CCRS Bit

March 2024

CONTENTS

Cybercrime 2
Digital Investigation and Digital Evidence 5
Digital Forensics 8
Digital Surveillance vs. Privacy 10
Cyber Security 17

Cybercrime

- FBI 2023 Internet Crime Report. Link
- FBI: Cybercrime Losses Exceeded $12.5 Billion in 2023. Link
- Group-IB Report. Hi-Tech Crime Trends 2023/2024 - Middle East and Africa. Link
- These Are Some of the Largest Darknet Markets That Pulled an Exit Scam and Completely Vanished. Link
- Telegram: social media giant or the new 'dark web'? Link
- Nation states buying hacking tools from underground Russian cyber forums. Link
- CISA forced to take two systems offline last month after Ivanti compromise. Link
- Serious security breach hits EU police agency. Link
- French unemployment agency data breach impacts 43 million people. Link
- French government agencies hit by cyberattacks of 'unprecedented intensity'. Link
- A bug in an Irish government website that exposed COVID-19 vaccination records took 2 years to publicly disclose. Link
- Ukraine claims it hacked Russian Ministry of Defense servers. Link
- Cyber-attack hits Malawi's immigration service. Link
- North Korea hacks two South Korean chip firms to steal engineering data. Link
- Microsoft confirms Russian spies stole source code, accessed internal systems. Link

- Russian spies keep hacking into Microsoft in ‘ongoing attack,’ company says. Link
- Nissan confirms ransomware attack exposed data of 100,000 people. Link
- Air Europa Customers Warned Of Data Leak By IAG, WSJ Says. Link
- A leaky database spilled 2FA codes for the world’s tech giants. Link
- Thousands of stolen Dutch passports published on the dark web. Link

  Data breaches caused by insiders can cost you over $15 million. Link
- Lessons from the iSOON Leaks. Link
- Don't Answer the Phone: Inside a Real-Life Vishing Attack. Link
- Generative AI enabling identity fraud at scale: Au10tix report. Link
- 'Criminal e-bank' launders 2.6 billion euros - and is only tip of the iceberg. Link
- The Chainalysis 2024 Crypto Crime Report. Link
- $12.5 billion lost to cybercrime, amid tidal wave of crypto investment fraud. Link
- Highland Park Man Led Hacker Crew's $400 Million Heist From FTX: Feds. Link
- Lazarus Group hackers appear to return to Tornado Cash for money laundering. Link
- Crypto firm moved $4.2m of assets to digital wallet linked to alleged Russian arms dealer. Link
- Firm related to sanctioned crypto exchange Garantex is a partner of Moscow gang leader and has links to Kremlin-controlled Rosneft. Link

- The Dark Side of Open Source AI Image Generators. Link
- LGBTQ+ community grapples with hidden wave of digital abuse. Link
- Tech bros need to realise deepfake porn ruins lives – and the law has to catch up. Link
- International Journal of Cybersecurity Intelligence & Cybercrime (IJCIC) - New Issue. Link
- Journal of International Criminal Justice - Special Issue Autonomous Weapon Systems and War Crimes. Link
- Cyberpsychology, Behavior, and Social Networking - New Issue. Link
- Caught in the Web: Virtual Kidnapping and Digital Scams. Cybercrimeology podcast, EP103. Link
- Behind the doors of a Chinese hacking company, a sordid culture fueled by influence, alcohol and sex. Link
- IntelBroker Interview: The Elusive Hacker in the Shadows Talks to The Cyber Express. Link
- How the Belarusian Cyber Partisans are fighting a digital war against two dictators. Link
- The quest for the righteous hack: revisited. Link

Digital Investigation and Digital Evidence

- FBI Director Wray talks takedown operations, nation-state hackers, and growing threats in cyberspace. Link
- FTC Goes Undercover Against Fake Antivirus Companies. Link
- Tracking Everything on the Dark Web Is Mission Critical. Link
- Staqu's biometric Crime GPT helps Uttar Pradesh police take a byte out of crime. Link
- BioID launches new version of deepfake detection software. Link
- This is what AI needs to become the primary tool for police investigations. Link
- Expert.AI supports Intelligence activities: exploring features of and differences among NLP, NLU, NLG. Link
- Click, click, arrest! The use of facial recognition by police in Germany. Link
- How crypto investigators uncover scammers' blockchain billions, scale of money laundering in Asia. Link
- Binance's Top Crypto Crime Investigator Is Being Detained in Nigeria. Link
- 57 men arrested for possessing and sharing over 100 000 depictions of child sexual abuse. Link
- Ukraine arrests hackers trying to sell 100 million stolen accounts. Link
- Ex-Google Engineer Arrested for Stealing AI Technology Secrets for China. Link

- US Charges China-Backed Hackers With 14 Years of Cyberattacks. Link
- Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians. Link
- Admin of major stolen account marketplace gets 42 months in prison. Link
- LockBit affiliate jailed for almost four years after guilty plea. Link
- 'Lifelock' hacker pleads guilty to extorting medical clinics. Link
- US sanctions alleged Chinese state hackers for attacks on critical infrastructure. Link
- Why the $1.2 bn trial of Tornado Cash dev Alexey Pertsev will decide the future of crypto privacy. Link
- US moves to recover $2.3 million from "pig butchers" on Binance. Link
- Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions. Link
- Questions raised over NHS deletion of thousands of emails during whistleblower tribunal. Link
- The searches for Ana Walshe: The end of Brian Walshe's 1st major criminal case. Episode about electronic evidence. Link
- How an infamous ransomware gang found itself hacked. Guardian podcast. Link
- The EU-funded FRISCO project (Fighting Terrorist Content Online) publishes the report of its first 2023 workshop in Berlin. LInk
- Meta Abandons Hacking Victims, Draining Law Enforcement Resources, Officials Say. Link

- Robotic police dog shot multiple times, credited with avoiding potential bloodshed. Link
- Jeffrey Epstein’s Island Visitors Exposed by Data Broker. Link

Digital Forensics

- NIST Report: Long-Term Vision and Strategic Priorities for Forensic Science in the United States: Summary Report of a Roundtable Discussion with Thought Leaders. Link
- NIST Report: Forensic Science Environmental Scan 2023. Link
- Memory Forensics: comparing the correctness of memory captures from locked Windows 10 machines using different boot capture vectors. Link
- Crypto tracing is revolutionizing crime-fighting, but critics call it a 'junk science.' Inside the raging debate over blockchain analytics. Link
- How Regulators Can Detect and Investigate Unregistered VASPs Using Blockchain Intelligence. Link
- Formation of the Open Source Digital Forensics Developer's Council. Link
- A technical analysis of the APT28's backdoor called OCEANMAP. Link
- The Anatomy of a BlackCat (ALPHV) Attack. Link
- Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit. Link
- WinFiHack - A Windows Wifi Brute Forcing Utility Which Is An Extremely Old Method But Still Works Without The Requirement Of External Dependencies. Link
- BlueSpy - PoC to record audio from a Bluetooth device. Link
- SquarePhish - advanced phishing tool that uses a technique combining the OAuth Device code authentication flow and QR codes. Link
- ThievingFox - Remotely retrieving credentials from password managers and Windows utilities. Link

- They’re watching us: How to detect Pegasus and other spyware on your iOS device? Link
- The best chrome extensions for OSINT professionals, researchers and journalists in 2024. Link
- How GEOINT is Transforming Intelligence for Business and Global Security. Link
- DarkGPT – AI OSINT Tool to Detect Leaked Databases. Link
- ASINT vs OSINT: Diving Deeper into Intelligence Gathering Techniques. Link
- Digital Forensics Lab - CYL2002. Link

Digital Surveillance vs. Privacy

- Kafka in the Age of AI and the Futility of Privacy as Control. Link
- The Atlas of Surveillance Removes Ring, Adds Third-Party Investigative Platforms. Link
- Secret Pentagon program echoes pedophile ring in "True detective" series. Link
- U.S. Spy Agencies Know Your Secrets. They Bought Them. Link
- US Lawmaker Cited NYC Protests in a Defense of Warrantless Spying. Link
- This Global Identity System Tracks Everything You Do Online. Link
- Some of the Most Popular Websites Share Your Data With Over 1,500 Companies. Link
- Every scary thing Meta knows about me — and you. Link
- Elon Musk Fought Government Surveillance — While Profiting Off Government Surveillance. Link
- Kids Online Safety Act Gains Momentum in the Senate. Link
- Feds Ordered Google To Unmask Certain YouTube Users. Critics Say It's 'Terrifying.' Link
- Signal's new usernames help keep the cops out of your data. Link
- Security News This Week: The Privacy Danger Lurking in Push Notifications. Link
- Police now need a warrant to get a person's IP address, Supreme Court rules. Link
- R. v. Bykovets - Privacy and the Internet. Link

- Turns out cops are super interested in subpoenaing suspects' push notifications. Link
- Facebook snooped on users’ Snapchat traffic in secret project, documents reveal. Link
- Experian Is Trying To Force WhatsApp To Hand Over User Data In An ‘Odd’ Court Battle. Link
- New report examines redress for systemic human rights violations in Turkish messaging app prosecutions. Link
- NI Policing Board pressed to open inquiry into PSNI spying on journalists’ phones. Link
- Swedish data brokers claim journalists’ legal protection to evade EU privacy law. Link
- US Blacklists Sandvine for Censorship, Web Monitoring Abroad. Link
- House passes bill to bar data brokers from selling sensitive personal information to U.S. adversaries. Link
- 'Like a stalker': Data broker LiveRamp reported to UK, French regulators. Link
- The Predator spyware ecosystem is not dead. Link
- Predator Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices. Link
- The Predator spyware ecosystem is not dead. Link
- Predator spyware endures even after widespread exposure, analysis shows. Link
- DSIRF – Spionagesoftware aus Österreich. Link
- Israeli Spyware Vendor Ordered to Reveal Source Code to Meta. Link
- Court orders maker of Pegasus spyware to hand over code to WhatsApp. Link
- Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium. Link

- US Announces First-Ever Sanctions Against Commercial Spyware. Link
- Spyware makers express concern after US sanctions spyware veteran. Link
- Request to cross-check lists of surveillance targets pending. Link
- Will the Brussels spyware scandal finally convince the EU to act? Link
- Apple, Okta and others help human rights groups fight spyware. Link
- A leading spyware combatant on what's next as governments continue to crack down. Link
- Finland, Germany, Ireland, Japan, Poland, South Korea added to US-led spyware agreement. Link
- Investors' pledge to fight spyware undercut by past investments in US malware maker. Link
- A European digital identity? – Pros and cons of seamless access to private services. Link
- EU agencies and interoperable databases. Link
- Home Office immigration database errors hit more than 76,000 people. Link
- More German authorities introduce facial recognition, while the police photo database breaks through 5 million mark. Link
- Privatised municipal surveillance on the stage of security theatre in Slovenia. Link
- Une caméra de surveillance inviolable et un logiciel israélien pour surveiller le bastion de l'extrême gauche à Brest. Link
- Exclusive: Musk's SpaceX is building spy satellite network for US intelligence agency, sources say. Link

- How governments are using facial recognition to crack down on protesters. Link
- Europe's borders are a surveillance testing ground. The AI Act could change that. Link
- The EU AI Act: a failure for human rights, a victory for industry and law enforcement. Link
- EU: Artificial Intelligence rulebook fails to stop proliferation of abusive technologies. Link
- Council of Europe AI treaty does not fully define private sector's obligations. Link
- Bundesregierung soll Biometrie-Überwachung zumindest in Deutschland verbieten. Link
- A Virtual Reality Tour of Surveillance Tech at the Border: A Conversation with Dave Maass of the Electronic Frontier Foundation. Link
- 85 civil society organisations call on MEPs to uphold fundamental rights and reject the harmful Schengen Borders Code recast. Link
- Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move. Link
- UK struggles with biometric border crossing software. Link
- War in Ukraine and the private sector. Link
- AI warfare is already here. Link
- Warbot 2.0: Reflections on the fast-changing world of AI in national security. Link
- The Air Force Bought a Surveillance-Focused AI Chatbot. Link
- Israel Deploys Expansive Facial Recognition Program in Gaza. Link
- Drone Swarms Are About to Change the Balance of Military Power. Link

- ICO finds the Home Office’s pilot of GPS electronic monitoring of migrants breached UK data protection law. Link
- U.S. Government seeks “unified vision of unauthorized movement”. Link
- Biometrics giant Accenture quietly took over la residents’ jail reform plan. Link
- Revealed: a California city is training AI to spot homeless encampments. Link
- Remote ID Proofing - Good practices. ENISA Report. Link
- Cops Running DNA-Manufactured Faces Through Face Recognition Is a Tornado of Bad Ideas. Link
- Facial Recognition: Coming Soon to an Airport Near You. Link
- Clearview facial recognition added to to the Department of Defense’s Tradewinds Solutions Marketplace. Link
- UK’s £230 million plan to implement police facial recognition and drones. Link
- Buenos Aires’ controversial facial recognition network remains in limbo. Link
- Ukraine prepares law to unify its biometric surveillance systems. Link
- Granular biopolitics: Facial recognition, pandemics and the securitization of circulation. Link
- Bridging values: Finding a balance between privacy and control. The case of Corona apps in Belgium and the Netherlands. Link
- Unregulated, Exploitative, and on the Rise: Vera Institute's Report on Electronic Monitoring. Link
- Age Verification Laws Drag Us Back to the Dark Ages of the Internet. Link

- Privacy Is Just No Longer a Thing in Augmented Reality?
- Skepticism mounts over Apple's modest claims on Vision Pro data. Link
- These Video Doorbells Have Terrible Security. Amazon Sells Them Anyway. Link
- This $4 Billion Car Surveillance Startup Says It Cuts Crime. But It Likely Broke The Law. Link
- How Your New Car Tracks You. Link
- Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies. Link
- GM cuts ties with 2 data firms amid heated lawsuit over driver data. Link
- Vehicle Cloning — Another Reason Not To Use Automated License Plate Readers. Link
- Car cloning: innocent UK motorists get fines as scams accelerate. Link
- Glassdoor Wants to Know Your Real Name. Link
- GM, LexisNexis Sued For (Nontransparent) Sale Of Driver Behavior Data To Insurers. Link
- FTC investigating Reddit plan to sell user content for AI model training. Link
- ECHR published its updated factsheet on personal data protection. Link
- ECtHR: Judgment in Wa Baile v. Switzerland – Allegations of discrimination on the ground of skin colour during an identity check - Police failed to observe non-discrimination principle during identity check in Zürich railway station. Link
- European Court of Human Rights Confirms: Weakening Encryption Violates Fundamental Rights. Link

- ByLock Prosecutions and the Right to Fair Trial in Turkey: The ECtHR Grand Chamber's Ruling in Yüksel Yalçınkaya v. Türkiye. Link
- Court of Justice of the European Union: Judgment in Case C-61/22 - The mandatory insertion in identity cards of two fingerprints is compatible with the fundamental rights to respect for private life and to protection of Personal Data. Link
- Court of Justice of the European Union: Judgment in Case - The supervisory authority of a Member State may order the erasure of unlawfully processed data. Link
- European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies. Link
- Tracking-ads industry faces another body blow in the EU. Link
- Sam Altman's Eye-Scanning Worldcoin Venture Blocked in Spain. Link
- AEPD confirmed that telecommunication service providers have to provide access to location data they process under national data retention legislation contrary to the controller who argued that such legislation provided a full exemption for the right to access. Link
- BNSF Railway to pay $75 mln to resolve biometric privacy class-action. Link
- Surveillance & Society - New Issue. Link
- The Pleasures of Surveillance. Link
- The Problem of Consent with Teledildonics and Adult Webcam Platforms.Link
- "Stalk Me to the End of Love": Mutual Watching and Intimate Affections through the Use of Smartphones. Link

Cyber Security

- Check Point's 2024 Cyber Security Report. Link
- NIST National Vulnerability Database Disruption Sees CVE Enrichment on Hold. Link
- Google. A review of zero-day in-the-wild exploits in 2023. Link
- Zero-days exploited in the wild jumped 50% in 2023, fueled by spyware vendors. Link
- Chinese hackers target family members to surveil hard targets. Link
- A Flaw in Millions of Apple, AMD, and Qualcomm GPUs Could Expose AI Data. Link
- Unit 42 Collaborative Research With Ukraine's Cyber Agency To Uncover the Smoke Loader Backdoor. Link
- New Gtpdoor Backdoor Is Designed To Target Telecom Carrier Networks. Link
- New acoustic attack determines keystrokes from typing patterns. Link
- PrintListener: remote fingerprint theft. Link
- Cybersecurity enthusiast collects Wi-Fi passwords using homemade device, sounds warning. Link
- Hackers exploit Windows SmartScreen flaw to drop DarkGate malware. Link
- Threat Brief: WordPress Exploit Leads to Godzilla Web Shell, Discovery & New CVE. Link
- Remote Stuxnet-Style Attack Possible With Web-Based PLC Malware: Researchers. Link

- Hackers Using Cracked Software on GitHub to Spread RisePro Info Stealer. Link
- Cybercriminals Using Novel DNS Hijacking Technique for Investment Scams. Link
- Germany warns of 17K vulnerable Microsoft Exchange servers exposed online. Link
- Chinese hacking group APT31 uses mesh of home routers to disguise attacks. Link
- Russia's spy leak reveals military communications risk. Link
- How to: Detect Bluetooth Trackers. Link
- SIM swappers hijacking phone numbers in eSIM attacks. Link
- Phishing mobile devices, with DeviceCode phishing and QR codes. Link
- Apple warns users against critical memory-corrupting attacks. Link
- Location Tracking on The Battlefield: how mobile devices are being tracked, ENEA report. Link
- APIs Drive the Majority of Internet Traffic and Cybercriminals are Taking Advantage. Link
- Lurking in the Shadows: Attack Trends Shine Light on API Threats. Link
- Burglars Using Wi-Fi Jammers to Disable Security Cameras. Link
- Say Friend and Enter: Digitally lockpicking an advanced smart lock (Part 2: discovered vulnerabilities). Link
- Massively Popular Safe Locks Have Secret Backdoor Codes. Link
- $700 cybercrime software turns Raspberry Pi into an evasive fraud tool. Link

- The Architects of Evasion: a Crypters Threat Landscape. Link
- StopCrypt: Most widely distributed ransomware evolves to evade detection. Link
- PixPirate Android Banking Trojan Using New Evasion Tactic to Target Brazilian Users. Link
- Infostealer Disguised as Adobe Reader Installer. Link
- LLM Agents can Autonomously Hack Websites. Link
- How to weaponize LLMs to auto-hijack websites. Link
- Malicious AI models on Hugging Face backdoor users' machines. Link
- Here Come the AI Worms. Link
- Adversarial Intelligence: Red Teaming Malicious Use Cases for AI. Link
- Navigating cyberthreats and strengthening defenses in the era of AI. Link
- A bug in an Irish government website that exposed COVID-19 vaccination records took 2 years to publicly disclose. Link
- IMF Investigates Cyber-Security Incident. Link
- MGM Resorts says regulators probing September cyberattack. Link
- Four things we learned when US intelligence chiefs testified to Congress. Link
- A government watchdog hacked a US federal agency to stress-test its cloud security. Link
- FCC approves cybersecurity label for consumer devices. Link
- Flipper Zero's Co-Founder Says the Hacking Tool Is All About Exposing Big Tech's Shoddy Security. Link
- UK government's ransomware failings leave country 'exposed and unprepared'. Link