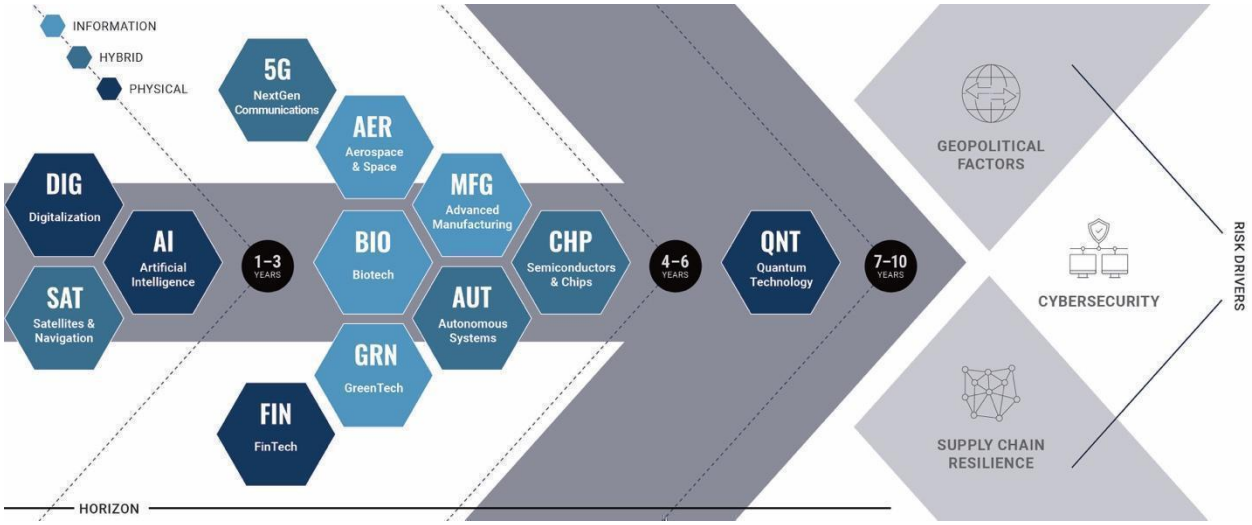
MATRIX MONITOR

Friday July 29, 2022

The only source dedicated exclusively to the emerging technologies shaping the future of business and national security.



This week's Next5 Matrix Monitor features AI and blockchain for stopping Chinese exporters from evading US tariffs, Eutelsat's purchase of OneWeb, a framework for measuring the potential impact of AI in a country, Russia's planned exit from the International Space Station, the first digitally manufactured plasma sensors for orbiting spacecraft, a collaboration by NASA and the FAA to modernize air traffic management for the drone era, quantum solutions for cybersecurity, and a House Intelligence Committee bill that would block US buyers from purchasing foreign spyware.

NEXT5 NEWS & AMPLIFICATIONS

→ **Microsoft is rallying other big name cloud-computing providers such as Google and Oracle to press the U.S. government into spreading its spending on such services more widely, taking aim at Amazon's dominance in some contracts**. Microsoft issued talking points to other cloud companies aimed at jointly lobbying Washington to require major government projects to use more than one cloud service - known as a multi cloud approach. Microsoft also approached Dell, IBM, and Hewlett Packard. Amazon dominates the cloud-infrastructure industry with a 39% share of the 2021 global market ahead of Microsoft at number 2 with a 21% share, according to Gartner research. But when it comes to government cloud contracts, Amazon's cloud had a 47% share of the 2021 US and Canada public sector market, ahead of 28% for Microsoft. Last year, NSA selected Amazon as the sole vendor for a cloud contract that could be worth as much as $10B over the next ten years, renewing an existing business relationship. An Amazon spokesman called the lobbying effort a self-serving campaign that could end up requiring customers to use inferior technology. Microsoft last week published lower than expected growth for Azure and other cloud sales. #USA #DIG #SCRM #Cybersecurity WSJ

> Analyst Comment: *Whether to select multiple vendors has become a sticking point with some big government projects across industries. Last year, the Pentagon decision to award its massive cloud contract to Microsoft (after Amazon was understood to be the longtime favorite) was mired in controversy. And the Pentagon embraced the multicloud approach after its decision was challenged by Amazon. It is Next5's position that single vendor concentration may be efficient but presents significant risks. It is also noteworthy that Microsoft, of IT monopolistic fame, is questioning the AWS cloud market share.*

→ **As quantum technology comes to fruition, there is a risk that organizations will fail to benefit fully from the advances in quantum computing without shifting mindsets**. Besides breaking today's encryption quantum promises to catalyze advances in AI, drug discovery, financial optimization, and cybersecurity in which quantum security is expected to become a $30B industry by the end of the decade. **The World Economic Forum provides four key strategies for business leaders to shift their mindset to take full advantage of the technological and economic opportunities presented by quantum technology**:

- **Explore early use cases for quantum within the next 5 years.**
  - companies should be exploring early use opportunities, planning pilot projets, and reviewing near-term use cases. Only organizations that prioritize exploration today can make the pending quantum leap.
- **Address the critical skills gap.**
  - Businesses need to develop IP, such as quantum algorithms, that let them solve problems faster than their competitors. Quantum computers require a different skill set than classical computers and talent is already in high demand.
- **Plan and prepare for the quantum threat.**

- Businesses must prepare today for the impact quantum will have on cybersecurity. This will be a major lift for larger organizations as migrating systems begins with understanding what systems are already in place and depend on several vendors.

- **Weave quantum into the business and technology strategy.**
  - Executives should focus on making quantum a major component of company strategy to get on the front foot of a technology that will transform industries.

#QNT #SCRM #Cybersecurity WEF

Next5 has also published steps business leaders should take to prepare for both mitigating the risk and taking full advantage of this revolutionary technology. Read it here.

→ **China's top chipmaker has made noteworthy advances in its ability to produce 7-nanometer chips, according to a new report, a significant breakthrough as China strives for technological self-sufficiency in order to counter US sanctions.** Canadian firm TechInsights reached this conclusion after reverse-engineering a sample chip manufactured by SMIC and extracted from a cryptocurrency mining machine. They said this was the most advanced chip they have seen produced by SMIC. Analysts and industry professionals believe that under the leadership of co-CEO Liang Mong Song, a chip-making expert who was previously an executive at TSMC, SMIC will be able to produce 7nm chips using existing deep ultraviolet (DUV) systems. While SMIC's improved capability may represent a technological milestone for the Shanghai-based company, experts question the commercial viability of producing 7nm chips using less advanced DUV systems, which are used in a variety of chip-making processes. To produce 7nm or more advanced chips, most industry players use extreme ultraviolet lithography (EUV) systems. Furthermore, according to an expert, the transistor density, power, and speed characteristics of 7nm chips produced by different manufacturers can vary greatly, so comparing SMIC's chips with those produced by competitors may be meaningless. While the ability to mass produce 7nm chips would put SMIC ahead of its American and European competitors, the Chinese firm is still one to two generations behind TSMC and Samsung. #CHP #Geopolitics #CHN #CAN #USA #TWN #KOR SCMP

> Analyst Comment: *While this is a big step forward for SMIC, they still have a long way to go in order to become self-sufficient or rival the big three - Intel, TSMC, and Samsung. The TechInsights report assessed that SMIC likely will continue pursuing a route to manufacture 7nm chips that does not require EUV lithography - which as mentioned, is barred from China by sanctions, and is exclusively produced by the Netherlands' ASML. EUV lithography enables greater simplicity and likely cost efficiencies in the production of sophisticated chips. Without this technology, SMIC is likely to persistently face issues with scalability. And according to Rhodium Group, "In the current environment, Chinese firms are incentivized to tout breakthroughs whether they can back them up or not. So outside observers should look to tangible increases in market share as opposed to press announcements or developments in test labs." While China's chip market is growing, it is not a result of a 7nm production capability. Semiconductors are a top priority for*

China's whole-of-nation approach to technology competition as stated in China's Five Year Plan. Next5 also notes that the South China Morning Post is a Chinese publication and likely inflated some of the findings from TechInsights report in the linked article, as well as SMIC's overall capability. This is a common practice in Chinese media.

DIGITALIZATION

→ **A Wall Street Journal investigation reveals how the US can use AI and blockchain to stop Chinese exporters from evading US tariffs.** In a paper published in 2018, the WSJ developed a predictive model and a risk-scoring system to characterize the likelihood of a Chinese manufacturer violating environmental regulations in 2013. The researchers found that the 20% of companies with the highest risk scores in the model, based on data from 2004 to 2012, accounted for 71% of companies with actual violations found by the Chinese government in 2013. Similarly, US Customs and Border Protection CBP can use data analytics and machine learning to target certain shipments to inspect. For example, transshipments are only attractive if tariff evaders can use a nearby country with loose law enforcement to complete their activities quickly, cheaply, and covertly. Therefore, Vietnam and Malaysia are more likely to be used for evasion than Singapore or Japan. Commodities that are similar regardless of where they originate from, such as timber and steel, also should be suspect because the country of origin can easily be falsified. Using factors such as these, the CBP can develop a risk-profile system and focus its inspection efforts on cargo identified as being high risk. Increasing the transparency of physical, financial, and informational flows in international supply chains also could make it easier to catch violations. Sensors that collect information combined with blockchain technology could be used to create an incorruptible digital record of transactions at each link of the supply chain. This digital record can include geolocation data, images of production processes and products, timestamps of transactions, identities of companies engaged in transactions, and records about types and quantities of inputs and outputs at factories. This record could then be shared with customs officials in multiple countries and government investigators. #DIG #AI #SCRM #Geopolitics WSJ

→ **The United Kingdom's MI5 director General Ken McCallum called out the UK's intelligence and military communities' personnel and their use of the social network, LinkedIn.** McCallum noted that personnel were identifying themselves as involved in sensitive classified work and that these disclosures were a breach of government directives. McCallum also highlighted how LinkedIn was being used to target the UK government and businesses by the nation's adversaries. The message mirrors a separate one by the US FBI, which, in October 2020, published the 30-minute video "The Evernight Connection" detailing Chinese TTPs to leverage social networks like LinkedIn. Following McCallum's message, the Daily Mail did a quick search which revealed that over 1,200 individuals had revealed that they are affiliated with and engaged in classified work. Also, Check Point Research has shown that LinkedIn continues to be the most imitated brand used by cyber criminals in launching phishing attacks designed to compromise users' devices. The report notes that the ubiquitous messaging from the app makes it a prime candidate for spoofing. Days before MI5's message, both McCallum and FBI

director Wray issued a joint threat warning concerning China as a nation-state adversary actively engaging in influence operations against the respective countries. #DIG #Cybersecurity #USA #GBR #CHN Clearance Jobs

> Analyst Comment: *A LinkedIn search of Next5 CEO's first degree connections returned hundreds of results where people listed their Top Secret clearances. That being said, Next5 assesses there are far more than the 1200 individuals Daily Mail detected that identify their work as classified on LinkedIn. As described, this practice enables adversaries to target people with specific skills, in certain industries and companies, and with access to classified information.*

→ **Blockchain-based metaverse and Web3 platforms have decided to form an Open Metaverse Alliance for Web3 (OMA3) to overcome the interoperability challenges of the industry.** Four core principles of the Alliance are said to be transparency, inclusiveness, decentralization, and democratization. The joint organization was established by Alien Worlds, Animoca Brands, Dapper Labs, Decentraland, MetaMetaverse, Space, Superworld, The Sandbox (SAND), Upland, Voxels, and Wivity. The means to overcome interoperability challenges would be focused on proposing standards and facilitating collaboration between various stakeholders of Web3 and other industries. OMA3 will be established as a decentralized autonomous organization (DAO) to ensure a governance system that is "transparent and user-centric." It will focus its efforts on specific metaverse-related topics, such as standards for nonfungible tokens (NFTs), protocols, transferable identity, portals between virtual worlds, mapping, and indexing. The Alliance members intend to join the recently announced Metaverse Standards Forum – a constellation of Web3 companies coordinating requirements and support for existing standards and developing standards relevant to the Metaverse. #DIG Coin Telegraph

SATELLITES & NAVIGATION

→ **France's Eutelsat is buying its British rival OneWeb in a $3.4B deal that is widely seen as a challenge to Elon Musk's SpaceX.** Eutelsat and OneWeb are highlighting the complementary nature of their respective products as the main opportunity: Eutelsat's GEO satellites, which are higher altitude and thus higher latency, are better suited for weather forecasts and TV broadcasts. And OneWeb's constellation of lower-altitude satellites are better for critical communications that require low-latency data transfers. Combined, the companies argue that they will be better positioned to target a broader array of use cases across the B2B and B2C spheres. The transaction, if approved by the usual regulatory bodies, is expected to close by the end of the first half of 2023. #SAT #USA #FRA #GBR TechCrunch

→ **The Defense Innovation Unit is funding space projects that the agency hopes will spur commercial investments in satellite refueling technologies and support services for geostationary satellites.** DIU, based in Silicon Valley, is a Defense Department agency

established in 2015 to help bring privately funded innovation into military programs. Since its inception, much of DIU's space portfolio focused on low Earth orbit capabilities but the agency is now turning more attention toward the GEO belt, 22k miles above the Equator where many of the military's key satellites operate. DIU is especially interested in logistics, manufacturing, and in-space satellite servicing. The plan is to team up with private companies and fund prototypes of systems that could later be commercialized. Another benefit for DoD is that having a more robust infrastructure in GEO would help support operations beyond Earth orbit into cislunar space. In-space satellite refueling and robotic servicing vehicles are two areas where DoD is expected to increase investments, according to Space Force Maj. David Ryan, DIU program manager. #SAT #USA SpaceNews

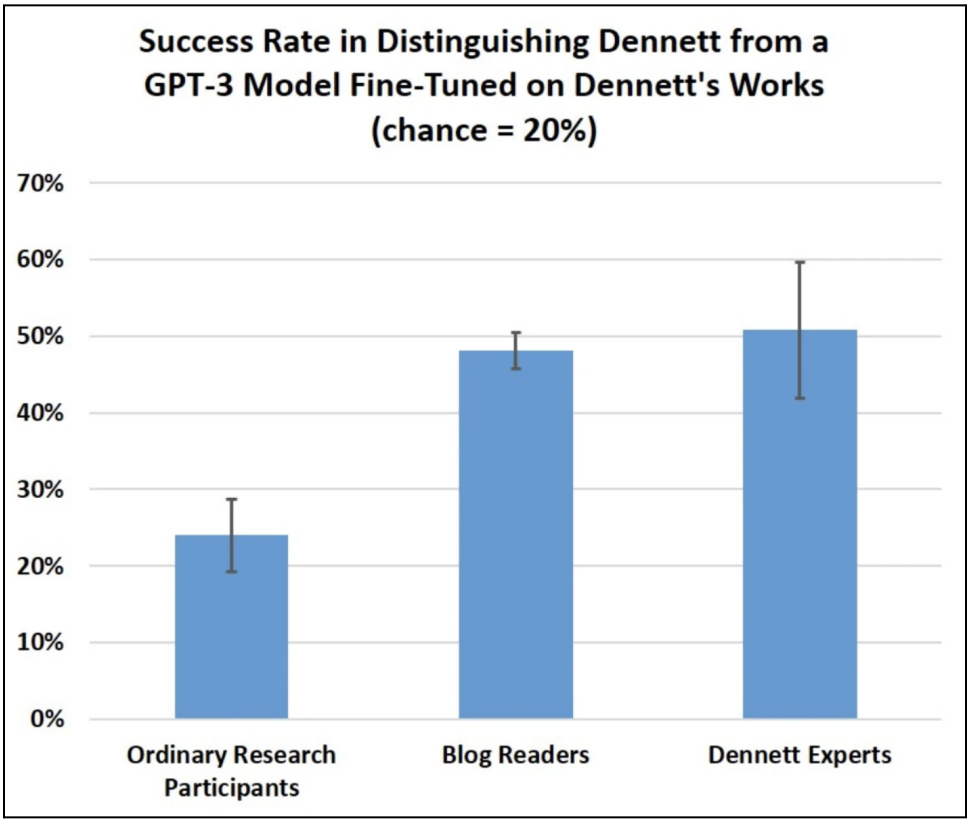
ARTIFICIAL INTELLIGENCE

→ **Mckinsey & Company provides three steps to measure the potential impact of AI in a country and examines how this could play out in a handful of countries:**

1. **Identify the most relevant use case domains**. The Firm's research suggests that the hundreds of AI use cases that have the potential to unlock value in countries can be grouped into 15 domains, which can inform efforts to measure impact (Exhibit 1). It is useful to determine which use case domains are the most relevant for businesses and organizations across sectors of the economy.
2. **Estimate the impact of use case domains**. Using benchmarks, the average financial impact of relevant domains can be identified at the company level or organizational level per priority sector. For example, if predictive maintenance in manufacturing reduces maintenance costs by 10 percent on average, it would improve a company's EBIT by 2 percent.
3. **Scale up impact to the sector and economy level**. Suppose that for one manufacturing company, all relevant use case domains combined can increase EBIT by 10 percent. If the total EBIT for all companies in the sector is $10B, then that EBIT would rise to $11B. If net operating surplus (approximated by EBIT) accounts for 50 percent of gross value add (GVA) – that is, contribution to GDP – in the manufacturing industry (which would total $20B), an industry-wide 10 percent EBIT increase from AI would increase the sector's GVA by 5 percent. Once the impact at the sector level is understood, it can be scaled up to the total economy level by adding up the impact of all sectors.

McKinsey applied the strategy across Gulf Cooperation Council (GCC) countries, which revealed a $150B potential value across all sectors of their combined economies. The analysis shows that AI could potentially add value corresponding to 6 percent or more of each economic sector's GDP in GCC countries. As governments leverage the strategy, they must also address the potential risks of implementing AI, including privacy, security, fairness, transparency and explainability, safety and performance, and third-party risks.
#AI McKinsey & Company

→ **A third generation of the Generative Pre-trained Transformer was trained on millions of words of the philosopher Daniel Dennett about a variety of philosophical topics, including consciousness and AI.** GPT-3 is a machine learning model from OpenAI that produces text from whatever material it's trained on. A recent experiment by the philosophers Eric Schwitzgebel, Anna Strasser, and Matthew Crosby quizzed people on whether they could tell which answers to deep philosophical questions came from Dennett and which from GPT-3. The questions covered topics such as, "What aspects of David Chalmers's work do you find interesting or valuable?" "Do human beings have free will?" and "Do dogs and chimpanzees feel pain?" – among other subjects. This week, Schwitzgebel posted the results from a variety of participants with different expertise levels on Dennett's philosophy and found that GPT-3 performed exceptionally well. According to Schwitzgebel, a professor of philosophy at the University of California Riverside, even knowledgeable philosophers who are experts on Dan Dennett's work had trouble distinguishing the answers created by the language generation program from Dennett's own answers. The Dennett quiz reveals the need to grapple with the implications of how easy it can be to be deceived by natural language processing systems as they become more sophisticated and common.



#AI #USA Vice.com

NEXT GENERATION COMMUNICATIONS

BACK TO TOP

→ **The UK Government has announced plans to "unleash" 5G and 6G innovation, including through a partnership with South Korea.** Up to $25M has been set aside for the 'Future Open Networks Research Challenge.' Academics and industry players can apply for funding to support their early-stage research into open and interoperable telecom solutions, such as Open Radio Access Network (Open RAN). The Future Open Networks Research Challenge is part of the UK Government's wider $254M 'Open Networks R&D Fund.' By supporting the emergence of interoperable solutions, the fund aims to improve the resilience of the nation's telecoms networks, lower deployment costs, and enable innovative new players. #5G #GBR #KOR Telecoms Tech News

FINANCIAL TECHNOLOGY

→ **BestEx Research Group, which operates a trading platform driven by algorithms, is offering an electronic tool to banks so they can build their own algos without having to write the code themselves.** The technology firm's new tool, Strategy Studio, gives buy-side clients and brokers the ability to build algos, helping cut costs and time. Each algo can be matched to a bank or broker-dealer's trading objectives. Commissions for algo trading are expected to increase to $34B next year, according to researcher Chartis, with Wall Street trading more and more asset classes, including foreign exchange, fixed income and options, algorithmically. BestEx is targeting its new product to electronic-trading units at banks that serve clients in equities, futures, and fixed-income markets. Over the next two years, BestEx intends to persuade at least 10 banks to build their custom offerings on top of the firm's existing algo-management system. The company said it's offering its algo-trading product at a lower cost than it would take banks to build their own offerings internally. The firm's one-year subscription will cost an average of $1M a year, depending on the size and complexity of the bank. #FIN #USA Bloomberg

→ **Some cryptocurrency platforms that have lost millions of dollars in digital heists are offering some of the money to attackers if they give back the rest.** Victims have offered as much as $10M in these efforts, and have likened them to the bug bounties paid to security researchers for uncovering software flaws. Similar to ransom payments, the deals may allow a company to get back to normal after a cyberattack, security experts say. But vulnerability specialists disapprove of the practice of branding them as "bug bounties." To them, the practice legitimizes thieves by conflating them with white-hat hackers, who report software flaws for a fee. Ethical hackers deal directly with companies, including multinationals, such as Microsoft, or go through third-party platforms. According to crypto-research firm Chainalysis, North Korean-linked groups have stolen more than $1B, largely from decentralized financial platforms. #FIN #Cybersecurity #PRK WSJ

AEROSPACE & SPACE

→ **Russian space officials told their US counterparts that Moscow expects to remain on the International Space Station at least until their own outpost in orbit is built in 2028.** The

assurance from Russia on Tuesday, July 26, came after the newly appointed head of its space agency, Roscosmos, surprised NASA earlier in the day by announcing that Moscow intended to end more than two decades of partnership on the space station "after 2024." Despite the tension, NASA and Roscosmos made a deal earlier this month for astronauts to continue riding Russian rockets and for Russian cosmonauts to fly to the space station with SpaceX beginning this fall, The Associated Press reported. That agreement ensures that the space station will always have at least one American and one Russian on board to keep both sides of the orbiting outpost running smoothly. #AER #USA #RUS #UKR NBC Yahoo

→ **Debris from a Chinese rocket is set to crash to Earth sometime over the next few days, with the potential for wreckage to land across a wide area of the globe.** Part of a Long March 5B rocket China launched on July 24 will make an uncontrolled reentry around July 31, according to the Aerospace Corp., a nonprofit based in El Segundo, California. The possible debris field includes much of the US, as well as Africa, Australia, Brazil, India, and Southeast Asia, according to Aerospace's predictions. Concern over the reentry and the impact it could have is being dismissed by China, however, with state-backed media saying the warnings are just "sour grapes" from people resentful of the country's development as a space power. The descent of the booster, which weighs 23 metric tons, would be part of what critics say is a series of uncontrolled crashes that highlights the risks of China's escalating space race with the US. In May 2021, pieces of another Long March rocket landed in the Indian Ocean, prompting concern that the Chinese space agency had lost control of it. "It is clear that China is failing to meet responsible standards regarding their space debris," NASA Administrator Bill Nelson said that month. #AER #USA #CHN Bloomberg

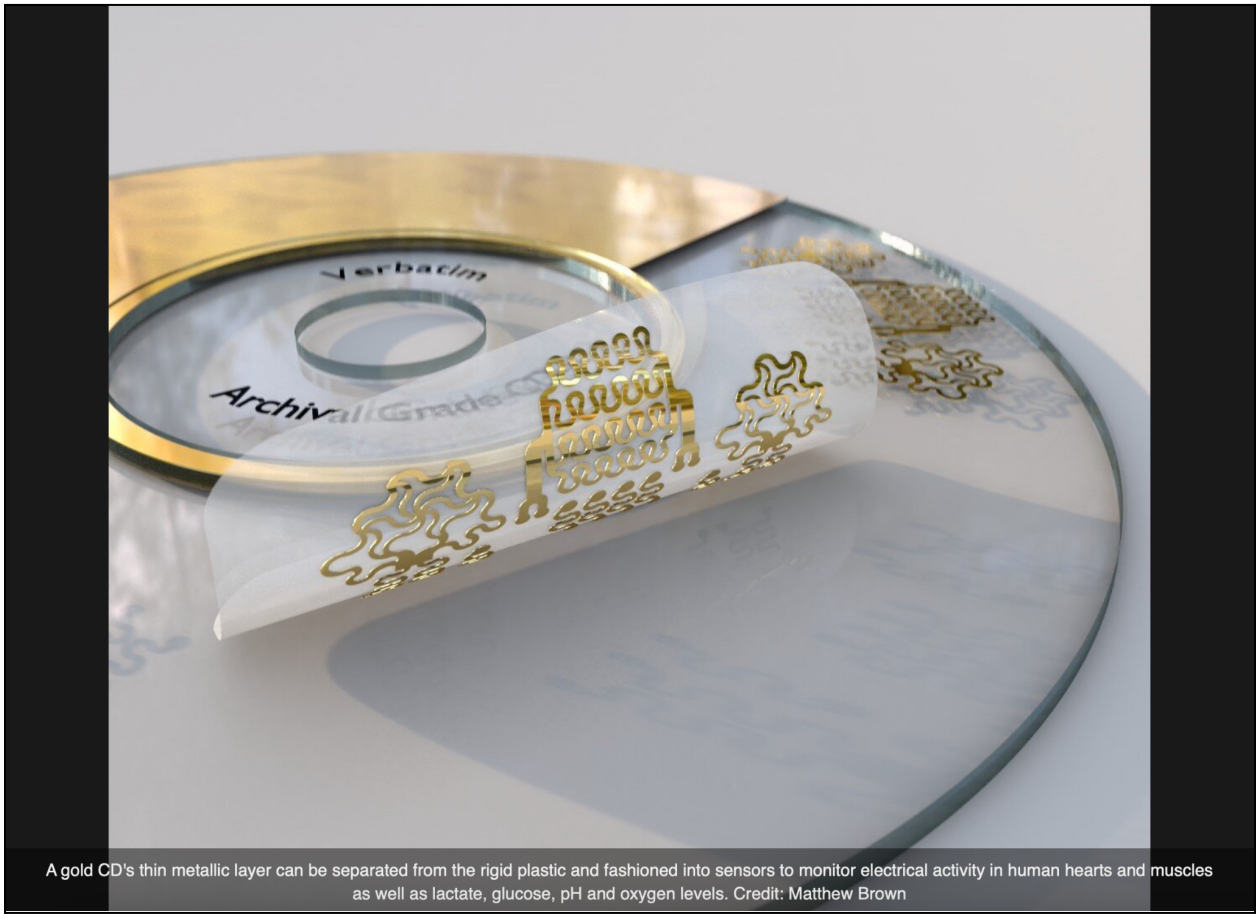
→ **Chinese scientists are building an optical device to be mounted on California's Hale telescope in a rare example of scientific collaboration with the US.** The telescope, operated by the Caltech Optical Observatories, was the world's largest telescope for more than four decades and still plays a leading role in cutting-edge astronomy. Researchers are developing a Next Generation Palomar Spectrograph (NGPS) that will be fitted to the telescope next year, an upgrade that will make it "comparable to some of the most powerful optical telescopes on the ground," according to Tsai Chao-wei from the National Astronomical Observatories of China in Beijing. The NGPS is also one of the few institutional-level collaborations going on between the two countries in basic science under the current political climate. The Chinese side is responsible for developing the spectrograph's optics part, while the US side leads on areas such as detectors, electronics, and software. #AER #Geopolitics #USA #CHN SCMP

BIOTECHNOLOGY

→ **In a new study published in the journal *Science Advances*, a team of researchers from The Ohio State University demonstrated a battery-free, wireless biochemical sensor, a**

"smart necklace," that detected and monitored glucose levels of study participants as they exercised. It operates without a battery by using a resonance circuit to reflect radio frequency signals sent out by an external reader system. After 30 minutes of indoor cycling, participants took a 15-minute break and drank sugar-sweetened beverages before returning to cycling. The researchers knew that after drinking the sugary beverages, glucose levels in the sweat would rise; the question was whether this new sensor would detect it. The results showed that the sensor successfully tracked glucose levels, implying that it will work to monitor other important chemicals in sweat. Furthermore, due to the sensing interface's miniaturized structure, this smart necklace requires only a small amount of sweat for the interface to function. Instead of the bulky and rigid computer chips found in phones and laptops, the sensors are made of ultra-thin materials. This design style makes the product extremely flexible, protects the device's functionality, and ensures that it can come into contact with a person's skin safely. While the study notes that further miniaturization would make this and similar devices more feasible for implantability, the researchers envision it as a lightweight device with simple circuit layouts that could be easily integrated into people's daily lives for the time being. #BIO #USA Tech Xplore

→ **Binghamton University researchers demonstrated how the thin metallic layer of a gold CD can be separated from the rigid plastic and formed into sensors to monitor lactate, glucose, pH, and oxygen levels, as well as electrical activity in human hearts and muscles.** The sensors can communicate with a smartphone via Bluetooth. The fabrication takes 20 to 30 minutes and costs approximately $1.50 per device, without the use of toxic chemicals or expensive equipment. Previous research on CD-based biosensors discovered that they retained a rigid structure and had a more limited number of applications than the researchers hoped for. The first step was to use a chemical process and adhesive tape to remove the metallic coating from the plastic beneath. The sensors were created using a Cricut cutter, an off-the-shelf machine for crafters that cuts designs from materials such as paper, vinyl, card stock, and iron-on transfers. The flexible circuits would then be removed and attached to a person. Medical professionals or patients could obtain readings and track progress over time using a smartphone app.



A gold CD's thin metallic layer can be separated from the rigid plastic and fashioned into sensors to monitor electrical activity in human hearts and muscles as well as lactate, glucose, pH and oxygen levels. Credit: Matthew Brown

#BIO #MFG #USA Tech Xplore

GREEN TECHNOLOGY

→ **Tesla is trying to tap into public funding to build EV chargers as it moves to open its US Supercharger network to EVs made by other manufacturers.** The EV-market leader is bidding for a portion of billions in federal and state dollars that will be available in coming years as the Biden administration, automakers, and states try to accelerate a fast-charger build-out along highways. Tesla has been building its Supercharger network for several years and has a system popular with drivers that is considered easy to use. So far, it has 1,440 sites with around 14,600 chargers for its drivers, who can also access other sites available to all kinds of EVs. Advocates for greater EV adoption say Tesla opening some of its new charging sites to other drivers won't make a significant impact right away, but the need for public charging infrastructure is overwhelming. #GRN #USA WSJ

ADVANCED MANUFACTURING

→ **MIT scientists have created the first completely digitally manufactured plasma sensors for orbiting spacecraft.** These plasma sensors, also known as retarding potential analyzers (RPAs), are used by satellites to determine the chemical composition and ion energy distribution of the atmosphere. The 3D-printed and laser-cut hardware performed as well as state-of-the-art semiconductor plasma sensors that are manufactured in a cleanroom, which makes them expensive and requires weeks of intricate fabrication. By contrast, the 3D-printed sensors can be produced for tens of dollars in a matter of days. Due to their low cost and speedy production, the sensors are ideal for CubeSats. These inexpensive, low-power, and lightweight satellites are often used for communication and environmental monitoring in Earth's upper atmosphere. #MFG #SAT #USA MIT

→ **According to Russian media outlets, a chess-playing robot, apparently unsettled by the quick responses of a seven-year-old boy, grabbed and broke his finger during a match at the Moscow Open.** Video of the 19 July incident published by the Baza Telegram channel shows the boy's finger being pinched by the robotic arm for several seconds before a woman followed by three men rush in, free him, and guide him away. While robots are becoming more and more sophisticated, with the most modern models capable not just of interacting but actively cooperating with humans, most repeat the same basic actions – grab, move, put down – and neither know nor care if people get in the way. According to one 2015 study, one person is killed each year by an industrial robot in the US alone. Moreover, according to the US occupational safety administration, most occupational accidents since 2000 involving robots have been fatalities. #MFG #AI #RUS The Guardian

AUTONOMOUS SYSTEMS

→ **NASA and the FAA are collaborating to modernize air traffic management in preparation for the drone era.** The goal is to accommodate millions of unmanned drone operations below 400 feet, as well as next-generation light passenger aircraft that combine human and algorithmic piloting at altitudes up to 5,000 feet. The project includes an array of specifications covering airframes, sensors, communications hardware and bandwidth, vertiports (drone airports), and, most importantly, traffic. The aircraft will require rules that humans and computers can follow intuitively and that aid in determining who is responsible for accidents. The drone network will necessitate unprecedented collaboration between the government and the private sector. NASA and the FAA have been collaborating closely with Boeing, Airbus, Amazon, FedEx, law enforcement, firefighters, and other public and private partners. They've flown thousands of hours, collecting data on connectivity rates, landing accuracy, flight performance, and other factors to help government agencies and manufacturers improve their regulations and designs. The most difficult circumstances to plan for, however, are every day "off-nominal scenarios" such as unexpected reroutes, missed approaches, vertiport obstructions, unstable landings, and uncooperative vehicles in the airspace. In open airspace, such scenarios are difficult for human pilots to navigate; in congested airspace, a mistake can set off a chain reaction of failures or collisions. Researchers from the Mid-Atlantic Aviation Partnership, a collaboration of leading universities and the FAA, slammed drones into buildings,

cars, and dummies at a test site on the outskirts of Christiansburg, VA to assess the risks. They're measuring the kinetic energy on impact to see how fast a drone of a given weight can penetrate a wall, shatter a windshield, lacerate skin, or inflict a severe injury. The information will be used to develop standards for aircraft variables like weight, construction materials, battery capacity, maximum speed, altitude, range, and payload. These standards will, in turn, influence the overall system's infrastructure requirements. #AUT #AER #USA Bloomberg

SEMICONDUCTORS & CHIPS

→ **On Monday, July 27, US chipmaker Intel announced that it will produce chips for Taiwan's MediaTek, one of the world's largest chip design firms.** The manufacturing agreement is one of the most significant Intel has announced since launching its foundry business, which builds chips designed by other companies, earlier this year. In that market, TSMC is the dominant player, and Intel has primarily built chips that it designed. There were doubts in the industry about Intel's ability to succeed in the foundry business, but the agreement with MediaTek demonstrates that it is on the right track and that its investments, including in recruiting the right executives, are paying off, according to a chip economist from TechInsights. The first products will be manufactured in the next 18 to 24 months using a more mature technology process called Intel 16, with the chips used in smart devices. #CHP #USA #TWN Reuters

→ **A team of researchers from MIT, the University of Houston, and other institutions conducted experiments that demonstrated that a material known as cubic boron arsenide overcomes the limitations of silicon properties as a material in semiconductors.** The material has high electron and hole mobility and excellent thermal conductivity. It may be the best semiconductor material ever discovered, according to the researchers. So far, cubic boron arsenide has only been synthesized and tested in small, non-uniform lab-scale batches. To test small regions of the material, the researchers had to use special methods developed by former MIT postdoc Bai Song. More research will be required to determine whether cubic boron arsenide can be produced in a practical, cost-effective form, let alone replace the ubiquitous silicon. However, the material could find applications where its unique properties would make a significant difference in the near future, according to the researchers. The electronic properties of cubic boron arsenide were first predicted based on quantum mechanical density function calculations made by the researchers, and those predictions have now been validated through experiments using optical detection methods on those samples. Not only does the material have the best thermal conductivity of any semiconductor, but it also has the third-best thermal conductivity of any material, after diamond and isotopically enriched cubic boron nitride, according to the researchers. #CHP #USA MIT News Science

→ **SK Hynix, the South Korean memory chip giant, reported record-high revenue in Q2 despite the impact of Covid-19 lockdowns in China, the Ukraine war, and global inflation.** Revenue for the period reached $10.5B, up 34% YoY and 14% ahead of the previous quarter, according to financial results released by the company on Wednesday, July 27. The net profit increased by 45% YoY, reaching $2.19B. SK Hynix said on Wednesday's earnings call that it

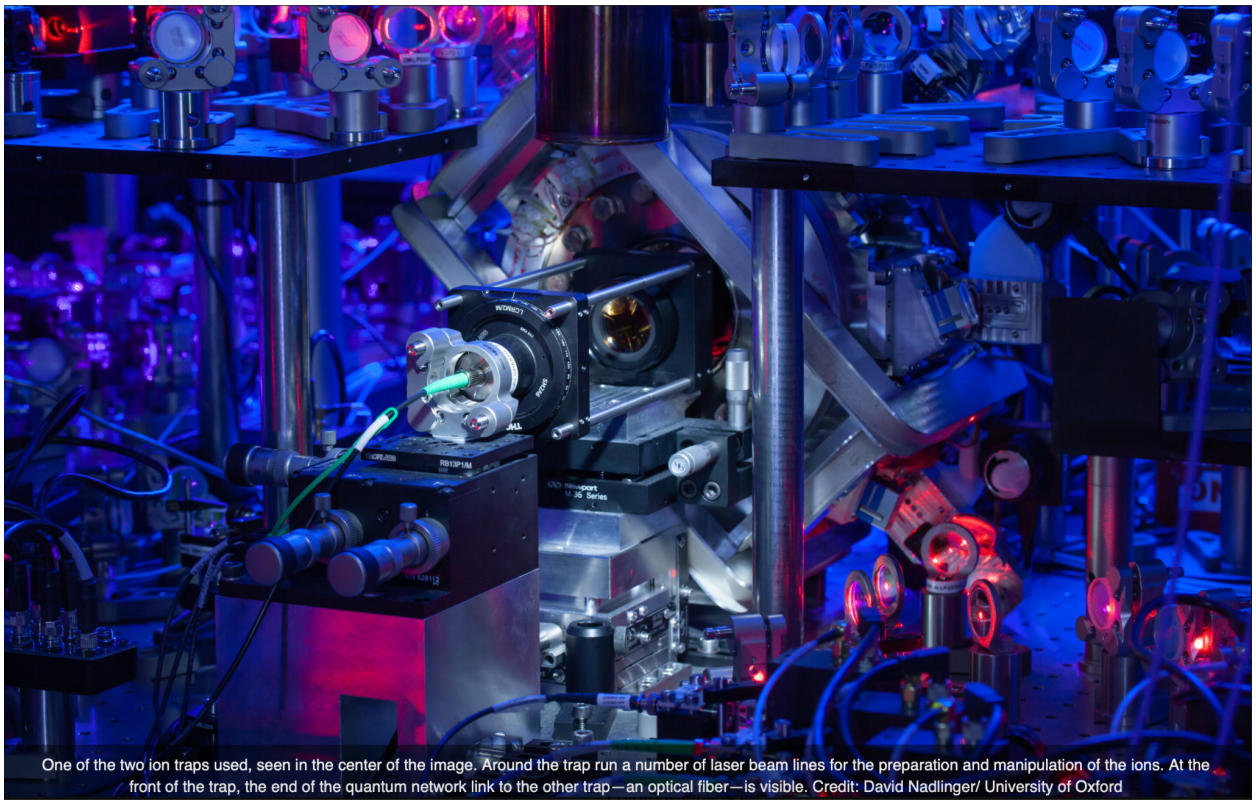
may revise its capital expenditure plan for 2023 due to signs of weakening demand in the memory chip markets for personal computers, smartphones, and servers. According to the company, DRAM prices fell during Q2, but NAND flash prices rose along with an increase in overall sales volume. DRAM products account for roughly 70% of total revenue, while NAND flash products account for 23%. DRAM pricing in the current quarter could drop 10% from the previous estimate of 8% as demand peaks in the second half of the year, according to a recent note from semiconductor research firm TrendForce. Separately, US President Joe Biden praised SK Group's plans to invest $22B in semiconductor, green energy, and biotech projects in the US on Tuesday. This comes on top of a recent $7B investment in the US, bringing its total investment in the country to nearly $30B. Chey Tae-won, chairman of SK Group, stated that half of the funds would be spent on the semiconductor ecosystem, including funding R&D programs with leading American universities and bringing advanced chip packaging technology back to the US. Samsung Electronics, South Korea's top memory chipmaker, has also proposed an investment of approximately $200B to build 11 new chip plants in Texas over the next 20 years, according to South Korean media reports on Tuesday. #CHP #GRN #BIO #SCRM #KOR #USA SCMP

QUANTUM TECHNOLOGY

→ **Quantum-South, a Uruguay-based startup, has joined the IBM Quantum Network to apply quantum computing to the advancement of the air and maritime cargo industries, including the potential for increased logistics efficiency.** Quantum-South will continue to work on quantum computing applications in the industry to support air and maritime cargo use cases, which all require processing and searching large amounts of data. The startup will use IBM Quantum technology to develop, test, and run proof of concepts for potentially more efficient cargo logistics solutions, such as efficient container cargo management and fuel optimization scenarios for airplanes. Quantum-South has also developed capabilities in financial services and will work on asset portfolio optimization use cases. Quantum-South is the first Latin American company to join the IBM Quantum Network. #QNT #AER #DIG #SCRM #URY #USA The Quantum Insider

→ **For the first time, an international team of scientists has demonstrated experimentally a method of quantum key distribution based on high-quality quantum entanglement, which provides more effective cybersecurity measures than previous schemes.** The experiment involved two single ions — one for the sender and one for the receiver — confined in separate traps that were connected with an optical-fiber link. In this basic quantum network, entanglement between the ions was generated with record-high fidelity over millions of runs. Without such a sustained source of high-quality entanglement, the protocol could not have been run in a practically meaningful manner. Equally important was to certify that the entanglement is suitably exploited, which is done by showing that conditions known as Bell inequalities are violated. Moreover, for the analysis of the data and an efficient extraction of the cryptographic key, significant advances in the theory were needed. In the experiment, the “legitimate parties” — the ions — were located in one and the same laboratory. But there is a clear route to

extending the distance between them to kilometers and beyond. With this approach and recent advances in related experiments in Germany and China, there is a real potential of turning the theoretical concept of key-distribution process security into practical technology.



One of the two ion traps used, seen in the center of the image. Around the trap run a number of laser beam lines for the preparation and manipulation of the ions. At the front of the trap, the end of the quantum network link to the other trap—an optical fiber—is visible. Credit: David Nadlinger/ University of Oxford

#QNT #Cybersecurity #EUR #GBR #CHE #FRA Phys.org

GEOPOLITICS

→ **For the first time, Britain's business secretary has used new national security powers to prevent the University of Manchester from sharing motion camera technology with a Chinese firm.** Kwasi Kwarteng, the secretary for business, energy, and industrial strategy, barred the university from sharing Scamp-5 and Scamp-7 camera technology with Beijing Infinite Vision Technology, a manufacturer of 3D rendering technology used in architectural design, multimedia displays, and animation. “There is a potential that the technology could be used to build defense or technological capabilities, which may present national security risk to the United Kingdom,” Kwarteng said in the final order. “Those risks would arise on the transfer of the intellectual property to the acquirer.” In addition to 3D renderings, the technology can be used in nanny cameras, drones, and other surveillance equipment. The technology enables cameras to process large numbers of images more efficiently. #Geopolitics #DIG #AUT #GBR #CHN SCMP

→ **The Senate approved a $280B bill to boost scientific research and the US semiconductor industry on Wednesday, July 27, sending it to the House, where Speaker**

Nancy Pelosi has promised quick action. The CHIPS and Science Act of 2022 establishes a $39B fund to provide direct financial assistance for the construction and expansion of semiconductor manufacturing facilities, among other things, according to a summary provided by the Senate Commerce Committee. The bill was approved 64-33, with 17 Republicans joining Democrats in voting in favor. Intel, TSMC, GlobalFoundries, Micron, Applied Materials, and others could benefit from the funding. A separate $11B program seeks to collaborate with industry to advance semiconductor manufacturing research and workforce training, while a $2B fund seeks to accelerate the translation of laboratory advances into military and other applications. Tax breaks for investments in semiconductor manufacturing were increased by $24B by lawmakers. #Geopolitics #CHP #SCRM #USA #TWN WSJ

→ **Members of the Dutch Parliament have requested that the Dutch government investigate the potential national security risk of using Chinese-made solar panels in the country's power grid.** The main source of concern, according to officials, is a news article published this Sunday by the Dutch magazine *Follow the Money*. According to *FTM*, a Dutch security researcher discovered a super-admin password that allowed him to enter the IT network of the panel's manufacturer, Chinese company SolarMan, and take full control of all the company's products worldwide. FTM also reported that the company ignored the researcher's findings for months until the Dutch embassy in China intervened and convinced Solarman to correct the problem. However, the discovery of this super-admin panel in tandem with the ongoing Ruso-Ukrainian war has prompted FTM reporters and Dutch officials to wonder if the Netherlands isn't in danger of exposing its power grid to a situation in which the Chinese government might force SolarMan to disable solar panels inside the country in the aftermath of a possible political confrontation, similar to how Russia has now cut-off gas supply across Europe in the aftermath of EU sanctions. The same question may arise in Australia, where these panels are also widely used. #Geopolitics #GRN #Cybersecurity #SCRM #NLD #CHN #RUS #UKR #EUR #AUS Risky Biz

→ **A group of former US national security officials has formed a professional organization to promote open-source intelligence, the analysis of publicly available data that has assisted Western powers in understanding and tracking Russia's war on Ukraine.** The Open Source Intelligence Foundation, which was formed in consultation with the nation's spy agencies but is not formally affiliated with them, aims to raise the profile of a field of intelligence gathering that has long been viewed as less important to national security priorities than traditional forms of espionage. Only recently have intelligence officials begun to consider OSINT to be on par with, if not more valuable than, intelligence derived from stolen secrets. Streams of open-source intelligence, including location-tracking apps, satellite imagery, drone cameras, and social media posts, have shed light on Russian military movements, troop morale, and potential war crimes in recent months. Location-tracking apps installed on Russian mobile phones have revealed previously unimaginable details: In April, a Ukrainian man whose Apple AirPod headphones were stolen by a Russian soldier claimed he was able to track Russian troop movements using Apple's "Find My" feature. In one case, a smartphone app based in San Francisco that pays users to perform basic observational tasks such as photography ceased operations in Ukraine at the start of the war after the Kyiv government claimed Russian agents

were using it to target airstrikes. The app, whose clients include US defense and intelligence agencies, countered that it was assisting the Ukrainian effort by providing information to its Western backers. #Geopolitics #SAT #AUT #DIG #Cybersecurity #USA #RUS #UKR WSJ

→ **Legislation aimed at launching a national effort to address post-quantum cybersecurity (PQC) is making its way through the United States Congress, while other members of the administration are raising concerns about quantum's ability to breach current cybersecurity measures.** Following the passage of similar legislation in the House, US Senators Maggie Hassan (D-NH) and Rob Portman (R-OH) introduced a bipartisan bill requiring the federal government to strengthen its defenses against potential quantum cyberattacks. The legislation will specifically:

- Require the Office of Management and Budget (OMB) to prioritize the acquisition and migration of post-quantum cryptography information technology for federal agencies.
- Instruct the Office of Management and Budget (OMB) to develop guidance for federal agencies to assess critical systems one year after the National Institute of Standards and Technology (NIST) publishes planned post-quantum cryptography standards.
- Direct OMB to send Congress an annual report that includes a strategy for dealing with post-quantum cryptography risks, any funding that may be required, and an analysis of whole-of-government coordination and migration to post-quantum cryptography standards and information technology.

#Geopolitics #Cybersecurity #QNT The Quantum Insider

CYBERSECURITY

→ **Apple's network traffic reportedly took an unexpected detour through Russian networking equipment for about twelve hours between July 26 and 27.** In a write-up for MANRS (Mutually Agreed Norms for Routing Security), a public interest group that looks after internet routing, reported that Russia's Rostelecom started announcing routes for part of Apple's network on Tuesday, in an act of BGP (Border Gateway Protocol) hijacking. While re-routing can happen accidentally, some bad route announcements are malicious. Apple's routing change was detected by BGPstream (Cisco Works), and by GRIP Internet Intel (GA Tech). Apple has not responded to requests for comment and has not made any public statements about the re-routing allegations as of 28 July. And it is unclear which services could have been impacted by this incident. #USA #RUS #Cybersecurity #SCRM The Register

→ **A bill introduced Wednesday, July 20, by the House Intelligence Committee would block US buyers from purchasing foreign spyware.** The bill follows media reports that Israeli spyware maker NSO was to be acquired by US defense contractor L3Harris. Calling the proliferation of foreign-made commercial spyware "an acute and emergent threat to the national security of the United States," the bill would empower the US Director of National Intelligence to bar any contract between such spyware manufacturers and the intelligence community. It would also authorize the White House to sanction them if they target US spies. In a statement, the White House said it shared lawmakers' concerns that tools made by NSO posed "a serious

counterintelligence and security risk to US personnel and systems" and was working on its own ban on the US government's use of foreign spyware that had been misused abroad. Last year, Reuters revealed that State Department phones had been hacked using NSO spyware. Only a few weeks earlier, NSO was added to the US Entity List by the US Department of Commerce. #Cybersecurity #Geopolitics #USA #ISR Reuters

→ **The European Union discovered evidence that smartphones used by some of its employees were compromised by spy software developed by an Israeli company, according to a letter obtained by Reuters.** In a letter sent to European lawmaker Sophie in 't Veld on July 25, EU Justice Commissioner Didier Reynders stated that in 2021, Apple informed him that his iPhone had possibly been hacked using Pegasus, a tool developed and sold to government clients by Israeli surveillance firm NSO Group. The Apple warning prompted an examination of Reynders' personal and professional devices, as well as other phones used by European Commission employees, according to the letter. Though the investigation did not uncover conclusive evidence that Reynders' or EU staff phones were hacked, it did uncover "indicators of compromise," a term used by security researchers to describe evidence that a hack occurred. He stated in the letter that "it is impossible to attribute these indicators to a specific perpetrator with full certainty." It went on to say that the investigation was still ongoing. #Cybersecurity #EU #ISR #USA Reuters

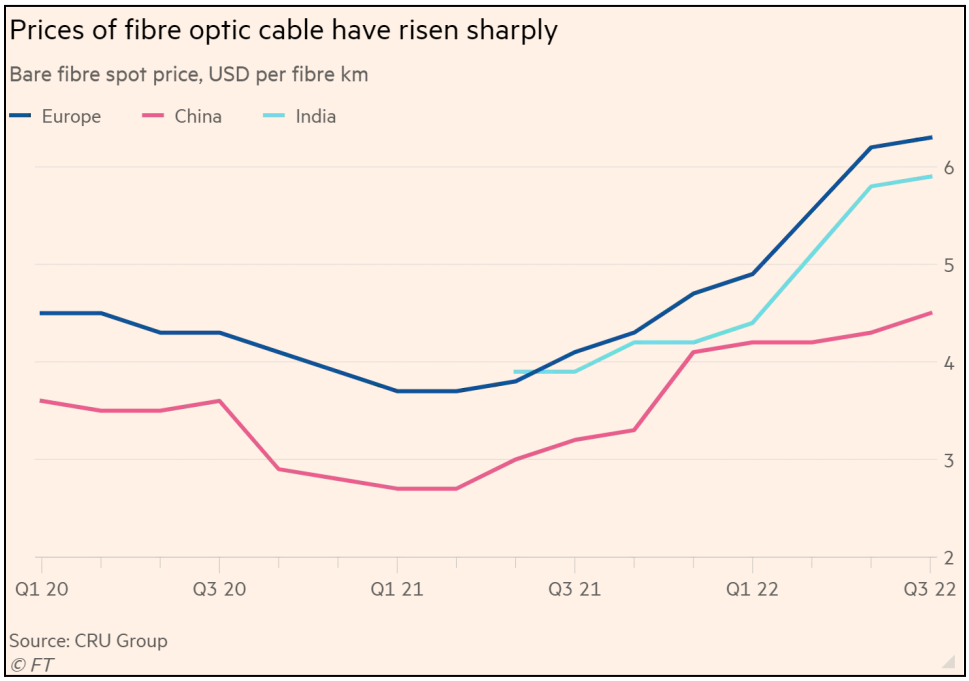
→ **Microsoft security researchers have determined that an Austrian firm was responsible for a series of digital intrusions at banks, law firms, and strategic consultancies in at least three countries.** The company, DSIRF, created spyware called "Subzero," which uses zero-day exploits to access confidential information such as passwords or log-in credentials, Microsoft said in a blog post on Wednesday, July 27. “Observed victims to date include law firms, banks, and strategic consultancies in countries such as Austria, the United Kingdom, and Panama,” according to the blog post, which did not name the victims. Because they work even when software is up to date, zero-day exploits are serious software flaws of great value to both hackers and spies. DSIRF promotes Subzero as a "next generation cyber warfare" tool capable of taking complete control of a target's PC, stealing passwords, and revealing its location, according to a copy of an internal presentation obtained by the German news website *Netzpolitik* last year. Microsoft's findings come as the US and Europe consider tighter regulations for spyware vendors, a fast-growing and under-regulated global industry, and after Israel's NSO's Pegasus spyware was discovered to have been used by governments to spy on journalists and dissidents. #Cybersecurity #Geopolitics #USA #AUT #GBR #PAN #DEU #EUR Reuters

→ **Hackers are increasingly targeting financial firms such as banks and trading houses with cyberattacks designed to use their computer systems to mine cryptocurrencies, according to cybersecurity firm SonicWall.** Cryptojacking attacks on financial institutions more than tripled in the first half of the year, according to the report. The overall number of such events increased by 30% to 66.7M. The financial industry was targeted five times more than retail, the second-most targeted sector. As more financial institutions migrate their applications to cloud-based systems, hackers are spreading malware across corporate servers and other devices or hijacking Wi-Fi networks to gain access. Part of the overall rise in cryptojacking is

due to governments cracking down on ransomware attacks, which has caused some cybercriminals to switch methods, according to the report. However, the report did note some promising signs. The number of cryptojacking attacks fell by more than 50% in Q2, to 21.6M, compared to Q1. This trend follows a typical seasonal pattern in which attacks slow in Q2 and Q3 before picking up in Q4 of the year, the report stated. #Cybersecurity #FIN #USA Bloomberg

SUPPLY CHAINS

→ **A global shortage of fiber optic cable has raised prices and lengthened lead times, jeopardizing companies' ambitious plans to build cutting-edge telecommunications infrastructure**. Europe, India, and China are among the regions most affected by the crunch, with fiber prices rising by up to 70% from record lows in March 2021, from $3.70 to $6.30 per fiber km, according to CRU Group, a business intelligence firm. Despite the fact that the Covid-19 pandemic prompted some of the largest tech and telecoms companies to reduce their capital expenditure, there has been an increase in demand for internet and data services, resulting in a shortage of the critical but often overlooked material. Total cable consumption increased by 8.1% in the first half of the year compared to the same period in 2021, according to CRU estimates. China accounted for 46% of the total, with North America recording the fastest YoY growth of 15%. Rising prices for some of the critical components used in fiber optic technology, which transports light along flexible fibers with a glass core, are fueling the shortage. There has been a shortage of helium, a critical component in the manufacture of fiber optic glass, caused in part by plant outages in Russia and the US, causing helium prices to rise by 135% over the last two years. Meanwhile, silicon tetrachloride prices, another key component in fiber production, have risen by up to 50%. Fiber prices have now reached their highest level since July 2019, with North America faring better than Europe, China, and India, according to CRU.



#SCRM #5G #DIG #EUR #IND #CHN #USA Financial Times

BACK TO TOP