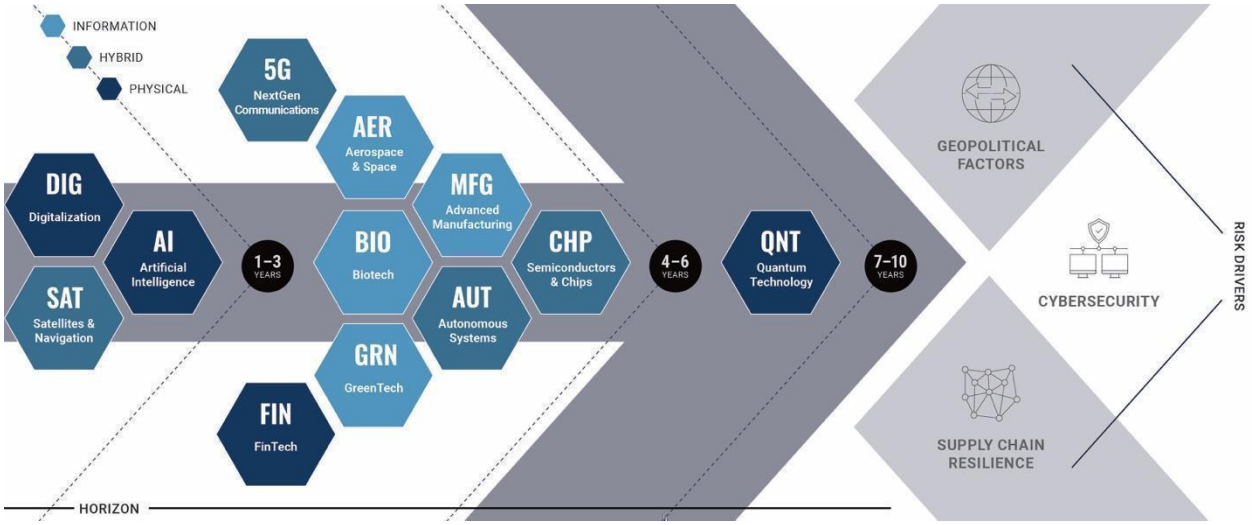
MATRIX MONITOR

Friday March 3, 2023

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



This week's Next5 Matrix Monitor features chipmakers looking to benefit from the CHIPS Act cannot expand in China for a decade, the top apps in the Google Play Store have false or misleading data privacy labels, China's plan to compete with Starlink, 49% of U.S. companies are currently using ChatGPT, European regulations for the crypto market, a proposed biological supercomputer powered by human brain cells, 2022 investment in low-carbon energy technology was equal to the amount invested in fossil fuels, the U.S. Air Force's AI-powered facial recognition technology for autonomous drones, and Chinese companies continue to supply chips and chip components to Russia via intermediaries.

NEXT5 EDITOR'S HIGHLIGHTS

→ **The Biden Administration released its national cybersecurity strategy this week. The administration will pursue a policy of more aggressive regulation to secure critical infrastructure in a shift from the past twenty years of efforts to get companies in critical sectors to voluntarily strengthen their cybersecurity.** The strategy, which was orchestrated by the White House's Office of the National Cyber Director, is the first new cyber strategy in five years. It outlines a vision for the federal government to use existing authorities to protect critical sectors from cyber threats. Where there are gaps in relevant authorities, the administration will work with Congress to build new regulatory tools over key sectors. The strategy also says the government may need to provide resources to critical infrastructure groups that may not have the funds needed to implement the new requirements. The industry has long pushed back against greater cyber regulations, and it's something that Congress has hesitated to move on. The strategy also makes clear that the U.S. plans to be aggressive against foreign adversaries who try to hack into American networks. On the international front, the strategy calls for the Biden administration to develop mechanisms to help identify when and how to respond to cyberattacks on other countries. #Cybersecurity #USA Politico

→ **The new House China Select Committee previewed its agenda for this Congress in a prime-time evening hearing on Tuesday February 28.** Committee chair Mike Gallagher (R-Wis) laid out a GOP vision of an external facing "existential struggle" against China's "ideological, technological, economic, and military threat." Democratic committee members countered with a more domestic-focused approach hinged to bolstering U.S. democracy and backed by government funding for an industrial policy that ranking member Raja Krishnamoorthi (D-Ill) said could thwart China's challenge through "investments in technologies of the future, workforce improvement, and by fixing weaknesses in our economy." Congress held a total of seven hearings about China concerns Tuesday, ranging from Taiwan, trade, and Tiktok, to supply chain security and human rights. Between tensions over the recent spy balloon over U.S. airspace, increased scrutiny over China's role in American fentanyl deaths, Biden administration revelations that Beijing is considering supplying Moscow with lethal weaponry in its war against Ukraine, and new reports that Covid leaked from a lab in China - just to name the most recent issues - China remains one of the few issues this divided Congress is poised to address together. However, the hearing did appear to reveal division between the two parties, and highlighted they face serious challenges from day one. #Geopolitics #USA #CHN Politico

→ **A new report from the Department of Energy this week assesses with low confidence that Covid-19 likely originated from a lab in China, triggering a new wave of concerns surrounding pandemic disinformation**. FBI Director Chris Wray also openly spoke about the origins of the pandemic for the first time, saying it most likely came from a lab. He also said we are talking about "a potential leak from a Chinese government-controlled lab that killed millions of Americans and that is precisely what it was designed for." He also highlighted the Chinese continued efforts to thwart and obfuscate the origins. However, as a journalist at AP News warns: When it comes to COVID-19 misinformation, any new report on the virus' origin quickly

triggers a relapse and return of misleading claims about the virus, vaccines, and masks. Within hours of the DOE's report leaking, online conspiracy theories involved Covid began to rise, with many commenters saying the classified report was proof they were right all along. The Covid origin story has been a huge dividing line in American and international politics over recent years, some initially treating the lab leak theory as disinformation, highlighting how challenging it can be to control the narrative in a digitalized world. #Geopolitics #USA #CHN #BIO AP News ABC

→ **Chipmakers must agree not to expand capacity in China for a decade if they are to receive money from the $39B allocated by the CHIPS Act, which is designed to build a leading-edge U.S. semiconductor industry**. In announcing the move, commerce secretary Gina Raimonda stressed the department would be implementing safeguards to ensure the program was not abused. Companies engaging in the program must also not "knowingly engage in any joint research or technology licensing effort with a foreign entity of concern that involves sensitive technologies or products." #CHP #USA #CHN #SCRM #Geopolitics Financial Times

DIGITALIZATION

→ **According to a study, the top apps in the Google Play Store have false or misleading data privacy labels.** Mozilla conducted the study by comparing the privacy policies and labels of the 20 most popular paid apps and the 20 most popular free apps on the Google Play Store. The study discovered:

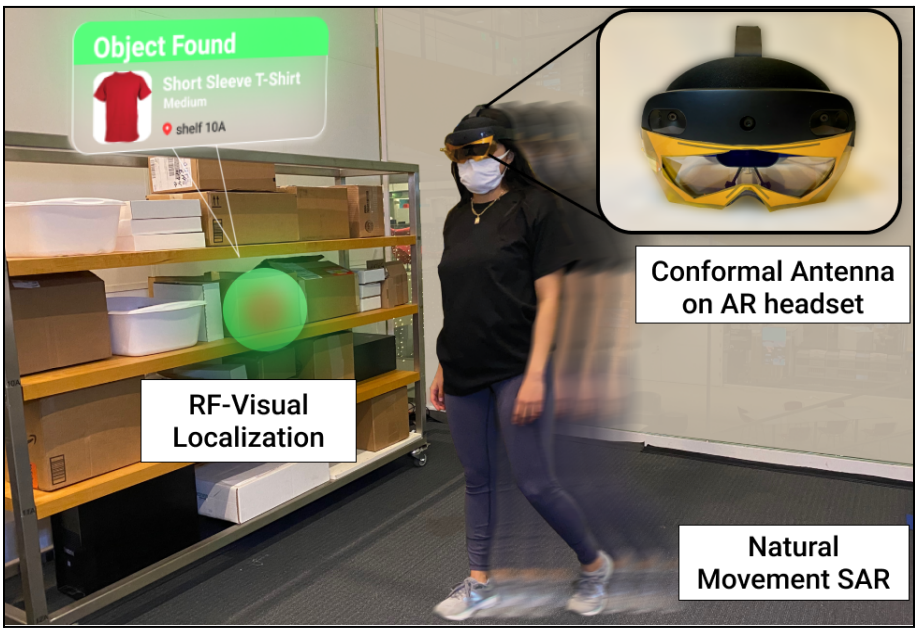
- ➔ ~80% of the apps reviewed had discrepancies between the apps' privacy policies and the information they reported on Google's Data Safety Form.
- ➔ 40%, had major discrepancies between their privacy policies and their Data Safety Forms, earning a "Poor" rating.
- ➔ 37.5%, received a "Needs Improvement" rating, which indicated some discrepancies between the privacy policies and the Data Safety Form.
- ➔ 15%, received an "OK" rating, indicating few to no discrepancies between their privacy policies and their Data Safety Form.
- ➔ The most concerning issues involved misleading information discovered about how apps collect, share, and use data, which resulted in consumers not having accurate information to make important privacy decisions.
- ➔ Google's Data Safety Form includes significant loopholes, like failing to require the apps to report data sharing with "service providers."
- ➔ Google uses narrow definitions for data "collection" and "sharing," making it easier for app developers to mislead users.
- ➔ Google also exempts "anonymized" data from its disclosure requirements, which is problematic due to questions about whether true anonymization is even possible.

The researchers made the following recommendations to address these shortcomings:

- ➔ Google, in collaboration with all app stores, should create and implement a universal standard app disclosure form that accurately, completely, and clearly describes how app developers use consumer data.
- ➔ Most companies have global privacy policies that apply to all their websites and products, but mobile apps should have their own specific policies, which would increase the accuracy of their disclosures.
- ➔ Google, along with other hosting platforms, should be required to state clearly that the information on their data safety disclosures and labels is self-reported by app developers, and that they don't take responsibility for ensuring the veracity of the information.
- ➔ Google should regularly review the privacy policies of the apps in its Play Store and provide quarterly public reports about actions taken against those with discrepancies between their policies and the Google Data Safety Form, as well as against those who have failed to complete the form.
- ➔ Google should expand its definitions of data "collection" and "sharing" to enhance clarity about how apps are using consumers' data and to help protect users from misleading information. Google should also narrow its definition of "anonymization," or eliminate it for the same reasons.

#DIG #Cybersecurity Mozilla Foundation

→ **MIT researchers have built a new x-ray augmented reality (X-AR) headset that enables users to see things that are hidden.** The headset uses holograms to guide users toward desired items and verify when they have picked them up. The headset also uses wireless signals and computer vision to enable users to perceive things that are invisible to the human eye. It combines new antenna designs, wireless signal processing algorithms, and AI-based fusion of different sensors. The AR-conformal wide-band antenna that matches the shape of the AR headset visor and provides Radio Frequency (RF) sensing capabilities to the headset. It uses an AR-Based synthetic aperture radar (SAR) localization algorithm that fuses RF sensing from the antenna and visual sensing from the headset's cameras to localize RF-tagged objects, even when they are hidden from the view, as the user naturally walks in the environment. Another component, the RF-Visual Verification Primitive, fuses RF and vision to deliver actionable tasks to end users such as picking verification. When the researchers tested X-AR in a warehouse-like setting, the headset could locate hidden items to within 9.8 cm on average and verify picking up items with 95% accuracy.



#DIG #5G #AI #USA MIT Media Lab

SATELLITES & NAVIGATION

→ **China is allegedly planning to launch almost 13k satellites under the project codenamed "GW" to compete with Elon Musk's Starlink and provide internet services worldwide.** This attempt aims to prevent Starlink from monopolizing the low-Earth orbit space and stop it from barring other businesses or nations from using it. The China Satellite Network Group Co also hopes to use its own constellations to track and potentially deactivate Starlink satellites. The launch date for these satellites is yet to be set, and it is uncertain how Elon Musk and the U.S. will respond to this development. Chinese researchers are concerned about the maneuverability of Starlink satellites because they believe Musk's satellites could be used to target and destroy other spacecraft. Chinese researchers want to match that potential by introducing their own fleet of satellites to respond to Starlink's potential military applications, which continue to grow amid the ongoing conflict in Ukraine. #SAT #USA #CHN #RUS #UKR SCMP

→ **British smartphone firm Bullitt launched a new phone capable of sending text messages via geostationary satellites, joining a crowded race to commercialize satellite-enabled devices.** The new phones offer 5G connectivity and the company says the battery can last up to two full days. With Bullitt's phones, a message is beamed to geostationary satellites about 22k miles above the equator, then sent back down to earth-based network infrastructure before reaching a user's device. Texts take around 10 seconds to go through, as opposed to the near-instant speed of cell phones. Satellite connection is only turned on when a user falls outside the reach of Wi-Fi or mobile network signals. Device makers like Apple and chip firms like Qualcomm are betting on the untapped opportunity of putting satellite phones in

the hands of people in remote areas that fall outside the reach of terrestrial telecoms infrastructure. #SAT #USA CNBC

→ **The US Space Force is considering setting up a Commercial Augmentation Space Reserve (CASR) of commercial satellites to aid the military during emergencies.** The Pentagon's expensive, large satellites are vulnerable to anti-satellite weapons, so assembling a fleet of commercial satellites would help bolster defense in space. China and Russia recognize how much the US military depends on satellites. Both have developed ASAT capabilities that can disable or destroy US space assets. These capabilities include electronic warfare, cyber operations, jamming, directed energy, and destructive kinetic ASAT weapons. China also possesses commercial and scientific satellites with maneuvering capabilities that could serve as ASATs by violently colliding with US space assets. To mitigate the threat from adversary ASATs, the US Space Development Agency is bolstering space resiliency by purchasing hundreds of small (and cheap) low-Earth orbit satellites. Rather than relying on large, expensive geosynchronous-orbit satellites, this new approach will require an adversary seeking to disrupt US space capabilities to knock out a few hundred small satellites instead of just a few. Commercial satellites have proven their utility for security purposes during the war in Ukraine. SpaceX's Starlink is providing the Ukrainian military with high-speed internet, allowing forces to stay in contact with each other and with Ukrainian high command. It also allows units to deploy weapons systems such as precision-guided artillery, drones, and loitering munitions. #SAT #USA #CHN #RUS #UKR Atlantic Council

ARTIFICIAL INTELLIGENCE

→ **The US State Department released the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, which outlines principles for the development, testing, and verification of military systems using AI.** The US military considers the use of AI as vital for maintaining an edge in conflict with adversaries like China and Russia. While the declaration does not legally bind the US military, the hope is that it will guide the development of military AI and create a global standard for responsible AI use. The declaration states that military AI needs to be developed according to international laws, that nations should be transparent about the principles underlying their technology, and that high standards should be implemented for verifying the performance of AI systems. It also states that humans alone should make decisions around the use of nuclear weapons. When it comes to autonomous weapons systems, US military leaders have often reassured that a human will remain "in the loop" for decisions about the use of deadly force. But the official policy does not require this to be the case. Attempts to ban autonomous weapons have failed, and a few nations already have weapons that operate without direct human control in limited circumstances, such as missile defenses. Greater use of AI might mean more scenarios where systems act autonomously. #AI #AUT #USA #CHN #RUS Wired

→ **Researchers have developed a new computational method using a long short-term memory (LSTM) model – a type of recurrent neural network (RNN) – to more effectively and reliably detect Distributed Denial of Service (DDoS) attacks.** This method is based on

two separate models that can be integrated into a single intrusion detection system. The first model is designed to determine whether the incoming network traffic is adversarial and block it if it is deemed fraudulent; the second model identifies if the traffic constitutes a DDoS attack. The DDoS detection tool proposed by the team is robust and adaptable, with the potential to meet the unique needs of specific businesses or users. Initial tests have shown an accuracy exceeding 91%, even when faced with sophisticated attacks specifically engineered to fool machine learning algorithms. The method could soon be integrated into existing and newly developed security systems. Furthermore, it might inspire the development of similar machine-learning techniques for detecting DDoS attacks. #AI #Cybersecurity #USA Tech Xplore

→ **A survey conducted by ResumeBuilder.com in February 2023 reveals that 49% of U.S. companies are currently using ChatGPT, with 30% planning to use it in the future.** Of the current users, 48% say that ChatGPT has replaced workers, and 25% of the companies have already saved over $75k. The majority of companies use ChatGPT for writing code, copywriting, customer support, and hiring-related tasks such as drafting job descriptions and responding to applicants. The quality of work produced by ChatGPT is generally well-received by business leaders, with 55% saying it is 'excellent.' However, the survey also indicates that the use of ChatGPT may lead to more layoffs, with 33% of business leaders saying it will 'definitely' lead to layoffs by the end of 2023 and 63% saying it will 'definitely' or 'probably' lead to layoffs within the next five years. Furthermore, 90% of business leaders believe that ChatGPT experience is a beneficial skill for job seekers, and 92% say that having AI/chatbot experience is a plus when assessing candidates to hire. #AI #USA Resume Builder Futurism

NEXT GENERATION COMMUNICATIONS

→ **The Biden administration is considering revoking export licenses issued to U.S. suppliers for sales to Chinese telecom company Huawei, in part of a broader tightening of technology trade over national security concerns.** The administration previously indicated that it was considering not granting any new export licenses to companies such as Qualcomm and Intel which provide chips needed for smartphones and other devices. The action would cover products that used advanced 5G technology as well as older 4G products. The new action would take that a step further by revoking existing licenses. A revocation of existing licenses could have significant impact on U.S. chipmakers, many of which have received permission to continue selling to Huawei older-generation phone chips and other processors that are widely available globally. Chip companies have argued that restrictions on such products are detrimental to the U.S. industry because they deprive them of revenue to fund domestic research and development. #5G #USA #CHN #SCRM #Geopolitics WSJ

→ **NTT and KDDI, Japan's top two telecommunications firms, will collaborate to develop technology for ultra-energy-efficient 6G networks and optical equipment.** The firms plan to build infrastructure around NTT's next-generation Innovative Optical and Wireless Network (IOWN). IOWN employs a photonics-electronics convergence technology that uses light to process signals in communication lines, devices, servers, and semiconductors. Even today, light

is used to transmit signals in communication lines via optical cables. However, signals are transmitted using electricity rather than light inside telecom equipment at base stations and data center servers, resulting in energy loss and increased power consumption. Each optical fiber's transmission capacity can be increased by 125x because of the technology's low energy loss and high data transmission efficiency. NTT will invest $490M in IOWN-related research and facilities. Both firms expect this technology to be used in 6G network infrastructures. Moreover, by addressing current technical challenges, the two firms intend to take the lead in creating 6G standards, as part of the country's national technology strategy. #6G #DIG #CHP #JPN Nikkei Asia

FINANCIAL TECHNOLOGY

→ **The Securities and Exchange Commission (SEC) is investigating Robinhood, with a subpoena issued in December covering topics including cryptocurrency listings and custody.** The probe comes as U.S. financial watchdogs take a more aggressive approach to crypto in the wake of FTX's collapse. In the months following FTX's November bankruptcy, top financial watchdogs have fanned out across the industry, extracting major penalties and issuing broad warnings. #FIN #USA Bloomberg

→ **European officials have crafted industry-specific regulations for the crypto market.** The Markets in Crypto-Assets law (MiCA) sets strict rules for stablecoins and creates investor safeguards, capital requirements, and corporate governance rules for the broader crypto market. While some European officials believe the law isn't sufficient to prevent a future disaster at a global crypto company like FTX, the industry is welcoming it as a positive step in the right direction. Meanwhile, U.S. regulators are enforcing decades-old rules for trading and banking in the crypto world. #FIN #USA Politico

AEROSPACE & SPACE

→ **A new solution for congested launch sites is being proposed by a start-up, The Spaceport Company.** The company plans to demonstrate a mobile launch pad operating at sea, which will conduct four sounding rocket launches in May from a modified ship in the Gulf of Mexico. Those tests will be a precursor to developing a full-scale sea-based platform, based on a ship design called a liftboat. That ship can sail to a location and lower legs to anchor itself on the seafloor. The boat can then lift itself out of the water and serve a launch platform. The advantage of The Spaceport Company's concept is that it doesn't rely on any fixed infrastructure on land: all the resources needed for a launch are on the ship, and the rockets that launch from it would use autonomous flight termination systems that do not require radars or other tracking assets. The platform is scalable, and it doesn't need an FAA spaceport license known as Part 420. The company proposes to operate several kilometers offshore, based at any major industrial port, and host small launch vehicles up to the size of Firefly Aerospace's Alpha, which can place about one ton into orbit. Recently, China has demonstrated the use of converted ships as launch platforms for small vehicles.

The Spaceport Company is working to develop mobile sea-based launch pads it argues can help address congestion at existing launch sites. Credit: The Spaceport Company

#AER #USA #CHN Space News

→ **Vast Space, a company focused on building artificial gravity space stations in low Earth orbit, has acquired space tug startup Launcher.** The acquisition will give Vast access to Launcher's Orbiter space tug and payload platform and its liquid rocket engine, E-2. Vast will use the tug to test space station subsystems and components in orbit as soon as June of this year, and then again around October. Those two missions, which will be Orbiter's second and third flights, will also carry customer payloads. Vast will continue to operate Orbiter as a commercial product, and the first station the company will send to space will be zero G, with artificial gravity stations following. Vast will compete with other established players in the private space station industry, including Northrop Grumman, Nanoracks, Blue Origin, and Axiom Space. #AER #USA TechCrunch

→ **The U.S. Space Force is working to ensure the resiliency of its launch ranges in the face of adverse conditions such as natural disasters or enemy attacks.** Florida's Eastern Range, which is the world's busiest launch range, is projected to support 92 launches this year, up from 57 in 2022 and 31 in 2021. To improve resiliency as launch rates increase, the Space Force is pushing for all of its spaceports to offer the same level of security and reliability. The Space Force is also part of a National Spaceport Interagency Working Group that aims to develop a strategy to make U.S. spaceports more resilient and interoperable. The group also includes representatives from the Federal Aviation Administration, the departments of state and commerce and NASA. A draft of a spaceport strategy is expected to be completed this year. #AER #USA C4ISRNet

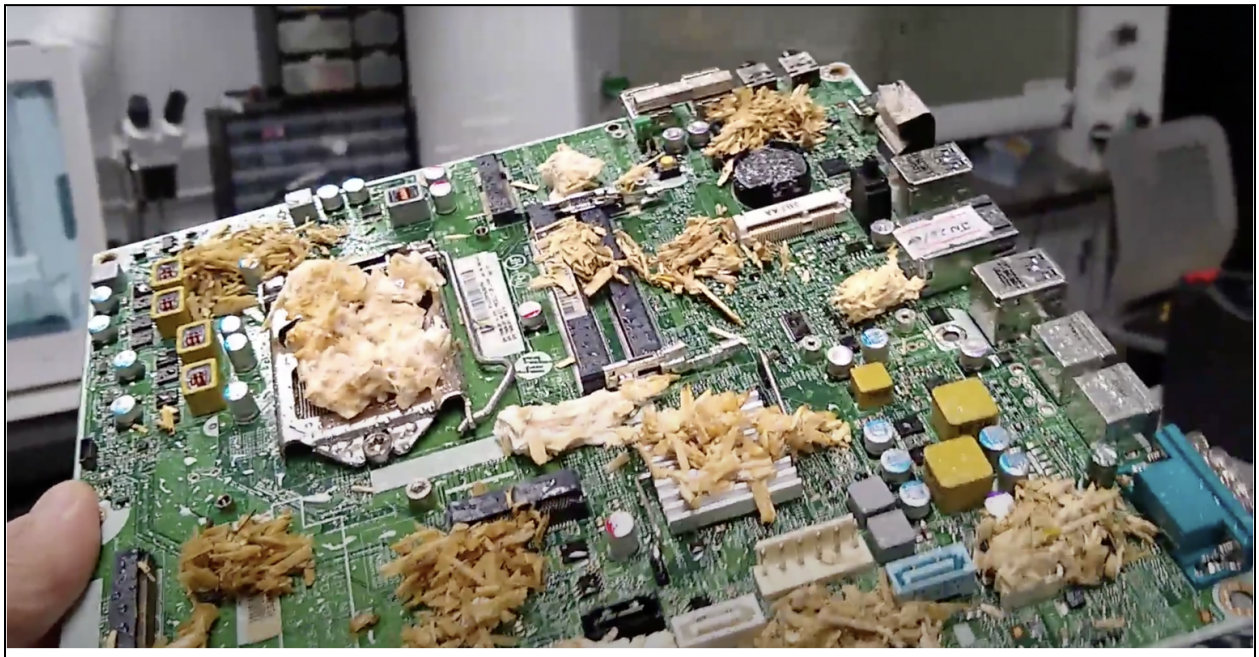
BIOTECHNOLOGY

→ **A new ODNI report says Havana Syndrome was unlikely tied to a foreign adversary. U.S. intelligence agencies also found "no credible evidence" that any foreign adversary possesses a weapon or intelligence collection device that is causing the injuries.** The report does not pinpoint a cause for the wide range of symptoms that have been reported by more than 1,500 U.S. government employees since the first cases emerged in Havana, Cuba in late 2016. It says they were probably caused by a combination of factors, including pre-existing medical conditions, conventional illnesses, and environmental factors. A U.S. intelligence official familiar with the new assessment said, "We cannot tie a foreign adversary to any incident." #BIO #Geopolitics #USA WSJ

→ **A team of 40 international scientists led by John Hopkins University have proposed creating a biological supercomputer powered by millions of human brain cells, which they claim will outperform silicon-based machines while using far less energy.** In the journal *Frontiers in Science*, the scientists detailed a road map to what they call "organoid intelligence". The hardware will include arrays of brain organoids — tiny 3D neural structures grown from human stem cells — connected to sensors and output devices and trained by machine learning, Big Data and other techniques. One necessary step is to enable individual organoids to grow larger by finding a better way to suffuse them with nutrients in laboratory dishes, according to Professor Thomas Hartung of Johns Hopkins. These tiny neural constructs need to be scaled up from about 50k-10M cells to help achieve what scientists would recognize as organoid intelligence. The researchers are also developing technologies to link organoids together and communicate with them, sending them information and decoding their "thoughts". Hartung's lab has tested an interface, "a flexible shell that is densely covered with tiny electrodes that can both pick up signals from the organoid and transmit signals to it". The first applications of organoid intelligence will be in neuroscience and medicine. #BIO #DIG #MFG #AI #QNT #USA Financial Times Interesting Engineering

→ **Scientists at the Unconventional Computing Laboratory are building mushroom computers, to see if mushrooms can carry out computing and sensing functions.** The scientists combined mycelium cultures with hemp or wood shavings and placed them in closed plastic boxes to allow the mycelium to colonize the substrate, resulting in a white appearance. They then inserted electrodes and recorded the mycelium's electrical activity. So, the stimulation causes electrical activity, which results in the response. Scientists already know that mushrooms communicate with their surroundings and the environment through a type of "Internet" communication. Scientists may be able to gain insights into the state of underground ecosystems and improve current information systems by deciphering the language fungi use to send signals through this biological network. Mushroom computers may have some advantages over traditional computers. They may be more fault tolerant (they can self-regenerate), reconfigurable (they naturally grow and evolve), and consume very little energy. Neurons in the human brain communicate signals using spiking activities and patterns, and this property has been mimicked to create artificial neural networks. Mycelium performs a similar function.

Therefore, researchers can use the presence or absence of a spike as their zero or one, and code the different timing and spacing of the detected spikes to correlate to the various gates seen in computer programming languages (OR, AND, etc). Furthermore, stimulating mycelium at two different points increases conductivity between them, allowing them to communicate faster and more reliably, allowing memory to be established. This is similar to how brain cells develop habits. Different geometries of mycelium can compute different logical functions, and they can map these circuits based on the electrical responses they receive.



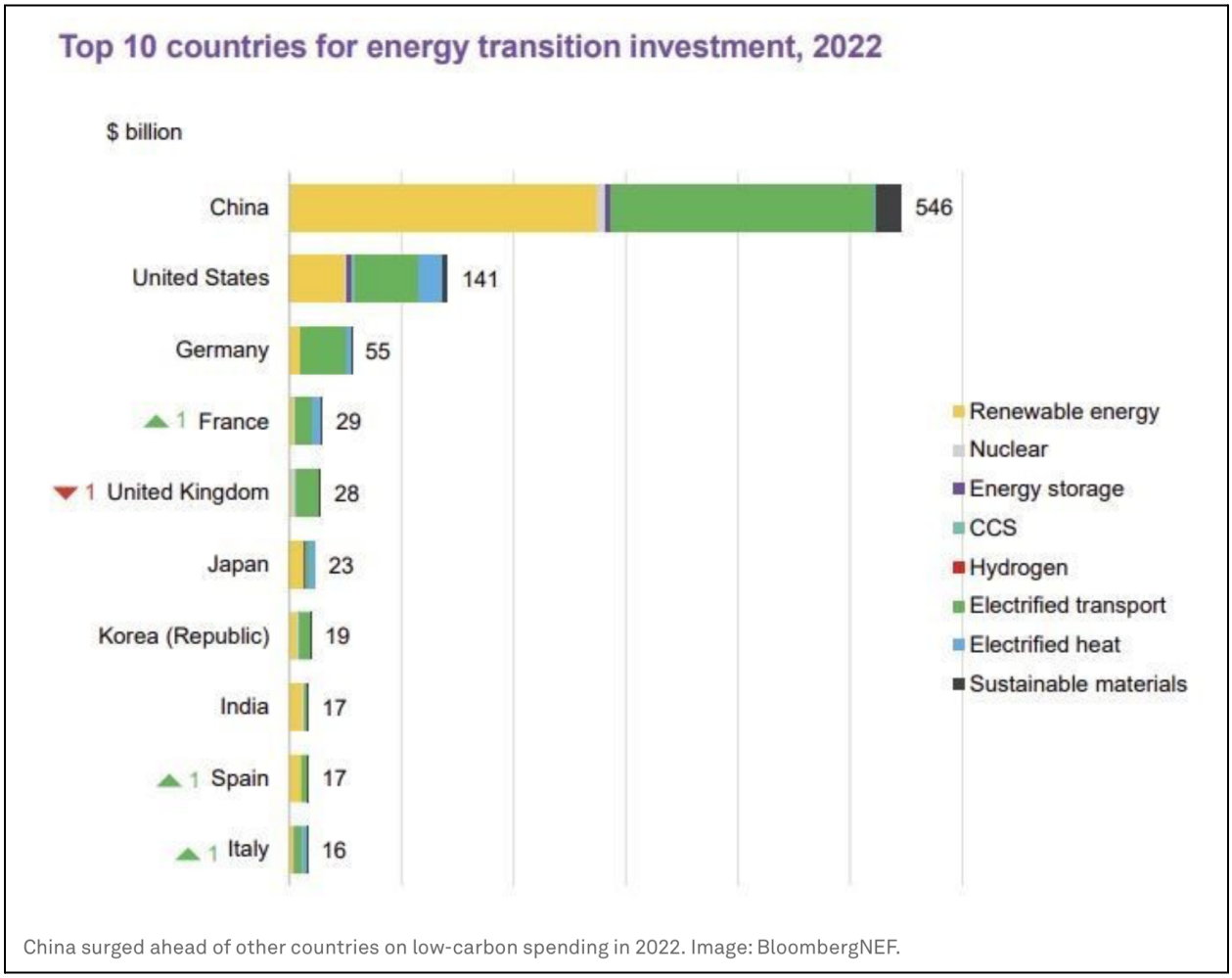
A mushroom motherboard. *Andrew Adamatzky*

#BIO #DIG #GBR Popular Science

GREEN TECHNOLOGY

→ **Investment in low-carbon energy technology reached a record $1.1T in 2022, up 31% from 2021 and equal to the amount invested in fossil fuels, according to a BloombergNEF report.** Russia's war on Ukraine caused a spike in energy prices and talk of potential winter blackouts. But it also triggered an overdue shift away from gas and other fossil fuels towards cleaner forms of energy. The low-carbon investment measured in the report includes renewables, carbon capture and storage, zero-emission vehicles, charging infrastructure, hydrogen production, energy storage, nuclear, recycling, and heat pumps. Spending broke records in every area except nuclear power, where investment was essentially unchanged compared with a year earlier. Renewable energy received the biggest share of investment, followed by electrified transport. China was the leader in low-carbon spending in 2022, followed by the U.S. and the EU. China accounted for almost half of the global investment, pumping $546B into energy transition technologies, the report shows. This was almost four times higher than the second-placed US with $141B. However, annual investment needs to more than triple

to an average of $4.55T between 2023 and 2030 to make net zero possible by 2050.



China surged ahead of other countries on low-carbon spending in 2022. Image: BloombergNEF.

#GRN #USA #CHN #RUS #UKR WEF

ADVANCED MANUFACTURING

→ **Robotic boots with superhuman reflexes have the potential to improve people's balance, according to a new study.** The research team sought to determine whether wearable robots – like powered lower-limb exoskeletons or prostheses – can improve balance beyond a normal baseline. They discovered that wearable robots could act faster than human reaction times, enabling test subjects to stay upright. The study also found that the faster-than-human exo-boot balance response eliminated calf muscle stretch signals, but control signals to those same muscles, in response to the nervous system, persisted. This finding highlights that the nervous system is more than a set of simple reflexes that react to local muscle stretch but instead acts to gather information from throughout the body to remain upright in both standing and walking. While wearable robots have long been studied to help mobility, the field has not

focused much on balance. The study is a first step towards helping older adults or people with stroke or spinal cord injuries with balance issues. #MFG #BIO WEF

→ **The Department of Defense has extended its contract with New Frontier Aerospace (NFA) for the development of its 3D-printed Mjölnir rocket engine.** The National Security Innovation Capital (NSIC) has granted NFA $1.5M after the successful delivery of Mjölnir's first component under an initial $750K contract awarded in August 2021. NFA's 3D-printed design runs full-flow staged combustion, which features fully vaporized propellants before they mix, and a high thrust-to-weight ratio. This makes it an efficient choice for a wide range of applications, including hypersonic aircraft, upper stages, maneuvering spacecraft, and planetary landers. NFA's Mjölnir rocket engine serves as the cornerstone of its plan to build a hypersonic aircraft for delivering passengers and cargo safely to any airport or vertiport on Earth in less than two hours. The firm's engines are designed to run on renewably sourced liquid natural gas, with net zero greenhouse gas emissions. #AER #GRN #USA Interesting Engineering

AUTONOMOUS SYSTEMS

→ **The US Air Force has developed AI-powered facial recognition technology (FRT) for autonomous drones, according to a contract between the Department of Defense and RealNetworks.** The drones will be used by special operations personnel for overseas missions, intelligence gathering, and other operations, with the software identifying faces through machine learning techniques. The drones may also potentially be used for domestic search operations, perimeter security, and rescue missions. The U.S. military is not the only entity employing facial recognition technology. According to the U.N., Libyan troops equipped drones with weapons and facial recognition software in 2021. Moreover, China has been using FTR and the Dubai police have been employing drones using facial recognition technology to find reckless drivers. There are concerns that this technology could be used to target individuals for assassination, with privacy advocates cautioning against employing facial recognition technology on drones. #AUT #AI #USA #CHN #ARE #LBY Interesting Engineering

→ **Amazon has filed the highest number of patent applications for next-generation vehicle driving technology among five major US tech giants over the past two decades,** according to a Nikkei survey**.** To examine tech giants' strength in intellectual property, Nikkei, jointly with Tokyo-based research firm Astamuse, tallied the number of patent publications by five U.S. big tech companies over the past 20 years. This includes Alphabet, Apple, Meta, Amazon, and Microsoft. Amazon has made a total of 1,649 patent applications, followed by Alphabet at 1,355. Apple ranks fourth. Amazon filed more than 200 applications annually for four years in a row since 2016. The increase has been led by Zoox, a developer of self-driving technologies acquired by Amazon in 2020. Zoox has accumulated technologies through repeated auto-driving experiments on public roads. #AUT #AI #USA Nikkei Asia

SEMICONDUCTORS & CHIPS

→ **Switzerland-based microchip startup Unisers has raised $14M in a funding round led by Intel Capital to build machines that would offer a new level of performance in the difficult task of detecting extraneous extremely small particles that ruin chips in production.** A tiny particle that lands on a silicon wafer, from which chips are created, can cause a chip to malfunction, however the issue may not be noticed for months, at the end of a production process involving thousands of steps. As a result, detecting particles as soon as they corrupt wafers saves money. Smaller articles become an issue as processors perform quicker and their circuitry becomes smaller. The method applied uses a unique coating on wafers to improve particle visibility when light is bounced off them. The technology is also aimed at detecting impurities in materials, another source of defects. Unisers is the only company which can detect these extremely small particles, smaller than 10 nm particles on wafer, according to CEO Ali Altun. #CHP #CHE #USA Reuters

QUANTUM TECHNOLOGY

→ **Softbank and SandboxAQ have successfully tested proof-of-concept classical and post-quantum cryptography algorithms using a hybrid approach.** They combined elliptic curve cryptography (ECC), a traditional encryption algorithm, with post-quantum cryptography (PQC) algorithms and validated the approach for use on existing networks with minimal performance impact. The companies used handset devices and servers to simulate network traffic on a hybrid mode of classical algorithms and PQC algorithms, and evaluated metrics such as encryption and decryption latency, CPU load, memory utilization, connection rate, and amount of traffic data, among others. As a result, the companies confirmed that hybrid mode performance is feasible. Furthermore, a comparison of standardization candidate PQC algorithms revealed that a combination of structured lattice-based PQC algorithms and classical algorithms outperformed any other alternative cryptographic schemes discussed in the PQC standardization process while incurring the least amount of overhead on SoftBank's network infrastructure. #QNT #DIG #Cybersecurity #JPN #USA Enter Quantum HPCwire

→ **An international team of scientists claims to have discovered a way to use the properties of quantum physics to speed up, slow down, and even reverse time in a given system.** The team from the Austrian Academy of Sciences and the University of Vienna detailed their findings in a series of six papers. The team stated that by developing a "rewind protocol," they were able to revert an electron to a previous state. They claim to have demonstrated the use of a quantum switch to return a photon to its original state before passing through a crystal in experiments. While this is a scientific breakthrough, scaling up the technique may prove extremely difficult, if not impossible, according to the researchers. Furthermore, the system can only reverse the state of a single particle. On the other hand, the researchers discovered that it is possible to transfer evolutionary time between identical physical systems. In a year-long experiment with ten systems, it would be possible to take one year from each of the first nine systems and give them all to the tenth. The researchers expect practical applications for their discovery, such as the ability to reverse the qubit states of a quantum processor, effectively

allowing researchers to undo errors made during development. #QNT #ESP #AUT Futurism EL PAÍS

GEOPOLITICS

→ **The European Commission has banned TikTok from being used on corporate and personal devices enrolled in the commission's mobile device service over data privacy concerns.** Similar bans have been introduced in the U.S., U.K., and Canada. The ban follows TikTok's recent apology for inappropriately obtaining user data for analysis purposes. ByteDance, TikTok's parent company, is currently negotiating with the US government to prevent a ban on the app, which could involve selling a part of TikTok to a US firm or allowing US third parties to manage the app's internal systems. #Geopolitics #DIG #USA #CHN #GBR #CAN Financial Times BBC WSJ

→ **Chinese semiconductor companies are stockpiling chip-making equipment, spare parts, and other materials amidst tighter export rules enforced by the US, Japan, and the Netherlands.** The de facto ban on sales to China of advanced chip-making gear has raised concerns among buyers in the country, leading to panic buying from chip firms. Some companies are overbuying beyond what is needed for current production plans due to fears of greater export restrictions in the future. One major Beijing-based chip equipment firm has "filled several large warehouses" with materials and components, including those not even on the US export control list, according to one person involved in the semiconductor supply chain. The restrictions impact China's pursuit of technological self-reliance as the semiconductor supply chain is complex and spans several countries globally. China's imports of chip-making equipment plunged in November and December, according to official data due to Washington's stricter rules. The country imported 4,789 units in December, down 35.3 percent year on year. #Geopolitics #SCRM #CHP #USA #CHN #JPN #NLD SCMP

→ **Chinese experts warn that China's ambitions to develop ChatGPT-like services may be constrained by U.S. export controls, which restrict access to advanced chips required for AI engines.** The US government last year announced its decision to restrict Nvidia from selling the A100 to clients in China – the chips have surged in price by 50 percent over the past two weeks amid the frenzy around ChatGPT. Many Chinese companies expressed optimism about ChatGPT, but China has yet to make its own chips and software to support at least 50-70% of the computing capacity needed to run ChatGPT. However, investors are gearing up for a "gold rush" in ChatGPT-like technologies, with the value of generative AI projected to reach $60B by 2025. #Geopolitics #AI #CHP #USA #CHN SCMP

→ **Reshoring efforts to bring manufacturing jobs back to the U.S. from China and nearshoring attempts to shift production to Mexico and Canada have not been effective.** Despite 25% tariffs on Chinese products, U.S.-China trade volume and value have only shifted slightly. The U.S.-Mexico-Canada Agreement (USMCA) Forward 2023 report suggests that the economic conflict between the U.S. and China is more of a tech war than a trade war. Supply

chain concerns have heightened the rivalry between Washington and Beijing, adding to many other challenges as relations have soured. While some American lawmakers and corporations call for a US-China “decoupling," this is easier said than done, as bureaucracy, inadequate coordination, and higher costs have impeded broad-based nearshoring to the US, Canada, and Mexico. And while some supply chains are getting shorter, others are getting longer, the report said. Meanwhile, China has better logistics, human capital, specialization, and intellectual property protection than many of its rivals – including Southeast Asian countries, India and Mexico. #Geopolitics #SCRM #USA #CHN #CAN #MEX SCRM

CYBERSECURITY

→ **Synopsys researchers discovered at least one known open-source vulnerability in 84% of all commercial and proprietary code bases examined in 2022.** In addition, almost 50% of all code bases analyzed contained high-risk vulnerabilities, which are those that have been actively exploited, already have documented proof-of-concept exploits, or are classified as remote code execution vulnerabilities. The research is based on audits of code bases involved in M&A transactions and highlights trends in open-source usage across 17 industries. The audits examined 1,481 code bases for vulnerabilities and open-source licensing compliance, and 222 other code bases were analyzed only for compliance. All of the code bases examined from companies in the aerospace, aviation, automotive, transportation, and logistics sectors contained some open-source code, accounting for 73% of total code. 63% of all code in this sector (open-source and proprietary) contained high-risk vulnerabilities with a CVSS severity score of 7 or higher. Moreover, those companies recorded a 232% increase in high-risk vulnerabilities in the 5-year period. High-risk vulnerabilities in IoT-related code bases have jumped 130% since 2018. Moreover, 91% of the code bases contained outdated versions of open-source components, which means an update or patch was available but had not been applied. #Cybersecurity #DIG #USA CSO Online

→ **CrowdStrike published its annual Global Threat Report, which identified 33 new threat actors and various campaigns in 2022. Key findings include:**

- CVE-2021-44228 discussions among threat actors in the criminal underground continued in 2022, indicating a continued interest in Log4Shell exploitation.
- There was a 20% increase in the number of threat actors conducting data theft and extortion campaigns without using ransomware in 2022.
- Cyberespionage groups linked to China targeted 39 industries all around the world. While the majority of hacking activity was aimed at China's Asian neighbors, 25% of it was directed at North America. China's techniques have become more sophisticated, involving campaigns to steal credentials and quietly enter networks.
- China-linked threat actors overwhelmingly targeted Taiwan-based technology organizations, which is consistent with the likely economic espionage mission undertaken by China-linked actors in support of CCP goals for technological independence and dominance.

- China-linked groups of varying sophistication were increasingly targeting zero-day and publicly available vulnerabilities in web-facing services for initial access, representing a significant tactical shift. When compared to the widespread reliance on exploitation of external-facing vulnerabilities, initial access techniques historically associated with China-linked threat actors, such as spear-phishing, credential harvesting, and strategic web compromises, were identified as less frequently used in 2022.
- Zero-day exploits were most commonly observed in intrusions targeting North American organizations in 2022; China-linked threat actors used zero-day exploits to compromise entities in the aerospace, legal and academic sectors.
- Following the public disclosure and release of proof-of-concept code, China-linked threat actors continued to rapidly adopt and exploit vulnerabilities in enterprise software throughout 2022.

#Cybersecurity #USA #CHN #TWN CrowdStrike

→ **Chip manufacturer Intel has paid out more than $4.1M through its bug bounty program since 2017, according to its product security report.** Between 2018 and 2021, Intel paid out, on average, $800k through its bug bounty program each year. In 2022, it paid out $935k. In 2022, 243 vulnerabilities were reported, roughly the same as the previous three years. The majority of the vulnerabilities were found in Intel software, processors, and network communications products. Only two issues received a "critical" severity rating, but 79 received a "high" severity rating. To find these vulnerabilities, Intel hosted 120 hackathons per year and funded more than 40 academic research teams in addition to its product security staff. #Cybersecurity #DIG #5G #CHP #USA SecurityWeek

→ **In 2022, Google addressed over 2,900 security vulnerabilities in its products and platforms, awarding more than $12M in bug bounty rewards to security researchers, exceeding its previous record of $8.5M in 2021.** Meanwhile, the invite-only Android Chipset Security Reward Program, which is run in collaboration with Android chip manufacturers, awarded $486k in collective bounties across 700 valid security reports in 2022. The Chrome Vulnerability Reward Program (VRP) paid out $4M for approximately 470 valid security bug reports. Security researchers received $3.5M for 363 reports of security bugs in Chrome Browser, and nearly $500k for 110 reports of security bugs in ChromeOS. In addition, the company's open-source software VRP, which was developed to address software supply chain issues in Google packages, distributed more than $110k in rewards to ~100 security researchers. #Cybersecurity #DIG #SCRM #CHP #USA Dark Reading BleepingComputer

SUPPLY CHAINS

→ **Despite U.S. sanctions on semiconductor exports to Russia, Chinese companies continue to supply chips and chip components to Russia via intermediaries such as Turkey**. China, which has refused to join Western sanctions on Russia, maintains a central role in the global chip trade as the largest importer and a significant manufacturer of low-end chips. Public data shows a certain number of semiconductor devices, for example, continuing to flow to Russia—but not who sold them or whether they were in fact sanctioned items. That makes

curbing the flow of semiconductors from China to Russia—directly or via third countries "repackaged" as new goods—extremely difficult without completely halting chip exports to China and bringing the world's electronics industry to a halt. Turkey, which also declines to endorse U.S. and European sanctions on Russia, has become a major exporter of electronics to Russia. The situation highlights the difficulty of trying to stifle trade flows of more-commoditized items like basic semiconductors, particularly when large portions of the developing world are openly skeptical of Western sanctions. #SCRM #CHP #Geopolitics #USA #RUS #CHN #TUR WSJ