CCRS Bit

September 2024

CONTENTS

Cybercrime

- The Influence of Regional Conflicts on the Hacktivist Landscape. Link
- Silicon Valley Hasn’t Revolutionized Warfare—Yet. Link
- Israel behind deadly pager explosions that targeted Hezbollah and injured thousands in Lebanon. Link
- Ransom War: How Cyber Crime Became a Threat to National Security. Book. Link
- From Protests to Profit: Why Hacktivists Are Joining the Ransomware Ranks. Link
- Ransomware: Attacks Once More Nearing Peak Levels. Link
- Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations. Link
- Services disrupted as local council near GCHQ’s headquarters hit by cyberattack. Link
- Biggest Cybersecurity Attacks in Oil And Gas Extraction Industry (2023-2024). Link
- Oil titan Halliburton confirms data was stolen in cyberattack. Link
- Did Israel infiltrate Lebanese telecoms networks? Link
- German air traffic control agency confirms cyberattack, says operations unaffected. Link
- German radio station forced to broadcast 'emergency tape' following cyberattack. Link
- Nightsleeper-style’ cyber attack hits 20 railway stations: Passengers logging on to public wi-fi at UK’s biggest transport hubs ‘are met with screen about terror attacks in Europe’. Link

- All Dutch police officers' contact details stolen in cyberattack. Link
- US Capitol Hit by Massive Dark Web Cyber Attack: Reports. Link
- TfL hit by major cyber attack as National Crime Agency launches investigation. Link
- Hacktivist group Mr Hamza Allegedly Leaked French Health Records. Link
- Data on nearly 1 million NHS patients leaked online following ransomware attack on London hospitals. Link
- U.S. govt agency CMS says data breach impacted 3.1 million people. Link
- AU: I-MED data breach exposes tens of thousands of patient files using details shared online for a year. Link
- Ransomware Gang Claims Cyberattack on Planned Parenthood. Link
- Confidant Health database exposed 5.3 terabytes of patient information. Link
- CISA: Hackers target industrial systems using "unsophisticated methods". Link
- The government isn't ready for cyber chaos in the food and agriculture sector. Link
- Data of nearly 300,000 exposed in Avis cyberattack. Link
- TIDRONE Espionage Group Targets Taiwan Drone Makers in Cyber Campaign. Link
- Ransomware in the Cloud: Scattered Spider Targeting Insurance and Financial Industries. Link
- Payment provider data breach exposes credit card information of 1.7 million customers. Link
- 100 million+ US citizens have records leaked by background check service. Link

- Massive French citizens data leak exposes 95 million records. Link
- Popular French retailers confirm hackers stole customer data. Link
- French news agency AFP hit by cyberattack. Link
- Fortinet Data Breach Impacts Customer Information. Link
- Hacker behind Snowflake customer data breaches remains active. Link
- Chinese hacking compromised hundreds of thousands of devices containing personal PII. Link
- Hacker Leaks 3.3 Billion Emails and Yes Every Single One Is Unique. Link
- APWG Phishing Activity Trends Report 2nd Quarter 2024. Link
- Top 10 Trends in Phishing Attacks (2024). Link
- Top Phishing Techniques. Link
- Phishing Via Typosquatting and Brand Impersonation: Trends and Tactics. Link
- Business Email Compromise Costs $55bn Over a Decade. Link
- H1 2024 Check Fraud Report: Geographic Trends and Threat Actor Patterns. Link
- Hackers Use Fake Domains to Trick Trump Supporters in Trading Card Scam. Link
- ATO attacks surge in Q2 2024, Sift warns of growing ‘Fraud-as-a-Service’ threat. Link
- Buy-now-pay-later plans lead to rampant scams and bad debt across Southeast Asia. Link
- Website operators promised fraudsters profit within minutes if they subscribed to illegal service. Link
- PartnerLeak scam site promises victims full access to “cheating” partner’s stolen data. Link

- Researching the boundaries of sexual integrity, gender violence and image-based abuse. Link
- Worry over identity fraud rises. Link
- Deepfake financial fraud to surge over the next 12 months, Deloitte reveals. Link
- The Emerging Dynamics of Deepfake Scam Campaigns on the Web. Link
- Deepfakes explode in Japan, tearing down language barrier. Link
- Inside the deepfake porn crisis engulfing Korean schools. Link
- South Korea battles surge of deepfake pornography after thousands found to be spreading images. Link
- A Pedophile Filmed Kids At Disney World To Make AI Child Abuse Images, Cops Say. Link
- Harmful “nudify” websites used Google, Apple, and Discord sign-on systems. Link
- Stalker Allegedly Created AI Chatbot on NSFW Platform to Dox and Harass Woman. Link
- New twist on sextortion scam includes pictures of people's homes. Link
- ‘I thought my life was over’: Escaping the sextortion scammers. Link
- Your partner “is cheating on you” scam asks you to pay to see proof. Link
- Man accused of using bots and AI to earn streaming revenue. Link
- FBI Publishes 2023 Cryptocurrency Fraud Report. Link
- 2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks On The Rise, Pig Butchering Scams Remain Lucrative. Link

- Cryptocurrencies and financial crime: a strategic approach to ensure security. Link
- DeFied Expectations — Examining Web3 Heists. Link
- More than $44 million in cryptocurrency stolen from Singaporean platform BingX. Link
- DeltaPrime Suffers $5.98M Loss as Hacker Exploits Admin Key on Arbitrum. Link
- First Mobile Crypto Drainer on Google Play Steals $70K from Users. Link
- Cambodian scam giant handled $49 billion in crypto transactions since 2021, researchers say. Link
- From Amazon to Target: Hackers Mimic Top Brands in Global Crypto Scam. Link
- Hackers Posed as Google Support to Steal $243 Million in Crypto. Link
- Report on virtual currencies in gaming: Getting played. Link
- Money laundering through video games, a criminals' playground. Link
- Feds say 'Terrorgram' white supremacists used Telegram to incite attacks. Link
- The rise of Telegram as a hub for cybercrime: a closer look at its misuse and the implications of Pavel Durov"s arrest. Link
- Exclusive-Hacker uses Telegram chatbots to leak data of top Indian insurer Star Health. Link
- Telegram's Uncertain Future: Hacktivist Reactions and the Potential Shift to New Platforms. Link
- Concealed networks: Are dark web syndicates turning to social media for cybercrime? Link

- Federal government to outlaw doxxing, impose up to seven years' jail for malicious sharing of personal data. Link
- New Issue: International Journal of Cybersecurity Intelligence and Cybercrime. Link

Digital Investigation and Digital Evidence

- AI and policing: the benefits and challenges of artificial intelligence for law enforcement. Link
- The "Budapest" Convention on Cybercrime and the draft United Nations treaty. Link
- Government Aims to Modernize Cybercrime Laws, Not Target Citizens. Link
- New Thai Legislation Bolsters The Battle Against Cybercrime. Link
- Jordan: Marking a year of oppression, fresh calls to scrap Cybercrime Law. Link
- Labor bill proposes up to seven years' jail for doxing but drops promised new hate speech laws. Link
- France uses arcane cyber law to charge Telegram CEO. Link
- Research highlights officers' lack of training and understanding around digitally enabled coercive control. Link
- UK National Crime Agency, responsible for fighting cybercrime, 'on its knees,' warns report. Link
- Behind the arrest of Telegram boss, a small Paris cybercrime unit with big ambitions. Link
- Tron, Tether and TRM Labs Start Financial Crime Fighting Force. Link
- Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere. Link
- Operation Kaerb – A Global Sting Cripples Phishing Empire and Secret Chat Network. Link

- Global Coalition Takes Down New Criminal Communication Platform. Link
- Australian Police conducted supply chain attack on criminal collaborationware. Link
- Police Broke Tor Anonymity to Arrest Dark Web Users in Major CSAM Bust. Link
- Germany seizes leak site of 'Vanir' ransomware operation. Link
- South Korea Police Investigates Telegram Over Deepfake Porn. Link
- Italy: 1,000 social media pages closed for promoting migrant trips. Link
- Justice Department Seizes Four Web Domains It Said Were Used to Create Over 40,000 Spoofed Websites and Store the Personal Information of More Than a Million Victims. Link
- US-led operation disrupts crypto exchanges linked to Russian cybercrime. Link
- Germany seizes 47 crypto exchanges used by ransomware gangs. Link
- Criminal phishing network resulting in over 480 000 victims worldwide busted in Spain and Latin America. Link
- Poland dismantles cyber sabotage group linked to Russia, Belarus. Link
- Police make arrests after hacking Ghost encrypted comms app. Link
- Teenager in Britain arrested over cyberattack on London transport agency. Link
- Man arrested over rail terror message hack. Link
- Chinese hackers linked to cybercrime syndicate arrested in Singapore. Link

- Singapore Arrests 6 Suspected Members of African Cybercrime Group. Link
- Police nab Vietnam-based smishing scam ring over 10 bln-won scam. Link
- Three arrested for selling pornographic material on Telegram. Link
- US: Alaska man busted with 10,000+ child sex abuse images despite his many encrypted apps. Link
- UK national hacked public companies for stock trading intel, DOJ says. Link
- Canadian arrested by France after cooperating with US on Sky ECC cryptophone investigation. Link
- Criminal phishing network resulting in over 480 000 victims worldwide busted in Spain and Latin America. Link
- Russian And Kazakhstani Men Indicted For Running Dark Web Criminal Marketplaces, Forums, And Trainings. Link
- U.S. Indicts 2 Top Russian Hackers, Sanctions Cryptex. Link
- Two Russian Nationals Charged in Connection with Operating Billion Dollar Money Laundering Services. Link
- US posts indictments, rewards in Russia's WhisperGate hacks against Ukraine. Link
- US charges five Russian military hackers with targeting Ukraine's government with destructive malware. Link
- Iranian hackers charged for 'hack-and-leak' plot to influence election. Link
- Justice Department Announces Charges Against Four Iranian Nationals for Multi-Year Cyber Campaign Targeting U.S. Companies. Link
- Chinese National Charged for Multi-Year "Spear-Phishing" Campaign. Link

- IT worker charged over $750,000 cyber extortion plot against former employer. Link
- Indictment Charges Two in $230 Million Cryptocurrency Scam. Link
- Admins of MFA bypass service plead guilty to fraud. Link
- Ex-Police Scotland employee charged with 44 data breaches. Link
- Star Health sues Telegram after hacker uses app's chatbots to leak data. Link
- New York Cyberstalker Is Sentenced To 15 Years In Prison. Link
- Man posing as teen YouTuber gets 17 years for horrific global sextortion scheme. Link
- California Man Who Participated in Email Fraud to Steal More Than $3 Million From Boatbuilding Companies Sentenced to 16 Months in Prison. Link
- Two foreign nationals sentenced for victimizing U.S. companies through business email compromise scheme. Link
- Russian Citizen Sentenced to 40 Months for Selling Stolen Financial Information on the Criminal Internet Marketplace Slilpp. Link
- Defendants Sentenced for Global Darknet Conspiracy. Link
- Man Convicted for $110 Million Cryptocurrency Scheme in Justice Department's First Cryptocurrency OpenMarket Manipulation Case. Link
- Courts seize £110,000 of crypto cash in Scots legal first. Link
- Seizure of 7 million euros of crypto currency and 2 crypto currency exchanges offline. Link
- Cambodian Tycoon Sanctioned for Forced Cyber Labor, Trafficking. Link

Digital Forensics

- Today, I rant - AKA: The Last Thing We Want in DF/IR is the First Thing We Need in DF/IR, Part Deux. Link
- A Word on DFIR Credentials. Link
- Essential Certifications for Digital Forensics. Link
- Why DFIR Investigative Thinking is Critical—and Why It's So Hard to Teach. Link
- The hidden risks of Cherry-Picking in Incident Response and Digital Forensics. Link
- Crowdsourcing forensics: Creating a curated catalog of digital forensic artifacts. Link
- Market Guide for Digital Forensics and Incident Response Retainer Services. Link
- Criminal IP Teams Up with IPLocation.io to Deliver Unmatched IP Solutions to Global Audiences. Link
- Enabling Smooth On-Scene Investigations With Detego Global's Rapid Deployment Kits. Link
- DFIR Toolkit. CLI tools for forensic investigation of Windows artifacts. Link
- Forensic acquisition of ChromeOS devices. Link
- Disk Forensics: A Comprehensive Guide. Link
- Memory Forensics Cheat Sheet. Link
- Bitlocker Key Finder v3.3. Link
- Unlocking the Power of Volatile Memory. Link
- Remote Wiping and Secure Deletion on Mobile Devices: A Review. Link
- Recovering Deleted Messages to Help Uncover the Criminal Mindset. Link

- How Digital Forensics Experts Read Your Encrypted WhatsApp Messages. Link
- Hybrid optimization algorithm helps detect hidden messages in digital images. Link
- Unmasking the Power of URLDNA: A Deep Dive into URL Behavior Analysis. Link
- Favicon Forensics: hunting phishing sites with Shodan. Link
- How Chainalysis Made Their Way into Popular Monero Wallets. Link
- E mail crawler will visit all pages of a provided website and parse and save emails found to a csv file. Link
- Peeper: an image analysis tool for screenshots and other images containing text. Link
- Leveraging metadata in social media forensic investigations: Unravelling digital clues - A survey study. Link
- Find the Right Open Source Research Tools With Bellingcat's New Online Investigations Toolkit. Link
- H.I.V.E: The Automated OSINT Multi-Tool for Streamlined Data Gathering. Link
- SOCMINT Awareness: Understanding Social Media Intelligence. Link
- How Reverse Phone Lookups Work [with OSINT Industries]. Link
- How to Find an Image's Location Using OSINT. Link
- Unmasking the Web's Dark Corners: A Look at Pipl.com for Cybersecurity Professionals. Link
- Overpass Turbo & GEOINT: How to Leverage OpenStreetMap for Location Analysis. Link
- Fighting Child Abuse with OSINT. Link
- OSINT resources for researching ransomware. Link

- How to use OSINT for Detailed Personal Information Searcher. Link
- Using Covert Research Accounts in OSINT Investigations. Link
- Computer Forensics in Scotland: Why would I need an independent review of expert evidence? Link
- OSINT in Legal Proceedings: Leveraging Open Source Intelligence in Modern Law. Link
- Open-source imagery is transforming investigations of international crimes – but how do judges know if it’s real? Link
- New Issue: Forensic Science International: Digital Investigation. Link

Digital Surveillance vs. Privacy

- Expanded Police Surveillance Will Get Us "Broken Windows" on Steroids. Link
- How private intelligence companies became the new spymasters. Link
- Ein neues Strafrecht für autoritäre Herrscher? Link
- Gaza: Israeli Military's Digital Tools Risk Civilian Harm. Link
- Venezuela's many means of surveillance and control. Link
- Surveilling Europe's edges: when digitalisation means dehumanization. Link
- Civil society warns Europe's digital borders making life harder for migrants. Link
- EU fingerprint and facial recognition checks expected to be delayed again. Link
- France, Germany, Netherlands not ready for EES: report. Link
- German police recommend "intensive" social media investigations into visa applicants. Link
- House advances bill to require plan for deploying AI, new sensor tech at US borders. Link
- Locked In, Locked Out: How Data Breaches Shatter Refugees' Safety. Link
- Whitepaper: Enhancing Cybersecurity Resilience for Transnational Dissidents. Link
- The Civil Rights Implications of the Federal Use of Facial Recognition Technology. Link
- US IRS seeks a multi-modal biometric ID solution for criminal investigations. Link

- New PIA for US Secret Service’s use of facial recognition raises questions. Link
- FBI seeks options for facial recognition searches against online images. Link
- Bavaria's interior minister calls for surveillance with live facial recognition. Link
- Solingen: Police to carry out facial and voice recognition online. Link
- Belgische politie mag gezichtsherkenningssoftware gebruiken, maar “het zogenoemde ‘scrapen’ kan niet door de beugel”. Link
- Controversy surrounding police use of FRT in Denmark and Germany continues. Link
- This AI claims to predict crimes before they happen based on real-time CCTV analysis. Link
- Buffalo Police Department aims to boost surveillance capability with amended Axon contract. Link
- San Francisco's artificial intelligence mobile surveillance cameras ready to deter crime. Link
- FRT, AI, body cams in the plan for Police Scotland by 2027. Link
- AI played a crucial role in investigations into Eritrea festival. Link
- Emails show cops knew buying drones broke state law. They did it anyway. Link
- We Hunted Hidden Police Signals at the DNC. Link
- An algorithmic strategy for measuring police presence with GPS data. Link
- How to surveil a federal regulator. Link
- Green Berets Hijacked WiFi To Control Home Security System Then Vanish In Mock Raid. Link

- Tracking devices increasingly used by DV offenders to ‘stalk, harass, intimidate and monitor victims’. Link
- Surveillance: Germany requests the most user data in Europe. Link
- Mass hacking and fundamental rights: a missed opportunity for the Court of Justice of the Euorpean Union? Link
- EU will weiter Verschlüsselung bekämpfen – Ungarn prescht voran. Link
- Australia’s Security Chief Says It’s Time To Start Forcing Companies To Break Chat Room Encryption. Link
- How encrypted messaging apps conquered the world. Link
- Messaging app makers' dilemma: Keeping comms private and funding open source. Link
- Telegram’s Security Sham. Link
- Telegram Agrees to Share User Data With Authorities for Criminal Investigations. Link
- Ghost, Encrypted Phone for Criminals, Was an ‘Absolute Mess’. Link
- Strafverfolger hebeln Tor-Anonymisierung aus. Link
  Tor insists its network is safe after German cops convict CSAM dark-web admin. Link
- Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and its Threats to National Security and Human Rights. Link
- Colombian president suggests prior administration illegally sent $11 million in cash to Israel for spyware. Link
- Big brother in Bratislava: does Robert Fico have Pegasus? Link
- Slovakia: Use of Pegasus a threat to democracy and human rights. Link
- Predator Files:Die Schweiz als Drehscheibe. Link

- Promoting Accountability for the Misuse of Commercial Spyware. Link
- New U.S.-led Actions Expand Global Commitments to Counter Commercial Spyware. Link
- UK spyware victims file criminal complaint against NSO Group. Link
- Apple Files to Drop Lawsuit against NSO Following Revelations by Forbidden Stories. Link . Link
- Israel's High Court Bars 'Pegasus Panel' From Calling Cops to Testify. Link
- Poland's Supreme Court Blocks Pegasus Spyware Probe. Link
- Treasury hits Predator spyware makers with more sanctions. Link
- Use of Predator spyware rebounds after a dip from Biden sanctions, researchers say. Link
- Predator Spyware Infrastructure Returns Following Exposure and Sanctions. Link
- Ex-Cop Wields Law That Only Protects Cops To Sue Data Broker For Selling His Personal Data. Link
- Federal Communications Commission Fines AT&T, Sprint, T-Mobile and Verizon Nearly $200 Million After Finding They Illegally Shared Access to Customers' Location Data. Link
- Sandvine to Exit Dozens of Countries, Replace CEO in Revamp. Link
- Web tracking report: who monitored users' online activities in 2023–2024 the most. Link
- A Look Behind the Screens Examining the Data Practices of Social Media and Video Streaming Services. Link
- Marketing Company Claims That It Actually Is Listening to Your Phone and Smart Speakers to Target Ads. Link

- FTC exposes massive surveillance of kids, teens by social media giants. Link
- Facebook admits to scraping every Australian adult user's public photos and posts to train AI, with no opt-out option. Link
- A comparative review of 10 Fundamental Rights Impact Assessments (FRIA) for AI-systems. Link
- Making Tangible the Long-Term Harm Linked to the Chilling Effects of AI-enabled Surveillance: Can Human Flourishing Inform Human Rights? Link
- No Man’s Hand: Artificial Intelligence Does Not Improve Police Report Writing Speed. Link
- Australia’s biggest medical imaging lab is training AI on its scan data. Patients have no idea. Link
- Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition. Link
- Update on Recall security and privacy architecture. Link
- Cops Are Testing Apple Vision Pro For Use In Surveillance. Link
- Apple Vision Pro’s Eye Tracking Exposed What People Type. Link
- Ford seeks patent for tech that listens to driver conversations to serve ads. Link
- Study finds many European car resellers fail to delete driver data. Link
- Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online. Link. Link
- New issue of Surveillance & Society. Link

Cyber Security

- ENISA Threat Landscape 2024. Link
- H1 2024: Malware and Vulnerability Trends Report. Link
- SANS Institute: Top 5 dangerous cyberattack techniques in 2024. Link
- Attack tool update impairs Windows computers. Link
- YubiKeys are vulnerable to cloning attacks thanks to newly discovered side channel. Link
- Unveiling Mobile App Vulnerabilities: How Popular Apps Leak Sensitive Data. Link
- Shining a Light on Shadow Apps: The Invisible Gateway to SaaS Data Breaches. Link
- ChatGPT macOS Flaw Could've Enabled Long-Term Spyware via Memory Function. Link
- Unexplained 'Noise Storms' flood the Internet, puzzle experts. Link
- For Just $20, Researchers Seize Part of Internet Infrastructure. Link
- Where The Wild Tags Are & Other AirTag Stories. Link
- Flipper Zero releases Firmware 1.0 after three years of development. Link
- Remote Access Sprawl Strains Industrial OT Network Security. Link
- Millions of Vehicles Could Be Hacked and Tracked Thanks to a Simple Website Bug. Link
- Hackers Could Remotely Control Kia Cars by Exploiting License Plates. Link

- Concerns Over Supply Chain Attacks on US Seaports Grow. Link
- Chinese scientists use Starlink signals to detect stealth aircraft and drones. Link
- New RAMBO attack steals data using RAM in air-gapped computers. Link
- The Duality of the Pluggable Authentication Module (PAM). Link
- Necro Trojan Infects Google Play Apps With Millions of Downloads. Link
- Phishing Pages Delivered Through Refresh HTTP Response Header. Link
- New Octo2 Android Banking Trojan Emerges with Device Takeover Capabilities. Link
- New Android SpyAgent Malware Uses OCR to Steal Crypto Wallet Recovery Keys. Link
- 'Hadooken' Malware Targets Oracle's WebLogic Servers. Link
- Spoofed GlobalProtect Used to Deliver Unique WikiLoader Variant. Link
- Researcher reveals ‘catastrophic’ security flaw in the Arc browser. Link
- North Korean threat actor Citrine Sleet exploiting Chromium zero-day. Link
- Ransomware gangs now abuse Microsoft Azure tool for data theft. Link
- Hidden in Plain Sight: Abusing Entra ID Administrative Units for Sticky Persistence. Link
- New Octo Android malware version impersonates NordVPN, Google Chrome. Link
- Attackers Exploiting Public Cobalt Strike Profiles. Link

- An Offer You Can Refuse: UNC2970 Backdoor Deployment Using Trojanized PDF Reader. Link
- Critical Ivanti vTM auth bypass bug now exploited in attacks. Link
- ‘Clipper’ malware is being used to steal crypto, Binance warns. Link
- Jamf Threat Labs observes targeted attacks amid FBI Warnings. Link
- People’s Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations. Link
- New research explores AI manipulation attacks on face biometric systems. Link
- Hackers deploy AI-written malware in targeted attacks. Link
- Ajina attacks Central Asia: Story of an Uzbek Android Pandemic. Link
- Earth Baxia Uses Spear-Phishing and GeoServer Exploit to Target APAC. Link
- Mallox ransomware: in-depth analysis and evolution. Link
- Inside SnipBot: The Latest RomCom Malware Variant. Link
- Kimsuky-linked hackers use similar tactics to attack Russia and South Korea, researchers say. Link
- APT Lazarus: Eager Crypto Beavers, Video calls and Games. Link
- Inside the Dragon: DragonForce Ransomware Group. Link
- Dark Web Profile: Abyss Ransomware. Link
- Dark Web Profile: GlorySec. Link
- Threat Assessment: Repellent Scorpius, Distributors of Cicada3301 Ransomware. Link
- #StopRansomware: Blacksuit (Royal) Ransomware. Link
- Threat Assessment: North Korean Threat Groups. Link

- "Marko Polo" Navigates Uncharted Waters With Infostealer Empire. Link
- DragonRank, a Chinese-speaking SEO manipulator service provider. Link
- New Morphisec report finds links between emerging Cicada3301 ransomware and BlackCat. Link
- Head Mare: adventures of a unicorn in Russia and Belarus. Link
- I Spy With My Little Eye: Uncovering an Iranian Counterintelligence Operation. Link
- ENISA to establish cybersecurity certification scheme for EU's digital ID wallets. Link
- AI Act could inform biometrics standards for European identity regulation. Link
- Press Release: White House Office of the National Cyber Director Releases Roadmap to Enhance Internet Routing Security. Link
- Western powers make plans to secure submarine communications cables, excluding Chinese firms and technology. Link
- Ban Sought for Chinese, Russian Software and Hardware Used in Autonomous Vehicles on US Roads. Link
- US House votes to bar new DJI drones as 'China week' gets underway. Link
- UK's ICO and NCA Sign Memorandum to Boost Reporting and Resilience. Link
- Congress Advances Bill to Add AI to National Vulnerability Database. Link
- CISA Faces Challenges Sharing Cyber Threat Information as Required by the Cybersecurity Act of 2015. Link

- DOJ, FBI need better metrics for tracking ransomware disruption efforts, audit finds. Link
- City of Columbus tries to silence security researcher. Link. Link
- Franklin County judge grants city request to suppress cyber expert’s efforts to warn public. Link
- Japanese media giant investigating another reported data leak by BlackSuit hackers. Link
- Ireland fines Meta €91 million for storing passwords in plaintext. Link
- FTC issues $3 million fine for security camera firm, issuing penalties for a range of violations. Link
- Verkada Facing Penalty After Hackers Viewed Sensitive Video Footage. Link
- Hospital system to pay $65 million for dark web data leak, including images of nude cancer patients. Link
- HHS Office for Civil Rights Settles Ransomware Cybersecurity Investigation for $250,000. Link
- 23andMe Agrees To $30 Million Settlement For Last Year's Data Breach. Link
- Northern Ireland cops whose info was leaked in 2023 may get £240M+ damages. Link
- Did a Chinese University Hacking Competition Target a Real Victim? Link