks on SaaS platforms.

Equally important, people often reuse passwords—another element of the human factor— making even badly dated credential dumps useful sources of information for attackers looking to compromise SaaS accounts and platforms. Recent Proofpoint research discovered that 45% of organisations have at least one compromised account and 6% have at least one VIP account compromised, making effective internal phishing and BEC relatively easy for attackers.

IMPOSTOR ATTACKS

Impostor attacks leverage a range of techniques to convince victims that they are communicating with a trusted entity. These include display-name spoofing, domain spoofing, and look-alike domains and may lead to wire transfer fraud, angler phishing, malware attacks and more. The unifying attribute, however, is "identity deception,"



where threat actors pretend to be a CEO, a colleague, a business partner, or even support staff for a given brand interacting with customers. These are differentiated from more common attacks that simply use throwaway attacker-owned addresses and domains to launch and host malware and phishing attacks.

While impostor attacks were initially most closely associated with BEC, they are proving highly useful tools for a range of payloads and attacks. If employees receive a document that appears to be from <ceo name>@yourcompany.com, they are far more likely to open it than if it comes from <randomname>@gmail.com.

Impostor attacks continue to evolve. Figures 5-8 suggest many seasonal and industry trends, with threat actors continuing to focus on so-called many-to-many attacks. While early BEC attacks usually involved a single spoofed identity targeting a small number of users, attackers now often spoof many identities and send impostor attacks to many individuals within a given organisation.

These attacks tend to be much smaller in scale than traditional malware attacks that can blanket an organisation. Still, the broader targeting appears to be netting higher returns for actors than earlier approaches.

The attacks are also tailored to the targeted industry, with education, for example, favouring subjects related to "Requests" and "Greetings". At the same time, engineering firms are more likely to see "Urgent" subject lines. Seasonal trends, on the other hand, show payment demands, for example, accelerating in the first quarter of 2018 and 2019. Yet company size continues to have no appreciable effect on the frequency or nature of impostor attacks. Social engineering in these attacks is effective and lucrative, regardless of company size.

This type of tailor-made attack represents the current state of the art in social engineering and exploitation of the human factor.

CONCLUSION

The human factor defines the actions and motivations of most threat actors today. The vast majority of attacks prey on people and human nature. Even automated exploits are frequently deployed in ways that still require initial execution by users rather than devices. With the widespread deployment of SaaS platforms and rising incidence and sophistication of impostor attacks, the stakes are higher than ever for organisations.

People remain the primary target of attackers and the last line of defence for organisations, making a focus on people, as well as more traditional layers of security and training, critical to a holistic approach to defence.

RECOMMENDATIONS

Today's threats require a people-centric approach to keeping users safe. We recommend the following as a starting point:

- Adopt a people-centred security posture. Attackers do not view the world in terms of a network diagram. Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.
- Train users to spot and report malicious email. Regular training and simulated attacks can stop many attacks and help identify, especially vulnerable people. The best simulations mimic real-world attack techniques. Look for solutions that tie into current trends and the latest threat intelligence.
- At the same time, assume that users will eventually click some threats. Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. Isolate suspicious and unverified URLs in the email. And stop outside threats that use your domain to target customers.
- Build a robust email fraud defence. Email fraud can be hard to detect with conventional security tools. Invest in a solution can manage email based on custom quarantine and blocking policies.
- Protect your brand reputation and customers in channels you don't own. Fight attacks that target your customers over social media, email, and the web—especially fake accounts that piggyback on your brand. Isolate users' browsing and webmail from your environment. And look for a complete social media security solution that scans all social networks and reports fraudulent activity.
- Partner with a threat intelligence vendor. Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics and targets—and then learns from them. wn

© Article courtesy of Proofpoint.

Does information security come with French fries?

Protecting sensitive information goes as far back as the early to mid 20th century. An encryption machine known as Enigma was used extensively by Nazi Germany in World War II. Text was typed on the machine and "scrambled" and then deciphered. Fast forward to 2020, and we have the most technologically advanced encryption systems. To crack a document with 128-bit Advanced Encryption Standard (AES) would take a billion billion (no that's not a typo) years. Encryption tools are not just exclusively for military or government sectors but are readily available for us to use in our businesses and on our home computers.

BY | ULANDI EXNER
CISSP CISA CGEIT CERTDIR PMIITPSA
B COM INFOMATICS
PAST PRESIDENT | IITPSA

So, I beg the question, why are we not protecting our personal and private information? It is as easy as boiling an egg (ok for me that doesn't know my way around the kitchen, this is a bit more difficult). Not only should we protect ourselves against identity theft and loss of information assets, but it is now legislation. The Protection of Personal Information Act (POPIA) was signed into law on 19 November 2013. It is not yet in force, and word on the street is that the commencement date will likely be in April 2020. The Information Regulator has been hard at work at setting up the required structures to monitor and enforce compliance by public and private organisations with the provisions of the Act. Once the enforcement date is announced, companies have 12 months grace period to ensure compliance. If organisations are found to be non-compliant, the penalty is a R10 million rand fine (not exceeding) or trade-in your Gucci suit for an orange overall to serve a ten-year sentence.

The purpose of POPIA is to protect

individuals' personal information and privacy.

In essence, it will be unlawful for anyone to process personal information without your consent and having obtained permission, must take reasonable steps to protect your information. Personal information is any data which can be used to identify an individual, eg, identity number, e-mail address, race, gender, age, religion etc.

I ask with tears in my eyes, why do companies that we entrust our data to, which not only have access to sophisticated encryption tools but also need to comply with the law, allow my data to be compromised? The Green bank recently made the headlines when their service provider's IT systems were compromised. As a client of the Green Bank, I am furious that not only was my personal information shared with a third party, but it was done without my consent which is in direct contradiction of POPIA. The Green bank released a press statement advising clients that our bank accounts have not been compromised, but what about my name, ID number, telephone number and physical as well as electronic mail address that has now been exposed? It doesn't require much effort or information to commit identity theft and fraud.

Another major data breach which occurred in South Africa was in 2018. Unfortunately for me, once again, it is a service I subscribe to. (I need to rethink my choices). I shall refer to them as the Blue Insurer, and as the synonym for their business name suggests, my data was made "freely" available. The company was subject to illegal and unauthorised access to its

Information Security & French Fries

continues from page 51

IT infrastructure, which was primarily e-mails and attachments. Similar to the statement made by the Green bank, the Blue insurer advised clients that the data that was accessed was "unstructured data" and that there is no evidence that any of its customers have suffered any financial loss. That is a comprehensive statement to make because the damage may not be realised immediately. The horse has bolted, you can't unring a bell. My data is out there, thanks to the Green Bank and Blue Insurer. I go to great lengths to protect my privacy and secure my data, but companies I entrust with my data don't seem to have much regard for data security. Is information security an afterthought or entirely just overlooked? Do companies cross their fingers and hope data breaches don't happen to them?

A data breach is not just about dealing with financial loss but also leads to reputational damage for both companies and individuals. In July 2015 a commercial website which is a platform for extramarital affairs was hacked. The hackers obtained personal information from the site's user base and threatened to release the data if the website was not shut down. The company did not cede to the hacker's demands, and in August, the hackers released more than 25 gigabytes of company data, including user details. I will reserve my judgement on the ethical practice of the site but releasing names of the subscribers had far-reaching consequences for some.

Picture this – you have been married for 15 years to your partner that adores you and you have two beautiful children. You are a well-respected member of your community, and you are at the pinnacle of your career and life could not get any better. The morning of 20 August 2015, your kids are crying, the dog wants to bite you, and your partner is nowhere to be found. You notice an envelope placed on the dressing table. You open it up, and the mystery to the unusual sequence of events of this morning is solved. Your details were listed on the website, which facilitates extramarital affairs. But you never signed up on the website! How can this be? You grab your phone and call your best friend and explain the situation them. Your friend suddenly remembers that as a prank they registered your details on the site and completely forgot about it. See the implications of websites not securing personal data? While it was wrong of the friend to post personal details of you on the site if there were security measures in place, this prank wouldn't have gone so wrong. My story was fictitious, but it is not far from the truth.

While I lament the lack of controls that exist within organisations who store our personal information, we unwittingly "sell our souls" for freebies. We provide personal information such as name, e-mail address and telephone numbers when we enter competitions. Maslow's hierarchy of needs lists the necessities that man need for survival which is food, clothing, air and shelter, but wi-fi has become one of the primary human needs in today's developed world. There is no such thing as a free lunch, so to gain access to free wi-fi we part with personal data in exchange for connectivity. So now that we are connected, we are back on Instagram posting pics of our calamari salad and tagging all our friends on Facebook and oh, while we are at it I forgot to pay my account so let's do some banking quickly. Sitting in the corner is not a guy with a hoodie but a 15-year-old girl capturing your data because you connected to her "free wi-fi access point hotspot". This doesn't just happen in the movies. This is reality.

As a society, we have been trained to cover our hand while keying in our pin at the ATM, or when swiping our credit card. We don't want unscrupulous characters to gain access to our bank accounts and withdraw our hard-earned money. Do we afford our data the same level of protection and care as our atm pin? In some respects, we are very security conscious and other times not. I am not advocating that we hide in a corner with tinfoil on our heads, but we need to be mindful at all times when we give out information. Our parents taught us to never talk to strangers, but yet we share all sorts of information with strangers online all over the world.

According to Stats SA cellphones dominated the list of items lost through theft of personal property affecting 69.1% of the victims for the period 2017/2018. It amazes me to see how many people don't have a screen lock on their cellphones. Smartphones are computing devices that fit in your pocket. Other than watching cat videos on your phone, you use it to communicate and store data. Yes, you may not have Coca Cola's secret recipe on your phone, but your information is valuable to someone.

Securing personal information is not rocket science—question why companies need your personal information and what mechanisms they have in place to secure it. Be vigilant with your own storage devices such as mobile phones and computers and like you don't share your underwear, don't share your passwords with ANYONE! wn

4 CHANNEL CAMERA

- Remote Viewing: C-CMS, Smart Phone, Surveillance and IE Browser
- Recording Mode: Motion Detection, Schedule and Full Day Recording
- Alarm: Optional
- Resolution: 1280 x 960 (960P)
- Day and Night: Auto I CR
- Box includes: 4x Outdoor Cameras, 1x DVR, 1x 1TB Hard Drive
- Product code: Q0010241

Bloemfontein 051 448-0996 Cape Town 021 593-1114
Durban 031 319-5400 Johannesburg 011 677-2500
Port Elizabeth 041 374-1687

info@wacoelec.co.za www.wacoelec.co.za

WACO®
industrial electrical distributor

SAFE HOUSE™
Suppliers you can trust

Proudly Bidvest

2019 IEC Young Proffesionals Essay Competition Winners

In July 2019, the South African Bureau of Standards (SABS) ran an essay competition for the IEC Young Professionals Programme where candidates were required to write an essay about the following topic:

Artificial Intelligence (AI) is becoming common in everyday application, from search engines to autonomous vehicles. Which areas of AI should the IEC prioritise standardising and why do you think these areas are essential?

The two winners are: Mr Mpendulo Dlamini & Ms Ntitiseng Moloi.

About the IEC Young Professionals programme:

The IEC Young professionals' (YPs) programme was started by the International Electrotechnical Commission (IEC) in 2010, targeting engineers aged between 20s to mid-30s, working in the electrotechnical industry.

The objective is to ensure that the technical work of the IEC would be future-proofed with a growing number of new generation technical experts familiar with standardisation and the role of the IEC.

The first IEC YP programme took place in 2010, and South Africa was represented then and every year. Since 2013, the South African National Committee (SANC) of the IEC has been organising this competition every year and select two candidates to represent South Africa at the IEC Young Professionals programme which is held in conjunction with the IEC General Assembly meeting.

The interest in the competition and the local South African journey of IEC Young Professionals has been growing each year. This year nine essays received and evaluated.

Two local participants obtained the highest scores from their essays, and they won the prize. The prize for this competition included attending the IEC Young Professionals workshop which took place in Shanghai, China between 21-25 October 2019. The winners were part of the South African delegation, and these candidates were also given an opportunity by SABS to become part of the National Technical Committee of South African of their choice.

The two South African IEC Young Professional delegates participated in a three-day workshop. They learned about the following IEC work and its objective: IEC Strategy overview presentation, Foundation for leadership, IEC Standards development processes, Advanced management of standards development, Simulating of an IEC technical meeting exercise, IEC Conformity Assessment System.

AREAS WHICH THE IEC NEEDS TO PRIORITIES DURING STANDARDIZATION OF ARTIFICIAL INTELLIGENCE

By Mpendulo Dlamini

The 21st century has experienced a rise on the application of Artificial Intelligence (AI), due to improvements in computing power, storage capacity, advanced algorithms and increased data volumes which has become part of the technology industry and has assisted in solving many complex problems. Machine ability of significant data processing coupled with an ability to recognise patterns has made it possible for machines to learn experiences, adjust to new inputs and perform human-like tasks.

There are several features of AI mentioned by Statistical Analysis System (SAS) that have accelerated its application. The ability to perform high volume task reliably and without fatigue, the ability to add intelligence to existing products, the ability to adapt through progressive learning algorithms, ability to analyse more and more in-depth data (i.e. using a neural network) and high accuracy.

Due to these incredible features, AI has, therefore, become an essential and unique

technology. Andrew Ng, the creator of the deep-learning Google Brain Project and an adjunct professor of computer science at Stanford University, describe it as the 'new electricity', which will soon control most of our activities in society and business. This will change how we work and live, and therefore, we must learn as much about AI at an early stage!!

Lasses Rouhainen identifies nine reasons why everyone needs to seek more information about AI technologies. The speed in which AI is being introduced is incredibly fast, which makes it challenging to keep up with and as a result, only a few people understand all the implications brought by it. There will be a definite impact on society as it is applied to many different areas of life. Nearly every large tech company, for example, Google, is investing in AI research and development; which demonstrates the level of importance it holds for businesses. Due to the rapid growth of AI, there is a need for knowledgeable workers such as data Scientist, machine learning experts and other technical professionals who can build AI.

Both big and small companies can apply it, and those who do it first and correct will enjoy the competitive advantage it brings. Laws and regulations of each country will need to be reviewed and updated to incorporate the new trends. Companies need to develop new technologies that ethically and responsibly serve humanity for the better and improve the standard of living; thus, these types of policies need to be introduced sooner than later.

Advantages and opportunities that are offered by AI need to be communicated effectively; tech companies tend to provide the most positive outlook. However, people often have negative impressions about AI tools due to lack of understanding. Sharing information about the advantages will help people to feel comfortable about adopting these new technologies. There needs to be a true and open collaboration internationally; between the private and public sectors.

Artificial Intelligence or deep learning is becoming common in everyday applications and industries. There are several areas in which AI is applied today, such as Health care, retail, banking sector and mining sector. These will be reviewed in this paper. Furthermore, the benefits and the current challenges faced within each industry will be explored. This will then inform which areas of AI need to be standardised.

In Health care, it is employed to analyse relationships prevention or treatment techniques and patient outcomes. The AI programs have been developed and applied to practices such as; treatment protocol development, drug development, personalised medicine, diagnosis processes, and patient monitoring. Large companies such as IBM and Google have developed AI algorithms for healthcare. AI can assist medical doctors in making better clinical decisions or replacing human judgement in specific functional areas of healthcare (e.g. radiology). This is enabled by the increasing availability of healthcare data and rapid development of big data analytics.

According to Accenture, the growth in AI healthcare market is expected to reach $6.6 billion by 2021, compound annual growth of 40%. Although AI technologies are attractive in medical research, real-life implementation is still facing challenges. The General Data Protection Regulation (GDPR) directives, which was introduced in May 2018, will result in new regulations that need to be complied with of which in some cases are not clear. For example, some degree of transparency in automated decision making; it is difficult to establish from the directive what level of transparency will be sufficient. Secondly, the requirement for informed consent

IEC YP Competition Essays

continues from page 55

since the AI system needs to be trained continuously by data from clinical studies; data exchange remains a problem. The current healthcare environment does not provide incentives for sharing data on the system; for startup companies, it is difficult to gain access to data that would be pivotal in developing new products or business cases. Transparency is paramount to medical AI; a doctor needs to be able to understand and explain why an algorithm recommended a particular procedure.

The challenge from a social culture point of view is getting doctors to consider suggestions from an automatic system can be difficult. Ideally, AI literacy would need to be introduced into medical curricula so that it is not perceived as a threat to doctors but rather as aid and an amplifier of medical knowledge.

A survey of 400 retail executives conducted by Capgemini in August 2018, revealed that AI could save retailers as much as $340 billion by 2022. Capgemini estimates that 80% of savings would come from AI enabling for efficient processes for supply chain and returns. It would increase promotion efficiency and reduce customer complaints. Payment and retail firms have used AI for; spotting fraudulent charges and giving customers a more personalised online experience to reduce claims and increase customer satisfaction.

Derrick Johnson CEO of Encounter AI created 'Mai', the world's most advanced artificial intelligence voice-enabled systems which assist with ordering for retailers and restaurants that also provides accessibility for the visually impaired. It can quickly and efficiently handle complex situations; for example, if a visually impaired person has dietary restrictions; Mai can process that information and only offer items that fit their requirements. One of the challenges in the retail environment is that data is often too vague to translate directly into machine learning. Another problem is that the people who create the algorithms do not have clean data to work with or fully understand which data is most important.

AI in the financial industry has increased productivity, particularly in the accounting and banking areas. One of the key drivers of AI adoption in this sector is the time-saving benefits. Instead of long hours being spent working on spreadsheets, processing data or handling customer enquiries; AI allows workers to focus on complex tasks. Amalgamated Banks of South African (ABSA) has invested more than R350-million in the past three years on specifically robotics and AI.

The banking sector is one sector where the availability of large amounts of information is not a problem. For many years the banking sector has been accumulating information on our preferences, credit history or family situation and consumer behaviour. The challenge arises in enabling the use of this data in machine-learning systems while protecting the client data.

Another limitation of machine learning in this context is reliability on historical data sets; as a result, it can become repetitive and potentially be giving way to conscious or unconscious bias. According to Naadiya Moosajee, a serial entrepreneur by passion and a civil engineer by profession, although the race and gender information may not be explicitly captured. AI can, however, use location data and habits to predict gender and race; thus discriminating against applicants.

According to Andrew Ng, AI will perform the following tasks in manufacturing: quality control, reduce material waste, shorten design time, improve production reuse, predictive maintenance and more. Ongoing support of production line machinery represents a significant expense. Furthermore, unplanned downtime can cost manufacturers an estimated $50 billion annually, and asset failure is the cause of 42% of unforeseen downtime events. Therefore, predictive maintenance using AI has become critical for manufacturers who have much to gain from being able to predict the next failure of a part, machine or system. This can reduce unplanned downtime and extend equipment and machine life. Manufacturers are experiencing difficulty maintaining high levels of quality and complying with regulations and standards. Thus, AI algorithms can notify the manufacturing teams of emerging production faults that are most likely to cause quality issues. These AI algorithms can also be used to optimise manufacturing supply chains; this can assist companies to anticipate market changes giving management a considerable advantage moving towards a strategic mindset rather than reactionary.

Data required to establish rare but expensive failures does not exist. Hence, no matter how much data can be collected from a real-world process; usually, this data is incomplete. However, building better algorithms that can make sense of data stored in manuals and can also tap into the knowledge of experts. AI process automation still needs the architecture to be developed; this can enable secure development and deployment of the machine learning algorithm and allow quick switch-out when better algorithms

are phased in. Robustness, rather than just accuracy needs to be focused on; it should be designed to alert humans when the algorithms have trouble reaching a conclusive prediction or recommendation.

In the mining sector, AI has improved areas such as mineral exploration, safety and maintenance, autonomous vehicles and drillers. AI has a potential of assisting mining companies in locating minerals to extract. Thus, many mining companies are excited by this prospect. So finding metals such as gold will no longer be art but rather a science with the aid of AI learning. IBM Watson and Goldcorp are using it to review all the geological information available to establish better drilling location. Since these methods can be more precise; it can help the mining industry to be more profitable. Similar to the manufacturing industry, the mining equipment can be monitored before breakdowns occur; thus transforming preventative maintenance to predictive maintenance. This can be achieved by analysing real-time data obtained which will ultimately lead to safer mining operations for all involved.

Several companies, including; Rio Tinto, BHP, Stanwell and Fortescue, have begun using autonomous haulage trucks at their mines. Companies such as Komatsu have developed driverless vehicles in the mining operation which utilise a combination of wireless communication, on-board computers, GPS systems and AI software that enable the trucks to operate autonomously.

Mining companies do not have data problems, and global mining does not have an innovation problem either. Instead has what can be loosely described as a "technology adoption" problem. This stems from three main barriers, as defined by Don Duval: 'Try before you buy', 'Vet before you buy' and 'Innovation is a team sport'. Before mining companies invest in new technology, specific validations and balances are required to validate that it can operate in a mining environment, rather than just in an academic lab setting. Mining companies need assurance that the life expectancy of the new technology is substantial to deliver ongoing service and support over the life of the deployed technology. If the vendor is questionable or appears unreliable; this becomes a concern. Lastly, mining companies are increasingly seeking meaningful partnerships to form in both the development and deployment space of technology solutions.

In this paper, different applications of AI in economic sectors have been presented and discussed. There are undoubtedly added benefits of utilising AI across the mentioned commercial or industrial areas which can be summarised as efficiency, precision, time-saving and increased profitability. However, there are some challenges and concerns encountered in each of these areas, of which some are common. Some worries and problems can be summarised as; data security and privacy, data quality and integrity, and transparency. There are no definitive standards that outline the level of privacy, security and clarity that is required for AIs, nor are there processes or methods that ensure the integrity and quality of datasets used. This becomes pivotal for the industry adoption process. Perhaps we need also to understand why standardisation of the AI is crucial. Irrespective of the fact that AI is being applied differently and in different areas of the economy, it depends on; gathering, analysing and sharing large volumes of data which are being exchanged between applications. Thus, standardisation will enable a consistent base for reuse of data. This will then ensure visibility over whether the quality is adhered to and reduce human error; this will ultimately promote morale and facilitate the adoption of this technology.

So which areas of AI must the International Electrotechnical Commission (IEC) give priority in standardising? The concerns around data security and privacy preservation have been expressed. If not handled in a delicate manner, most notably in the health and financial sector; it can be misused, or the deep learning networks can be vulnerable to malicious attacks. IEC first needs to standardise the level of security and privacy features applied to machine learning devices.

Deep learning relies on large amounts of good quality and correct data to train algorithms. The importance of this has been seen in these different sectors discussed. The impact of using incorrect data can be anything from misdiagnosing equipment or humans; resulting in a financial or human loss. Furthermore, the handling of bias in the data needs to be considered. It has been illustrated how the application of machine learning techniques to drive personal decision-making can introduce an ethical dilemma when making decisions that affect peoples' lives, as shown in the financial sector. A combination of these factors, in turn, can breed trust issues – with the general populace losing faith in AI.

It is imperative that the data set used is clean, calibrated and synchronised with other data sources to produce useful results. It is

IEC YP Competition Essays

continues from page 57

essential to consider carefully the processes that generate the data. Is the dependent variable a result of a subjective decision? Failing to consider bias will lead to poorly performing models. The IEC needs to standardise the minimal data set required for an AI system, specify methods to verify the level of data cleanliness and define processes that generate the data. There can be instances where the algorithms are unable to predict or recommend a solution conclusively, or instead, the outcomes are not comprehendible nor explained. There must be some alerts introduced in the AIs to cater for events where the answer cannot be conclusively deduced. Where solutions are not comprehendible, the AI must provide some insight to the user as to the factors that were considered in determining the solution. The IEC needs to prescribe the level of alerts and types of signals that need to be embedded in an AI system. Lastly, there needs to be some level of transparency that the AI system must provide for it not to completely operate like a "black box". This also needs to be considered by the IEC.

WHICH AREAS OF ARTIFICIAL INTELLIGENCE SHOULD THE INTERNATIONAL ELECTROTECHNICAL COMMISSION PRIORITISE AND WHY?

By Ntitiseng Christinah Moloi

Standardisation holds a great responsibility in ensuring that there is uniformity in aspects such as terminology, product dimensions, as well as functional requirements. This, in turn, simplifies universal communication and establishes mutual understanding across industries. There must be no inter-industry barriers to ensure an efficiently run industry.

The technical industry is not immune to this fact. Standardisation is essential as the end products and services of this sector are usually designed such that human beings can interact with them. In setting standards for the end products, the safety and protection of fundamental human rights should be protected. In doing so, innovation in the Artificial Intelligence space should not place a threat to the environment or harm wildlife. These can be regarded as the primary requirements that can be considered when new inventions or upgrades are developed.

Artificial intelligence is a product of the highly anticipated fourth industrial revolution and is rapidly growing. It is without a doubt that the definition of standards will have to keep up with this rapid change. The fact that a forever changing field requires an agile environment that is open to change and the unalterable/rigid nature of standards, in general, creates a contradiction, and this poses a challenge. Multiple conversations arise from this contradiction as a result. One such discussion is the question of the order in which the areas of Artificial Intelligence should be standardised.

One thing to consider in setting these standards is that bodies such as the International Electrotechnical Commission (IEC) need to prioritise setting standards for products or devices whose impact is predicted to be the most disruptive. This negative disruptiveness can be measured in different ways, for instance, a violation of fundamental human rights is an extreme disruption and any inventions that have the potential to violate a human right should be standardised first.

There has been a rise in the production of smart personal assistants such as Siri and Google Now. These are prime examples of how AI has been successful in simplifying human life. These services provide real-time assistance with day to day tasks, more efficiently than a human personal assistant would. There are, however, concerns around the data that these services require so that they can be able to function. A new term "ubiquitous surveillance" has since been developed to define the ongoing collection of personal data by these technologies. It is inevitable that the general public, especially the users, would feel uneasy about this, despite the disclaimers and reassurance statements that are issued by the manufacturers of these devices.

Artificial intelligence is one of the by-products of the fourth industrial revolution, and the nature of this revolution has been defined as fast-evolving. The effect of this may require that the adopted

standardisation process be an innovation-friendly framework so that it can suit discoveries such as the smart personal assistants described above, which are going to be fast-paced in their development. Standardisation in this field is to emphasise data security, in turn protecting the user's right to privacy.

Over and above, ensuring data security, the algorithms that are developed to design these devices should also be standardised. This means that a collaborative effort between the existing regulatory bodies as well as the individuals skilled in programming and algorithm development would need to be established.

For the sake of ensuring that users are not in danger, the prioritisation of electronic devices that human beings interact with will need to be considered. More particularly, the applications of Artificial Intelligence that are to be in physical contact with the human body. In the electronic space, Artificial Intelligence has the potential for growth in the smart appliances space. The overloading of a specific device/appliance with information may jeopardise its functionality and may turn it into a hazard. This may occur because, initially, the apparatus may have been created to perform a specific task that would not need interaction with the internet nor need to collect and store data. Once these functionalities are incorporated into the device, the electrical specifications of the appliance/device will change.

Standardisation in this field will ensure that the transition from usual appliances or devices to smart devices or machines is a smooth one. The importance of doing this is for safety assurance purposes. A simple example would be a smart electric blanket that changes temperature according to your body temperature. This is different from a standard electric blanket that requires that the user manually controls the temperature.

The smart electric blanket would then be considered as an upgrade from the traditional electric blanket as temperature sensors would now need to be incorporated into the design. Artificial Intelligence, in this sense, would be the programming of the decision making that happens "in" your little blanket. How Artificial Intelligence solves a complex problem is as follows: Firstly, recognising that the user is feeling cold by the use of sensors, Secondly, remembering the temperature at which the user usually appears to be at rest during the night and thirdly, heating the blanket to that temperature sooner. Owing to this upgrade, the number of components that need to be powered would have increased, and the power rating of the blanket would then need to change.

The commercialisation of inventions such as the smart electric blanket, standards has to be set on a maximum number of subcomponents that are allowed to exist in a single design. Rules such as the maximum allowable temperature are to be such that they agree with the optimum operating conditions of the human body.

Autonomous vehicles have stirred discussions on safety, ethical considerations as well as mortality rate reduction. The prevailing concern is that the system might cause the death of many other road users in an attempt to save the life of the vehicle's occupant. There has, however, been sufficient proof indicating that the overall road accident mortality rate will decrease as a result of this invention. It is therefore worth pursuing and implementing standards to which the vehicles should abide.

Setting standards for autonomous vehicles should be focussed on ensuring that the implemented system is secure. The manufacturers should provide proof of anti-hacking measures. The importance of this is easy to deduce. According to the World Health Organisation; on average, one person is killed every 25 seconds in the world as a result of vehicle accidents on the roads. The era of autonomous vehicles has the potential to reduce the mortality rate caused by road accidents significantly. There are, however, concerns that this invention places a high level of dependency on technology and the developed software. There exist many malicious attacks in this space, and this can have extreme effects if not monitored.

A system that is highly dependent on technology is vulnerable to system hackers who might have malicious intentions, for instance, competitors in the same market. In setting standards for this, components that are to be integrated to form a completely autonomous vehicle must be evaluated in an attempt to achieve ultimate safety. Each element of the vehicle that is to work hand in hand with the developed code should have anti-hacking measures incorporated into it.

This is where regulatory bodies such as the International Electrotechnical Commission will have to play a rather important role. Ensuring that electronic devices that are to be integrated to form a more significant system are safe independently before they can get embedded into something bigger.

IEC YP Competition Essays

continues from page 59

Discussions around the Fourth Industrial Revolution and the different areas that exist within it is the possible digitisation of tasks that require human empathy. If the advancement of Artificial Intelligence is not controlled, it has potential to digitise functions that require human to social interaction.

In innovation, it is essential to identify the tasks that cannot be left to a robot to do - tasks that require empathy as well as emotions. If any applications of Artificial Intelligence have the potential to wipe out the need for human-human interaction completely, the standardisation of such areas should also be prioritised where limitations will be put in place. Uniformity in this aspect will require identifying such tasks and ensuring that certain restrictions are put in place to ensure that such tasks are not digitised.

An example I often refer to is a hypothetical scenario - where a non-interactive solution is ensuring that lessees are up to date with their rent payments. A digital system can be established at which point discovering that occupant (x) hasn't paid their utilities for (y) number of months, the water supply and electricity supply can be automatically switched off for the consumer.

In theory, this appears to be an efficient system for municipalities. Still, in cases where the household is occupied by minors and people living below the minimum wage, human interaction would be necessary because the system would not have the moral capacity to identify and deal with these kinds of problems.

Artificial intelligence and the environment
The manufacturing industry is one of the sectors that are to benefit significantly from Artificial Intelligence. The application of Artificial intelligence in digitising manufacturing tasks has proven to improve productivity and efficiency. Artificial Intelligence introduces new processes into the manufacturing system; these are processes such as predictive maintenance, quality control which ultimately play a role in reducing the overall task time.

Manufacturing Industries, in their current state, contribute a lot to the CO2 emissions into the atmosphere. Increasing the number of automated processes within the manufacturing industry could place a threat to the environment by increasing the intensity of this very emission.

More automated means will ultimately increase the overall emissions produced by a factory. Limiting the number of electronic sub-components in a factory could help curb this problem. It is setting technical standards such that they assist in meeting the requirements set by the environmental laws.

The importance of minimising the emission of harmful chemicals into the atmosphere can never be overrated. With the current climate crisis that has contributed to the earth's temperature rising at nearly twice the rate, it was 50 years ago. The effects of global warming are endless, and the standardisation of the technology that could potentially contribute to this should, therefore, be prioritised.

AI AND THE GOVERNMENT

Governments can benefit from the application of AI in some of their processes. Still, careful attention needs to be given to the use in sensitive areas such as health care and criminality. The healthcare industry can benefit significantly from the high rate of accuracy that artificial intelligence possesses. But when it comes to the preservation of human life, how much skill is enough accuracy?

In cases where Artificial Intelligence is used for medical procedures, should the method fail, how do we then determine on the entity that must take responsibility, should it be the hospital (owned by the state) or the manufacturers of the equipment that was used for the procedure. These are some of the questions that would need to be answered when drafting the standardisation of the merger between health care practises and Artificial Intelligence. Robotic surgery is one application of this merger.

Another point to consider is the significant consequences that come about if the procedure is unsuccessful. Apart from the concerns around the application of Artificial Intelligence in the health industry, the use of Artificial Intelligence in the criminal law system is one worth considering. The primary care concerning this is the fear all around that the employed automated system might wrongfully accuse innocent people. Standardisation of the Artificial Intelligence applications in this sector is, therefore, one that should be prioritised.

At a minimum, the standardisation process should provide clarity on the following points:

- How do we measure the accuracy of the designed system?
- Are there systems put in place to assist with the verdict before a proper sentence is picked?
- How much does the evidence provided

by the Artificial Intelligence system count towards predicting the outcome of a case?

- What is the technology that is prohibited from being used in the assembly of an AI judgement system?

The introduction of Artificial Intelligence application is an overall good move as it will introduce an element of accuracy and efficiency. These are generally attractive traits for a system to have in this day and age. This means that more and more systems will be migrating to Artifical Intelligence owing to that fact, which would then mean that every single one of such industries would need to undergo a standardisation reprogramming.

In setting standards for these industries, preference needs to be given to the protection of fundamental human rights.

A collaborative Standardisation process was then suggested where it was proposed that professional regulatory entities collaborate with electrotechnical standardisation bodies such as the International Electrotechnical Commission.

In Exploring, it was found that no industry is immune from being upgraded to Artificial Intelligence; this includes the health system, the criminal system, to name a few. The standardisation of these sectors should inevitably be taken into consideration an attempt.

The unification of these sectors should necessarily be taken into account an effort of keeping up with the fast-paced nature of the Fourth Industrial Revolution. wn

Load Research Chapter 2019 Review and 2020 Plan

INTRODUCTION

The emerging context in South Africa, and globally, is such that the load behaviour is 'disrupted' from what it used to be and this is caused by a number of changes that redefine the customers' behaviour. These changes are as a result of initiatives such as energy efficiency, distributed energy resources and alternative energy sources.

Historically load models for use in South Africa were derived from the old metering data. It has become evident that these load models are starting to deviate from the actual load behaviour due to the recent changes on the customer's side. The gap is expected to be larger in future. The SAIEE Load Research Chapter (LRC) has been established to provide an information sharing platform for load researchers and applicators to share their knowledge and ultimately improve the load modelling and application industry-wide. The scope of the LRC includes exposing the historical developments, the relevance of the current load models and the development of future load models that are mainly dictated by the technological developments on the customer's side and on the power system's side. In this article, the LRC outlines the developments that took place in 2019, which is the year of its establishment and also shares the plan for 2020.

REVIEW OF 2019

4th April 2019 ushered in the successful launch of the Load Research Chapter, during which many entities, companies and institutions were represented. These representatives with consensus, elected the Executive Committee (EXCOM) comprising the Chairman - Monde Soni; Deputy Chairman - Marcus Dekenah and Secretary - Lloyd Setlhogo. The membership is steadily increasing from the 38 members as at 19 December 2019.

At our launch event, attendees were polled in order to determine their needs and interest areas. Their substantial feedback was used to map out a programme of topics and events which formed the agenda of the Load Research Chapter for next 3 years. Topics range from metering of load data through to use of Artificial Intelligence (AI) in applications of load research data. We intend showcasing local academic work on our agenda as well.

Since its inception, the LRC has successfully conducted monthly meetings including presentations covering various topics which attracted huge interest from members. All meetings were conducted from the main venue of SAIEE with a remote connection (Skype) for members outside Gauteng Province. The LRC started holding online Webinars (using SAIEE's facilities) which were well attended.

Ensuring members are kept actively involved and benefit from the information disseminated through the LRC, the following activities were embarked upon: 7 monthly meetings were held, these included 6 presentations covering various interesting topics by LRC members, and we conducted two Webinars.

Our highlight was the seminar held on 3 September 2019 at University of Pretoria. The keynote speaker was Dr Rob Stephen (President of Cigre) and various speakers covered interesting topics. Grateful thanks to the South African National Energy Development Institute (SANEDI) for sponsoring the catering and to University of Pretoria for availing the venue.

The Load Research Chapter has established a landing page on SAIEE's website. All presentations, seminars, webinars and other reference materials are being stored on this site as lasting assets for review and reference by members. We are endeavouring to record our events, which are then added as videos to the LRC webpage and as well as being uploaded to SAIEE's YouTube Channel. The list of content on is growing steadily.

LRC was represented by Monde and Marcus at the SAIEE National Conference held in November 2019 when they manned a table that promoted the chapter.

The Executive Committee (EXCOM) meets monthly to ensure smooth running of meetings, planning events and consultation with presenters. The EXCOM submitted an Events Plan and calendar for 2020 to the chapter members which were well received by members.

2020 PLAN

In 2020, the LRC is planning to intensify the initiatives on knowledge sharing. The plan is to attract experts from international institutes as well as beginning the interrogation of the challenges associated with the 'future customer'. The application of load research in emerging fields of interest, such as energy storage, micro grids and smart grids will be explored. To this end, the Chapter presents table 1.

MONTHLY MEETINGS

There will be 11 monthly meetings – one every month excluding December. The meetings are generally on the third Tuesday of the month. The content of the monthly member presentations is aimed at addressing data challenges and the application of load research at different

MONDE SONI (CHAIRMAN)
MSC ENG (ELEC), PR ENG, SMSAIEE

MARCUS DEKENAH (VICE CHAIR)
NHD (ELEC HC), M.DIP TECH (ELEC HC), BSC ENG (ELEC), MBLII, AMSAIEE

LLOYD SETLHOGO (SECRETARIAT)
M ENG (ELEC), PR TECH ENG, MSAIEE

scales. These meetings will be take place at SAIEE House, and for those who cannot attend in person, you can connect via Skype. During these monthly meetings, the LRC will also discuss industry standards that are up for revision or suggest a revision if a requirement has been identified.

WEBINARS

A total of 6 webinars are planned – one every second month. The content will be diverse and will includes contributions by other international institutes. Webinars will remain free of charge, however, the attendees must register in advance using the link that will be provided in the Webinar advertisement.

PANEL DISCUSSIONS

Carefully selected contentious topics will be discussed in two panel discussions during the course of 2020. One panel discussion is planned for during the first semester of 2020 while the second one will take placed during the second semester.

These panel discussions will also provide a social platform for attendees to meet other industry players, so they will be held at a local venue and may not be available on remote connections.

SEMINARS

Two seminars are planned for 2020, one during each semester. Similar to the seminar we hosted in 2019, subject matter experts will be carefully selected to deliver quality presentations. These seminars provide an opportunity for delegates to meet experts, that, in some cases, they may have referenced or used in their work. The seminars are helpful to both students (especially at post graduate level) and industry engineers.

2020 CALENDAR

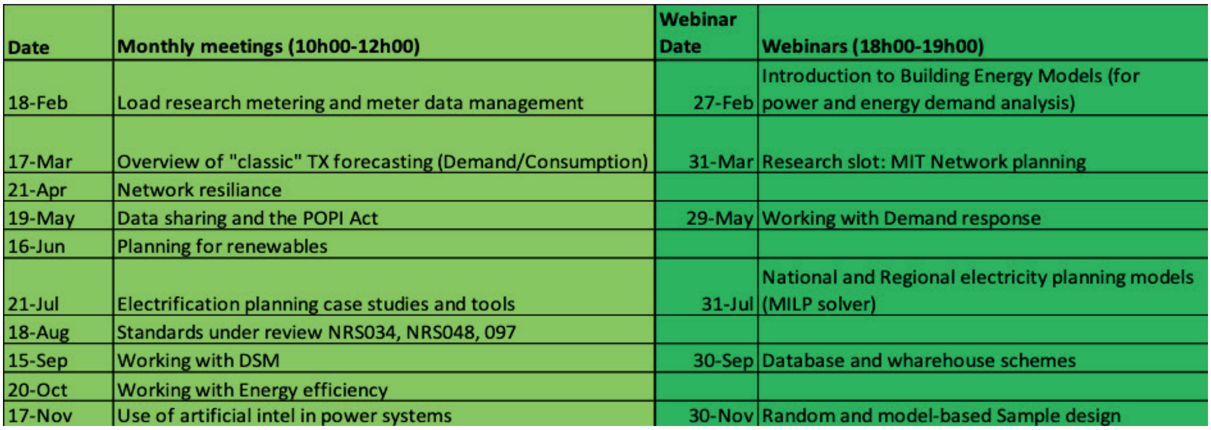
The planned 2020 calendar of events will be made up of monthly meetings, webinars, seminars, and Panel discussions. Refer to Table 2 for more details about seminars and panel discussions.

CONCLUSION

The SAIEE Load Research Chapter was launched in 2019 and has managed to host several events aimed at sharing information amongst its members. The main focus was the historical developments that have taken place in South Africa. The plan for 2020 was discussed and finalised. The aim of the LRC is to uncover aspects of the subject and applications that are futuristic and not well understood industrywide.

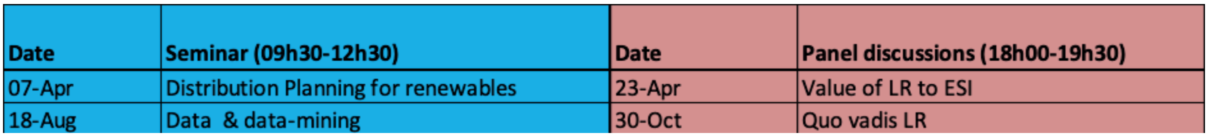
THANKS

The authors would like to thank the support of presenters, committee members, SAIEE's staff, SANEDI and mentors for providing assistance in hosting online meetings and webinars, substantial support at our "maiden" seminar and the launch of Load Research Chapter's web presence with growing online multimedia. wn



Date	Monthly meetings (10h00-12h00)	Webinar Date	Webinars (18h00-19h00)
18-Feb	Load research metering and meter data management	27-Feb	Introduction to Building Energy Models (for power and energy demand analysis)
17-Mar	Overview of "classic" TX forecasting (Demand/Consumption)	31-Mar	Research slot: MIT Network planning
21-Apr	Network resiliance		
19-May	Data sharing and the POPI Act	29-May	Working with Demand response
16-Jun	Planning for renewables		
21-Jul	Electrification planning case studies and tools	31-Jul	National and Regional electricity planning models (MILP solver)
18-Aug	Standards under review NRS034, NRS048, 097		
15-Sep	Working with DSM	30-Sep	Database and wharehouse schemes
20-Oct	Working with Energy efficiency		
17-Nov	Use of artificial intel in power systems	30-Nov	Random and model-based Sample design

Table 1: Calendar of topics for monthly meetings and webinars



Date	Seminar (09h30-12h30)	Date	Panel discussions (18h00-19h30)
07-Apr	Distribution Planning for renewables	23-Apr	Value of LR to ESI
18-Aug	Data & data-mining	30-Oct	Quo vadis LR

Table 2: Calendar of topics for seminars and panel discussions

Fourier Series – 200 Years

The Fourier Series and Transform are so fundamental to alternating current and harmonic study that it may seem that these were developed specifically for use in electrical engineering, but this is not the case.

BY DUDLEY BASSON

Jean-Baptiste-Joseph, Baron Fourier (1768 - 1830)

It was 200 years ago, when Danish Professor Ørsted first discovered that an electric current could deflect a magnetic compass; the first connection found between electricity and magnetism and the first hint that electricity could be of engineering significance, that Fourier discovered his famous infinite series while studying the conduction of heat through a solid object.

Jean-Baptiste-Joseph, Baron Fourier (1768 - 1830) was born on 21 March in Auxerre, France. His father was a tailor but he was orphaned at the age of nine. His first schooling was at Pallais's school run by the music master from the cathedral, where he studied French and Latin. He proceeded in 1780 to the *École Royale Militaire of Auxerre*. By the age of 14 he had completed a study of the six volumes of *Bézout's Cours de mathématiques*, and in 1783 he received the first prize for his study of Bossit's *Mécanique en general.*

His intention to follow a mathematical career appeared in a letter:
"Yesterday was my 21st birthday, at that age Newton and Pascal had already acquired many claims to immortality."

Having left St Benoit in 1789, he visited Paris and read a paper on algebraic equations at the *Académie Royale des Sciences*. In 1790 he became a teacher at the Benedictine college, *École Royale Militaire of Auxerre*, where he had studied.

In 1793 he took a prominent part in

promoting the French Revolution, serving on the local Revolutionary Committee but fell foul of the revolutionaries when he defended the victims of the Reign of Terror. Resigning from the committee was not possible. In 1794 he was imprisoned briefly but escaped the guillotine, unlike his unfortunate contemporary scientist Lavoisier.

Later in 1794 he was nominated to study at the Paris *École Normale* where he was taught by Lagrange, whom he described as *"the first among European men of science."*

By 1 September 1795 Fourier was back teaching at the *École Polytechnique*. In 1797 he succeeded Lagrange in being appointed to the chair of analysis and mechanics.

Fourier accompanied Napoleon on the 1798 Egyptian invasion as scientific advisor and was appointed as secretary of the *Institut d'Égypte*. A most significant discovery made by the expedition in 1799 was the Rosetta Stone which, inscribed in three languages, provided the key to the eventual decipherment of the ancient Egyptian hieroglyphs.

Napoleon's invasion of Egypt was at first successful. Malta was occupied on 10 June 1798, and Alexandria taken by storm on 1 July and the Nile delta also quickly taken. On 1 August 1798 Napoleon suffered a humiliating defeat at Abukir bay when most of his warship fleet, under the command of *Amiral* François-Paul Brueys D'Aigalliers was destroyed or captured by Nelson's fleet in the Battle of the Nile. The most horrific event of the battle was the destruction of the French flagship *L'Orient*, when it was blown to smithereens by the explosion of the powder magazines.

The badly injured Brueys remained heroically in command to the end. The explosion was so violent that it destroyed ships in the vicinity and set fire to others. The flagstaff of *L'Orient* was salvaged and kept by Nelson as a souvenir at his home in Merton.

Watch a video clip of this battle.

French *Contre-amiral* Pierre-Charles Villeneuve was able to escape from the battle but would later be defeated by Nelson at Trafalgar.

Fourier Series - 200 years

continues from page 65

Fourier acted as an administrator of French type political institutions, and administration was set up. In particular, he helped establish educational facilities in Egypt and carried out archaeological explorations.

When Napoleon returned to France in 1801, he sent Fourier to Grenoble as Prefect of Isére.

An accomplished scholar and well known mathematical physicist, Fourier had been entrusted by Napoleon with the publication of the results of the expedition in the monumental series of publications titled *Description de l'Égypte*.

Fourier worked with astonishing energy; he built roads, engineered a large land-drainage program, wrote papers on mechanics and a book on Egypt. After being made a baron he resigned his post in 1815 and went back to full-time research.

One biographer has stated that Fourier invited the 11-year-old Champollion to his home and showed him his collection of ancient Egyptian artefacts and documents. Champollion was enthralled, and upon seeing the hieroglyphs and hearing that they were unintelligible, he declared that he would be the one to succeed in reading them. Jean-François Champollion (1790-1832) achieved international acclaim in 1822, when after continuing from the work of Thomas Young, he announced that he had deciphered the ancient Egyptian hieroglyphs.

Fourier had started thinking about heat flow when in Egypt, where he assisted Napoleon by determining the fastest rate at which cannons could be fired without overheating. He submitted his famous paper *"Théorie analytique de la chaleur"* (Analytical theory of heat) which described heat flow in solid bodies, to the *Académie des Sciences*. This was more than a treatise on heat – he had created a form of mathematics that let engineers and scientists solve problems that had previously been unthinkable.

He showed how the conduction of heat in solid bodies may be analysed in terms of infinite mathematical series (Fourier series). Transcending the subject of heat conduction, his work stimulated research in mathematical physics, which has since been often identified with the solution of boundary-value problems, encompassing many natural occurrences such as sunspots, tides and the weather. The atomic orbitals of chemistry are partially described by spherical harmonics, which can be used to produce Fourier series on the sphere.

Fourier's work also had a great influence on the theory of functions of a real variable - a main branch of modern mathematics.

Fourier's first announcement of his great discovery was made before the *Académie des sciences* in 1807.

Early ideas of decomposing a periodic function into the sum of simple oscillating functions date back to the 3rd century BC, when ancient astronomers proposed an empiric model of planetary motions, based on deferents and epicycles.

Fourier's work offended many of the mathematicians at the time, and for several years he fought to get it published. It finally appeared in book form in 1822 and was the most important mathematical book of the time.

Fourier died on 16 May 1830, possibly from a chronic illness contracted in Egypt and was buried in the Pére Lachaise Cemetery in Paris. His name is one of the 72 famous names inscribed in the Eiffel Tower.

A century after Fourier's famous discovery, the Fourier Series became fundamental and indispensable in electrical engineering in the study of harmonics in alternating current.

Harmonics can be troublesome when using power electronics such as variable speed drives for induction motors. Harmonics are produced when voltage waves are electronically clipped, generating a Fourier series of harmonics.

The series is not only applicable to voltage and current waves, it is applicable to any wave motion and is of fundamental importance in the storage, amplification and reproduction of sound waves.

Watch: An excellent mathematical treatment of the Fourier Series.

$$f(x) = a_0 + \sum_{n=1}^{\infty}\left(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L}\right)$$

Fourier Series template supplied by MS-Word

For an excellent visual introduction to the Fourier Series (25 minutes)

Fourier on the chalkboard (16 minutes)

In physics and mathematics, the heat equation is a partial differential equation that describes how the distribution of some quantity such as heat evolves over time in a solid medium, as it spontaneously flows from places where it is higher, to places where it is lower. It is a special case of the diffusion equation. This illustrates the law of entropy.

$$\frac{\partial u}{\partial t} = \alpha \left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2} \right) \quad or \quad \acute{u} = \alpha \nabla^2 u$$

Heat equation

This equation was first developed and solved by Fourier in 1822 to describe heat flow. It is however of fundamental importance in diverse scientific fields. In probability theory, the heat equation is connected with the study of random walks and Brownian motion, via the Fokker-Planck equation. In financial mathematics it is used to solve the Black-Scholes partial differential equation. In quantum mechanics it is used for finding the spread of wave function in a potential free region. A variant was also instrumental in the proof of the longstanding Poincaré conjecture of topology.

See the following link for an excellent treatment of the Heat Function:

The Fourier transform decomposes a function of time (a signal) into its constituent frequencies. This is similar to the way a musical chord can be expressed in terms of the volumes and frequencies of its constituent notes. The term Fourier transform refers to both the frequency representation and the mathematical operation that associates the frequency domain representation to a function of time.

The Fourier transform is not limited to functions of time, but the domain of the original function is commonly referred to as the time domain. There is also an inverse Fourier transform that mathematically synthesizes the original function from its frequency domain representation.

For an excellent mathematical treatment of the Fourier Transform.

For a visual depiction of the Fourier Transform – 20 minutes.

In the late 1400's, Leonardo da Vinci, on noticing how dust motes on his worktable stirred to create shapes when he vibrated the table wrote:

"I say that when a table is struck in different places the dust that is upon it is reduced to various shapes of mounds and tiny hillocks."

Da Vinci's close observation of dust under the influence of vibration was, quite literally, sound made visible.

German musician and scientist, Ernst Chladni, (1756–1827) applied this simple physics principle with great flair. He made sand-strewn metal plates ring by playing their edges with a violin bow, creating beautiful sand patterns known today as *"Chladni Figures."* Chladni became famous throughout Europe and even demonstrated this seemingly magical phenomenon to Napoleon. The French leader was so impressed that he sponsored a competition at the Paris *École Polytechnique* to acquire a mathematical explanation of the sound patterns.

In 1816, the famous mathematician and student of Lagrange, Sophie Germain, became the winner of the competition which was originally announced in 1811 but was twice extended due to the lack of successful entries. Sophie is best known for her work on number theory and the Fermat theorem. She was on friendly terms with Fourier who assisted her with gaining access to academic events which were normally barred to women. Sophie's work was held in very high regard by Gauss.

A new study of the vibrations on the surface of water, developed in 2002, known as Cymatics, shows how music and other sounds can produce patterns on the surface of water in a circular container. Initially thin circular membranes were tried but the best results were achieved using ultra-pure water.

Piano octave notes visible with CymaScope (4 minutes):

Claude Debussy's Clair de Lune visible with CymaScope (6 minutes)

Fourier Series - 200 years

continues from page 65

$$N^2\left(\frac{\partial^4 z}{\partial x^4}+2\frac{\partial^4 z}{\partial x^2\partial y^2}+\frac{\partial^4 z}{\partial y^4}\right)+\frac{\partial^2 z}{\partial t^2}=0$$

Sophie Germain's 1816 prize winning differential equation for the vibration of an elastic surface.

Sophie Germain

There is much current interest in the use of sound induced vibrations within organic cells for possible therapeutic purposes.

The Fourier series is of profound importance in the understanding of musical sounds. Musical instruments are tuned to a frequency of 440 Hz for the A above middle C. When orchestras tune before a performance, the A is given by the piano if available, otherwise by the oboist. The range of instruments will span several octaves – the same note in the next higher octave will have double the frequency. Each octave is divided into 12 semitones. Musical scales of seven notes are selected from the 12 semitones. Several scales have been in use but currently only the major and minor scales are used. On printed music, the scales are indicated by key signatures containing 0 to 6 sharps or flats at the beginning of the staves. In Bach's 48 preludes and fugues he systematically uses all 24 major and minor scales.

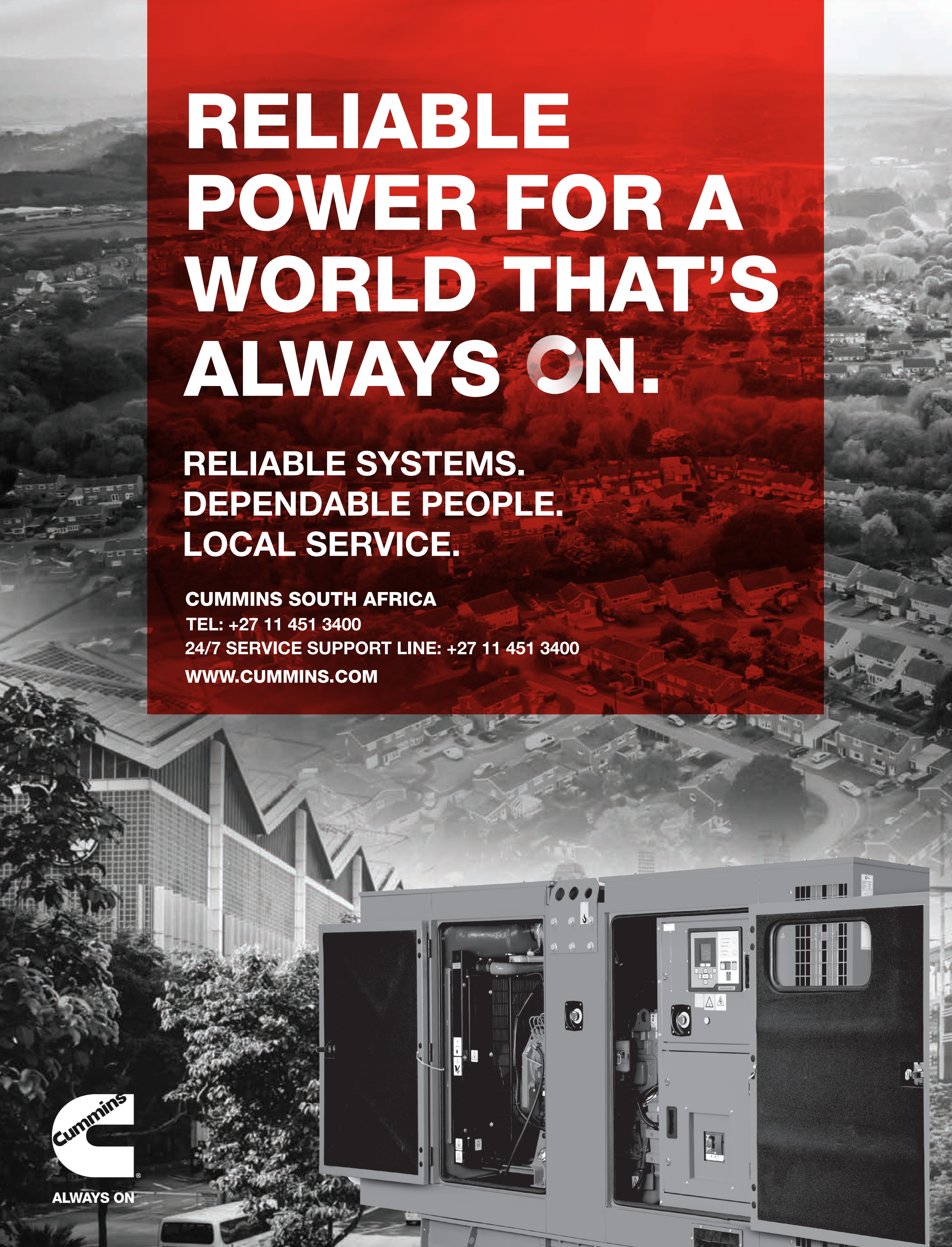
In an even tempered instrument each successive semitone will increase in frequency by the 12th root of 2 (1,059463). Pianos are normally tuned this way but this is not perfect for all musical intervals. Pianos are used to play music in any scale and cannot be quickly re-tuned to better suit a particular scale. Music frequently modulates from one key to another. Chord intervals sound best when the frequencies are in simple integer ratios but this is not precisely possible with even temperament tuning, however only professional musicians can notice the difference.

Different instruments playing the same note will of course sound quite different to each other – this is due to the timbre. The instruments may play the same fundamental but will have different harmonics and overtones. The harmonics are the higher frequency Fourier waves but the overtones can be jarring or scratchy and make the difference between a good and a not-so-good instrument.

Sound reproduction equipment must be capable of producing sound of much higher frequency than the fundamentals, in order to include the harmonics and overtones, to give accurate rendition of instrumental and voice sound.

White noise is chaotic sound without any discernible fundamental frequency. This can be a hissing noise or the sound of a waterfall and if not excessively loud can be quite soothing.

Fourier could have had no idea that his ground-breaking discovery of two centuries ago would have immense implications for future developments in mathematics, science and engineering. wn


RELIABLE POWER FOR A WORLD THAT'S ALWAYS ON.
RELIABLE SYSTEMS.
DEPENDABLE PEOPLE.
LOCAL SERVICE.
CUMMINS SOUTH AFRICA
TEL: +27 11 451 3400
24/7 SERVICE SUPPORT LINE: +27 11 451 3400
WWW.CUMMINS.COM
Cummins
ALWAYS ON

February in History

Why Do We Have Leap Years?

Leap days keep our modern-day Gregorian calendar in alignment with Earth's revolutions around the Sun. It takes Earth approximately 365.242189 days, or 365 days, 5 hours, 48 minutes, and 45 seconds, to circle once around the Sun. This is called a tropical year, and it starts on the March equinox.

However, the Gregorian calendar has only 365 days in a year. If we didn't add a leap day on February 29 almost every four years, each calendar year would begin about 6 hours before the Earth completes its revolution around the Sun (see illustration).

As a consequence, our time reckoning would slowly drift apart from the tropical year and get increasingly out of sync with the seasons. With a deviation of approximately 6 hours per year, the seasons would shift by about 24 calendar days within 100 years. Allow this to happen for a while, and Northern Hemisphere dwellers will be celebrating Christmas in the middle of summer in a matter of a few centuries.

Leap days fix that error by giving Earth the additional time it needs to complete a full circle around the Sun.

COMPILED BY I
JANE BUISSON-STREET
FSAIEE I PMIITPSA I FMIITSPA

1 FEBRUARY

1944 DNA was identified as the hereditary agent in a virus, published in a report by O.T. Avery, Colin MacLeod, and Maclyn McCarty. This crucial discovery in molecular genetics - that genetic information is carried in the nucleotide sequence of DNA - arose incidentally while studying pneumococcus to monitor the epidemic spread of pneumonia.

2 FEBRUARY

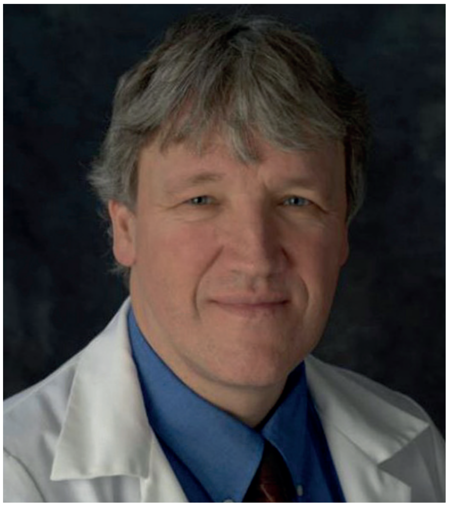
1995 News of research linking brain structure and artistic talent was released by at a press conference in Washington. Dr Gottfried Schlaug announced the work of his team of researchers at Beth Israel Hospital in Boston, Mass. Persons with perfect pitch were found to have a region in the left hemisphere of the brain, the plenum temporal, to be enlarged.

3 FEBRUARY

1966 Three days after its take-off, the unmanned Soviet Luna 9 spacecraft landed safely on the moon in the Ocean of Storms. It was the first ever soft landing on another celestial body, and opened the way for manned trips to the moon, by removing doubts lest the surface was an unsafe dusty quicksand.

4 FEBRUARY

1600 Johannes Kepler, the German astronomer who formulated three major laws of planetary motion which enabled Isaac Newton to devise the law of gravitation, arrived in Prague to collaborate with Tycho Brahe. Brahe was the Danish astronomer whose work in developing astronomical instruments and in measuring and fixing the positions of stars paved the way for future discoveries.



Kepler had the mathematical calculation skills to make sense of the wealth of data that Brahe had accumulated as an enthusiastic and accomplished astronomical observer. Brahe gave Kepler the task of determining a way to reliably compute the orbit of Mars. What Kepler initially thought would take eight weeks, actually extended to eight years work.

5 FEBRUARY

1962 The Sun, the Moon, and the five naked-eye visible planets - Mercury, Venus, Mars, Jupiter, and Saturn - were in conjunction. Though not in a straight line along their orbital paths, as viewed in the sky, they were within 16 degrees of each other (meaning all appeared within a circle just 16º across).

6 FEBRUARY

1911 The official Rolls-Royce mascot was chosen. It is a silver-winged animal called "The Spirit of Ecstasy" and it is still used as the Rolls bonnet ornament to this day. Initially Royce made sure it was officially listed as an optional extra, but in practice it was fitted to almost all cars after that year, becoming a standard fitting in the early 1920s.

7 FEBRUARY

2005 English sailor Ellen MacArthur set a new single handed round the world voyage in the record-breaking time of 71 days and 15 hours covering 27,354 nautical miles (50,660 km).

8 FEBRUARY

1672 Isaac Newton read his first optics paper before Royal Society in London, UK. He had been elected a member only the previous month after recognising his original design of the first reflecting telescope. Newton had already spent several years investigating optics, beginning in 1665. His studies of the colours from glass prisms with their dispersion of light were recorded in his essay New Theory about Light and Colours (1672), and expanded later in Opticks (1704).

9 FEBRUARY

1991 Japan's worst nuclear accident happened at Mihama. A pipe in the steam generator burst, leaking 55 tonnes of radioactive primary (reactor) coolant water into the secondary steam-generating circuit. Some radioactivity was released to the atmosphere and the plant's emergency core cooling system was activated.

10 FEBRUARY

1943 Vesta Stroudt worked at an ordnance plant during World War II, and noticed the way ammunition boxes were sealed made them difficult to open quickly and this could cost them precious time in battle. So, she developed a waterproof, tearable cloth tape to solve the problem. Her bosses at the plant were unimpressed, so she wrote a letter to U.S. President Franklin D. Roosevelt: *"I suggested we use a strong cloth tape to close seams, and make tab of same. It worked fine, I showed it to different government inspectors they said it was all right, but I could never get them to change tape."*

Roosevelt liked the idea and sent it to the War Production Board who implemented her tape idea.

11 FEBRUARY

1954 The largest light bulb, rated at 75,000-watts, was lit at the Rockefeller Centre in New York, USA, to commemorate the 75th anniversary of Thomas Edison's first light bulb.

12 FEBRUARY

1935 A patent was issued to Robert Jemison Van de Graaff (an American physicist) for his Electrostatic Generator design

February in History

continues from page 71

(U.S. No. 1,991,236), able to generate direct-current voltages much higher than the 700,000-V, which was the state of the art at the time, using other methods.

13 FEBRUARY

2019 NASA announced that their Opportunity rover on Mars had ended. The rover had stopped communicating in June 2018 after a Martian dust storm, and attempts to re-establish communications had not been successful.

14 FEBRUARY

1978 Texas Instruments patented the first "Micro on a Chip". Gary Boone and Michael Cochran of Texas Instruments designed the chip (1971) and then led the group to the patent – spanning from 1974 to 1978. This chip was used in multiple inventions such as garage door openers, burglar alarms and many electronic toys.

15 FEBRUARY

1770 English chemist Joseph Priestley discovered that a piece of latex can be used to remove pencil marks. Nowadays we know his invention as an eraser.

16 FEBRUARY

1892 Thomas A. Edison was issued two U.S. patents, for a "Converter System for Electric Railways" and a "Commutator Brush for Electric Motors and Dynamos".

17 FEBRUARY

1959 Vanguard 2, the first weather satellite, was launched by the United States Navy's Project - Vanguard as part of the space race between the United States and the Soviet Union. The satellite was designed to measure cloud-cover distribution over the daylight portion of its orbit, for a period of 19 days, and to provide information on the density of the atmosphere for the lifetime of its orbit (about 300 years). Currently it is still in orbit.

18 FEBRUARY

1678 English preacher John Bunyan published his famous religious work, The Pilgrim's Progress, in England. For over 200 years, except for the Bible, it was the most widely read book in the world.

19 FEBRUARY

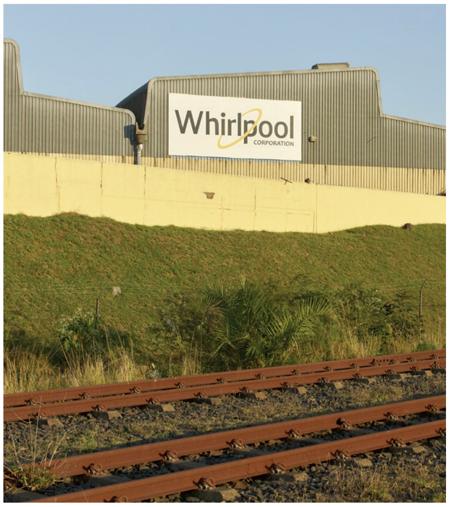
1878 The phonograph was patented by Thomas A. Edison. His first recording was made reciting "Mary Had a Little Lamb" into a large horn which transmitted vibrations to a needle which scribed a recording on a cylinder rotated by hand.

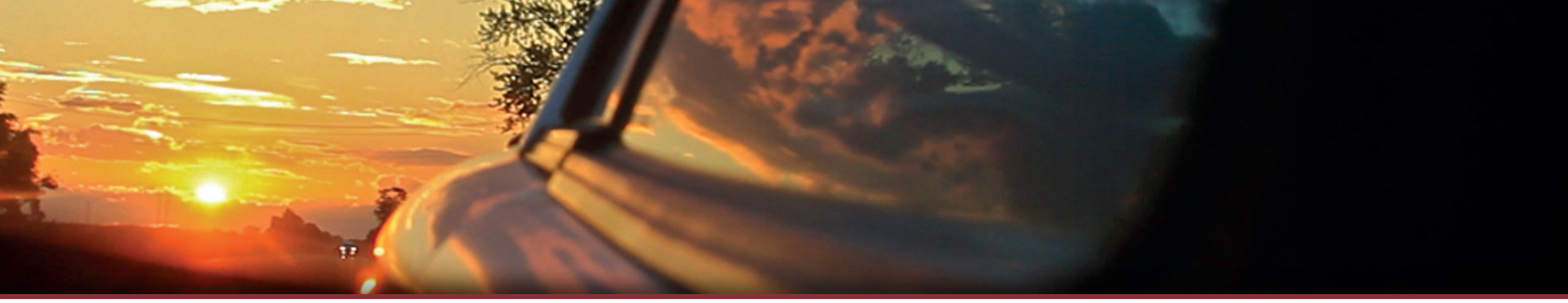
20 FEBRUARY

1986 The Soviet Union launched into orbit Mir, a new space station. Mir, the Russian word for peace, had six docking ports and special laboratories for scientific research.

21 FEBRUARY

1994 The Whirlpool Corporation began production of an energy efficient refrigerator that did not use freon.





22 FEBRUARY

1984 Apple Computer broadcast their now-famous "1984" commercial introducing the Macintosh, during the third quarter of Super Bowl XVIII. It was the first and last time the ad was truly broadcast.

23 FEBRUARY

1893 Rudolf Diesel received a German patent for the diesel engine, which burns fuel oil rather than gasoline, and uses high compressed of the gases in the cylinder rather than a spark to ignite the fuel. Diesel engines were used widely in Europe for their efficiency and power, and are still used today in most heavy industrial machinery.

24 FEBRUARY

1931 The Fields Medal was established to recognize outstanding contributions to mathematics. Although John Charles Fields probably thought of the medal at some earlier time, the first recorded mention was made on this day in minutes of a committee meeting.

25 FEBRUARY

1959 The Automatically Programmed Tools (APT) language, a high-level computer programming language most commonly used to generate instructions for numerically controlled machine tools, was demonstrated for the first time.

26 FEBRUARY

1983 The Lotus Development Corporation released Lotus 1-2-3 for IBM computers. While not the first spreadsheet program, Lotus was able to develop 1-2-3 because the creators of VisiCalc, the first spreadsheet, did not patent their software.

27 FEBRUARY

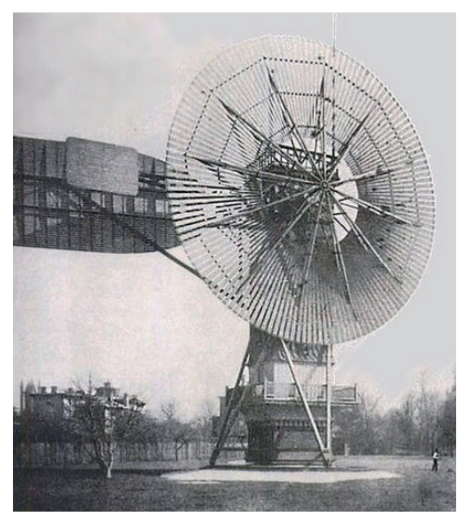
1892 *"Electricity From Wind"* was reported in the Cincinnati Enquirer, from the Philadelphia Record. It was reported that *"Owing to the comparative scarcity of water-power in many parts of England, attention has been given to wind power, of which the country is well supplied."*

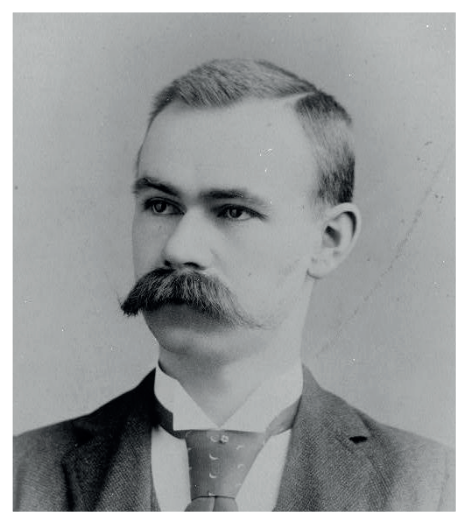
28 FEBRUARY

1997 GRB 970228, a highly luminous flash of gamma rays, struck the Earth for 80 seconds, providing early evidence that gamma-ray bursts occur well beyond the Milky Way.

29 FEBRUARY

1860 Herman Hollerith, founder of the Tabulating Machines Company, was born. In 1890 he developed the mechanical means for tabulating the US Census data. His tabulating machines were later used for the analysis of censuses around the world for many years. His company was one of three that came together in 1914 to form C-T-R (Calculating, Tabulating, Recording) Co. that Thomas J. Watson, Sr. was to take over and rename as the IBM Corporation. wn





SAIEE CENTRES

Eastern Cape Centre

Chairman | Simphiwe Mbanga

T|083 777 7916 **E**|MbangaS@eskom.co.za

Free State Centre

Chairman | Joseph George

T|082 263 1213 **E**|joseph.george22@gmail.com

Gauteng Central Centre

Chairman | Teboho Machabe

T|083 692 6062 **E**|MachabTB@eskom.co.za

Kwa-Zulu Natal Centre

Chairman | Jay Kalichuran

T|082 569 7013 **E**|KalichuranJ@elec.durban.gov.za

Mpumalanga Centre

Chairman | Louis Kok

E| louis.kok2@sasol.com

Northern Cape Centre

Chairman | Ben Mabizela

T| 073 708 0179 **E**| MabizeBG@eskom.co.za

Southern Cape Centre

Chairman | Steyn van der Merwe

E|steynvdm@gmail.com

Vaal Centre

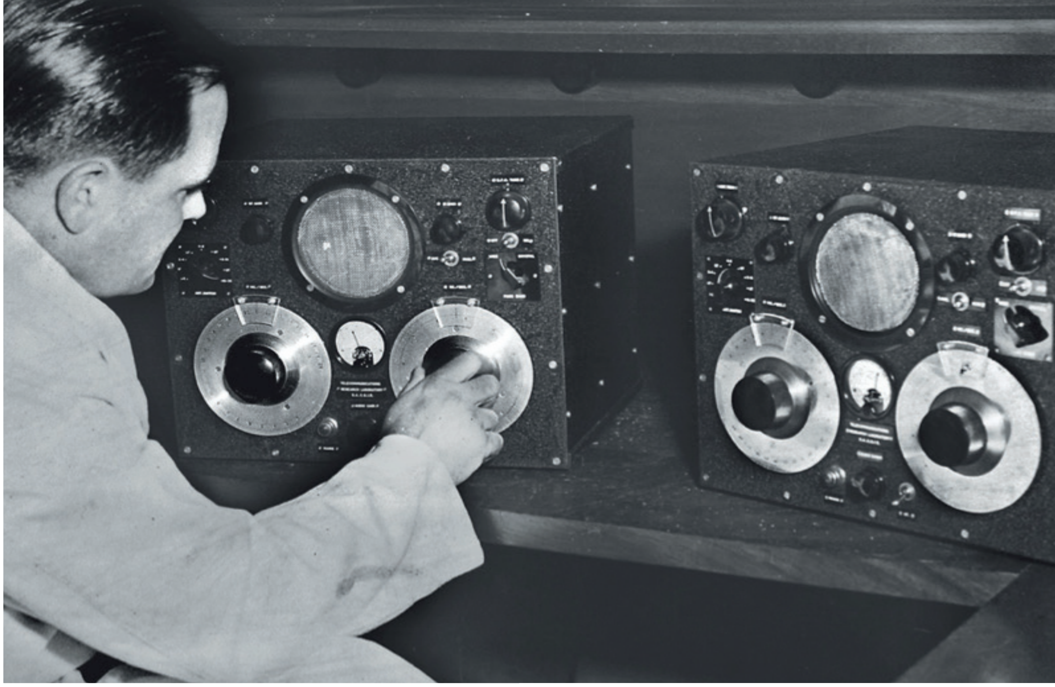
Chairman | Carlisle Sampson

T|083 397 8021 **E**|Carlisle.Sampson@sasol.com

Western Cape Centre

Chairman | Heinrich Rudman

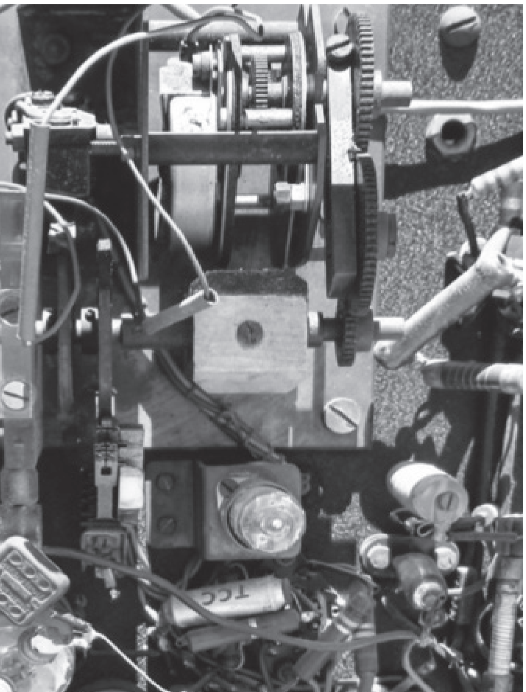
E| admin.wcape@saiee.org.za

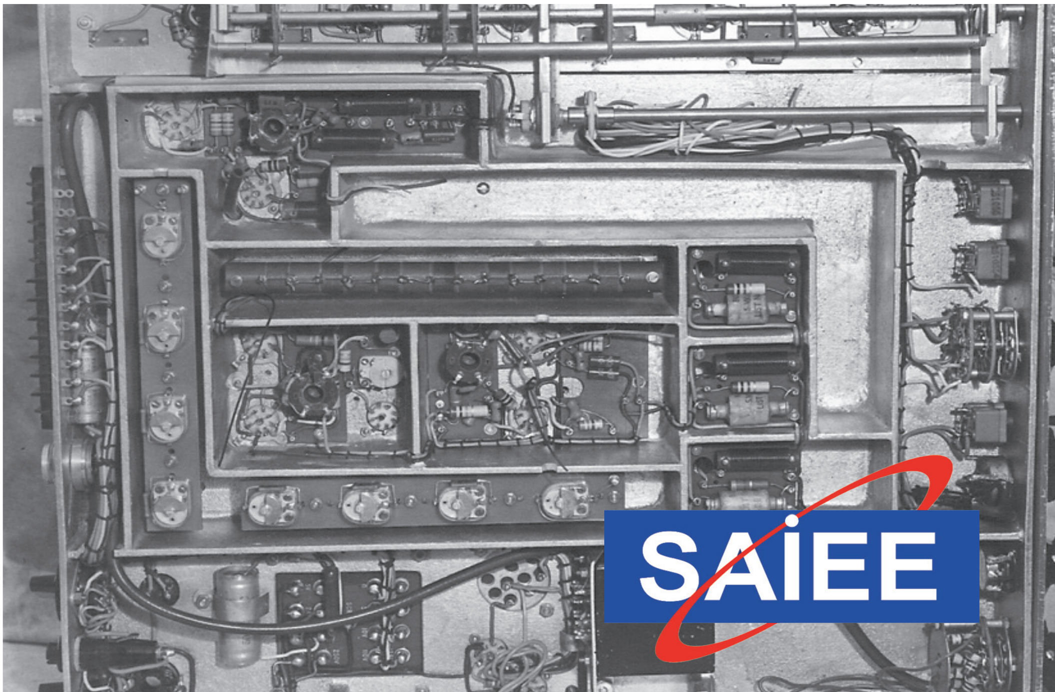


Wadley Masterpieces

- a centenary celebration -

By: Richard Dismore MA (Cantab) SMSAIEE





SAIEE

FOREWORD

THE WADLEY MASTERPIECES

The SAIEE is fortunate to be the custodians of several pieces of original equipment built at various times by Dr Trevor Wadley during his illustrious career. These are housed in the Institute's Innes House Museum, located on the Head Office site in Observatory, Johannesburg.

With February 2020, the Historical Section of the Institute considered that the 100th anniversary of his birth was an opportunity to honour his memory and at the same time pay tribute to his unique talents and the effect they had on the people of this planet.

The technical background and details of his work have been covered in great detail in various academic and professional over the years. This booklet is an attempt to bring as much of his work as possible into one handy format with sufficient detail to satisfy the needs of readers wishing for some depth on the subjects covered, but also readable for non-technical people with interest in this great man.

Due to the dedication and enthusiasm of SAIEE member, Richard Dismore, we attempted to do this through the publication of this booklet. We hope it will prove to be both interesting and informative and that it will go some way to achieving the objective of honouring the memory of a great engineer and a genius of his time.

Enjoy the read!

Max Clarke
Chairman,
SAIEE Historical Section

February 2020 marks the centenary of the birth of Trevor Wadley. To write about the man and his extensive achievements has been a privilege. On re-reading some of the oldest references, previously unconnected information emerged requiring a greenfield approach to this compelling subject. Myths abounded about Wadley before the advent of the internet, which only served to replicate them. Innovation by research and development is founded on a knowledge of prior art. As it progresses, the innovation itself becomes prior art over time from which further innovations depart. This booklet takes that approach to Wadley's technologies, identifying a continuous thread, date-stamped with snapshots of history, overlain with the personal story of a likeable genius.

THE MAN

Little would have been known about Trevor Lloyd Wadley's personal life had not his younger sister Mary published a book [1] about him 28 years after his death. It is an often poignant account detailing his early years and later years. However, detail is sparse concerning his wartime and post-war activities in the middle 20 years of his life, the period of his greatest creativity. This is largely due to the veil of secrecy surrounding him and his sister's lack of technical knowledge, having trained as a lawyer. The book was launched together with another [2], a technical treatise on Wadley's crowning masterpiece, the Tellurometer.

Born on 9th February 1920, Trevor was the seventh child of a London-born immigrant who was an accountant and who later became Mayor of Durban and a Union MP. Three more children followed him including Mary, the ninth, who was six years younger. Trevor was sandwiched between three sisters either side and suffered a domineering mother. Their home on a large property in rural Natal facilitated a small boy's activities and escape. He survived a kindergarten year at Durban Girls College. Once he was at Durban High School, his lifetime characteristics began to be apparent. A residue of low self-esteem was more than compensated by his clearly superior intelligence and eidetic memory. He was seen as a loner, very focused in areas of his interests, and was an inveterate dismantler of radios, telephones, and electrical appliances for his childhood inventions. This included relaying an elder sister's telephone conversations with her boyfriend over the home radiogram. He rarely made notes and would engage in bets (not gambling) with lesser mortals where his intellect had pre-determined the likely outcome.

He paid little attention to subjects that did not interest him and did not bother to become proficient at school sports. It surprised the whole school when he decided one year to enter the annual cross country athletics event. He predicted with seeming arrogance that he would win the event in a record time and laid wagers to that effect.

He kept to himself during training running regularly. On race-day Wadley, kitted out in his running shorts, sped off into the distance as the starter's gun was fired. Nobody could keep up with him and, as he had predicted, he won the event, the first in which he'd competed. His record stood for 15 years before it was broken.

Unbeknown to all the observers, Wadley had calculated exactly how long it would take him to cover the first hundred yards, then how long it would take to run the second, then the third and so forth. He had marked off each hundred-yard distance on Burman Drive and trained himself to run each stretch in the time he'd allowed.

Despite their different make up, Trevor remained close to his father, which was fortuitous because his school tipped the latter off that he was about to fail his matriculation year. The school agreed he could drop Latin and take up chemistry. He learned the whole syllabus in four months and passed with an A. Together with straight A's in maths and physics, he was admitted to an electrical engineering BSc course at Howard College, Durban, later University of Natal, graduating in December 1940. In writing exam papers, he would go beyond the choice of questions and answer all of them, sometimes exceeding a 100% mark. He joined the army in January 1941, the record showing sergeant SSS (Figure 1) within the SACS (SA Corps of Signals).

Figure 1: Wadley in the SSS

After three months basic training in Potchefstroom, he was promoted to 2nd Lt (in recognition of his degree) and engaged with his wartime unit based at BPI (Bernard Price Institute) at Wits (University of the Witwatersrand). He was rapidly promoted and achieved the rank of major by the age of 24, ending the war as Staff Officer, RADAR, attached to Cape Command, a title of recognition concealing what he really did.

Advancing rank was also conferred on key people so that they would not be killed by the enemy if captured. Post-war colleagues speak of him as an enigmatic genius. The enigma related to his existence in his own private world, often given to long periods of silence with his eyes closed, rarely writing anything down except key essentials. He would emerge periodically to engage in animated debate with those around him on matters of his interest, especially technical. This was particularly so with his colleagues concerning his innovations, a form of instant peer review. Presented with an idea, or a schematic, or a piece of physical equipment, he could visualise radio frequency pathways in the physical domain and would quickly understand how a device worked based on first principles, mentally computing operating frequencies from component dimensions and placement.

The hardest bit for onlookers to comprehend was that he could jump from a concept to a series of manufacturing drawings for the critical parts without a schematic, leaving out the peripheral stuff such as power supplies and all manner of conventional circuitry he deemed trivial. He would then hook it all up himself and it usually worked first time.

He was first married in 1941 with two sons from this marriage and then divorced and remarried in 1961, which produced twin daughters in record time and another daughter subsequently.

He was very musical throughout his life and played a piano which he also tuned. He was a regular pipe smoker, which must have had a bearing on his demise since he died too soon of colonic cancer, at age 61, in May 1981. The patents for his inventions were held by the CSIR (Council for Scientific and Industrial Research, an SA State entity) in terms of his employment conditions, so as a salaried man he did not accumulate the wealth that he deserved commensurate with the global impact of his achievements.

THE THREAD BEGINS

A digression is necessary here to set the scene for Wadley's innovations. In early 1939 at the prospect of outbreak of war with Germany, the UK cabinet determined that coastal defence of the Dominions would overstretch British resources and it was made clear to their governments that it was their responsibility. Steps were taken to disclose the British RDF (RADAR) under extreme secrecy at a technical level. This was done at Bawdsey, UK. John Cockcroft and Robert Watson-Watt played a leading role. Canada, Australia, and New Zealand sent Scientists to be briefed but South Africa sent a senior staff officer, UDF's Director of Technical Services, Brigadier General FRG Hoare. He well appreciated the strategic significance but was not able to understand enough technically to transfer the technology, nor did he bring home any materials.

For South Africa, a further complication was a strong body of support within its coalition government in favour of remaining neutral under pressure from a group in the Afrikaner civilian population sympathetic to Hitler. A narrow majority for joining in on the side of Great Britain was achieved and General Jan Smuts became prime minister, retaining the defence and external affairs portfolios. South Africa declared war on Germany on 6th September 1939, three days after Britain.

The New Zealand scientist Ernest Marsden did have all the materials and his journey home by sea was diverted, with the intervention of Smuts, to Capetown to be met by Basil Schonland, the Director of the BPI. Schonland was by then a FRS and had built an international reputation in the field of lightning studies, using direction finders to locate the storms. Already a Lt Colonel, he was best placed for the technology transfer, which took place in Marsden's cabin along with comprehensive photographic copies of the documentation during the three-day voyage from Capetown to Durban.

After reporting back to Hoare, the outcome was that a select group of scientists working at or associated with the BPI were incorporated into the SSS (Special Signals Services) unit of the SACS under Schonland's command. Other BPI activities were relocated to the faculties and work on RADAR commenced in the newly constructed purpose-built building which had a reinforced concrete roof to support aerial arrays for lightning research. By the time Wadley was deployed there in March 1940, Schonland's team already had a working RADAR since mid-December 1939 [3]. Schonland assigned himself the task of antenna design, with design of the transmitter, receiver, display, and switching circuitry delegated to four younger colleagues with relevant expertise. Frank Hewitt, who had just completed an MSc in Physics at Rhodes University, Grahamstown, was assigned the task of the design of a monitor. Hewitt was already well experienced in the complexities of radio receivers. At this stage Wadley was very much a junior, but his rapid promotion attests to the value Schonland placed on his contribution. Wadley experienced all aspects of building, installing, calibrating, trouble-shooting and 'development while in operation' of the South African RADARs. They eventually encircled the South African coastline with 17 installations. More units protected forces in East Africa and Suez, and some were later deployed in Sinai [4]. His roving lifestyle with seniority determining his own priorities within flexible orders suited the rather 'unmilitary' Wadley. He carried a radio wherever he went, with which he monitored the state of the war.

Professor (Boz) GR Bozzoli, assumed technical responsibility for the running of the Special Signals Services and Hewitt its command, after Schonland left for England in 1941 on secondment to the British Army. They ensured Wadley had all the resources necessary for him to thrive.

There is a first-hand account [5] that, in late 1941, at the request of the commander of the SACS Colonel Freddie Collins, Wadley met with a Major Cook of the SACS monitoring service (equivalent to the UK 'Y-service') who was engaged in monitoring the increase in Japanese activity. Cook had expressed the need for a piece of equipment that would display on a cathode ray tube a number of transmitting stations operating over a range of frequencies. Wadley said it was possible and he would design what was required. Within a few weeks, he presented Cook with all the details and Cook then used the workshop facilities within his monitoring section to build the unit. Once completed and connected to a Hallicrafters radio receiver, it worked perfectly. Cook recounted *"On the cathode-ray tube, the BBC had produced a blip about three inches high. We could recognize many military stations as we could read their call signs visually. We could pinpoint a blip and transfer the signal to a receiver to listen to it. We could also see the Japanese signals"*. Circumstantial facts support this story. Wadley would have been very familiar with the wobulator technique around since 1935 for aligning superheterodyne IF circuits. He would also have been fully au fait with the ionosonde built by GD Walker of the Johannesburg Technical College, an associate of BPI and himself a radio pioneer. Both these pieces of apparatus used a reactance valve circuit to generate the swept frequency. The USA only entered the war in December 1941 and The Panadaptor Corporation patents were only granted the following year, so this may be an early incidence of Wadley's ability to innovate.

When released to the Allied military, commercial panadaptors such as the BC1031-A could only sweep 100 kHz with the receiver frequency at the centre. By the end of the war, the best specialised models such as the AN/APA10 could achieve 2 MHz. Wadley would have been well aware of the limitations of the technique by the time he faced the ionosonde challenge.

THE MASTERPIECES

After hostilities had ended, The CSIR was legally constituted on 5th October 1945. Schonland was appointed as President directly responsible to Smuts, a post he would hold until 1950. He acted to keep the group of scientists at the core of the SSS together, naming the group the TRL (Telecommunications Research Laboratory) within the Wits/BPI environment but part of the CSIR. This included Frank Hewitt as its director, with Wadley and Jules Fejer, a Hungarian mathematician, among the staff. Professor Bozzoli remained heavily engaged from the Wits/BPI side. Hewitt, Bozzoli and Fejer became the key players providing the resources, personal support and an environment for Wadley to flourish. The research lines established by Schonland for the BPI before the war were continued but the newly constituted TRL commenced with two research programmes, namely, applying their collective RADAR knowledge to the development of an automatic Ionosonde and to the location of distant storm clouds. Hewitt's initial remit was to use RADAR to study inter-stroke processes in lightning, for which he was awarded a Ph.D. Lines of investigation soon included underground radio communication, high stability oscillators and receivers, and precision survey equipment. South Africa had resumed a massive programme of infrastructure building interrupted by the war. A key player was industrialist Hendrik Van der Bijl who had been Smuts' Minister of Supply in wartime and who, as Chairman of Escom the power utility and Iscor the national steel undertaking, controlled key resources required for the programme. He himself was an FRS, obtaining his doctorate for work in the field of electron emission, and he had written the first university textbook on thermionic valves before the war. Through Smuts he would have influenced the CSIR's agenda and would have supported the TRL's focus with the knowledge of pending massive investments in HF broadcasting and international HF telephony links.

THE IONOSONDE

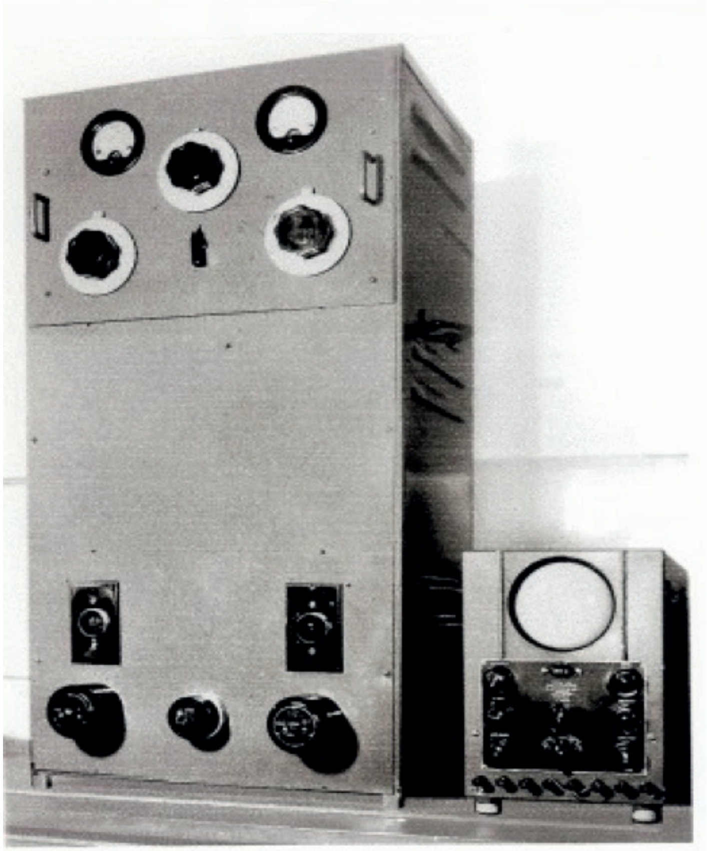


Figure 2: G D Walker's ionosonde

The name Ionosonde is a contraction of the name Ionosphere Sounder, a device for plotting the height of the radio refractive ionised layers above the atmosphere. An Ionogram is a graphical representation of this height on the Y-axis versus frequency on the X-axis. The layers were predicted mathematically by Heaviside in 1902, but the proof had to wait until 1924 when Appleton did his experiment with a broadcast transmitter after hours, varying the frequency and observing the reinforcement and cancelling of the ground wave by the sky wave at a distance.

Continuous ionospheric sounding was carried out at the Appleton Laboratory, Ditton Park, Slough, United Kingdom, from 1931. Often in literature Wadley is credited with the invention of the Ionosonde which is incorrect. Radio pioneer George David Walker had designed and built a manually operated ionosonde in 1936 to measure the height of the Ionosphere. Based on his work Dr BFJ Schonland invited him to work with the Bernard Price Institute team to carry out a variety of measurements during the solar eclipse of October 1940, when the equipment was set up in Middelburg CP for the observations.

In particular, Walker's machine at the BPI required manual tuning of the transmitter and receiver in 100 kHz steps and a scan took about 12 minutes. At the time of Wadley's achievement in 1947, the best machines available still used band-switching to achieve a frequency sweep and he would have known all the leading techniques through contacts in the scientific community.

Wadley's innovative new design completely automated the process, completing it in about 10 seconds. It followed the concept of a vertical firing RADAR but could scan the full 20 MHz bandwidth electronically with a variable capacitor driven through gears by a synchronous motor (Figure 3). This swept a variable frequency oscillator (VFO) between 30 and 50 MHz.

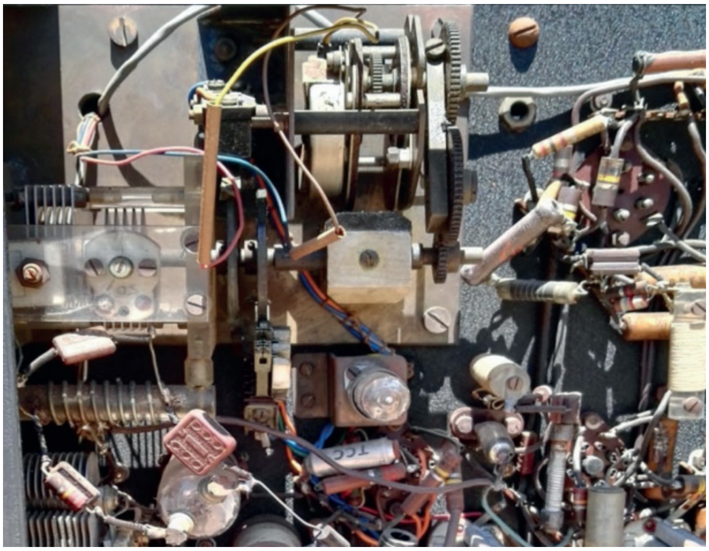


Figure 3:The motorised capacitor for the swept variable frequency oscillator in the surviving Wadley Ionosonde.

Another set of contacts operated by cams driven by another highly geared synchronous motor controlled the sweep interval and reset and triggered the camera at the beginning of the sweep. This was a Leica 16 mm movie camera adapted for single-shot operation, focussed on the face of the long-persistence CRT with a station ID and an event counter in its field of view. A second conventional oscilloscope screen was built in for on-board diagnostics and synchronising of the system. This philosophy carried over into his subsequent designs.

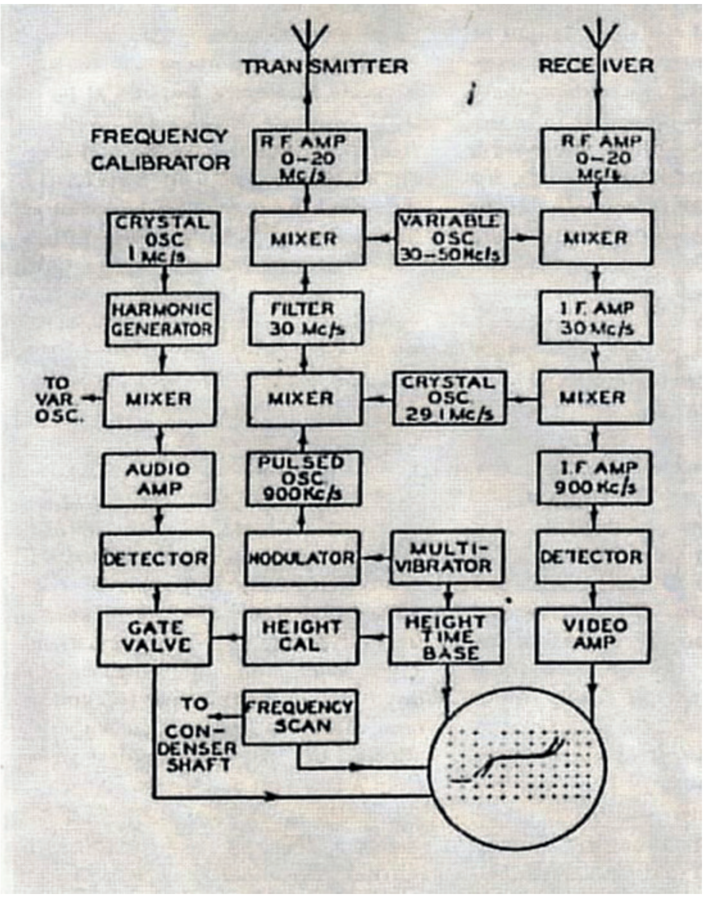


Figure 4: Wadley Ionosonde block diagram [6]

The same VFO signal and heterodyne oscillators were applied to the transmitter and receiver simultaneously, thus ensuring they were instantaneously on the same frequency. The VFO was also applied to the frequency calibrator which controlled the whole system. At its core was a 1 MHz crystal oscillator which drove a harmonic generator providing signals at 1 MHz intervals to beyond 50 MHz, known in modern parlance as a 'comb' signal. This was mixed with the scanning VFO signal and the result was an audio ‘chirp’ at each MHz coincidence as the beat point was approached and passed through. These were amplified in the audio amplifier and passed to a detector which generated evenly-spaced DC pulses of short duration at each MHz point. Contacts, operated by a cam on the rotating capacitor shaft, started the sweep and opened the 16 mm fixed camera for a single frame during the sweep. The design sweep time was 7 seconds corresponding to 180 degrees rotation of the VFO capacitor.

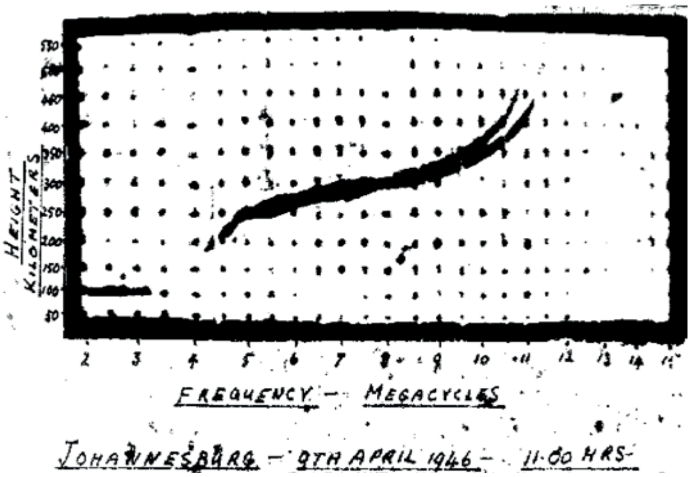


Figure 5: The first ionogram recorded with the Wadley ionosonde, initially with a 500kHz crystal oscillator. [6]

The display was a picture built up on a long-persistence RADAR-type CRT during each scan. A second cam switch inhibited the system and CRT to allow the image to decay while the VFO retraced to just below 30 MHz ready for the next sweep. The gate valve (sobriquet for gating circuitry) set in motion a number of functions. The horizontal deflection voltage came from a stepped timebase, synchronised with the MHz pulses, to give an even spacing for each vertical trace. The height timebase was a conventional sawtooth generator re-triggered by each MHz pulse. Its duration was set with the height calibration. At the same point, the multivibrator was triggered and a burst of audio entered the modulator and modulated the 900 kHz pulsed oscillator for about 70 milliseconds. This 900 kHz pulse train was mixed with the 29.1 MHz heterodyne crystal oscillator. The sum frequency was selected by the 30 MHz bandpass filter and mixed with the output from the VFO, leading to a pulsed signal varying from zero to 20 MHz in 1 MHz increments. An un-tuned class-A amplifier boosted the level, followed by a driver stage to feed the power amplifier valves coupled to a wideband nested rhombic antenna firing orthogonal to the earth’s mean circumference to produce a pulsed 1.5 kW transmission. The receiver amplified the return signals arriving in the transmitter dead time and then down-mixed them using the same heterodyne oscillators as the transmitter. The 900 kHz second IF signal was demodulated, amplified in the video amplifier and applied to the Z-axis input

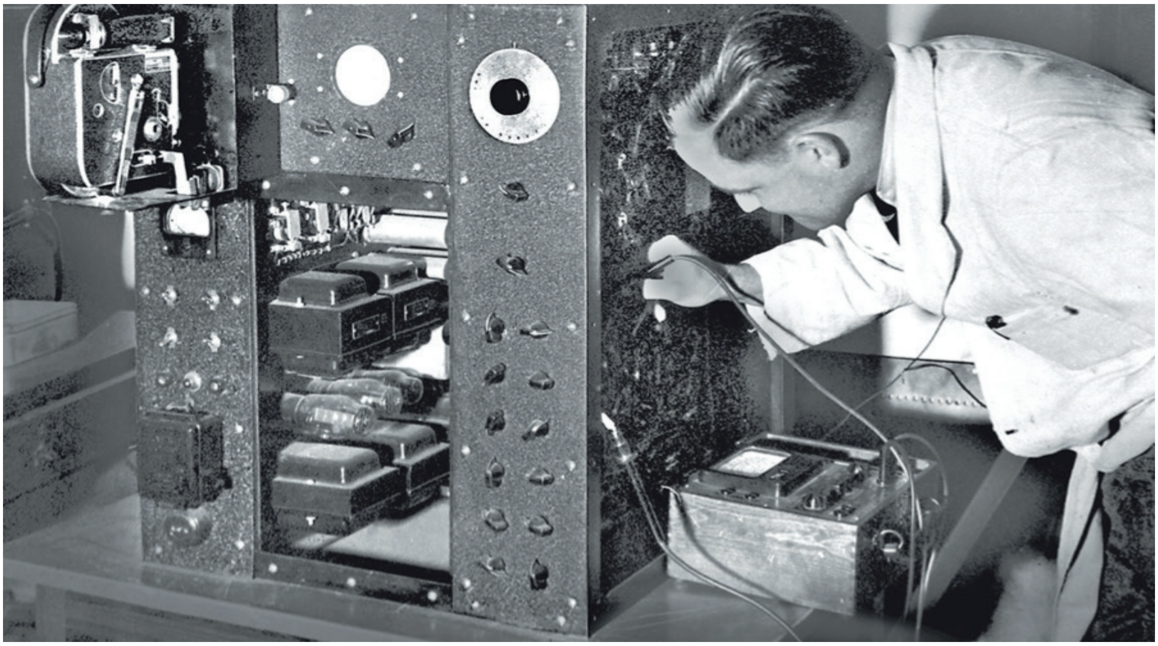


Figure 6: Wadley at work on the Ionosonde in 1947

to modulate the brightness of the trace at a point corresponding to the height of the refracting layer. Marker pips synchronised with the MHz pulse were also inserted onto the vertical trace through this input to facilitate reading the height. The first ionogram was actually recorded on 9th April 1946 (Figure 5).

News of the existence of the Ionosonde was first disclosed in a joint SAIEE paper co-authored by Wadley and Hewitt in July 1947 [7], later elaborated in Wadley's IEE (UK) paper in November 1949 [8].

Figure 6 shows Wadley at work on the Ionosonde in 1947 while the complexity of the equipment can be appreciated from Figure 7 which shows the ex-Capetown Ionosonde as discovered in 2017.

The techniques employed by Wadley in the Ionosonde design presage the design of his receivers and transmitters to follow. Particularly, mixing the VFO with the comb generator to generate a calibrated wideband transmission, but also the use of mirror mixing techniques for the transmitter and receiver to make them transceive synchronously, and the insensitivity of the system to VFO non-linearity as the wanted signals are accurately selected in the frequency domain. Remarkably, all the active circuits are built on one chassis without screening, using 43 valves of which 38 were metal octal. The two instruments built by Wadley served in Johannesburg and Capetown for almost 35 years. The former was extensively modified but the latter (Figure 7) is largely as built.

Jules Fejer provided the mathematical proofs for the functioning of the Ionosonde, and did extensive mathematical modelling of the results. He published his own paper on pulse techniques and amplification of weak echo signals in proximity to a high-power transmitted pulse [9]. It is clear that the technique of a double-gated amplifier with 31 dB gain using 17 metal octal valves had been necessary to make the Ionosonde work. However, another project was implied, not identified, and smokescreens abounded. He was so inspired by the performance of the Ionosonde equipment that he made ionospheric studies his life's work becoming, Professor Emeritus of Applied Physics at the University of California, San Diego [10].

However, 'storm clouds' were gathering, the nationalist Apartheid Government came to power in May 1948, DF Malan defeating the Anglophile Jan Smuts to become prime minister. Meanwhile, the escalation of the 'Cold War' introduced a paradox due to the western world's dependency on the Cape sea route. Fortunately, the nationalists were passionately ant-communist. South Africa became increasingly isolated politically as racial

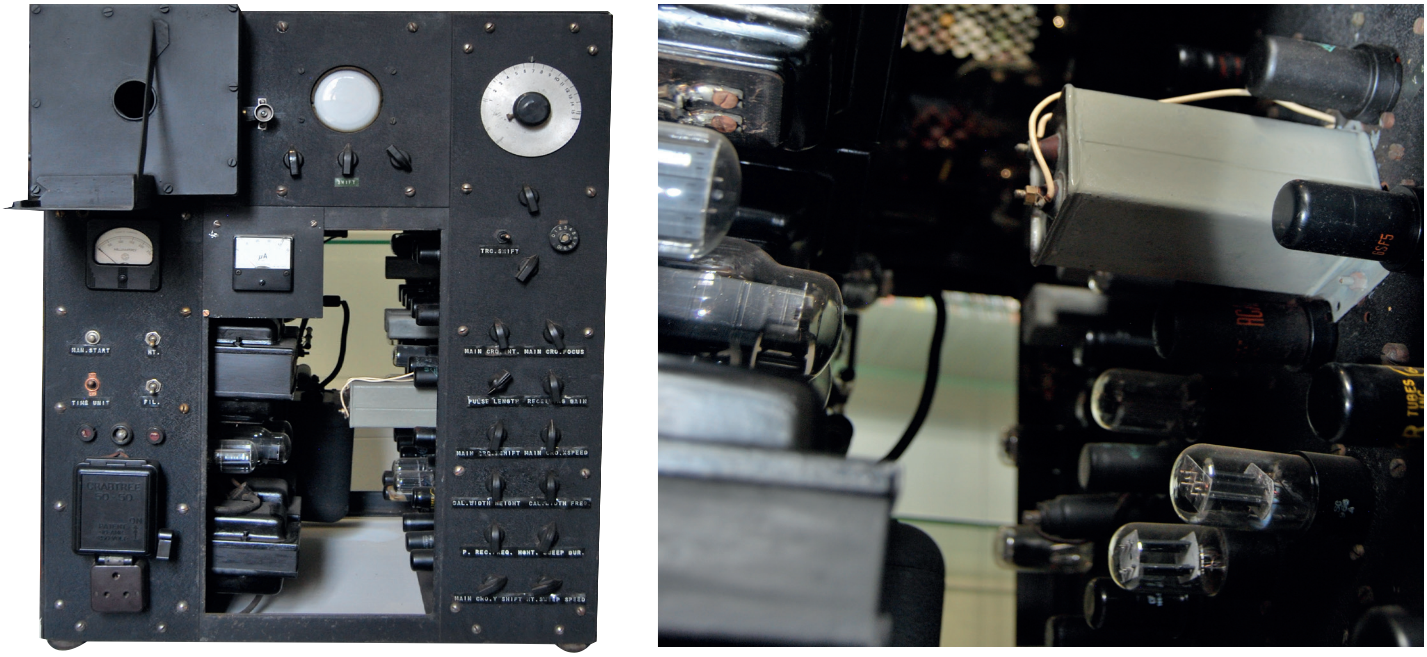


Figure 7: The ex Capetown Ionosonde as found in 2017

segregation legislation and policies were introduced, yet military dialogue and particularly a Royal Naval presence in Simonstown continued until June 1955, doubtless founded on relationships forged in WWII. The Simonstown agreement which followed endured until May 1975. It provided for the handover of the RN base and its South African assets to the SA Navy (including the communications and surveillance station at Silvermine in the mountains above Simonstown), allowed RN ships to use the Simonstown base and permitted South Africa to buy 20 naval vessels from the UK.

The initial effect of this on Wadley would have been minimal as he had no political aspirations. He had operated under the official secrets act for five years of the war and Wadley continued working under similar provisions until he left the CSIR in 1964. This accounts for the dearth of information on his activities, compounded by his personal modus operandi with minimal documentation. The Naval connection, however, would mitigate political barriers for Wadley's technology in later years.

HIGH STABILITY VFOS AND RECEIVERS

Wadley's high-stability variable frequency oscillator and receiver designs first entered the public domain when Wadley presented an SAIEE paper on the subject in August 1953 [12]. The South African Post Office was planning a massive infrastructure programme for international HF telegraphy and telephony links with the Commonwealth and the rest of the world, so it was de-facto the primary customer for high-stability oscillators and receivers. Wadley built two identical prototypes of the receiver (Figure 8) which were operating by the end of 1950. Fejer's mathematical proof of the drift-cancelling system was kept secret.

A third prototype was built by a Post Office engineer, Mr "Tess" Tessyman Peter under Wadley's close supervision by way of technology transfer. The key tool in the design toolkit was the comb generator, used so successfully in the Ionosonde. The paper is long, complex, arguably full of 'smokescreens' and omits the core principle of first local oscillator drift cancellation. The questions and contributions from the floor are more revealing. Manufacturing difficulties with the design were raised and understandably many listeners wrestled with how it worked. By the time of the papers presentation, the CSIR had engaged a local firm SMD to produce six examples (Figure 9), replicating the Wadley prototype for trials, particularly by the Union Defence Force.

This was undertaken after a marketing trip to the UK by Wadley where the BBC had also expressed an interest. One of these receivers was demonstrated alongside its progenitor at the presentation of the

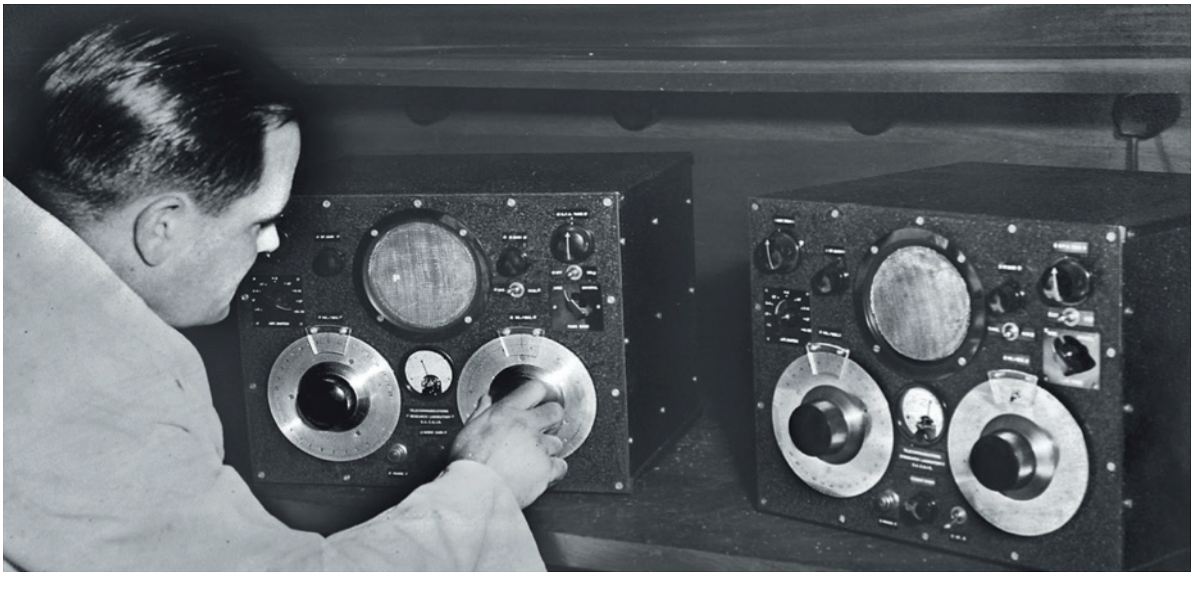


Figure 8: Wadley with his two prototype receivers

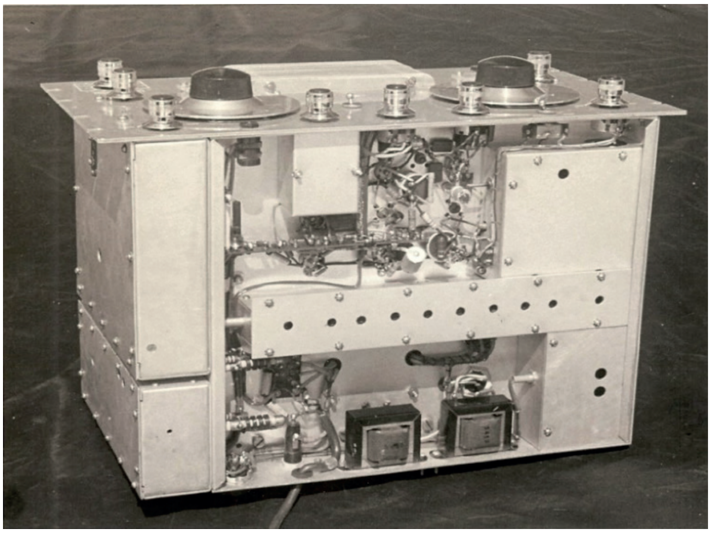


Figure 9: One of the 6 copies made by SMD

paper. The consumer styling received adverse criticism and slight deviations from Wadley's layout to facilitate production resulted in a significant rise of unwanted mixing products (birdies). Horace Dainty, MD of SMD, who was a respondent to Wadley's paper, attributed this to the fabricated construction and alluded to a cast aluminium chassis with pockets for the filters to be the ultimate solution.

The real break-through came when Frank Hewitt, while on an official trip to the UK in 1954, heard that Racal was in difficulties with a receiver tender to the British Admiralty. Believing that they had secured Collins' backing, Racal had tendered for a Royal Navy contract to build and supply a variant of the American Collins Model 51J-4 Radio Receiver.

The 51J-4 employed 10 crystals singly or in combination in a complex mixing scheme, covering up to 30 MHz in 1 MHz switched bands. Racal had submitted a 'sanitised' version of the receiver, devoid of identification, finished in Admiralty grey for pre-qualification.

When Collins realised it was serious, they inspected the Racal facilities and decided not to grant a licence to Racal for manufacture, nor to allow the use of British components. Through Hewitt, Wadley was hastily deployed to Racal to build a new radio receiver from scratch in a very short time using his triple conversion drift cancelling design. Fortunately, work on the die-cast chassis was well advanced in South Africa as seen in figures 10 and 11.

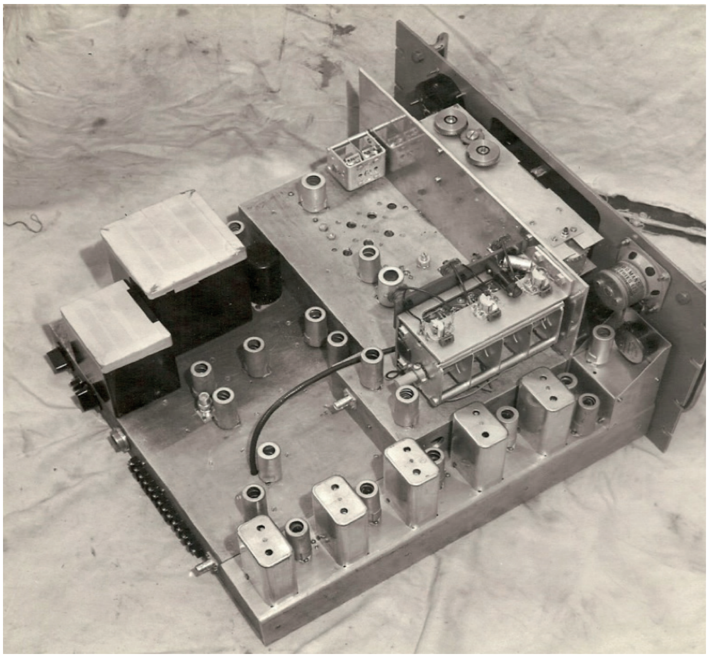


Figure 10: The pre-production prototype under construction.

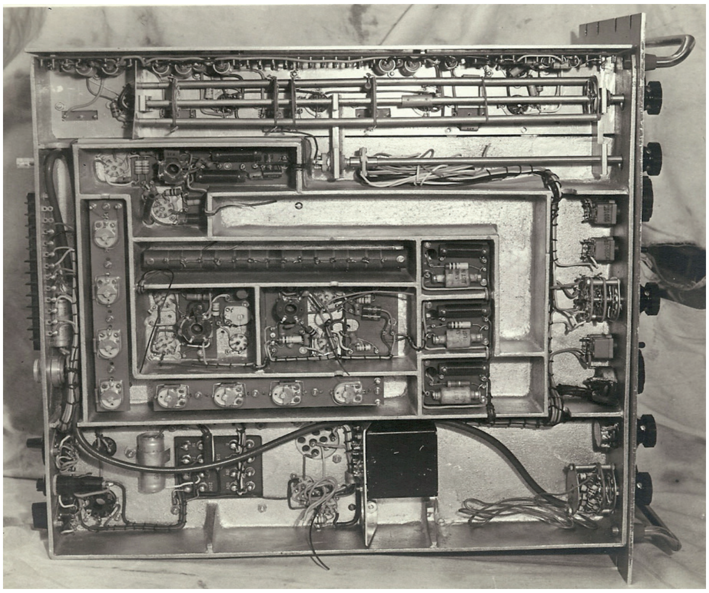


Figure 11: Underside view of the part wired pre-production prototype.

The L-shaped compartment contains the 8-pole 37.5MHz band-pass filter as yet un-connected, and the empty inverted L-shaped compartment in Fig 11 is awaiting the installation of the 40 MHz band-pass filter of similar design. The filter compartments were completely closed in by tightly fitting plated steel covers with a multitude of sprung fingers making contact with the compartment wall to create an “RF-tight” Faraday cage.

There were quite a few problems with spurious responses in the pre-production prototypes. In desperation, the chassis of one of the sets was cut in two and additional screening installed to quell the problem. In production models the first and second VFOs were in separate metal enclosures, due to their proximity on the main chassis. On the day, the receiver performed well at a demonstration of the ‘pre-production’ unit to the Royal Navy, explaining away the obviously hand-made nature of its construction as an advantage, as the Navy could include features that they had not put into their specification for final production.

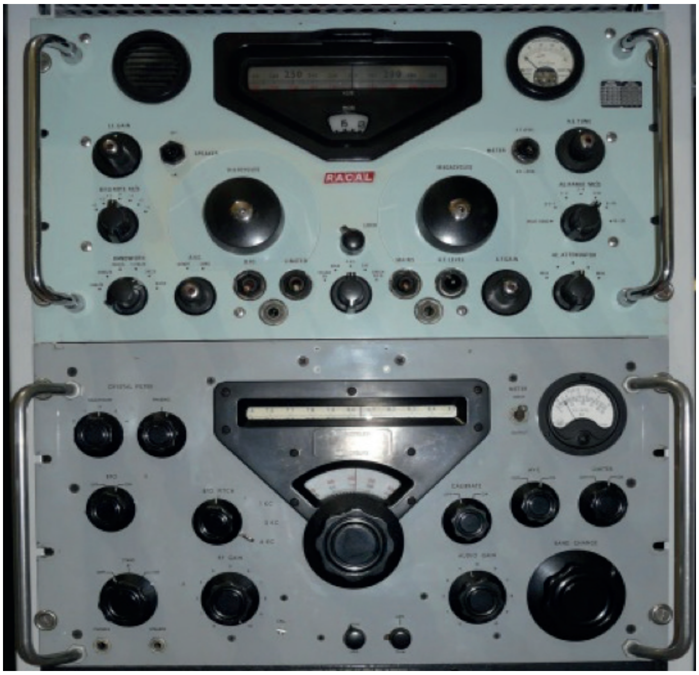


Figure 12: The Racal RA17 and below a 51J4 without makers markings.

The Navy were suitably impressed with the leap forward in technology, demonstrated by setting the dials of the submitted receiver and one of the original prototypes to a frequency where a clearly identifiable signal could be found, nominated by the client. Then, powering on from cold and as they warmed up, both were found to be accurately on-frequency. Providing that Racal could make the sets for £300 each, including the extras, then an initial order for five hundred receivers was theirs. The specification soon caught the attention of other UK Government agencies, notably GCHQ, then still based at Bletchley Park. This resulted in the restriction of sales under the UK Official Secrets Act for a while, suitably starving the Americans, However, there were more than enough orders for Racal as it became the UK Government standard ground station receiver for the next two decades. The receiver was, of course, the Racal RA17, a designation chosen to enhance Racal’s perceived experience. The visual similarity to the Collins, particularly the escutcheon, was not accidental (Figure 12).

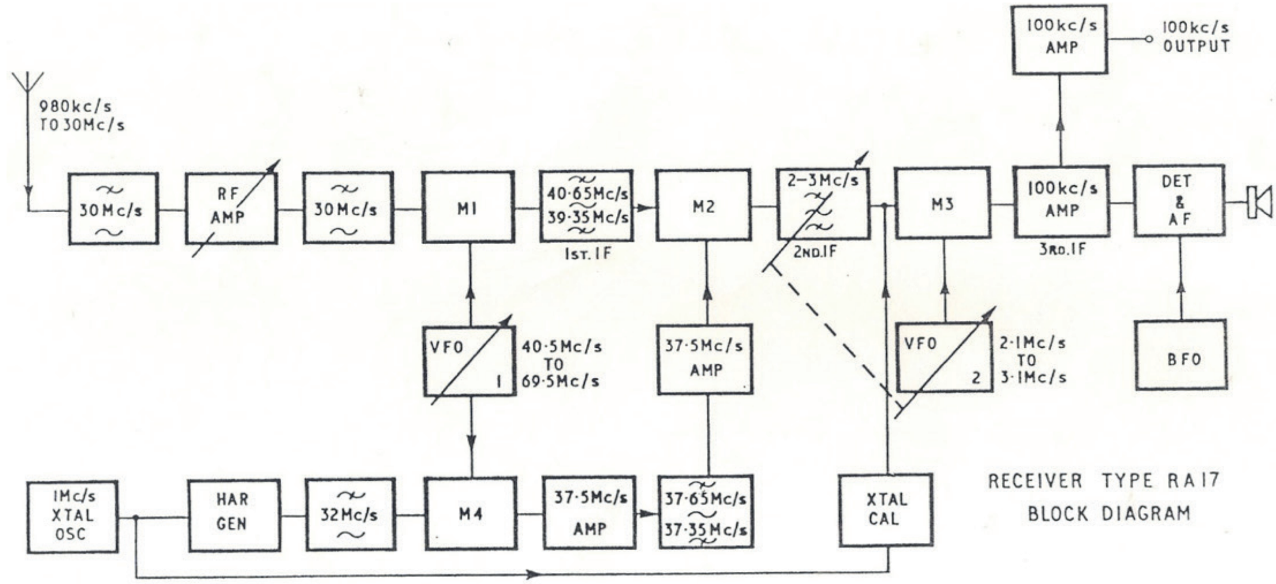


Figure 13: The Racal RA17 block diagram

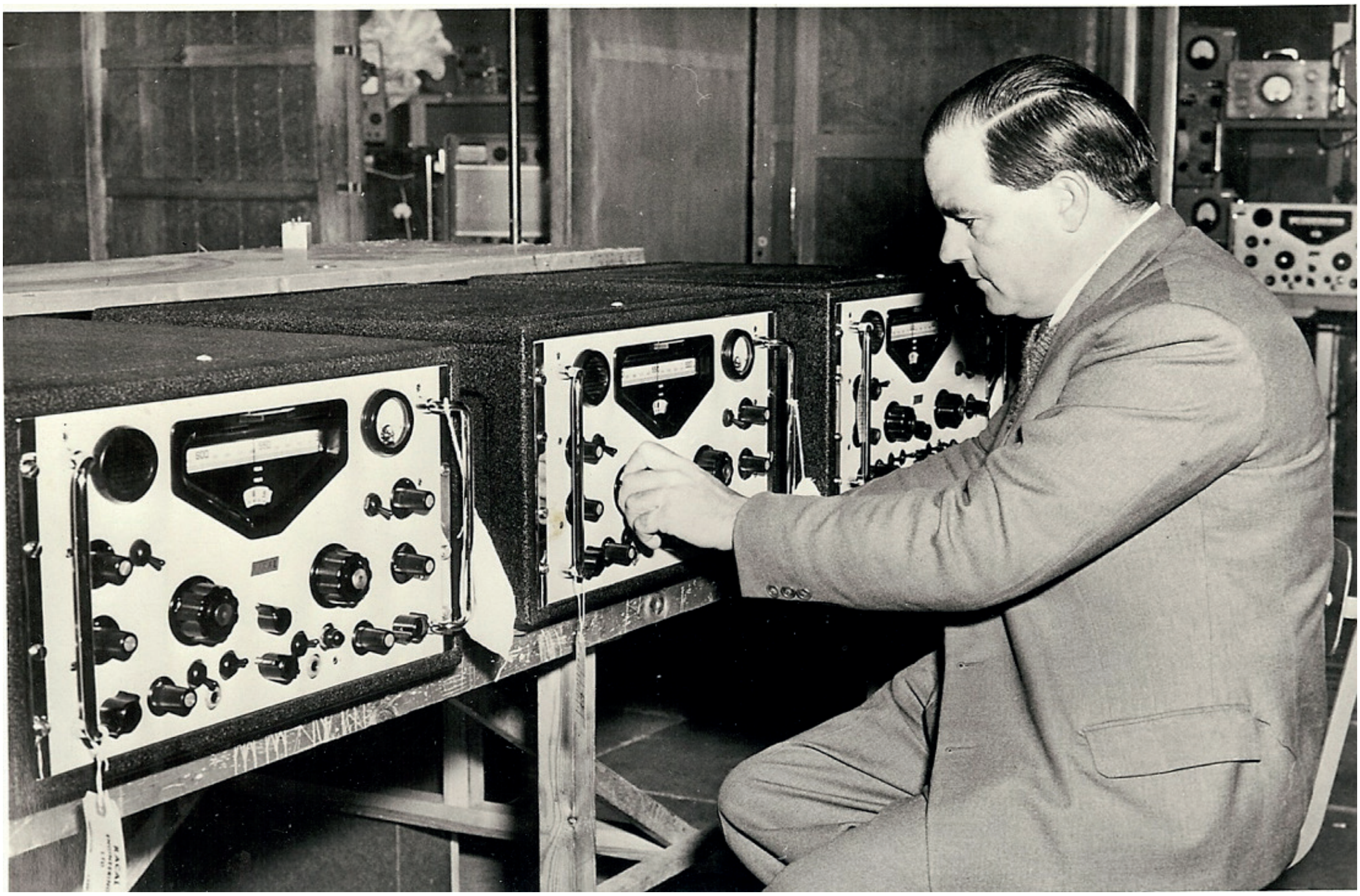


Figure 14: Wadley at Racal with production RA17's

Wadley's design was triple conversion over the entire range and he chose a high first conversion frequency to push any images way above the entire input range of the receiver, and a final IF of 100 kHz where audio bandwidth and selectivity were optimised. What made the Wadley design in the RA17 an order of magnitude more stable than the Collins was the drift-cancelling system he invented and that was proved mathematically by Fejer.

The first local oscillator (the MHz control) was mixed with the amplified incoming signal, and separately with a 1 MHz crystal signal that was rich in harmonics at 1MHz intervals (Figure 13). The signal path and the harmonic path were amplified separately in band pass amplifiers tuned 2.5 MHz apart and mixed in a third balanced mixer to produce a 2.5+_0.5 MHz (i.e. 2–3 MHz) variable IF. Whichever way the first local oscillator might drift, the one channel would see the difference signal and the other the sum of the drift and these would cancel out mathematically in the third mixer to leave a signal as stable as the crystal harmonic generator. What followed was a conventional superheterodyne circuit down-converting the 2–3 MHz signal to a low IF of 100 kHz for demodulation and audio output in the conventional manner, the second local oscillator tuning becoming the kHz control. This was a dilemma for Wadley. Despite the system being difficult to execute, its principle was extremely simple. Although patented in South Africa by the CSIR, a UK patent search revealed a prior patent, albeit unexploited, issued to a French company using similar techniques [13]. A strategy of non-disclosure was adopted, the Racal equipment manuals confined comment to levels and settings only, a policy also applied to future licencees of the system.

This account would, of course, be incomplete, without a photograph of Wadley alongside the finished RA17's (Figure 14).

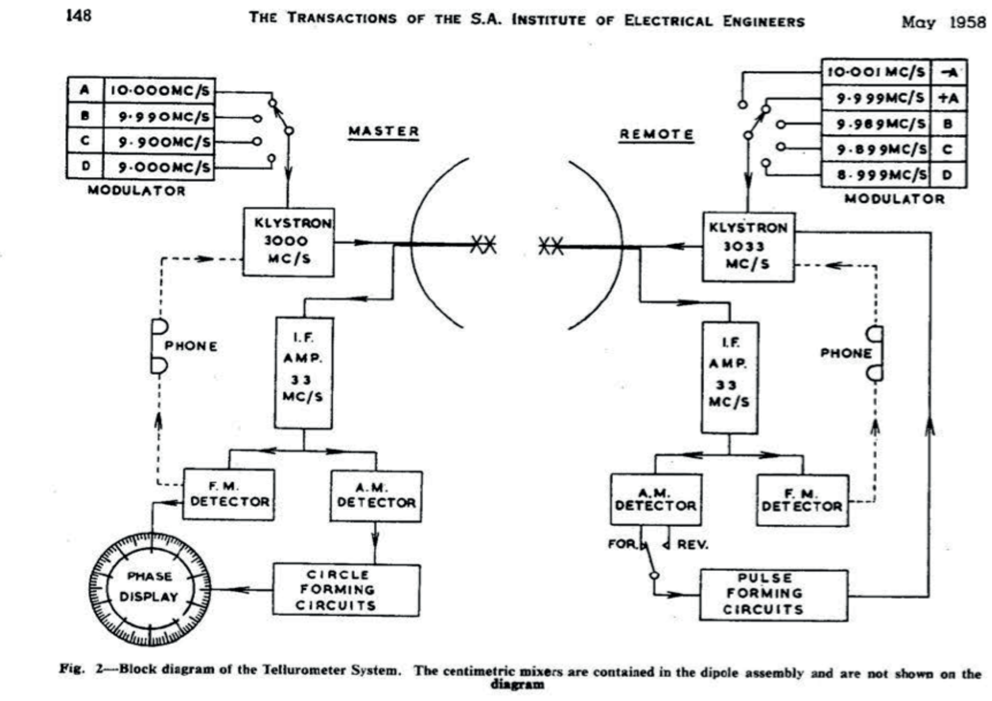
More than 20,000 Ra17's were manufactured between its inception in 1956 and obsolescence in 1967. From

1958 the RA117 was manufactured alongside the RA17 aimed at penetrating the American markets. It was distinguished by American hardware and valves and an additional heterodyne conversion to a 100kHz IF, plus a second VFO input to allow external synthesisers to be utilised. A transmitter exciter the MA79 followed with matching appearance to the RA17 and RA117 receivers. When used with an RA117 full transceive was possible by cross linking the VFO outputs to the VFO inputs. All of these had the same Wadley drift cancelling system and were mechanically the same. Racal produced a myriad of accessories for the receivers. Tha author notes that the sideband adapter RA63 and the panadapter RA66 bear signs of a contribution from Wadley, especially that the receivers provided the rear panel connectivity from the outset before the accessories were commercialised. The profitability from this long line of equipment and the RA17in particular transformed Racal from a small enterprise to an international business.

THE TELLUROMETER

The TRL had accurate radio distance measurement for survey on its agenda since 1946. However, it was not until 1952 when Colonel HA Baumann of the UDF asked for portable equipment capable of measuring ranges between 3–30 miles with an accuracy of 1 part in 100000, and not ambiguous to less than 2 miles, that Frank Hewitt applied TRL's resources to the project and assigned Wadley to lead the design. He determined that the highest frequency practical should be used and was in a position to make first measurements after a few months' work. The specification was exceeded by the prototype with accuracy of 3 parts per million. The new instrument was unveiled in Constantia, South Africa, in January 1957. Performance data were published in the latter half of the same year [13] but no technical details. With patents registered in 11 countries including the USA, a full disclosure of principle was made possible in Wadley's SAIEE paper [14] in May 1948.

The chosen carrier frequency was 3 GHz (Figure 15); S-band RADAR was a maturing technology derived from WWII airborne and portable RADARs. It avoided the use of waveguides for reasons of portability and had advantages of freedom from ground effects and ease of focussing the beam. The system comprised two klystron master oscillator transceivers, a master station on 3 GHz with the measurement CRT and a remote station which repeated the signal for the return path on 3.033 GHz, each operating at about 100 mW. The antennas consisted of a transmitting dipole situated at the focus of an 18-inch parabolic reflector, inclined at



148 THE TRANSACTIONS OF THE S.A. INSTITUTE OF ELECTRICAL ENGINEERS May 1958

Fig. 2—Block diagram of the Tellurometer System. The centimetric mixers are contained in the dipole assembly and are not shown on the diagram

Figure 15: The prototype Tellurometer block diagram.

45 degrees to the horizontal, and a receiving dipole at a right angle. Orthogonal polarisation avoided de-sensing of the receiver by the transmitter and ground echoes were minimised. The carrier was frequency-modulated with a selectable set of 'pattern' frequencies in the range of 10–9 MHz (A–D in Figure 15). At each end, a bleed from the master oscillator was used as a local oscillator for receive, giving rise to a receive IF of 33 MHz for both stations with a bandpass of 500 kHz, avoiding influence from harmonics of the pattern frequencies and keeping in tune automatically. The distance between the stations was inferred by measuring the phase shift between the transmitted and received signal at the master station.

This was done because the primary measurement at 10 MHz was more easily validated from transmitted standards than an odd frequency needed to give a distance reading, with attendant variables and correction factors. The measurement tube displayed a circular trace derived from the pattern frequency and the return pulse arranged to blank the trace so that the angle could be read on a graticule. Reverse readings were used on the A-pattern to eliminate display centring errors. The value at this stage was ambiguous because the whole number of phase rotations was unknown. Their detection is the reason for the alternative pattern frequencies employed in succession. The difference between the sent and received pattern frequencies at each selection A–D is 1KHz at which frequency the amplifier, display and return signal processing at the remote station operate. Down-conversion to the IF took place in a crystal detector mounted at the back of the dipoles. The small phase shift in these is cancelled as both ends are identical. The IF signal is detected by an FM discriminator to pick off the incoming pattern frequency and is also used for the duplex speech link. The function of the AM detector is more subtle. The FM-modulated incoming pattern frequency is mixed with the outgoing pattern frequency to derive a 1 kHz signal by AM detection, the phase of which replicates the phase shift in the pattern modulation frequencies. The integer rotations are determined by summation of the A and D pattern frequency results. Jules Fejer (now Dr) appended a mathematical proof of these principles to Wadley's paper.

On a practical note, the stability of the A-pattern crystal oscillator had to be greater than the measurement accuracy, i.e. better than 1 ppm. It was a specially cut crystal with a temperature calibration chart and ovened under thermistor control. The others only needed to be sufficiently accurate to discriminate complete numbers of cycles. The distance had to be calculated from the phase shift after correction for meteorological conditions that affected the velocity factor, principally humidity, using the speed of light in free space, then published as 299792.0 km/sec. The first field results were obtained on 14th June 1955 on an 18.7 mile baseline (surveyed with invar tapes) in South Africa.

Wadley's figure differed from the trigonometrical survey office figure by 9 inches. The uncertainty on the former was 6 inches. Wadley insisted he was right! A test programme ensued on a geodetic base called the Ridgeway in southern England reputed to be the most accurately taped base line in the world. Data showed that the measurement error increased with increasing range. The data were adjusted to self-consistency by a method of least squares and rescaled to a speed of light in free space of 299792.5 km/sec. The results were communicated to the National Physical Laboratory who confirmed the result after further laboratory experimentation. Wadley was right!

The first commercial Tellurometer, MRA 1 was a 'productionised' version of the prototype made by Tellurometer Pty Ltd, Capetown, The company was acquired by Plessey in 1967 and Tellumat grew into a global company. The next model, the MRA 2, was an X-band 10 GHz model with an accuracy of ±2 inches over 35 miles which appeared in 1959. The Tellurometer was developed over the next 20 years and was sold into 54 countries before being superseded by GPS technology. It was described by the professional press as the most notable surveying instrument since the invention of the Theodolite in the fifteenth century.

THE WADLEY MASTER OSCILLATORS

The transmission stations of Olifantsfontein and the receiving and control station of Derdepoort were officially opened on 26th June 1958. This was an immense undertaking with the Olifantsfontein site,

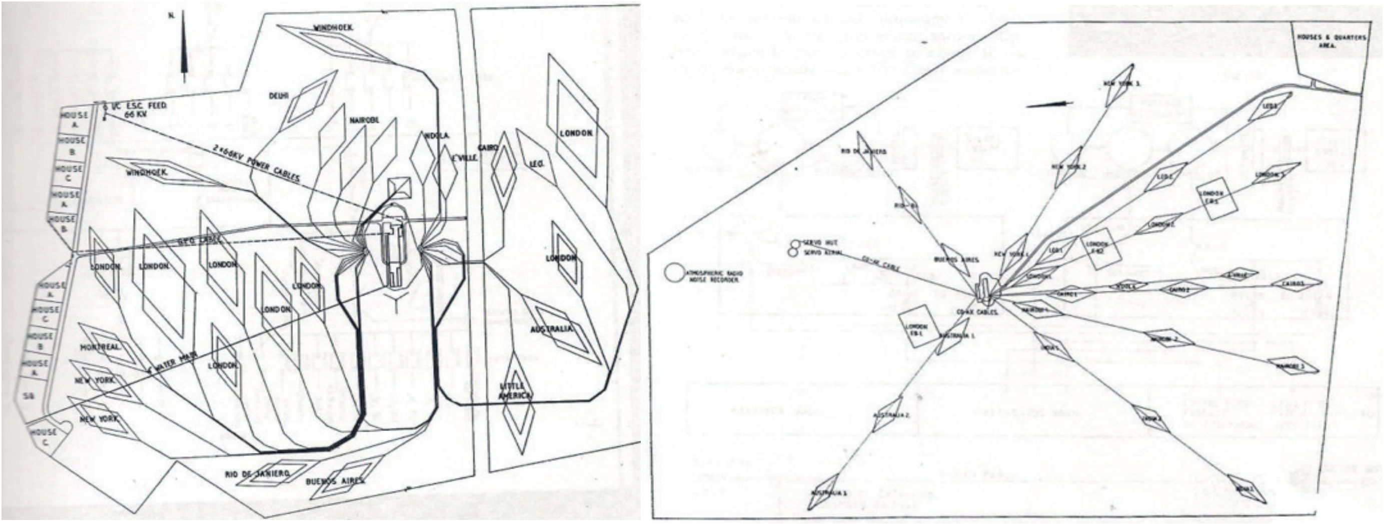


Figure 16: Olifantsfontein & Derdepoort site plans

27 km from Pretoria towards the then Jan Smuts airport, covering 900 acres and Derdepoort consisting of 1000 acres (Figure 16) situated 16 km north east of Pretoria. The real estate was chiefly needed for the rhombic antennas surrounding the central equipment buildings. They were supported on 110-foot wooden lattice masts, stacked in pairs at the former for the high-power transmitters and linear pairs and triples for diversity reception at the latter.

Derdepoort being the control station, housed all the telephony and telegraphy terminal equipment linked by high-grade physical circuits to the Johannesburg international switching centre and via landlines to the transmitters at Olifantsfontein. The modulation system employed was independent sideband (ISB) which can be likened to double-sideband suppressed carrier but with the ability to modulate the sidebands separately with different signals with up to 100 Hz to 6 kHz bandwidth, equating to two voice channels or 16 FSK circuits on each sideband. After modulation, a low-level pilot carrier was re-inserted before final mixing to enable synchronisation for demodulation to reproduce accurately the audio frequencies in the signal at the receiver.

The communications transmitters at Olifantsfontein, originally supplied by Marconi and others, were factory fitted with multi-frequency crystal master oscillators. As the service developed, the advantages of a variable master oscillator became clear if the stability of the crystal oscillators could be approached. The master reference at the stations was a highly accurate 100 kHz signal transmitted over a 100 MHz link from the Union Observatory, which also carried one second timing pulses.

A solution proposed by Wadley was adopted using

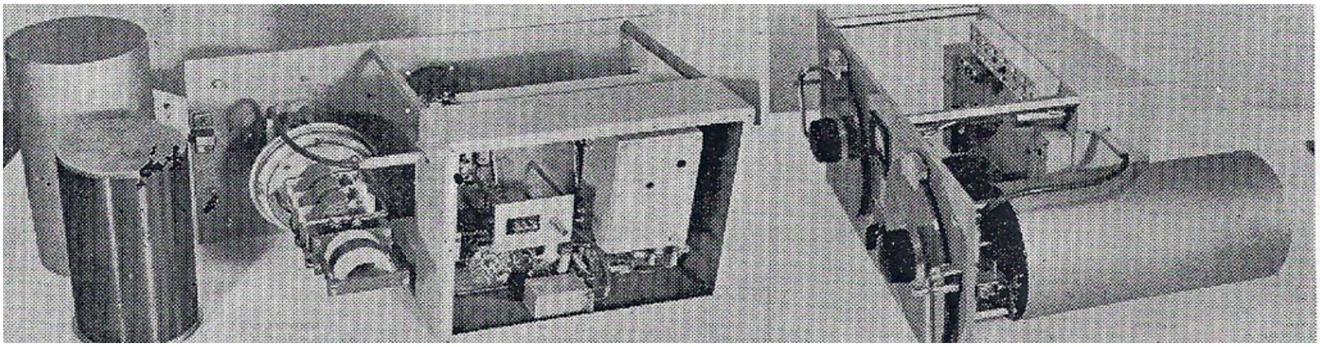


Figure 17: The oven enclosure surrounding the interpolation oscillator can be seen clearly in the only surviving picture.

the 28th to 68th harmonics generated by a harmonic generator fed from the station 100 kHz standard, mixed in a classic Wadley drift cancelling system with an ovened 200–300 kHz interpolation oscillator (Figures 17 and 18). They covered 3–7 MHz continuously with 2.5 Hz stability [12].

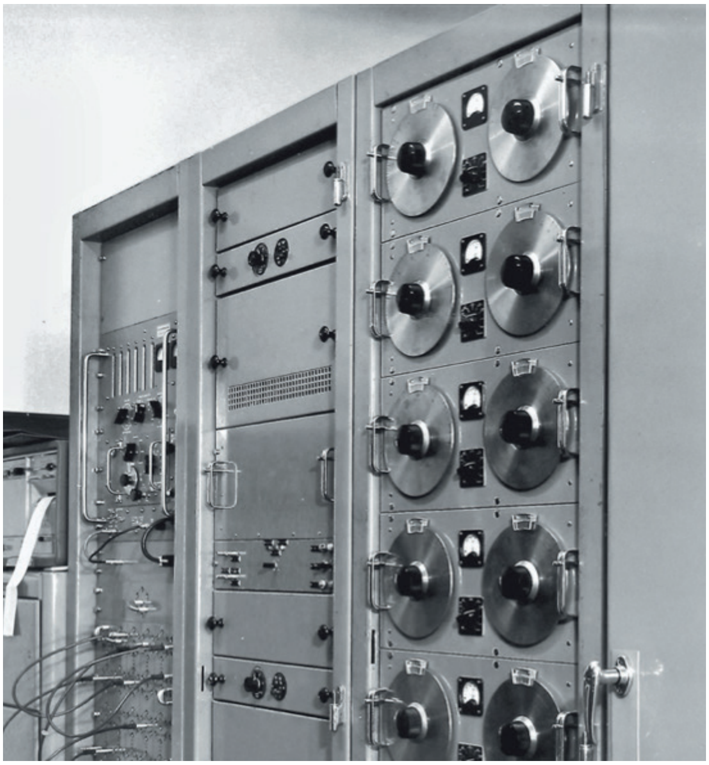


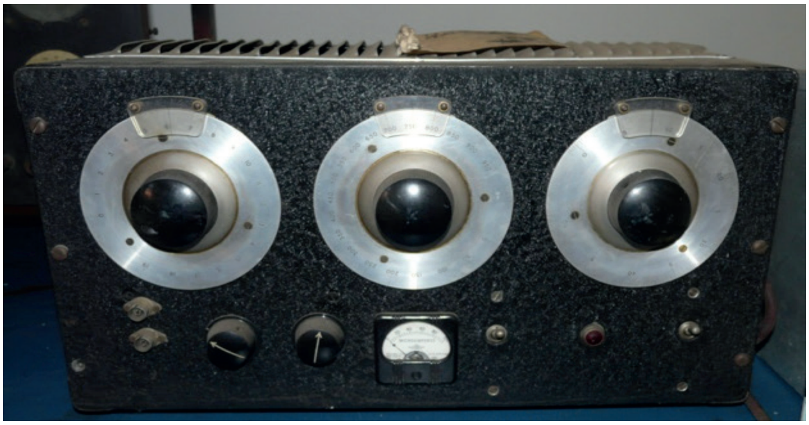
Figure 18: Ultimately 50 oscillators of this design were constructed by the SA Post Office.

The equipment was all destroyed when the stations were demolished in the name of secrecy and the sites sold to property developers.

In order to check the calibration of these oscillators, instruments of greater accuracy were required. Once again, Wadley's principle was applied and cascaded with finer levels of interpolation. A heterodyne wavemeter and a signal generator based on his principle survive in the SAIEE museum collection (Figure 19).

THE RA17 CLONES

Wadley was a regular visitor to the stations to check on the equipment. The site staff operated under the Official Secrets Act due to the handling of sensitive diplomatic and security traffic and this allowed him the opportunity for intense technical discussions with the technicians. It is not known whether Wadley knew, but a group of them in the early 1960s had a secret mission in collaboration with SABC personnel to build clones of the Racal RA17 which by now cost as much as a medium-luxury family car. At Derdepoort there was a pair of RA17s with a Plessey diversity FSK unit on a trolley and this system was used for monitoring and as the receiving station when running minor press or diplomatic news services. The spare unit for this was taken apart on night shift to copy and was re-assembled and put back into service.



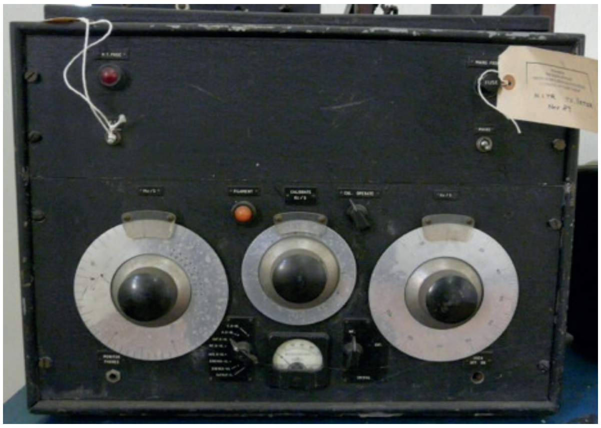


Figure 19: Cascaded Wadley heterodyne wavemeter and oscillator (note the front panel meters to monitor key voltages and currents like the prototype receivers)

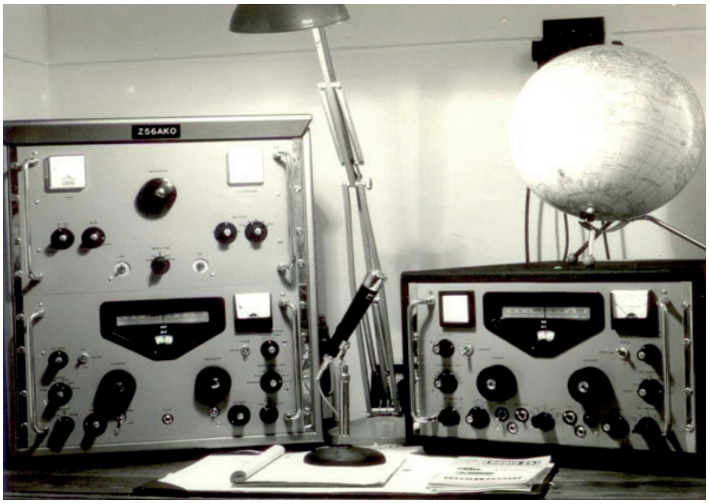


Figure 20: Gijs de Vries also constructed an exciter (L) in the genre of the Racal MA79 and a linear amplifier (top) to match the RA17 clone he constructed (R).

It is interesting to note that Gijs de Vries, ZS6AKO constructed a matching exciter (L) in the genre of the Racal MA79 (a transmitter exciter employing the Wadley drift cancelling system) and a linear amplifier using three TT21 valves (Figure20) feeding a cubical quad antenna. Normally, such a project would be beyond amateur capability but Gijs de Vries ZS6AKO was a master die-maker and had made the dies and moulds for the chassis and faceplate bezel. He was an exceptional radio engineer who included a product detector for SSB detection in the clone design. The author believes that ten of the RA17 clones were constructed of which five were located by him, described fully and pictured in his article [16].

LATER YEARS

By 1963 the CSIR resources, including Wadley, were increasingly devoted to defence with the 'Wind of change' in Africa, the rise of African nationalism on South Africa's borders and intensification of the Cold War. The marginalisation of English speakers by the Apartheid Government would have been obvious by this time. He resigned from the CSIR in 1964.

With his gratuity Wadley purchased a large property at Warner Beach on the coast of Natal – 'the last outpost'. He continued his itinerancy to Racal in Bracknell, Tellumat in Capetown and locally to Barlow Communications Ltd in Pinetown Natal, living on retainers, consultations and directors' fees. Post-retirement in 1964, Wadley produced a transistorised portable radio prototype (Figure 21) which became the Barlow-Wadley XCR 30.

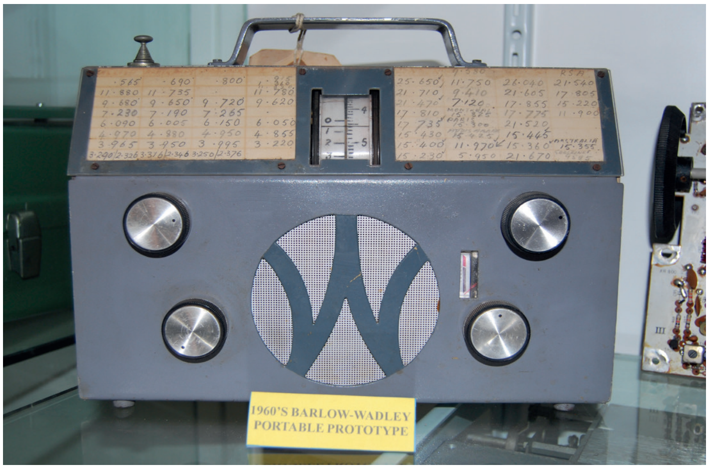


Figure 21: Wadley transistorised portable prototype.

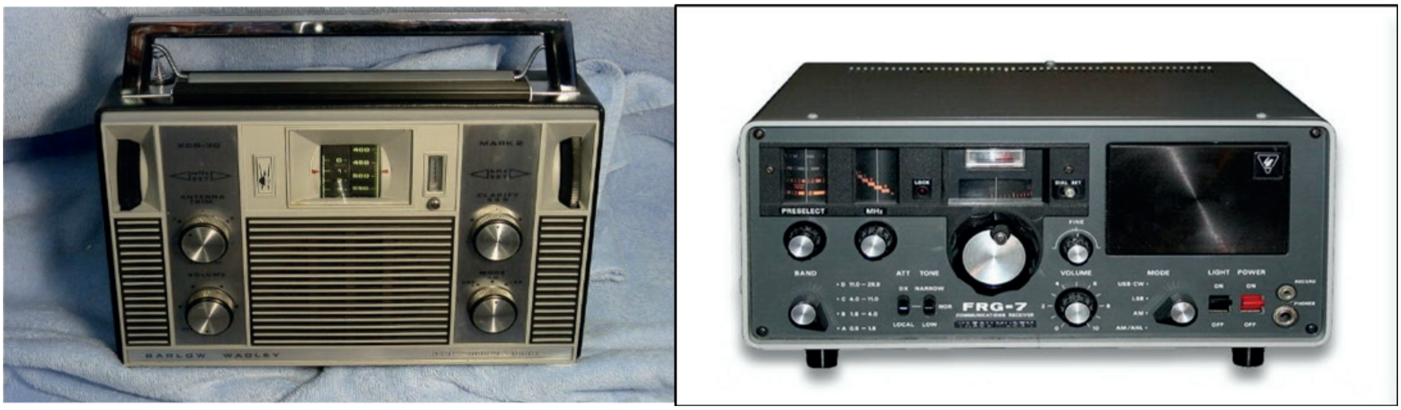


Figure 22: Barlow-Wadley XCR30 (L) & Yaesu FRG7 (R)

The drift-cancelling technology was licensed to several manufacturers, the most notable and best being Yaesu and the FRG7 (Figure 22). These were iterations of the original design with varying degrees of success which were all eventually superseded by synthesised and phase-locked loop designs.

GENIUS?

Wadley was a scientist amongst scientists with one foot firmly planted in the real world of engineering. His sister wrote that he had few friends and that he doted on his colleagues, even indulging in horseplay with them from time to time. The gambling trait developed in his schooldays reached new heights in his most prolific period. Almost every day, Wadley would challenge staff members, colleagues and students with one of his seemingly preposterous suggestions that appeared, at least on the surface, to be outrageously wrong. Vigorous arguments would soon follow and Wadley would bet anyone willing to accept the wager, that he could prove, beyond doubt, that he was right. He invariably was.

Bozzoli writes that his colleagues and students were eventually so exasperated by this that they decided to get their own back. They bet Wadley, who was reasonably portly that he would not be able to crawl through a five-metre length of mutton cloth. Wadley knew the mutton cloth would stretch, he was so quick he'd probably calculated by how much it could expand, so he took up the challenge believing he couldn't lose.

He climbed into the mutton cloth tube and gradually crawled through it until he'd reached the halfway mark. Then, his challengers tied a knot at either end of the mutton cloth, trapping him. They left him stranded, unable to cut his way out, as he didn't have a pocketknife or sharp instrument on his person. He was forced to admit, shame-facedly that he'd lost.

Many associates achieved great heights in their careers yet were unanimous in their appreciation of Wadley's abilities. Dr BFJ Schonland CBE FRS became Director of the Atomic Energy Research Establishment at Harwell in February 1958 and was knighted in the Queen's Birthday Honours List of June 1960. He died in England in November 1972. Dr Jules Fejer emigrated to Canada in 1959 and finished his career as Professor Emeritus in Applied Physics at the University College of San Diego. He died in 2002. Dr Frank Hewitt became the Vice President of the CSIR in 1964 and Deputy President in 1969. In 1995 he moved to Kelowna BC Canada where he died in 2007. Professor Bozzoli was Vice Chancellor of Wits University at the time of his death in 1998 aged 87. He was most famous for his resistance to Apartheid education policies, the barring of black students, and the Government's attempts to clamp down on student activism and protest. The high point occurred when he endured several face-to-face confrontations with PM John Vorster in defence of academic freedom.

On December 14, 1959 Wadley attained the degree of DSc (Eng.) from the University of Witwatersrand for his thesis entitled "Heterodyne Techniques in Specialised Instrumentation". He received a gold medal from the South African Institute of Electrical Engineers in 1960 for his work. He was later rewarded with an Honorary Doctorate on 18th June 1976 by the University of Cape Town and was also presented with a medal from the Franklin Institute in America. In February 1979, the SA Post Office issued a 15 cent postage stamp and a first day cover to commemorate the 25th Anniversary of the Tellurometer. It accurately depicted Wadley and his Tellurometer prototype (Figure 23).

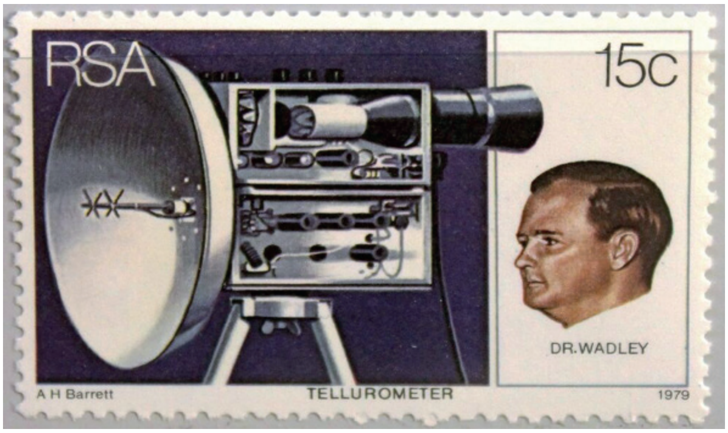


Figure 23.Commemorative stamp.

Recently, Durban High School instituted an annual mathematics prize in his honour in 2016 and Durban municipality has named a street "Trevor Wadley close" in his honour.

The genius component of his make-up was not just about the originality of the inventions in his masterpieces. His eidetic gift extended beyond just a photographic recall of something he had seen or read. He had a powerful associative mind and was a consummate lateral thinker. These traits combined to produce tangible engineered solutions where none existed before, which were first created and demonstrated by his own handiwork. The concurrency of the masterpieces confirm his superior intellect. Professor Bozzoli knew Wadley from the time of the formation of SSS, some 41 years. Bozzoli, in his book entitled "Forward", said of him "Trevor Lloyd Wadley, a genius in our time".

ACKNOWLEDGEMENTS

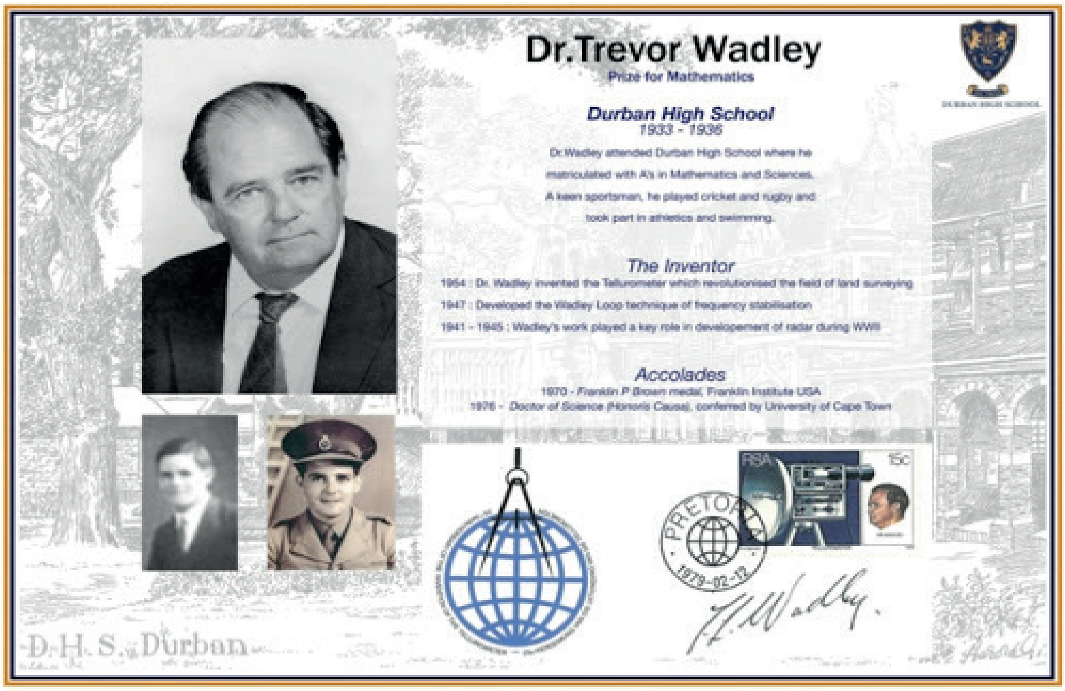
The author was privileged to serve on the Historic Section Committee of the SAIEE in the period 2013–2016, during which time he was given responsibility by Historic Section Chairman Max Clarke for the compilation from scratch of the exhibits in the 'Wireless room' and the Wadley radio exhibits in particular. The SAIEE is thanked for the opportunity and commended for displaying the prototypes of Wadley's radios, the Ionosonde and the Tellurometer under one roof in Innes House, Observatory Johannesburg, which may be visited by appointment. The role of Oliver Gerondeanos in recovering the Ionosonde and preparing it for display is highly commended.

AUTHOR'S FOOTNOTE

The terminology 'loop' is not used by the author in dealing with Wadley's drift-cancelling system because it was not presented as such in his original paper and the triple-conversion design does not have an error signal or a feedback loop, i.e. it is a free-running heterodyne system.

REFERENCES

1. M von Hirschberg. Wadley, Genius of the Tellurometer. 2009.ISBN 9780620438292 0620438290
2. JR Smith, B Sturman and AF Wright. The Tellurometer. From Dr Wadley to the MRA7. Tellumat (PTY) Ltd., Cape Town, 2008. ISBN 9780620423038
3. BA Austin. Schonland, Scientist and Soldier. Taylor & Francis Group, 2001. ISBN 9780750305013 075030501.
4. P Brain, South African Radar in World War II. published privately by the SSS Book Group, 1993.
5. From material obtained by Dr Brian Austin, while writing the book in reference [3]. Unpublished 'autobiography' of ER (Ted) Cook was recorded by Cook on tape in late 1995 just before he died at the age of 92. A copy transcribed afterwards was sent to Austin by Col. Bert Howes, formerly Director of Signals in the South African Army.
6. DC Baker. Ionosonde stations in Southern Africa – A review of current status and future prospects. Proceedings of Session G6 at the XXIVth General Assembly of the International Union of Radio Science (URSI) Kyoto, Japan, August 25 – September 2, 1993.
7. FJ Hewitt, J Hewitt, and TL Wadley. A frequency prediction service for Southern Africa. Proceedings of the SAIEE, 1947, Vol. 38 July, 180–197.
8. TL Wadley. A Single-Band 0-20 Mc/s Ionosphere Recorder embodying some new techniques. Proceedings of the IEE, 1949, Vol. 96, Pt.III, November, 483–486.
9. JA Fejer. Amplification of pulses by the gating methods. Proceedings of the SAIEE, 1949 Vol. 40, pt 2, February,
10. Obituary: Jules Andrew Fejer, Professor Emeritus of Applied Physics 1914–2002. Academic Senate, University of California, October 28, 2003.
11. TL Wadley. Variable-frequency crystal-controlled receivers and generators. Transactions of the SAIEE (presented to the Light Current Section on 11th August 1953)
12. BA Austin G0GSF. Racal in Africa – A tribute to Horace Dainty MBE (1916–2006). Radio Bygones 2007, Issue106, April/May.
13. TL Wadley. The Tellurometer system of distance measurement. Empire Survey Review, Volume XIV, July 1957 (No.105) October 1957 (No.106) and January 1958 (No. 107).
14. TL Wadley. Electronic principles of the Tellurometer. Proceedings of the SAIEE 1948, Vol. 49, pt 5, May.
15. RJ Dismore. More Wadley. AWA Newsletter 2014, Issue 101 June.



Dr.Trevor Wadley

Prize for Mathematics

Durban High School
1933 - 1936

Dr.Wadley attended Durban High School where he matriculated with A's in Mathematics and Sciences. A keen sportsman, he played cricket and rugby and took part in athletics and swimming.

The Inventor

1954 : Dr. Wadley invented the Tellurometer which revolutionised the field of land surveying

1947 : Developed the Wadley Loop technique of frequency stabilisation

1941 - 1945 : Wadley's work played a key role in developement of radar during WWII

Accolades

1970 - *Franklin P Brown medal*, Franklin Institute USA

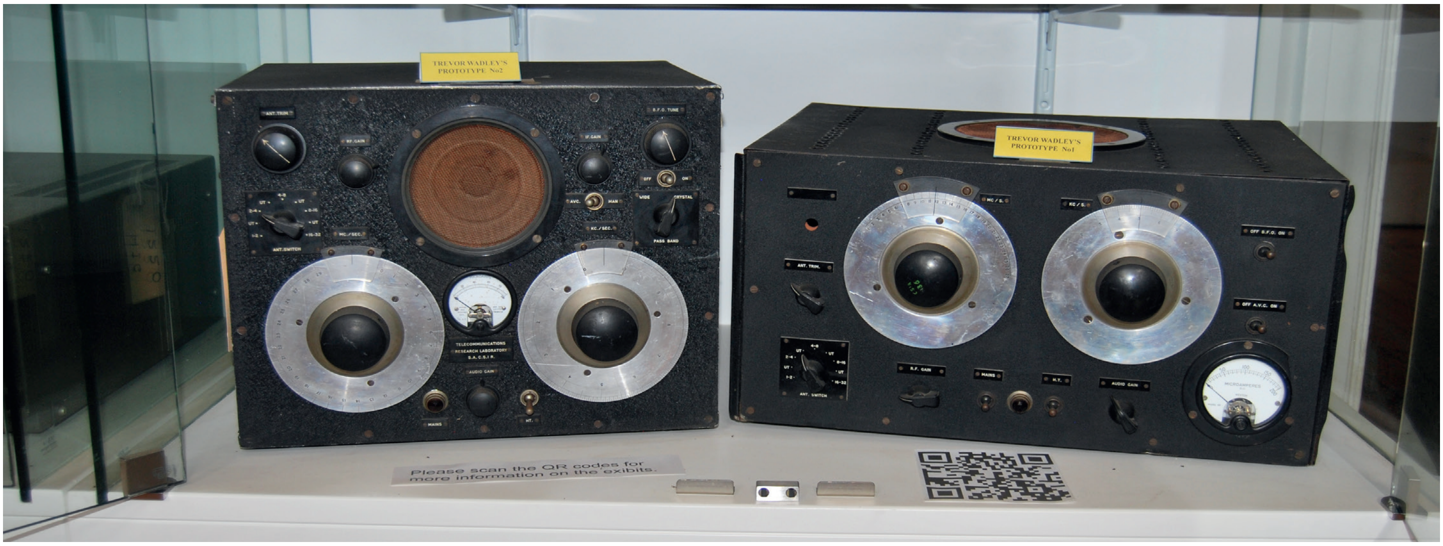
1976 - *Doctor of Science (Honoris Causa)*, conferred by University of Cape Town

RSA 15c

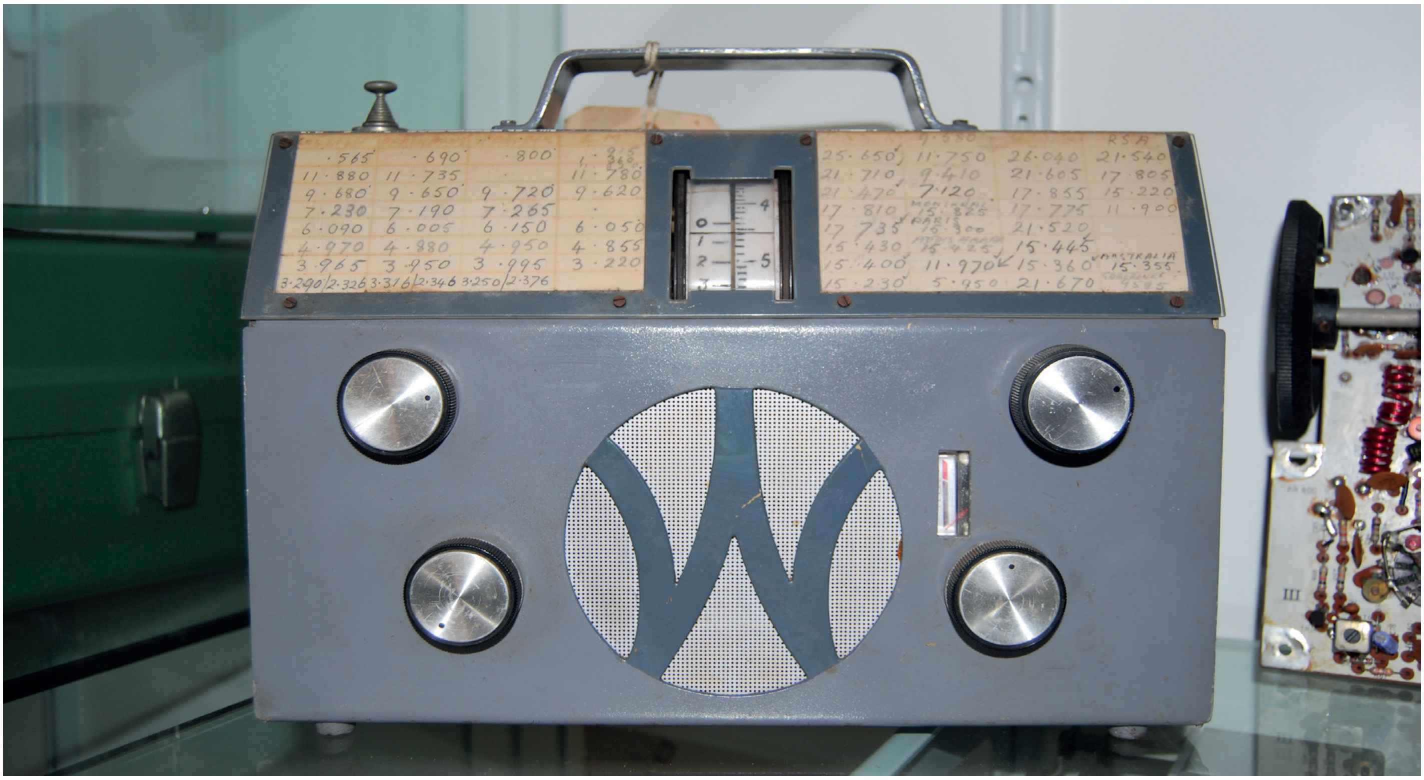
PRETORIA 1979-02-12

T.L. Wadley.

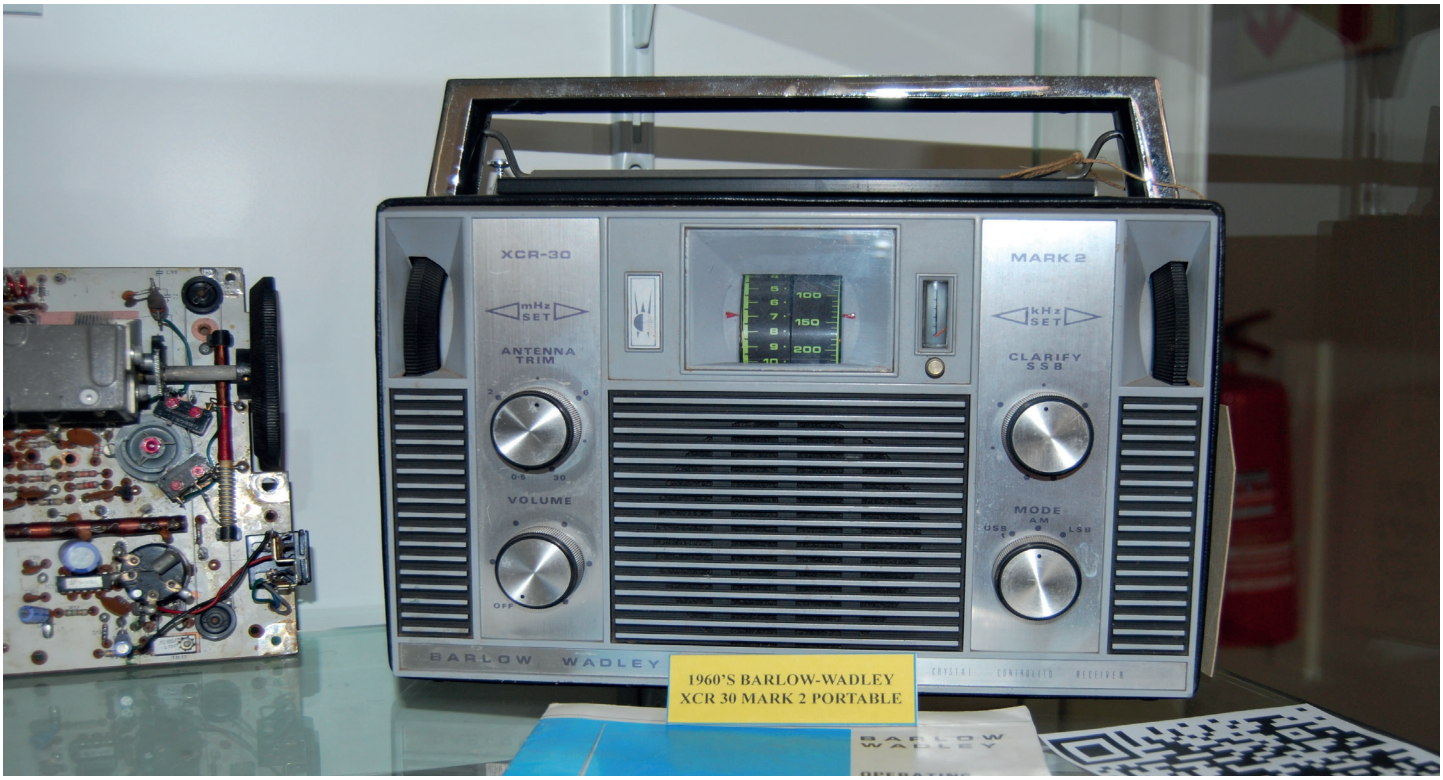
D.H.S. Durban


TREVOR WADLEY'S PROTOTYPE No2
TREVOR WADLEY'S PROTOTYPE No1
Please scan the QR codes for more information on the exibits.

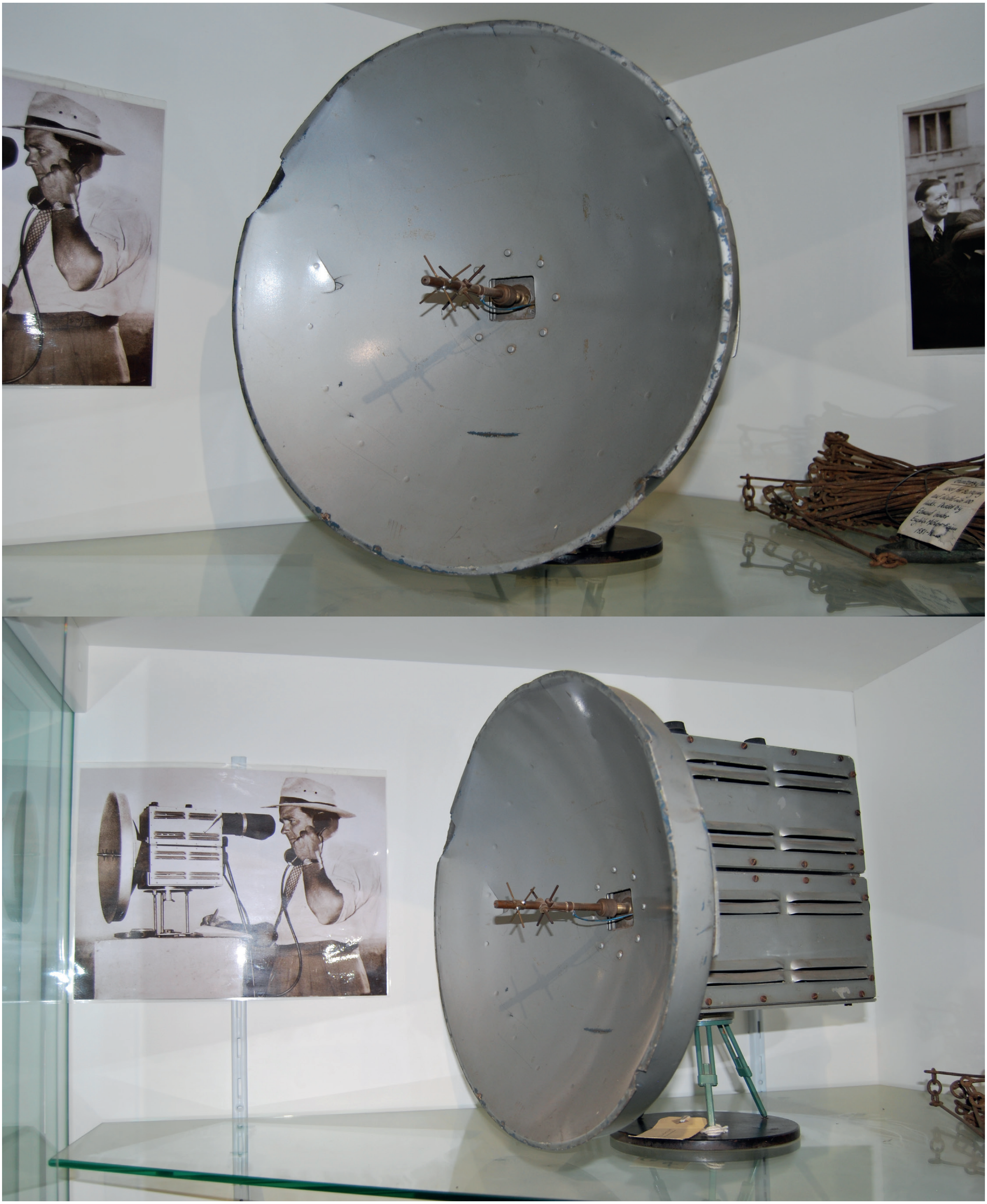
Trevor Wadley's Prototypes, No 1 on the right, and No 2 on the left.



1960's Barlow-Wadley Portable Prototype.



1960's Barlow-Wadley XCR Mark 2 Portable Radio.



Original Tellurometer

PUBLISHED BY

SAIEE

THE SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS

18A Gill Street, Observatory, Johannesburg

T 011 487 3003 **E** reception@saiee.org.za **W** www.saiee.org.za

To visit our Historical Museum, contact 011 487 3003.

To join the Historical Section, attend any of their weekly Thursday meetings, and be part of preserving history for the future.