

Criminal justice action on cybercrime (January 2026): Quick scan of investigations, prosecutions, trials around the world

While the threat of cybercrime keeps increasing, it is important to realize that also criminal justice measures against cybercrime are becoming more effective, not only in terms of disruption but also of actual arrests, prosecutions and convictions. This is illustrated by examples reported in January 2026.

Action taken against criminal organizations running scam hubs in Cambodia – involving “pig-butcher””, forced labour and human trafficking with victims all over the world – was major news in January 2026.

Acquittals (examples of Kenya and Spain) confirm rule of law requirements that need to be met when investigating and prosecuting cybercrime and other cases involving electronic evidence).

However, some cases (examples of **Niger**, **Pakistan** and **Tunisia**) illustrate how cybercrime laws can be misused by governments.

Contact: alex.seger@alexsas.net

Date	Country/region	Summary	Source
9 January 2026	Africa	<p>International Cybercrime Operation Leads to 574 Arrests and USD 3 Million in Recovered Fund</p> <p>“A coordinated law enforcement operation spanning 19 African countries resulted in 574 arrests and the recovery of approximately USD 3 million in illicit proceeds, marking one of the largest region-wide cybercrime crackdowns to date. Led by INTERPOL under the African Joint Operation against Cybercrime (AFJOC), Operation Sentinel ran from October 27 to November 27, 2025, and targeted cyber-enabled financial crime, including business email compromise (BEC), ransomware, digital extortion, and online fraud. These threats were identified as priority risks in INTERPOL’s 2025 Africa Cyber Threat Assessment, which documented a sharp increase in both the scale and sophistication of attacks across the continent.”</p>	TRMLabs
9 January 2026	India	<p>CBI arrests area sales manager of telecom service provider who procured 21,000 SIM cards for phishing scams</p> <p>India’s Central Bureau of Investigations arrested three persons, including the areas sales manager of telecom service provider, for procuring more than 20,000 SIM cards to criminals operating an organised phishing network.</p>	ANI
9 January 2026	Cambodia	<p>Pig butchering: Alleged cybercrime kingpin arrested and extradited from Cambodia to China</p> <p>In January 2026, Chen Zhi, a national of China and Cambodia, was arrested in Cambodia and extradited to China. Chen is the founder</p>	CNN BBC

		and chairman of Prince Group. He is suspected of being “the ringleader of a major cross-border online gambling and fraud criminal syndicate” that is operating a network of forced labour camps in Cambodia for online fraud (“pig butchering”) and more than 100 shell companies around the world for the laundering of crime proceeds. In October 2025, US authorities had already seized the equivalent of US\$ 15 billion in crypto assets from Chen.	
12 January 2026	Netherlands	<p>Dutch court sentences hacker who used port systems to smuggle cocaine to 7 years</p> <p>“A Dutch appeals court sentenced a 44-year-old man to seven years in prison for hacking a major port company in Belgium to help smuggle cocaine into the Netherlands.</p> <p>The Amsterdam Court of Appeal ruled Friday that the man played a central technical role in a criminal network that exploited port computer systems in 2020 and 2021, allowing traffickers to move drugs through Europe’s logistics hubs without detection.”</p>	TheRecord
12 January 2026	Kazakhstan	<p>Cybercrime Fight: Kazakhstan Blocks Millions of Scam Calls</p> <p>According to Interior Minister Yerzhan Sadenov “A total of 84.5 million fraudulent calls were blocked, helping to prevent significant financial losses and reduce citizens’ exposure to scams. Thirteen call centers were shut down, including some located abroad. Fifty-six criminal cases have been opened against individuals involved in so-called ‘dropperism,’ aiding internet fraudsters.”</p>	Caspian Post
14 January 2026	Germany	<p>Raid in Germany: Authorities shut down cybercrime hoster RedVDS</p> <p>RedVDS provided “cybercrime-as-a-service”, that is, the digital infrastructure (virtual hosting services) for the commission of large-scale phishing and online fraud. The core of this infrastructure is considered to have been a data centre in Germany. Cooperation between Germany prosecutors and criminal police with Microsoft led to the seizure of the servers, while no arrests have been made.</p>	Heise Online Microsoft
15 January 2026	Germany	<p>Investors defrauded of millions: Head of the Milton Group in court</p> <p>The trial has begun in Bamberg against the alleged mastermind of an international criminal group operating fake trading platforms, also known as the "Milton Group." The 50-year-old Israeli-Georgian citizen is accused of organized and commercial fraud. Between 2014 and 2019, approximately 1,000 people in German-speaking countries are alleged to have been victims.</p> <p>Victims worldwide have reportedly been defrauded by at least 178 million EURO.</p>	BR
15 January 2026	Senegal	<p>Cybercriminalité : un réseau transnational de modification de données démantelé</p> <p>Senegal’s Special Cybersecurity Division (DSC) is reported to have arrested four Russian, Senegalese and Ivorian nationals belonging to a network involved in "computer data manipulation, money laundering, and complex fraud".</p> <p>According to initial findings, the network used methods such as fraudulent data modification, system infiltration to alter strategic information, illegal use of identities or brands to lend credibility to</p>	PressAfrique

		their scams, transnational money laundering, and transforming dirty money into digital services (advertising, consulting) to cover their tracks.	
17 January 2026	Spain	<p>Europol: Blow against Nigerian Cybercrime Syndicate Black Axe</p> <p>In an internationally coordinated operation, European law enforcement agencies have dealt a significant blow to the Nigerian "Black Axe" group. Europol confirmed on Friday that a total of 34 suspects were arrested in Spain. The operation uncovered a complex network involved in cyber fraud, money laundering, and organized crime.</p>	B2b cyber security
19 January 2026	Germany	<p>Man convicted to 5 years in prison for online investment scam</p> <p>A court in Göttingen (Germany) sentenced a 39 years old man to five years in prison for organised fraud in 278 instances. He belonged to an international gang that defrauded German investors of around EUR 20 million.</p>	NDR
19 January 2026	Romania	<p>Dark web arrests in Romania linked to portal which offered services including murder</p> <p>A coordinated execution of search warrants on 14 January 2026 by the Cybercrime Unit of the Romanian Police and the UK's Eastern Region Special Operations Unit (ERSOU) reportedly led to the arrest of two suspects in Romania and the seizure of cash and crypto currency with a value of some EUR 700,000. "The enforcement was connected to a scam website called Online Killers Marketplace (OKM), which purported to facilitate criminal activities including the hiring of hitmen and extortion."</p>	Regional Organised Crime Unit Network (UK)
19 January 2026	Ghana	<p>53 Nigerian nationals arrested in major cybercrime crackdown</p> <p>Law enforcement authorities of Ghana have arrested 53 Nigerian nationals in several suspected fraud centres in the greater Accra region. It is suspected that you men were exploited and coerced to engage in cybercrime activities in these centres.</p>	Ghana Web
20 January 2026	Singapore	<p>Four Malaysian Nationals To Be Charged For Their Suspected Involvement In Government Official Impersonation Scam</p> <p>According to the Singapore Police Force, "three Malaysian men and one Malaysian woman, aged 24 to 30, will be charged in court on 21 January 2026 for their suspected involvement in three separate cases of Government Official Impersonation Scam (GOIS)".</p>	Singapore Police Force
20 January 2026	Cambodia	<p>Alleged scam mastermind arrested after being exposed by BBC</p> <p>"Cambodian authorities have arrested a prominent businessman featured in a 2023 BBC Eye investigation into alleged online scam operations as part of a wider effort to tackle organised online fraud. Kuong Li, a 50-year-old Cambodian national, was charged with illegal recruitment for exploitation, aggravated fraud, organised crime and money laundering relating to alleged offences committed in Cambodia and elsewhere since 2019."</p>	BBC
20 January 2026	Japan	<p>Man arrested for posting AI-generated sexual images of female celebrities online</p> <p>"Police in Tokyo have arrested a 31-year-old unemployed man on suspicion of using generative artificial intelligence (AI) to create</p>	Japan Today

		deepfake sexual images of female celebrities and posting them online where he sold them”	
20 January 2026	Thailand	<p>Phuket police arrest Russian cybercrime suspect</p> <p>“Police have arrested a 25-year-old Russian national suspected of involvement in a cybercrime gang and seized assets worth several hundred thousand baht, authorities said.</p> <p>Acting under the direction of provincial police commander Maj. Gen. Sinlert Sukhum, officers from Kathu police station and the Phuket Provincial Police Investigation Division launched a crackdown on technology-related crime following reports of suspicious financial transactions.”</p>	Khaosoenglish
20 January 2026	Kenya	<p>Nairobi court acquits Nuru Okanga in cybercrime case, cites lack of evidence</p> <p>“A Nairobi court has acquitted vocal political commentator Nuru Okanga of cybercrime charges related to the alleged publication of false, defamatory, and threatening content on social media. The acquittal comes after prosecutors failed to link Okanga to the disputed material.”</p>	Kenyans MSN
21 January 2026	Ukraine & Germany	<p>Black Basta’s alleged ringleader identified as authorities raid homes of other members</p> <p>Law enforcement authorities in Ukraine and Germany raided homes of Russian nationals accused of participating in the operations of the Black Basta ransomware group, and a third Russian national has been identified and added to the Europol and Interpol most-wanted list.</p>	Cyberscoop The Hacker News
22 January 2026	Tunisia	<p>Two popular Tunisian journalists handed three-year jail terms</p> <p>Press rights campaigners slammed the case against Bohran Bssaies and Mourad Zghidi as “legal persecution”.</p> <p>“A Tunisian court has handed new prison terms to two well-known media figures in what critics say is the government’s latest attempt to punish dissent.</p> <p>The criminal chamber of the Tunis Court of First Instance sentenced radio journalists Bohran Bssaies and Mourad Zghidi to three and a half years in prison on Thursday for “money laundering”, a judicial source told Tunisia’s state TAP news agency.”</p>	AlJazeera
22 January 2026	USA	<p>Leader of ransomware crew pleads guilty to four-year crime spree</p> <p>“Ianis Antropenko, a Russian national living in California, admitted to committing ransomware attacks against at least 50 victims. He faces up to 25 years in jail. “</p>	Cyberscoop
22 January 2026	USA	<p>Hacker Pleads Guilty To Breaching The US Supreme Court</p> <p>“A Tennessee man has pleaded guilty to hacking the US Supreme Court’s electronic filing system more than two dozen times and illegally accessing sensitive records from other federal platforms.”</p>	ImmuniWeb

23 January 2026	India	<p>Nigerian Woman Sentenced to Seven Years in Cyber Fraud Case by Gujarat Court</p> <p>“A court in Gujarat’s Amreli district has sentenced a Nigerian woman to seven years of simple imprisonment in a ₹14 lakh cyber fraud case, holding her guilty under multiple provisions of the Indian Penal Code (IPC) and the Information Technology Act. The case relates to a carefully orchestrated online scam involving social media deception, a fake international courier company and false promises of a valuable gift from London.”</p>	The420in
24 January 2026	Pakistan	<p>Pakistani human rights lawyers jailed for 17 years over social media posts</p> <p>ISLAMABAD (AP) — A Pakistani court on Saturday sentenced two human rights lawyers to 17 years in prison each over social media posts the authorities claimed were hostile to the state and its security institutions.</p> <p>Judge Afzal Majoka announced the verdict a day after Zainab Mazari and her husband Hadi Ali Chattha were arrested in Islamabad, according to court documents.</p> <p>The couple appeared briefly via video link but boycotted the hearing, prompting the court to conclude the trial and deliver the verdict. Family and friends denounced the ruling. The couple denied all the changes.</p> <p>The court verdict said Mazari had posted multiple tweets in recent years that “portrayed the agenda” of the outlawed Baloch separatist group and Pakistani Taliban.</p> <p>The case stems from a complaint filed in August 2025 with the National Cyber Crime Investigation Agency, alleging the couple used social media to malign the state and its security institutions. They were formally indicted last October and had repeatedly refused to appear in court.</p>	AP News EURASIA Review
25 January 2026	Sri Lanka	<p>Police Report Surge in Cybercrime as Hundreds Arrested Nationwide</p> <p>“Sri Lanka Police have revealed that more than 300 individuals were taken into custody over the past year in connection with a range of cyber-related offences, underscoring the steady rise of digital crime across the country.</p> <p>According to Police Media Spokesperson Assistant Superintendent F.U. Wootler, investigators handled over 2,000 complaints linked to online fraud, identity theft and other technology-driven crimes during 2025. He said the figures reflect an expanding threat landscape as internet use becomes more widespread.”</p>	LankaNewsWeb
26 January 2026	Spain	<p>Spanish court acquits suspects denied access to ‘raw’ Sky ECC intercepts in landmark decision</p> <p>“Prosecutors have been told they cannot rely on intercept evidence from the Sky ECC encrypted phone network in the absence of other evidence, unless they disclose the raw intercept data to defendants in decision that could have a significant impact on future prosecutions.”</p>	Computer weekly

26 January 2026	Niger	<p>Niger arrests DW correspondent over report on Nigerian refugees</p> <p>“Dakar, January 26, 2026—The Committee to Protect Journalists urges authorities in Niger to release Gazali Abdou Tasawa, a correspondent for the German public broadcaster Deutsche Welle (DW), who was arrested over a report on Nigerian refugees living by a cemetery.</p> <p>....</p> <p>“Separately, on December 23, 2025, Niger’s top court, the State Court, upheld the 2020 conviction of investigative journalist Samira Sabou who spent 48 days in detention while pregnant. Sabou won CPJ’s 2024 International Press Freedom Award.</p> <p>According to a copy of the decision, reviewed by CPJ, the court rejected Sabou’s argument that she should not have been prosecuted under the cybercrime law because she was a journalist, and that the press law would have been more appropriate.”</p> <p>....</p> <p>“The court ruled that the press law did not apply and the cybercrime law was the correct tool to use because the offense was committed by “electronic means” and that her status as a journalist was “of little importance.””</p>	CPJ
26 January 2026	India	<p>Southeast Asian cybercrime syndicates parking ‘digital arrest’ money in bogus bank accounts in India</p> <p>“BHOPAL: Bank accounts opened in the names of business firms/NGOs existing only on paper or in the names of individuals projecting as officials of bogus firms are being used to park proceeds of cybercrimes committed against Indians by gangs operating from Southeast Asia.</p> <p>A multi-layered international cybercrime racket being run from Cambodia recently used the services of multiple inter-state rings involved in opening and providing mule accounts to park Rs 1.34 crore extorted from a retired professor and wife from Ratlam district of Madhya Pradesh, by placing them under digital arrest for 28 long days.”</p>	New Indian Express
26 January 2026	Germany	<p>On trial for multi-million euro fraud: Bamberg Cybercrime Unit files charges against gang leaders</p> <p>Bamberg – Internet criminals rake in billions of euros every year in Bavaria. But investigators are hot on their trail, as a new indictment shows. Specialists from the Bamberg Cybercrime Unit (ZCB) have brought two individuals responsible for the fraudulent investment platform GetFinancial to court. They are accused of having held senior positions for a globally operating organization for years. One of the perpetrators is alleged to have caused €5.1 million in damages.</p>	TZ