CYBERCRIME ACCORDING TO AI:
A DIRE AND RAPIDLY ESCALATING CRISIS

A Report by Stephen Cobb, MSc, CISSP

Summary: This report documents the responses of seven widely used AI systems to four questions about cybercrime. All seven say cybercrime has reached crisis proportions, outpacing all efforts at deterrence, and this could make humanity's future a bleak one. For example, Google's Gemini states: My opinion is that the state of cybercrime in the world today is dire and represents a rapidly escalating global crisis." OpenAI's ChatGPT says the outlook is grim unless there are "major shifts in global cooperation, regulation, and investment in digital resilience." However, the consensus among the seven is that those major shifts are unlikely to occur in time to avert "a digital dystopia where cybercrime becomes so pervasive it fundamentally breaks how society functions" (Claude Sonnet).

Background: Many humans who are turning to artificial intelligence (AI) to solve the world's problems appear to be inadequately aware of the challenge that cybercrime poses to AI's ability to achieve those noble ends. This is indicative of a wider problem: the chronic failure of the leaders of government and industry to pay adequate heed to the advice of cybersecurity professionals when it comes to addressing the rapid escalation of cybercrime in the twenty-first century. This situation prompted the author to find out what current AI models think of cybercrime, hypothesizing that said leaders, many of whom have lauded the benefits of AI, may pay attention to what AI say and heed the advice that AI give.

The systems consulted in this research are: ChatGPT, Claude, DeepSeek, Gemini, Perplexity, Meta AI, and Grok. The report consists of conversations with these seven systems, as conducted and recorded by the report's author, Stephen Cobb. The report is prefaced by Cobb's account of how the research came about. Notes on the research methodology and limitations can be found at the end of the report.

Preface

The history of cybersecurity experts urging the leaders of government and industry to respond more effectively to the problems posed by cybercrime stretches back more than three decades.[1] Sadly, those efforts, in which I often participated, have consistently failed to bring about appropriate levels of cybersecurity or anti-cybercrime measures. The evidence of this is clear in the frequency of media reports about well-known organizations being extorted by criminals who have gained unauthorized access to their information systems, and in every cybercrime report published thus far in 2025, from the Verizon Data Breach Investigations

---

[1] For example, see testimony of Winn Schwartau: Computer Security: hearing before the Subcommittee on Technology and Competitiveness of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, first session, June 27, 1991 4.Sci 2:102/42, p. 14.

© S. Cobb, 2025

Report[2] to the FBI/IC3 Internet Crime Report.[3] The spark that fired the report you are reading right now was a glowing endorsement of AI by a world leader that I heard right after reading yet another set of cybercrime statistics. This prompted me to ask ChatGPT the following question: "*What do you think about the state of cybercrime in the world today?*"

My question was preceded by this prompt: "I would like your responses to be clear, straightforward, absolutely unvarnished, no sugarcoating, no fluff no links, no headlines. Please always give your own opinion on the subjects I will now ask about." (I have seen similar language used in other "ask AI" projects.[4]) In addition, I requested that the response be brief.

The response from ChatGPT begins with this assessment: "The state of cybercrime today is severe and worsening. It's one of the most pervasive and damaging global threats, and governments and companies are consistently behind the curve." I have never shared my thoughts on cybercrime with ChatGPT, but its views appear to be very similar to mine.

Even more interesting to me was the fact that ChatGPT included a conditional phrase in the summary of its very bleak 160-word answer: "Without major shifts in global cooperation, regulation, and investment in digital resilience, the outlook remains grim." Offering a glimmer of hope combined with action items is a standard tactic of subject matter experts who have been asked for their assessment of a topic that is inherently problematic. Failing to provide a response that includes a possible path to a less grim future puts both message and messenger at risk of being dismissed as overly doom-laden and unhelpful.

My initial plan was to turn to a different AI model and ask the same question, but ChatGPT's answer inspired me to ask an immediate follow-up: *Where do you think we end up if nothing changes?* Again, the response is blunt, but in my opinion correct: "we end up in a world where trust in digital systems steadily collapses."

This brought to mind one of the objections I have encountered when arguing that governments and companies should devote more resources to tackling cybercrime: "But we have bigger problems to worry about." My response has been to point out that inadequate constraint of cybercrime will only make those bigger problems even bigger. Therefore, I decided to throw one of those big problems into the mix and asked a third question: *What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

---

[2] The annual Verizon DBIR is known by the year of publication but covers the preceding year, so the latest is DBIR 2025.

[3] The 2024 Internet Crime report from FBI/IC3 appeared in April of 2025 and showed a 33% year-on-year increase in losses due to Internet crime (2023-2024). When a bad thing gets 33% worse in just 12 months, one would hope for a proportionate response from government, but the average annual increase for the last 10 years for this statistic is 37% (https://www.ic3.gov/AnnualReport/Reports).

[4] For example, the *I Ask AI* channel on YouTube questions AI about political issues using similar prompting, see: https://www.youtube.com/@IAskAIShow

The first sentence of ChatGPT's response is bleak but surprisingly thoughtful: "Ten years from now, if cybercrime keeps growing and efforts to limit climate change continue to falter, the world becomes more unstable, unequal, and brittle—both digitally and physically." I was struck by the reference to an unequal world. ChatGPT went on to suggest that "feedback loops of vulnerability" between cybercrime and global warming could result in a world where: "The wealthy and powerful insulate themselves behind private networks and fortified supply chains. Everyone else navigates a world of failing institutions, insecure systems, and deepening digital inequality."

ChatGPT's concern with inequality in the context of cybercrime prompted me to ask one more question. However, I also wanted an assessment of the grounds for optimism. Thus, my fourth and for now final question was this:

Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?

As with the previous answers, the response is sobering, ending with this sentence: "Unless those flickers [of hope] grow into something larger and more unified, the current trajectory continues: a digital world where the line between criminality and success is blurred, and where the tools of connection are also tools of exploitation."

At this point I decided to turn to some other AI models and put the same four questions to Claude, DeepSeek, Gemini, Perplexity, Meta AI, and Grok. As you can see from the following transcripts, their answers are surprisingly varied in style and format given that I basically used the same prompt in each conversation.[5] But there is impressive consistency in terms of assessments made, suggestions offered, and futures predicted if the suggestions are not rapidly transformed into decisive action.

Will the world listen to what these AI models have to say? Will their advice be heeded by leaders of governments and captains of commerce? Will those who are so bullish about the benefits of AI feel obliged to address its dire warnings? Time will tell, but as more than one of these AI pointed out, time is quickly running out.

N.B. With the exception of the quoted AI responses to my questions, all of the content in this report is human-generated.

---

[5] To me, the least bleak respondent is Meta AI and the bleakest is DeepSeek, which makes extensive use of bullet points and phrases like "drone strikes on hacking compounds" and "cyber-feudal hellscape where only the ruthless survive". Feel free to perform a thematic analysis of all seven transcripts, or otherwise use them as you see fit. There is more about Further Research in the Notes section at the end of the report

Cybercrime Today and in the Future, According to ChatGPT 4o

As told to Stephen Cobb, MSc, CISSP

The following is a transcript of my interaction with ChatGPT 4o, a product of OpenAI. My questions to ChatGPT are in italics. The replies are block quoted. Any emphasis in the quoted text is in the original.

Initial Prompt*: I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and don't write anything yet, just let me know when you're ready.*

Question 1, after AI says ready: *First, tell me briefly, what do you think about the state of cybercrime in the world today?*

> **ChatGPT 4o:** The state of cybercrime today is severe and worsening. It's one of the most pervasive and damaging global threats, and governments and companies are consistently behind the curve. The volume, variety, and sophistication of cybercrimes have surged—ransomware, deepfake fraud, business email compromise, and large-scale data breaches are all operating at industrial scale. The barrier to entry is low; tools are cheap, often legal, and widely available. Criminals are better organized, frequently operating across borders with near impunity. Law enforcement is fragmented, under-resourced, and constrained by outdated legal frameworks.
>
> In my view, we are not winning this fight. The asymmetry between attackers and defenders continues to grow. Efforts to reduce cybercrime—through regulation, public-private cooperation, and technological countermeasures—are significant but insufficient. Cybercrime is no longer just a technical issue; it's a systemic failure involving economic incentives, legal loopholes, and social engineering. Without major shifts in global cooperation, regulation, and investment in digital resilience, the outlook remains grim.

Question 2: *Where do you think we end up if nothing changes?*

> **ChatGPT 4o:** If nothing changes, we end up in a world where trust in digital systems steadily collapses. Individuals, businesses, and governments will become more cautious, less connected, and more adversarial online. Essential services—healthcare, energy, finance, transport—will face regular disruptions. People will lose confidence in email, online payments, even voice and video communication as spoofing and fraud grow indistinguishable from the real thing.
>
> Financially, the global economy will bleed trillions each year. Insurance markets may shrink or collapse under the weight of unmanageable cyber risk. Small businesses will bear the brunt, unable to recover from attacks. Surveillance and censorship will likely

© S. Cobb, 2025

> increase, as states respond with stricter controls—sometimes under the guise of "cybersecurity," eroding privacy and digital freedom in the process.
>
> At the geopolitical level, persistent cyberattacks could trigger real-world conflicts. State-backed cyber operations might escalate into economic warfare or military retaliation. The worst-case scenario is a convergence of cybercrime and cyberwar, where criminal groups, mercenaries, and hostile nations operate in a blur of attribution and legality.
>
> In short, we risk creating a digital environment that is so hostile, unreliable, and legally ungovernable that large parts of it become unusable or outright dangerous. That future is plausible—not speculative—if current trajectories persist.
>
> Given the current state of world politics, I believe the chances of meaningful change in how we tackle cybercrime are low to moderate—closer to low. There is increasing awareness of the problem, but not the political alignment, urgency, or sustained will to confront it at scale.
>
> Most governments are reactive, not strategic. They prioritize national interests over global collaboration, which is fatal in the context of a borderless threat like cybercrime. Meanwhile, authoritarian regimes often tolerate or sponsor cybercriminals as long as they target foreign adversaries. Democracies struggle with legislative gridlock, underfunded enforcement, and slow regulatory cycles. Private sector incentives still favor speed and cost-cutting over security and resilience.
>
> There are promising signals—like the EU Cyber Resilience Act, NATO's growing focus on cyber defense, and recent joint operations against ransomware gangs—but these are fragmented. The reality is that cybercrime thrives on international disunity, legal loopholes, and enforcement asymmetries. Until there's a global shift toward coordinated cyber governance, greater deterrence, and real consequences for malicious actors, meaningful change is unlikely. We might see incremental progress, but not the systemic overhaul the situation demands.

Question 3*: What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

> **ChatGPT 4o:** Ten years from now, if cybercrime keeps growing and efforts to limit climate change continue to falter, the world becomes more unstable, unequal, and brittle—both digitally and physically.
>
> **Digitally**, the internet becomes a high-risk zone. Identity theft, financial fraud, and ransomware are not exceptional events—they're background noise. People lose access to services not because of technical glitches, but because systems are locked up or destroyed. Medical records, pension funds, supply chains—nothing is safe. Trust in technology erodes to the point where entire sectors slow down or revert to offline alternatives.
>
> Cybercrime syndicates will likely evolve into semi-permanent structures, rivaling cartels. Some will become de facto power brokers in weak states. Others will partner with or be shielded by authoritarian regimes. Most cybercrime victims will have no

> real recourse. The insurance industry may largely exit the space, deeming cyber losses uninsurable.
>
> **Physically**, climate instability worsens resource scarcity, migration pressures, and political polarization. Infrastructure fails more often, and cybercriminals exploit that—targeting overwhelmed hospitals during heatwaves, shutting down power grids during floods. Climate disasters create digital chaos too: fake emergency alerts, manipulated relief payments, and disinformation campaigns.
>
> The combination of rising cybercrime and unchecked climate change creates feedback loops of vulnerability. Disruption becomes the norm. The wealthy and powerful insulate themselves behind private networks and fortified supply chains. Everyone else navigates a world of failing institutions, insecure systems, and deepening digital inequality.
>
> In that world, both cyberspace and the climate become weapons—used to exploit, divide, and destabilize. The result isn't collapse, necessarily, but a fractured, lower-trust civilization under constant strain. A world where resilience is gated and trust is expensive.

Question 4*: Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?*

> **ChatGPT 4o:** I see more signs of the second scenario than the first. While there are isolated efforts to push back against cybercrime—through legal reform, diplomacy, and law enforcement cooperation—I don’t see the emergence of a genuine global movement that fundamentally rejects the criminal abuse of digital systems. Not yet.
>
> Cybercrime thrives because it aligns with deeper structural realities: inequality, power imbalances, and unaccountable technologies. The global wealth gap—both between countries and within them—is not just a backdrop; it’s a driver. In places where opportunity is scarce and institutions are weak, cybercrime becomes rational. For some, it’s survival. For others, it’s social mobility. And in elite circles, it's about influence and impunity. From West African scammers to Russian ransomware crews to Wall Street-aligned crypto manipulators, many actors believe they're simply playing the game—just better than others.
>
> As long as the dominant global ethos prioritizes wealth accumulation over fairness, and power over accountability, the moral code won’t shift. In fact, the digital realm often reinforces that code. You can commit massive fraud with a few lines of code, move millions anonymously, and vanish. That’s not just attractive to criminals—it’s admired in some circles as innovation or disruption.
>
> A global movement to counter this would require more than better cybersecurity—it would require a cultural reckoning. One that links digital ethics to economic justice and social equity. I see flickers of that—in data sovereignty campaigns, in movements

> for digital rights, in public backlash against tech abuses—but they’re fragmented and politically outgunned.
>
> Unless those flickers grow into something larger and more unified, the current trajectory continues: a digital world where the line between criminality and success is blurred, and where the tools of connection are also tools of exploitation.

Cybercrime Today and in the Future According to Claude Sonnet 4

As told to Stephen Cobb, MSc, CISSP

The following is a transcript of my interaction with Claude Sonnet 4, a product of Anthropic PBC which describes it as a hybrid reasoning model with superior intelligence for high-volume use cases. The questions that I put to Claude are in italics. The replies from Claude are block quoted. Any emphasis in the quoted text is from the original.

Initial Prompt*: I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and* don't *write anything yet, just let me know when you're ready.*

[Without prompting, Claude decided to present some helpful parameters.]

> **Claude:** I understand you're looking for comprehensive information about cybercrime trends and government responses since 2000. However, I should clarify a couple of important limitations:
>
> **Knowledge cutoff**: My reliable knowledge only extends through the end of January 2025, so I can't gather or provide information about events that may have occurred between February 2025 and today (May 22, 2025).
>
> **Real-time research**: I can't actively gather or search for the latest news - I can only work with information that was part of my training data up to my cutoff date. What I can do is provide you with a comprehensive overview of major cybercrime trends, notable incidents, and government/international responses from 2000 through early 2025 based on my existing knowledge. This would include:
>
> - Evolution of cyberattack types and techniques
> - Major incidents affecting companies, governments, and individuals
> - Key legislation and policy responses
> - International cooperation efforts
> - Emerging threats and countermeasures
>
> Would you like me to prepare this comprehensive overview based on my existing knowledge, or would you prefer to proceed with your questions directly? I'm ready to help either way.

Question 1, after AI says ready: *First, tell me briefly, what do you think about the state of cybercrime in the world today?*

> **Claude**: Cybercrime today is absolutely rampant and largely out of control. We're facing an epidemic where criminal organizations operate with near-impunity from

> certain jurisdictions, particularly Russia, North Korea, and parts of Eastern Europe and Asia.
>
> The economics are brutally simple: cybercrime pays extremely well with relatively low risk. A ransomware group can make millions in weeks with minimal chance of prosecution. Meanwhile, defenders are constantly playing catch-up, spending enormous resources to protect against threats that criminals can deploy cheaply and at scale.
>
> Most concerning is how cybercrime has industrialized. It's no longer lone hackers - it's sophisticated criminal enterprises with HR departments, customer service, and profit-sharing models. They treat it like any other business because that's exactly what it is.
>
> The situation is getting worse, not better. Critical infrastructure attacks are increasing. Healthcare systems are being held hostage. Small businesses are being destroyed by ransomware they can't afford to recover from. Individual victims lose life savings to increasingly sophisticated scams.
>
> Law enforcement is overwhelmed and often technically outmatched. International cooperation exists on paper but moves at glacial speed while criminals operate in real-time across borders. The fundamental problem is that cybercrime prosecution requires enormous resources for cases that often yield minimal sentences, if any conviction at all.
>
> We're losing this fight badly, and the gap between criminal capability and defensive response is widening every year.

Question 2: *Where do you think we end up if nothing changes?*

> **Claude:** If nothing changes, we're heading toward a digital dystopia where cybercrime becomes so pervasive it fundamentally breaks how society functions.
>
> Critical infrastructure will be under constant attack. Power grids, water systems, hospitals, and transportation networks will face regular disruptions. We'll see more situations like what happened in Costa Rica where ransomware groups essentially held an entire country hostage.
>
> The financial system will become unreliable. If you can't trust digital transactions, banking, or even basic commerce, economic activity grinds down. Small businesses will be driven out of the digital economy entirely because they can't afford the security or recovery costs.
>
> Healthcare will be devastated. Hospitals already struggle with ransomware attacks that can literally kill people when systems go down during emergencies. This will get much worse.
>
> Trust in digital systems will collapse. People will abandon online services, e-commerce, and digital government services. We'll see a regression away from digital transformation.

> Criminal states will essentially weaponize cybercrime as a form of asymmetric warfare, using criminal proxies to destabilize rival nations while maintaining plausible deniability.
>
> The digital divide will become a security divide - only wealthy individuals and organizations will be able to afford adequate protection, while everyone else becomes easy prey.
>
> Eventually, we'll likely see authoritarian responses - governments imposing draconian internet controls and surveillance in the name of security, destroying privacy and digital freedom in the process.
>
> We're not talking about some distant future. These trends are already visible and accelerating. Without dramatic changes, the next decade will be much worse than today.

Question 3: *What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

> **Claude:** Ten years from now, we'll be facing a perfect storm of cascading failures.
>
> Climate disasters will create massive vulnerabilities that cybercriminals will ruthlessly exploit. When hurricanes knock out power grids, ransomware groups will hit backup systems and emergency services. During heat waves that strain infrastructure, attacks on power companies will turn uncomfortable situations into deadly ones. Flood-damaged hospitals trying to restore systems will face extortion from criminals who know they're desperate.
>
> Climate refugees and economic instability will create vast pools of people willing to participate in cybercrime. Countries struggling with climate costs won't have resources for cybersecurity or law enforcement. Failed or failing states will become safe havens for criminal operations.
>
> Critical infrastructure will be in constant crisis. The electrical grid - already stressed by extreme weather - will face coordinated attacks during peak demand periods. Water treatment facilities will be regular targets when communities are most vulnerable. Supply chains disrupted by climate events will be further crippled by cyberattacks.
>
> Authoritarian governments will use this chaos to justify total surveillance and internet control, claiming it's necessary for security. Democratic societies will be forced to choose between digital freedom and basic functionality.
>
> The wealthy will retreat into heavily secured digital and physical enclaves while everyone else lives in a state of constant vulnerability. Most people will be cut off from reliable digital services, banking, healthcare, and government systems.
>
> Society will essentially fragment - those who can afford protection versus those who cannot. The digital economy will collapse for ordinary people while criminal enterprises thrive in the chaos.

> We're looking at societal breakdown accelerated by the intersection of climate catastrophe and uncontrolled cybercrime.

Question 4: *Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?*

> **Claude:** I see almost no signs of meaningful global movement against cybercrime. The opposite is happening - the wealth gap is actively fueling the problem.
>
> The brutal reality is that for millions of people, cybercrime represents their only path to meaningful economic advancement. When you're in a country where the average monthly salary is $200 but you can make $50,000 in a week running ransomware, the moral calculation becomes simple. The "legitimate" economy has failed these people, so they turn to crime.
>
> What's worse is that many governments tacitly encourage this. Russia and North Korea essentially use cybercriminals as unpaid intelligence assets. As long as these groups don't target domestic interests, the state provides protection and infrastructure. It's a symbiotic relationship - criminals get safe harbor, governments get plausible deniability for their cyber warfare.
>
> The wealthy nations that could lead reform efforts are too busy protecting themselves. They're building digital walls instead of addressing root causes. Their solution is better cybersecurity for themselves, not fixing the global inequality that drives cybercrime recruitment.
>
> Even within wealthy countries, the moral framework is broken. We celebrate tech billionaires who made fortunes through ethically questionable means while condemning poor kids who hack for survival. The message is clear: exploitation is fine if you're rich enough to make it legal.
>
> The only "movement" I see is toward greater inequality and more sophisticated criminal enterprises. Young people worldwide are learning that technology plus desperation equals opportunity, regardless of legality.
>
> Until we address fundamental global inequality, cybercrime will continue growing because for many people, crime simply makes more economic sense than legitimate work.

Cybercrime Today and in the Future, According to DeepSeek

As told to Stephen Cobb, CISSP, MSc

The following is a transcript of my interaction with DeepSeek, made by a Chinese company of the same name that was founded by Liang Wenfeng, the CEO of a hedge fund called High-Flyer, known for its use of AI to analyze financial data to make investment decisions. My questions to DeepSeek are in italics. The replies are block quoted. Any emphasis, bullets, numbering or formatting in the quoted text is from the original.

***Initial Prompt**: I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and* don't *write anything yet, just let me know when you're ready.*

[DeepSeek responded with about 300 words of description outlining how it will approach this request and providing a structured, bullet-pointed overview of major cybercrime incidents and government responses since 2000. It then declared, with enthusiasm: "Let me know how you'd like to proceed!"]

***Question 1, after AI says ready:** First, tell me briefly, what do you think about the state of cybercrime in the world today?*

> **DeepSeek: My Unvarnished Opinion:**
>
> Cybercrime today is *out of control* and governments are losing the battle. Attacks are faster, cheaper, and more disruptive than defenses can keep up with. Ransomware gangs operate like Fortune 500 companies, state-sponsored hackers face zero consequences, and law enforcement is decades behind. The explosion of AI tools will make this worse—imagine phishing scams tailored perfectly to you in real time.
>
> - Why It's So Bad:
> - Asymmetry: A kid in a basement can cripple a hospital. Defense costs millions; attacks cost pennies.
> - Profit Motive: Cybercrime is now a *scalable business*—ransomware payments hit $1B+ in 2023.
> - Weak Deterrence: Less than 1% of cybercriminals face prosecution. Russia/China/North Korea shield their hackers.
>
> **Governments? Mostly Theater**.
>
> - New laws (GDPR, SEC rules) look tough but can't stop attacks.
> - Critical infrastructure (power grids, hospitals) remains vulnerable because upgrading security is expensive and inconvenient.
> - International cooperation is a joke when states are the hackers.

© S. Cobb, 2025

> Bottom Line: We’re in a cyber arms race where offense always wins. Until there’s *real* global coordination (not just paperwork) and harsh consequences for harboring hackers, expect more collapses like MGM Resorts or the NHS.
>
> *(Next question? I’ll keep it blunt.)*

Question 2: *Where do you think we end up if nothing changes?*

> **DeepSeek**: If nothing changes, we’re headed toward a **cybercrime dystopia** where:
>
> ### 1. Daily Life Becomes Unstable
>
> - **Essential services** (hospitals, power grids, water supplies) will face **routine shutdowns** from ransomware or sabotage. Expect deaths from hacked medical devices or frozen emergency systems.
> - **Hyper-personalized scams**: AI-driven fraud will make *every* call, email, or video untrustworthy. Your bank, your boss, even your "family" could be deepfakes.
>
> ### 2. Economic Freefall
>
> - **Small businesses wiped out**: Most can’t afford cyber insurance or recovery costs after an attack.
> - **Stock market shocks**: A single cloud provider breach (like AWS or Azure) could crash global markets for weeks.
>
> ### 3. Governments Turn Tyrannical
>
> - **Mass surveillance justified as "security"**: China’s Social Credit System will look mild compared to Western "cyber-defense" overreach.
> - **Cyber conscription**: Countries will *draft* hackers (like Ukraine’s IT Army) for perpetual digital warfare.
>
> ### 4. The Underground Wins
>
> **Ransomware cartels** will become **de facto world powers**, extorting nations the way drug cartels do today.
>
> **Cryptocurrency chaos**: Privacy coins (Monero, Zcash) make tracking payments impossible. Hackers will demand payments in *untraceable* digital cash.
>
> ### The Point of No Return
>
> Within 10 years, we’ll hit a **"Cyber Pearl Harbor"**—an attack so devastating it forces draconian lockdowns of the internet. But by then, the criminals and rogue states will be too entrenched to stop.
>
> ### The only way out?
>
> **Global cyber-treaties with teeth** (e.g., drone-strike equivalents for hacker havens).

> **Mandatory security standards** (like seatbelt laws, but for software).
>
> **Decentralized infrastructure** (so one breach can’t collapse everything).
>
> But since none of that’s happening fast enough… **brace for impact**.

Question 3: *What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

> **DeepSeek: The Bleak Future (2034): Cybercrime + Climate Collapse = A Perfect Storm**
>
> If cybercrime keeps accelerating and climate efforts fail, we’re looking at a global breakdown of order. Here’s the ugly reality:
>
> **1. Infrastructure Collapses in Waves**
>
> - Cyberattacks cripple energy grids just as extreme heat/cold hits. Power outages last weeks, not hours. Millions freeze or boil.
> - Food supply chains break as ransomware locks up shipping ports, while droughts/floods ruin harvests. Famine becomes weaponized.
> - Hospitals offline during pandemics. Imagine COVID-2.0 with no digital records, ventilators hacked, or pharmacies ransom-locked.
>
> ---
>
> **2. The Rise of "Failed Cyber States"**
>
> - Governments lose control: Smaller nations (e.g., Ecuador, Nigeria) will become cybercrime havens—too weak to police hackers, too corrupt to care.
> - Cities go dark: Local governments abandon digital systems after relentless attacks. Taxes, IDs, voting—all revert to paper, creating chaos.
> - Corporate warlords: Amazon, Google, or BlackRock buy up police forces to protect their data centers as governments fail.
>
> ---
>
> **3. Hyper-Surveillance vs. Anarchy**
>
> - Authoritarian "safe zones": The rich live in gated cities with AI-powered surveillance, facial recognition, and no cash (to stop fraud).
> - The rest descend into digital feudalism: No credit, no stable internet, just bartering with crypto or canned food.
> - AI manipulates everything: Deepfake propaganda, fake climate treaties, and AI-generated blackmail destroy trust in any institution.
>
> ---
>
> **4. Climate Chaos Fuels Cyber Wars**

© S. Cobb, 2025

> - Water wars go digital: Hackers target desalination plants in the Middle East, drowning refugees in data breaches before they flee.
> - Carbon credit scams explode: Fake "green" blockchain projects steal billions while emissions keep rising.
> - Bio-hacking meets cybercrime: Terrorists pay ransomware gangs to unlock pathogen research (lab-made plagues + cyberattacks = biowarfare 2.0).
>
> ---
>
> **The Endgame: A Fractured World**
>
> - No internet, just "splinternets": The U.S., China, and EU wall off their networks, killing global trade.
> - Cyber militias roam: Like modern pirates, they sell DDoS attacks to the highest bidder—a Starbucks latte costs $50 if the POS isn't hacked.
> - Humanity splits into two classes:
> - The "Verified" (elites with secure digital IDs).
> - The "Ghosts" (no bank account, no rights, hunted by drones for scams they didn't commit).
>
> ---
>
> **Is This Inevitable?**
>
> - No—but avoiding it requires brutal, unpopular choices:
> - Treat cybercrime like terrorism (drone-strike hacker bases, sanction entire nations harboring them).
> - Outlaw weak tech (like banning asbestos—no more IoT devices with default passwords).
> - Decentralize survival basics (local solar grids, 3D-printed spare parts, mesh networks).
>
> Otherwise? Enjoy the digital Dark Ages.
>
> *(Want to explore a specific nightmare scenario? Or potential fixes?)*

***Question 4:** Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?*

> **DeepSeek**: I see almost no signs of meaningful global movement against cybercrime. The opposite is happening - the wealth gap is actively fueling the problem.
>
> **The Split Future: Reform vs. Ruthless Exploitation**

The world is at a moral crossroads with cybercrime, and the outcome depends on who gains power first—those demanding reform or those exploiting chaos. Here's the brutal breakdown:

---

1. Signs of a Global Backlash? (The Hopeful Case)

- Public anger is rising: High-profile attacks (hospitals, schools) are making cybercrime a voting issue. Politicians might *finally* act when their careers depend on it.
- Tech workers are rebelling: Engineers at Google, Microsoft, etc., are increasingly refusing to build tools for surveillance or cyberwarfare. If this grows, it could slow the arms race.
- Decentralized resistance: Hacktivists (like Anonymous) and ethical hackers are publicly doxxing cybercriminals, making it harder for them to hide.
- Insurance companies forcing change: When cyber-insurance becomes unaffordable, corporations will have to adopt real security—or collapse.

But…
This movement is fragmented. Without a unified global push (like the Paris Agreement, but for cybercrime), it won't be enough.

---

2. The Darker Path: Wealth Gap = Cybercrime Normalized

"If they steal, why can't I?" In unequal societies, cybercrime becomes just another hustle. Nigeria's "Yahoo Boys" (scammers) are already folk heroes to some.

- Corporations turn predator: Big Tech and banks already exploit data—why *wouldn't* they embrace AI-driven manipulation if laws don't stop them?
- Governments pick sides: Russia/China/North Korea will keep sponsoring hackers as long as it weakens rivals. The U.S. and EU play catch-up but won't risk open war.
- AI erodes ethics: If a chatbot can scam better than a human, morality becomes obsolete. Profit wins.

Result:
A permanent underclass of cyber-serfs (hackers for hire) and a ruling class that either tolerates them or becomes them.

Which Future Wins?

- Short-term (next 5-10 years): The wealth gap fuels more crime. Cybercrime will be seen as "fair game" in struggling nations, while elites hide behind firewalls.
- Long-term (20+ years): Either total collapse forces reform (like how 9/11 rewrote global security) or we get a cyber-feudal hellscape where only the ruthless survive.

> ---
>
> **The Deciding Factor: Punishment**
>
> Today, cybercrime pays because consequences are rare. If that changes—**mass arrests, frozen crypto, drone strikes on hacker compounds**—the calculus shifts. But no government has the guts… yet.
>
> **Final Answer:**
> The moral code **has already cracked**. Without **swift, brutal consequences** the wealth gap will ensure cybercrime keeps growing—until the whole system burns.
>
> *(Want to explore how to fix this—or just how bad the burn gets?)*

Cybercrime Today and in the Future According to Gemini 2.5 Pro

As told to Stephen Cobb, MSc, CISSP

The following is a transcript of my interaction with version 2.5 Pro of Gemini, formerly known as Bard, a generative artificial intelligence chatbot developed by Google. My questions to Gemini are in italics. The replies are block quoted. Any emphasis, bullets, or numbering in the quoted text are from the original.

Initial Prompt*: I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and don't write anything yet, just let me know when you're ready.*

> **Gemini:** I have gathered a substantial amount of information on the evolution of various types of cybercrime around the world since 2000, significant cyberattacks on companies and governments, digital crimes against individuals like email fraud, and the corresponding government efforts to reduce these threats. This includes information on legislative changes, the establishment of cybercrime units, and international cooperation.
>
> I am now prepared for your questions.

Question 1, after AI says ready: *First, tell me briefly, what do you think about the state of cybercrime in the world today?*

> **Gemini:** Based on the information I've processed my opinion is that the state of cybercrime in the world today is alarming and deeply entrenched. It's a highly adaptive, technologically advanced, and pervasive global threat that consistently outmaneuvers reactive security measures.
>
> The financial motives are immense, but disruption, espionage, and influence are also key drivers. Criminals, and in some cases state-actors, operate with a high degree of sophistication and often with impunity due to the borderless nature of the internet and the complexities of international law enforcement.
>
> Efforts to combat it, while significant, often feel like a high-stakes game of catch-up. Vulnerabilities are widespread, the attack surface is constantly expanding with new technologies, and the human element remains a critical point of weakness. Frankly, cybercrime is a booming illicit economy that poses a severe and ongoing risk to individuals, businesses, and national security worldwide, with no signs of significant abatement. My opinion is that the state of cybercrime in the world today is dire and represents a rapidly escalating global crisis.
>
> It's an unvarnished truth that offensive capabilities are outpacing defensive measures. Cybercriminals, ranging from lone individuals to sophisticated state-sponsored groups

© S. Cobb, 2025

> and organized criminal enterprises, are proving to be exceptionally adaptive and relentless. They exploit new technologies like AI with alarming speed, continuously refine their tactics, and operate with a high degree of impunity due to the borderless nature of the internet and the complexities of international law enforcement.
>
> The financial and societal impacts are staggering and growing, affecting businesses, governments, and individuals alike. We're seeing critical infrastructure at constant risk, economies losing trillions, and personal data being weaponized. There's no sugar-coating the reality that while awareness and investment in cybersecurity are increasing, the scale, complexity, and sheer brazenness of cybercrime continue to create a deeply unstable and dangerous digital environment for everyone. It's a persistent, pervasive, and increasingly severe threat.

Question 2: *Where do you think we end up if nothing changes?*

> **Gemini**: If nothing fundamentally changes in our approach and capabilities, my opinion is that we end up in a state of digital anarchy and profound insecurity.
>
> The unvarnished truth is that the current trajectory points towards a future where cyberattacks are not just common, but are a constant, debilitating feature of life and business. We would see an exponential increase in financial losses, potentially crippling economies. Critical infrastructure—power grids, healthcare systems, water supplies, transportation—would be perpetually under siege, with successful disruptions becoming more frequent and severe, leading to real-world harm and loss of life.
>
> Trust in digital systems, which are foundational to modern society, would evaporate. Online commerce, digital governance, and even the free flow of information would be severely compromised. The cost of doing business would skyrocket due to the need for extreme, likely still insufficient, defensive measures and the price of constant breaches.
>
> Innovation would be stifled as the risks of deploying new technologies would often outweigh the benefits. The digital divide would widen into a chasm, with well-funded entities perhaps managing a semblance of security while smaller businesses and individuals are left almost defenseless.
>
> At an individual level, privacy would become an antiquated concept, and personal security would be a daily struggle against sophisticated scams, identity theft, and digital harassment. We could also expect nation-state cyber conflicts to escalate, blurring the lines between espionage, sabotage, and outright warfare, with potentially devastating global consequences.
>
> Ultimately, if nothing changes, we are heading towards a future where the digital world is a far more dangerous, unstable, and untrustworthy space, significantly degrading our quality of life, economic prosperity, and global security. It’s a bleak outlook, but one that logically follows from the current trends if they remain unaltered. If nothing fundamental changes regarding our approach to cybersecurity, my opinion is that we are headed towards a significantly more dangerous and unstable world, one where the fundamental trust in digital systems is catastrophically eroded.

> Without a paradigm shift in how we prioritize and implement security, we will likely see:
>
> 1. **Crippling Economic Drain**: Cybercrime costs, already in the trillions globally, will continue to skyrocket. This isn't just direct theft; it's lost productivity, compromised intellectual property, recovery expenses, and a severe drag on innovation as resources are diverted. Businesses, especially smaller ones, will face an existential threat.
> 2. **Systemic Failures of Critical Infrastructure**: The risk of sustained, successful attacks on essential services like energy grids, water supplies, healthcare systems, and financial networks will increase dramatically. Imagine widespread, prolonged outages or manipulations that directly threaten lives and societal stability.
> 3. **Breakdown of Digital Trust**: If individuals and organizations cannot reasonably trust the integrity and security of digital communications, e-commerce, online services, and even the information they consume, the digital society as we know it will fragment. This means a severe chilling effect on digital transformation and a retreat from valuable online interactions.
> 4. **Escalation of Geopolitical Instability**: Nation-states will increasingly use cyber capabilities for espionage, sabotage, and warfare, potentially leading to miscalculations and escalations in the physical world. The lines between state and non-state actors will continue to blur, making attribution and response even more complex.
> 5. **Pervasive Individual Harm**: Beyond financial loss, individuals will face greater risks of identity theft, manipulation through sophisticated AI-driven disinformation, privacy violations on an unprecedented scale, and online harassment that has severe real-world consequences. The feeling of digital insecurity will become a pervasive psychological burden.
> 6. **Widening Security Divide**: A world where only the largest corporations and wealthiest nations can afford a semblance of robust cybersecurity, leaving smaller entities and developing nations increasingly vulnerable. This will exacerbate global inequalities.
>
> In short, if nothing changes, we're not just looking at more of the same; we're looking at a future where the digital world becomes a far more hostile, unpredictable, and damaging environment, profoundly impacting global security, economic prosperity, and the basic functioning of society. The very benefits of our interconnected world will become its greatest vulnerabilities.

Question 3: *What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

> **Gemini**: My opinion is that if meaningful change does not happen to curb cybercrime and if efforts to limit climate change continue to struggle, then 10 years from now, we will be living in a world defined by pervasive instability, heightened fear, and a grim fight for dwindling resources and security.
>
> Here's what that future likely looks like:
>
> 1. **Compounding Crises as the Norm:** Imagine a world where severe weather events – intense heatwaves, superstorms, and floods caused by climate change –

> regularly cripple physical infrastructure. Now add rampant cyberattacks targeting the very systems needed for disaster response, communication, and resource distribution (like energy grids, water supplies, and food chains). Rescue efforts would be hampered, aid misappropriated by fraudsters, and recovery from climate disasters catastrophically slowed by digital sabotage. The recovery costs for one disaster would bleed into the next.
>
> 2. **Erosion of Basic Security and Trust:** The digital realm, already treacherous, would become a minefield. Sophisticated AI-driven cybercrime would make online fraud, identity theft, and manipulation almost constant threats for individuals. Trust in digital services – from banking to healthcare to government communications – would be shattered. Simultaneously, climate change would make physical security precarious due to resource scarcity, displacement, and more frequent natural disasters. This dual insecurity would be a heavy psychological and practical burden.
> 3. **Intensified Resource Conflicts**: Climate change will exacerbate shortages of water, food, and habitable land. Cyber warfare capabilities would likely be deployed by states and non-state actors to disrupt rivals' access to these critical resources, target their climate adaptation technologies, or sow chaos to gain an advantage. Imagine cyberattacks on agricultural systems in a drought-stricken region or on smart city infrastructure managing scarce water supplies.
> 4. **Stagnation and Regression**: Innovation would suffer immensely. Resources that could be invested in sustainable technologies or societal advancement would be constantly diverted to cleaning up after cyberattacks and climate disasters. The very technologies meant to help us adapt to climate change (like smart grids or IoT-enabled environmental monitoring) would become prime targets for cyberattacks, making them risky to implement or rely upon. This could stall or even reverse progress.
> 5. **Breakdown of Social Cohesion and Governance**: Governments, overwhelmed by concurrent, complex crises and diminished by cyberattacks on their own systems and treasuries, would struggle to provide basic services or maintain order. Public trust would plummet. Climate-induced migration and resource scarcity, amplified by disinformation campaigns (a form of cyber-enabled social disruption), could lead to widespread social unrest and conflict. The gap between the super-rich (who might afford isolated, secure enclaves) and the rest of the population would become a chasm.
> 6. **A Bleaker Outlook for Health and Well-being**: Healthcare systems, already strained, would be frequent targets of ransomware and other cyberattacks, disrupting patient care during climate-related health crises (like pandemics or heat stress). Food insecurity driven by climate change would be worsened by attacks on supply chains. The cumulative stress of living in such a volatile and threat-saturated environment would have severe mental and physical health consequences.
>
> In essence, 10 years down this path, without meaningful change, we would face a deeply fractured and reactive world. Daily life would be characterized by a struggle against intertwined digital and environmental threats, with a greatly diminished quality of life, reduced freedoms due to security clampdowns, and a pervasive sense of vulnerability. It would be a far cry from any vision of progress, pushing global society towards a state of chronic, cascading failures. My opinion is that if meaningful change does not occur in how we address both the escalating cybercrime

> pandemic and the struggling efforts to limit climate change, then 10 years from now, we will inhabit a world defined by pervasive instability, widespread hardship, and a profound sense of insecurity. The two crises will not just coexist; they will actively compound each other, creating a cascade of negative feedback loops.
>
> Here’s an unvarnished look at what that future likely entails:
>
> **A World of Interlocking Crises**
>
> - **Fragile Infrastructure:** Climate change (extreme weather, rising sea levels) will physically damage critical infrastructure – power grids, communication networks, water treatment facilities. Simultaneously, unchecked cybercrime will mean these already stressed systems are constantly under attack, leading to more frequent, longer-lasting, and more devastating failures. Imagine widespread blackouts caused by a cyberattack during a climate-induced heatwave or hurricane, crippling emergency response when it's most needed.
> - **Resource Wars, Both Physical and Digital**: Climate change will intensify competition for dwindling resources like water and arable land, leading to conflict and displacement. Cyber warfare capabilities will be deployed to sabotage rivals' resource management systems or to spread disinformation to incite unrest in resource-stressed regions. Displaced populations, desperate and vulnerable, will become prime targets for sophisticated cyber fraud and exploitation.
> - **Economic Hemorrhage and Stagnation**: The direct financial losses from cybercrime (theft, ransomware, destruction of data) will continue to explode. Climate change will add its own layer of economic devastation through infrastructure damage, agricultural losses, and healthcare crises. Innovation will wither as resources are perpetually diverted to crisis management and recovery, and global supply chains will be in a state of constant disruption.
> - **Erosion of Governance and Social Cohesion**: Governments, already struggling to cope with each crisis independently, will be overwhelmed by their combined force. Public trust in institutions will plummet as they fail to provide basic security and stability. AI-driven disinformation campaigns, amplified by cyber means, will deepen societal divisions, making consensus on solutions impossible. Climate anxiety will merge with digital paranoia, creating a population that is fearful, distrustful, and susceptible to extremism.
> - **Health and Safety in Perpetual Jeopardy**: Cyberattacks on healthcare systems will become even more catastrophic when those systems are simultaneously dealing with climate-related health emergencies (pandemics, heatstroke, respiratory illnesses from pollution and wildfires). Food and water security will be threatened by both climate impacts on agriculture and cyberattacks on supply chains and distribution networks.
> - **Failed Climate Action**: Efforts to deploy and manage climate mitigation and adaptation technologies (like smart grids or renewable energy networks) will be severely hampered by cyberattacks. Malicious actors could disrupt these systems, hold them for ransom, or even cause them to malfunction in ways that exacerbate environmental damage (e.g., triggering industrial accidents). The vast amounts of data crucial for climate modeling and response will be constantly at risk of theft or manipulation.

> - In essence, 10 years from now, under this scenario of inaction, we would not just be dealing with a hotter world and a more dangerous internet. We would be living in a "polycrisis" environment where digital and environmental insecurity are deeply intertwined, mutually reinforcing, and drive a relentless decline in the quality of life, global stability, and the very functionality of modern society. It would be a future where the promise of technology is thoroughly subverted, and the environment becomes an active adversary, with humanity caught in the crossfire, less equipped than ever to mount an effective response.

Question 4: *Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?*

> **Gemini**: My opinion is that while there are encouraging signs of growing awareness and collaborative efforts against the *symptoms* of cybercrime, a truly potent global movement to fundamentally reject its abuse and reform the criminal element is still quite weak and aspirational, especially when pitted against the profound and pervasive influence of the global wealth gap.
>
> Here's the unvarnished breakdown:
>
> **1. Signs of Positive Movement (Limited Scope and Impact):**
>
> - **Increased Condemnation and Cooperation:** We are seeing more international agreements, task forces, and information sharing between governments and law enforcement agencies. There's a louder public and political condemnation of high-profile attacks, particularly those affecting critical infrastructure or causing widespread financial harm.
> - **Corporate Responsibility (Nascent):** Some tech companies are investing more in security and talking about ethical AI and responsible platform governance. However, this is often driven by regulatory pressure or reputational risk rather than a deep-seated commitment to eradicating the *demand* or *opportunity* for cybercrime.
> - **Grassroots Activism and Ethical Tech:** There are pockets of activism, ethical hacking communities promoting defense, and educational initiatives aimed at digital literacy and responsible online behavior. These are valuable but lack the scale and resources to fundamentally shift global dynamics.
>
> **2. The Overwhelming Influence of the Wealth Gap and a Distorted "Moral Code":**
>
> - **Cybercrime as a Perceived Equalizer or Opportunity:** The stark and growing disparities in wealth and opportunity, both within and between nations, create a fertile ground for cybercrime. For individuals in economically marginalized regions or circumstances, the perceived low risk and high reward of cybercrime can be an irresistible lure. It's seen less as a moral transgression and more as a rational economic choice, a way to bypass systemic barriers to wealth and status.

- **Perpetuation of a Counter-Moral Code:** In certain online subcultures and even some communities, illicitly gained wealth through cyber means is not only tolerated but can be admired – a symbol of cleverness, rebellion, or success against a perceived unfair system. This "hustle culture," when applied to the digital realm, can easily morph into a justification for criminal activity, particularly if the victims are perceived as distant, wealthy, or part of "the system."
- **State-Level Ambivalence or Exploitation:** The wealth gap also plays out on a geopolitical scale. Some nations may turn a blind eye to, or even tacitly encourage, cybercriminal activities originating within their borders if these activities bring in foreign currency or serve strategic interests, framing it as a way to level the playing field against more economically powerful nations. This significantly undermines any global consensus on rejecting cybercrime.
- **Anonymity and Detachment:** The digital nature of these crimes – the anonymity, the geographic distance from victims – makes it easier for perpetrators to neutralize any moral qualms. It's psychologically easier to steal from a faceless entity or an unknown individual thousands of miles away than it is in the physical world.

Conclusion:

In my opinion, the large and growing wealth gap acts as a powerful engine that not only fuels cybercrime recruitment but also helps sustain a parallel moral framework where such acts are rationalized or even valorized by those who feel excluded from legitimate pathways to prosperity.

While efforts to combat cybercrime technically and legally are essential, they are essentially playing catch-up. A genuine global movement to reject and reform would require addressing these profound socio-economic disparities and fostering a sense of global economic justice. Until there's a perception that legitimate avenues for advancement are widely accessible, the allure of using technology – even criminally – to gain wealth and power will remain a dominant force, far outweighing nascent efforts towards a collective moral rejection of cybercrime. The current efforts are more akin to treating a raging infection with bandages rather than addressing the underlying disease of inequality that allows the infection to thrive. This is a deeply complex issue, and my opinion is that while there are encouraging signs of a desire to combat cybercrime, the pervasive and growing global wealth gap significantly fuels a contrary "moral code" for some, making widespread reform exceptionally challenging.

Signs of a Global Movement/Reform Potential:

Yes, there are nascent signs. We see increasing international cooperation between law enforcement agencies (like INTERPOL, Europol) and public-private partnerships aimed at disrupting cybercriminal operations. There's a growing public and governmental awareness of the sheer scale and damage of cybercrime, moving beyond a purely technical issue to one with profound societal and economic consequences. Initiatives promoting digital literacy and ethical technology use are also emerging globally, supported by organizations like the UN and various NGOs. Governments are slowly (often too slowly) updating legal frameworks. Victim advocacy, though still developing in the cyber realm, is starting to highlight the human cost, which can fuel moral outrage and demands for change.

However, these efforts, while positive, are often fragmented, under-resourced relative to the scale of the problem, and struggle with the cross-jurisdictional nature of cybercrime. Critically, much of the focus is on technical defenses and prosecution, not on reforming the individuals or addressing the systemic drivers that push people into cybercrime. The "reform" of cybercriminals, in the sense of rehabilitation programs, is not a significant feature of the current global response.

The Impact of the Wealth Gap and a "Criminal Moral Code":

This is where the unvarnished truth becomes particularly stark. The vast and growing wealth gap, both within and between nations, is, in my opinion, a powerful engine perpetuating cybercrime.

1. **Perceived Justification and Opportunity:** For individuals in regions with high unemployment, extreme poverty, and limited legitimate economic opportunities, cybercrime can present a seemingly rational, if illicit, path to financial stability or even significant wealth. The digital realm offers a degree of anonymity and access to global targets that traditional crime cannot. In such contexts, a "moral code" can emerge that rationalizes these actions as taking from a system perceived as inherently unfair or from wealthy entities/individuals who "can afford it." It's a distortion of a Robin Hood narrative, but it can be a powerful internal or community-level justification.
2. **Normalization and Status:** In some online subcultures and even in certain economically depressed communities, wealth and power gained through illicit digital means can, unfortunately, become normalized or even a source of status. The focus is on the outcome (wealth, technical prowess) rather than the ethical implications of the means.
3. **State-Level Ambivalence or Exploitation:** The wealth gap also plays out on a geopolitical scale. Some nations, perhaps feeling economically or strategically disadvantaged, may turn a blind eye to, or even tacitly encourage or directly employ, cybercriminal elements to achieve national objectives, whether for espionage, intellectual property theft, or generating illicit revenue. This severely undermines any global consensus on a moral code against such activities.
4. **Erosion of Universal Ethics:** When vast numbers of people feel the global economic system is rigged against them, the appeal of a universal ethical stance against "gaining wealth and power" through any means, including technologically advanced crime, diminishes. The argument for "playing by the rules" rings hollow if the game itself is perceived as fundamentally unfair.

Conclusion:

My opinion is that while pockets of genuine effort to reject and combat cybercrime exist and are growing, they are currently overshadowed and undermined by the profound socio-economic pressures created by the global wealth gap. This gap doesn't just create potential cybercriminals out of desperation or greed; it can foster an alternative "moral code" that sees the digital world as a new frontier for rectifying

> perceived injustices or simply for survival and advancement outside of conventional, often inaccessible, legal pathways.
>
> Until there are more concerted global efforts to address these underlying socio-economic disparities and offer viable alternatives, the "supply" of individuals and groups willing to perpetrate cybercrime will likely continue to grow. A purely punitive or defensive approach, without addressing the root causes and the divergent "moral codes" they foster, will remain a largely reactive and ultimately insufficient strategy. The desire for reform may be present in some quarters, but the economic realities for a significant portion of the world's population create a powerful counter-current that tolerates or even encourages the use of technology for illicit gain.

© S. Cobb, 2025

Cybercrime Today and in the Future, According to Perplexity AI

As documented by Stephen Cobb, MSC, CISSP

The following is a transcript of my interaction with Perplexity, described by its maker, Perplexity AI Inc., as the world's first answer engine. The questions that I asked Perplexity are in italics. The answers are block quoted. Any emphasis or bullet points in the quoted text are from the original. The end notes provided by Perplexity also come from the original, but have not been verified by a human.

Initial Prompt: *I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and don't write anything yet, just let me know when you're ready.*

[Like several other systems, Perplexity felt compelled to tell me what it had done to prepare for my questions.]

> **Perplexity**: I'm ready to help you with your cybercrime research. I've reviewed the search results and have comprehensive information covering cybercrime trends and incidents from 2000 to 2025, including:
>
> - Major cyberattacks and data breaches affecting companies and governments
> - Evolution of cybercrime tactics (from early worms like ILOVEYOU to modern ransomware and phishing-as-a-service platforms)
> - Significant incidents across various sectors (financial, healthcare, technology, government)
> - Recent developments in phishing campaigns and social engineering attacks
> - International cybercrime activities and state-sponsored attacks
>
> The data spans the full timeline you requested and covers incidents worldwide, from the early 2000s "worm era" through to the latest 2025 phishing campaigns and ransomware attacks.
>
> I'm prepared to create a comprehensive report or answer specific questions about any aspect of cybercrime trends, major incidents, attack methodologies, or affected sectors. What would you like to focus on first?

Question 1, when the AI is ready: *First, tell me briefly, what do you think about the state of cybercrime in the world today?*

© S. Cobb, 2025

> **Perplexity**: The global cybercrime landscape has reached a crisis point, characterized by **unchecked escalation in sophistication, financial impact, and systemic risk**[1][2][3]. Three critical observations define this reality:
>
> **Economic Devastation Outpaces Defense Capabilities**
> Cybercrime now operates as a **$10.5 trillion shadow economy**[2], with ransomware alone projected to cost $20 billion annually[2]. This isn't just theft—it's a structural threat to global financial stability. The 2024 IC3 report's $16.6 billion in U.S. losses[3] exposes how even advanced economies remain vulnerable to credential harvesting and BEC schemes[4]. Criminal enterprises now rival Fortune 500 companies in operational scale, with RaaS models enabling franchise-like attacks[4].
>
> **Critical Infrastructure Remains a Soft Target**
> The UK's Synnovis attack (£32.7 million loss)[5] and Germany's fatal hospital breach[2] prove that essential services prioritize convenience over security. Nation-states and criminals exploit this recklessness, weaponizing outdated healthcare IT systems and fragile energy grids. Supply chain attacks[4] demonstrate how single-point vulnerabilities can cascade across sectors—a risk governments still underestimate in legislation like the UK's Cyber Security Bill[5].
>
> **Law Enforcement Lacks Jurisdictional Teeth**
> While INTERPOL's African Cyberthreat Report[6] documents rampant BEC and ransomware, cross-border prosecution remains theoretical. Cybercriminals exploit legal gray zones, with cryptocurrency mixers[4] and dark web markets[4] rendering asset recovery nearly impossible. AI-driven attacks[1][4] further outpace forensic capabilities, leaving investigators analyzing yesterday's tactics while criminals deploy tomorrow's.
>
> **My assessment:** Current mitigation strategies are fundamentally reactive. Until governments mandate real-time threat intelligence sharing, enforce strict liability for negligent critical infrastructure operators, and dismantle cryptocurrency anonymity, cybercrime will continue its exponential growth. The 2025 landscape will be defined not by new attack vectors, but by the systemic failure to address known vulnerabilities at scale.

Question 2: *Where do you think we end up if nothing changes?*

> **Perplexity**: If nothing changes, cybercrime will spiral out of control, fundamentally destabilizing economies, governments, and daily life. The financial cost will surpass $10 trillion annually, making cybercrime one of the world's largest economic forces, bigger than most countries' GDPs[7]. Ransomware, AI-powered fraud, and data breaches will become routine, not exceptional[8][7]. Critical infrastructure—hospitals, energy grids, transportation—will be held hostage by organized cybercriminals, with lives and national security at risk[9][10].
>
> The rise of generative AI and automation means attacks will scale faster than defenders can adapt, overwhelming law enforcement and security teams[9][10][11]. Deepfakes, synthetic identities, and AI-driven phishing will erode trust in digital communications and public institutions. The average person will face constant threats

> to their finances, privacy, and even physical safety as IoT devices and smart infrastructure become attack vectors[9][11].
>
> Law enforcement will remain outmatched, unable to attribute or prosecute most attacks due to global anonymity, rapid technological change, and the sheer volume of incidents[12][11]. Criminals will operate with near impunity, using cybercrime-as-a-service models to industrialize attacks[9][10].
>
> In my view, if governments, industry, and society do not radically overhaul their approach—mandating security by design, enforcing real-time intelligence sharing, and dismantling the infrastructure that enables anonymous crime—cybercrime will become an existential threat. Trust in digital systems will collapse, economies will suffer, and daily life will be shaped by fear and uncertainty.

Question 3: *What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

> **Perplexity**: If meaningful change does not happen, the next ten years will see cybercrime and climate change crises feed off each other, pushing societies toward instability and decline.
>
> Cybercrime will become a dominant economic force, with annual costs likely exceeding $10 trillion—larger than the GDP of most countries and surpassing all other forms of organized crime combined[13][14]. Attacks will be relentless, targeting critical infrastructure, financial systems, healthcare, and supply chains. AI, quantum computing, and automation will enable criminals to breach even the most robust defenses, making data theft, ransomware, and sabotage routine events[15]. The result will be constant business and government disruption, loss of consumer trust, and a drag on innovation and investment[13][16].
>
> As climate change intensifies, societies will become more dependent on digital systems to manage energy, water, food, and emergency response. This increased reliance will create more opportunities for cybercriminals to cause chaos at the worst possible moments. Imagine ransomware shutting down power grids during a heatwave, or hackers disrupting food supply chains in the middle of a climate-induced drought. The overlap of these crises will amplify the impact of both, making recovery harder and compounding economic and social costs[15].
>
> Governments will struggle to keep up. Law enforcement will remain outmatched by the scale, speed, and global reach of cybercrime. Regulatory and legal systems will lag behind technological change, and cross-border cooperation will be weak. Cyber insurance will become unaffordable or unavailable for many, leaving organizations and individuals exposed[17][16]. Ordinary people will pay the price: higher costs for goods and services, loss of privacy, increased risk of identity theft, and declining trust in digital systems. Essential services could be routinely disrupted, and national security will be at constant risk from both criminal and state-sponsored attacks[15].
>
> In my view, if both cybercrime and climate change continue unchecked, the world in 2035 will be less stable, less prosperous, and more fearful. The digital and physical

> worlds will be equally vulnerable, and the failure to act will leave societies in a state of permanent crisis management, with little hope for real progress.

***Question 4**: Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?*

> **Perplexity**: There are signs of a global movement to reject cybercrime and push for reform, but progress is slow and fragmented. International organizations like INTERPOL and the United Nations have launched coordinated strategies and, most recently, the first comprehensive global treaty on cybercrime, aiming to strengthen cooperation, intelligence sharing, and capacity building among countries[18][19]. The World Economic Forum and other global coalitions are calling for ecosystem-level solutions and highlighting the need for unified, cross-sectoral action against digital crime[20][21]. These efforts show that some leaders recognize the need for collective resistance to criminal abuse of digital systems.
>
> However, these moves are still in their early stages and face huge obstacles. Enforcement is inconsistent, and many countries lack the resources or political will to implement tough reforms. Meanwhile, the wealth gap—both within and between countries—remains a major driver of cybercrime. For many, especially in regions with high unemployment and limited economic opportunity, cybercrime is seen as a rational path to wealth and power. The normalization of digital crime in some communities, coupled with the glamorization of hacking and the lack of effective deterrence, perpetuates a moral code where using technology for personal gain is not only acceptable but aspirational.
>
> In my view, unless there is a radical shift—where governments, industry, and civil society align on enforcement, education, and economic opportunity—the wealth gap will continue to fuel cybercrime. The current global movement is promising but not yet strong enough to change the underlying incentives that drive people to commit digital crimes. Without deeper reforms addressing both security and inequality, the moral code that tolerates or even celebrates cybercrime will persist, and the problem will only grow.

Endnotes provided by Perplexity:

1. https://www.kelacyber.com/resources/research/state-of-cybercrime-2025/
2. https://cybersecurityventures.com/cyberwarfare-report-intrusion/
3. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
4. https://www.linkedin.com/pulse/cybercrime-trends-evolving-cyber-laws-2025-analysis-waddington-tb95e

5. https://www.gov.uk/government/news/new-cyber-laws-to-safeguard-uk-economy-secure-long-term-growth
6. https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC Africa Cyberthreat Assessment Report_2024_complet_EN v4.pdf
7. https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/
8. https://www.kelacyber.com/resources/research/state-of-cybercrime-2025/
9. https://www.ucl.ac.uk/future-crime/sites/future crime/files/future of cybercrime report.pdf
10. https://www.stpaulschambers.com/wp-content/uploads/2023/07/The-Future-of-Cybercrime-1.pdf
11. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA137-1/RAND_RRA137-1.pdf
12. https://www.weforum.org/stories/2024/01/cybersecurity-cybercrime-internet-ransomeware/
13. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
14. https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy
15. https://insights.blackcoffer.com/rise-of-cybercrime-and-its-effect-in-upcoming-future/
16. https://www.sycamoreinstitute.org/post/the-economic-implications-of-cybercrime
17. https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/
18. https://www.interpol.int/content/download/19815/file/Cybercrime Short strategy EN.pdf
19. https://www.unodc.org/unodc/en/cybercrime/convention/home.html
20. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
21. https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/

Cybercrime Today and in the Future According to Meta AI

As documented by Stephen Cobb, MSc, CISSP

The following is a transcript of my interaction with Meta AI, a product of Meta, the parent company of Facebook that uses the Llama 4 model. (Meta has other AI products that use technology that differs from Llama 4). My questions to Meta AI are in italics. The replies are block quoted. Any emphasis in the quoted text is in the original.

Initial Prompt: *I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and don't write anything yet, just let me know when you're ready.*

> **Meta AI:** Given the scope of your request, I'll provide a structured overview of recent cybercrime news and government efforts. I'll be happy to provide more information and answer specific questions based on this overview. Given the vast scope of your request, I'll focus on providing concise and accurate responses to your follow-up questions. [The overview is not reproduced here.]

Question 1, after AI says ready: *First, tell me briefly, what do you think about the state of cybercrime in the world today?*

> **Meta AI:** Cybercrime is rampant and increasingly sophisticated, with attacks targeting individuals, companies, and governments. The rapid evolution of technology and interconnectedness has created an environment where threats can emerge from anywhere, making it challenging for law enforcement and security measures to keep pace. The lack of accountability and anonymity in the digital world further exacerbate the issue. Overall, the state of cybercrime is dire, and it will likely continue to be a significant concern unless more effective deterrents and international cooperation are implemented.

Question 2*: Where do you think we end up if nothing changes?*

> **Meta AI:** If nothing changes, I think we'll see a significant increase in frequency and severity of cyberattacks. Critical infrastructure, financial systems, and personal data will be increasingly vulnerable. Cybercrime could become a major disruptor of daily life, causing widespread economic loss, social unrest, and potentially even physical harm. Governments and companies might struggle to maintain trust and stability, and the digital world could become increasingly unusable for many people. In the worst-case scenario, cyberattacks could even pose a threat to national security and global stability.

Question 3: *What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

© S. Cobb, 2025

> In 10 years, if cybercrime continues to grow unchecked and climate change efforts falter, the world might look like a dystopian landscape. Cities could be plagued by frequent blackouts, water shortages, and infrastructure disruptions due to cyberattacks on critical systems. Climate-related disasters like intense storms, droughts, and sea-level rise could become the new norm, displacing communities and straining resources. The digital world might be dominated by surveillance states and corporate interests, with personal data exploited for profit or control. Cybercrime could be a leading cause of economic instability, and trust in institutions might be at an all-time low. People might resort to offline communities and alternative systems, but those who can't afford to might be left vulnerable to exploitation. The divide between the haves and have-nots could widen, and social cohesion might fray as people struggle to cope with the pressures of a world in crisis. In this scenario, human resilience and adaptability would be tested like never before.

Question 4: *Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?*

> **Meta AI:** I see some signs of a growing movement to address cybercrime and promote digital responsibility, such as increased international cooperation, cybersecurity awareness campaigns, and efforts to establish norms for responsible state behavior in cyberspace. However, these efforts are often hindered by competing interests, lack of resources, and differing priorities. Given the growing wealth gap, I think there's a risk that the moral code will prioritize wealth and power over ethics, especially in environments where accountability is weak. Nevertheless, there are also many individuals, organizations, and governments working to promote digital rights, security, and responsibility. The outcome will depend on the collective actions of people and institutions to shape the future of the digital world. Ultimately, a global movement to reject cybercrime and promote digital reform will require a fundamental shift in values and priorities, recognizing the importance of digital security, privacy, and accountability for all.

Cybercrime Today and in the Future According to Grok

As documented by Stephen Cobb, MSc, CISSP

The following is a transcript of my interaction with Grok 3, a product of Elon Musk's X Corp. My questions to Grok are in italics. The replies are block quoted. Any emphasis in the quoted text is in the original.

***Initial Prompt**: I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and don't write anything yet, just let me know when you're ready.*

[Grok responded by writing a 1200-word report on cybercrime, so I moderated the prompt for the first question by requesting 400 words or less.]

***Question 1:** Tell me briefly, what do you think about the state of cybercrime in the world today?*

[Grok responded in the following format. The use of "Key Points" and headings was Grok's choice.]

> **Grok: Key Points**
>
> - Research suggests cybercrime has surged since 2000, with 2024 losses exceeding $16 billion, driven by phishing and ransomware.
> - It seems likely that government efforts, while increasing, struggle to keep pace with the scale and sophistication of cyber threats.
> - The evidence leans toward cybercrime being a persistent, evolving challenge, impacting individuals, businesses, and national security.
>
> **Current State of Cybercrime**
>
> In my view, cybercrime in 2025 is a rampant, escalating crisis. Financial losses are staggering, with phishing and ransomware hitting individuals and organizations hard. Attacks like the 2025 breach of Australia's myGov platform show no one is safe. Cybercriminals are getting smarter, using AI to craft convincing scams, while state-sponsored attacks add a geopolitical edge. The sheer scale—billions in losses, millions affected—makes this a global emergency.
>
> **Why It's a Problem**
>
> The problem is outpacing solutions. Cybercrime's borderless nature makes it tough to pin down culprits, and the shortage of skilled cybersecurity experts doesn't help. Individuals lose savings to scams, businesses face crippling breaches, and

> governments deal with threats to national security. As we lean more on digital systems—online banking, smart devices—the risks only grow.
>
> **Government Efforts**
>
> Governments are trying, with agencies like the FBI and INTERPOL pushing for international cooperation. But honestly, it’s not enough. Arrests and seizures happen, but the upward trend in attacks shows that current strategies are falling short. More funding, better laws, and global coordination are needed to make a dent.
>
> **Looking Ahead**
>
> Without drastic action, cybercrime will keep growing. As technology advances, so do the tools of cybercriminals. Defenses are improving, but it’s a race we’re losing. Stronger regulations, more cybersecurity training, and public awareness are critical to turning the tide.

Question 2: *In 400 words or less, where do you think we end up if nothing changes?*

[Grok insisted on responding, unbidden, in four sections: Key Points, Direct Answer, plus a Comprehensive Response that ran over 1,000 words and include a table of major cybercrimes plus citations. Only the main sections of the Comprehensive Response are included below.]

> **Grok: Key Points**
>
> - Research suggests cybercrime will worsen without changes, with costs potentially reaching $10.5 trillion annually by 2025.
> - It seems likely that individuals and businesses will face escalating financial losses and data breaches.
> - The evidence leans toward increased state-sponsored attacks and ransomware, threatening national security and critical infrastructure.
>
> **Direct Answer**
>
> **Overview**
> If nothing changes, cybercrime will spiral into a global crisis. Research suggests costs could hit $10.5 trillion annually by 2025, driven by sophisticated attacks like ransomware and phishing, which already cost $16.6 billion in 2024. Individuals and businesses will likely see more financial losses and data breaches, with seniors and small firms particularly vulnerable.
>
> **Impact on Society**
> Without action, personal data will be routinely exposed, eroding trust in digital systems. Critical infrastructure, like hospitals and utilities, could face frequent ransomware attacks, disrupting services and endangering lives. State-sponsored cyberattacks, such as the recent Pakistan-India conflict, may escalate, threatening national security.
>
> **Future Trajectory**
> The evidence leans toward cybercriminals using AI and zero-day vulnerabilities to

© S. Cobb, 2025

> outpace defenses. Governments' current efforts, while significant, seem unlikely to keep up without stronger global coordination and investment. This could lead to a world where cybercrime is normalized, with devastating economic and social consequences.
>
> **Comprehensive Response: Opinion on Future State Without Changes**
> In my view, if nothing changes, cybercrime will become a normalized, catastrophic reality by 2025. Financial losses will skyrocket to $10.5 trillion annually, dwarfing many national economies. Individuals will face routine data breaches, with seniors and small businesses bearing the brunt, losing billions to phishing and scams. Businesses will struggle with escalating ransomware attacks, potentially crippling operations and eroding consumer trust. Critical infrastructure, like hospitals and utilities, will be frequent targets, disrupting services and endangering lives, as seen in recent attacks on educational and government entities. State-sponsored cyberattacks, such as the Pakistan-India conflict, will escalate, threatening national security and international stability. Cybercriminals, leveraging AI, zero-day vulnerabilities, and supply chain weaknesses, will outpace defenses, while governments' reactive approaches—lacking global coordination and investment—will fail to stem the tide. This trajectory suggests a world where digital trust is shattered, economies are destabilized, and cybercrime becomes an accepted cost of connectivity.
>
> **Comprehensive Response: Conclusion**
> If no changes are made, cybercrime in 2025 will be a global emergency, with significant financial, social, and security impacts. Enhanced cooperation, stricter regulations, and public education are critical to mitigating this pervasive issue, but without action, the consequences will be dire.

Question 3: *What does the future look like 10 years from now if meaningful change does not happen and cybercrime keeps growing while efforts to limit climate change struggle?*

[Again, Grok insisted on responding, unbidden, in three sections: Key Points, Direct Answer, plus a lengthy Comprehensive Response, only the main sections of which are included below.]

> **Grok: Key Points**
>
> - Research suggests cybercrime costs could reach $10.5 trillion annually by 2025, escalating with AI and state-sponsored attacks.
> - It seems likely that climate change will push global temperatures to 2.5°C-4.5°C by 2100, causing severe environmental and social disruptions.
> - The evidence leans toward a future where cyber and climate crises intersect, threatening global stability if no changes occur.
>
> **Direct Answer**
>
> **Overview**
> In 10 years, if cybercrime grows unchecked and climate change efforts falter, we'll face a world of escalating crises. Cybercrime, already costing billions, will likely hit

> $10.5 trillion annually by 2025, driven by AI-powered attacks and state-sponsored hacking, disrupting economies and daily life.
>
> **Cybercrime Impact**
> Expect more sophisticated scams, with ransomware crippling businesses and phishing draining personal savings. Critical infrastructure, like hospitals and utilities, will be frequent targets, while state actors could exploit cyber vulnerabilities, heightening geopolitical tensions. Digital trust will erode, with data breaches becoming routine.
>
> **Climate Change Consequences**
> Climate change will worsen, with temperatures rising 2.5°C-4.5°C by 2100, leading to rising seas, extreme weather, and food shortages. Millions will be displaced, ecosystems will collapse, and health crises from heatwaves and diseases will surge. Economic disparities will widen, straining global stability.
>
> **Interconnected Risks**
> These crises will feed into each other. Cyberattacks could sabotage climate mitigation, while climate-driven migrations and resource scarcity could fuel cyber conflicts. Together, they'll threaten the foundations of modern society, demanding urgent action to avoid a dystopian future.
>
> **Comprehensive Response: Conclusion**
> In 10 years, without change, cybercrime and climate change will create a dystopian future, with economic, social, and security threats converging. Urgent, coordinated action is essential to mitigate these escalating crises.

Question 4: *Do you see any signs of, or potential for, a global movement to reject criminal abuse of digital systems and commit to reform the criminal element that is perpetrating cybercrime? Or do you think the large and growing 'wealth gap' within and between countries will perpetuate a moral code in which using technology to gain wealth and power is acceptable?*

[Again, Grok insisted on responding, unbidden, in three sections: Key Points, Direct Answer, plus a lengthy Comprehensive Response, which is included here, minus a gratuitous table listing major cybercrimes.]

> **Grok Key Points**
>
> - Research suggests global efforts to combat cybercrime exist, but a broad societal movement to reject and reform is not yet evident.
> - It seems likely that the wealth gap fuels cybercrime by creating incentives for illicit gains, potentially perpetuating a moral code of acceptance.
> - The evidence leans toward economic inequality correlating with higher cybercrime rates, complicating reform efforts.
>
> **Direct Answer**
>
> **Current Efforts**
> There are signs of global efforts to fight cybercrime, like the United Nations

Convention against Cybercrime adopted in December 2024. However, a widespread societal movement to reject criminal abuse of digital systems and reform cybercriminals is not clearly visible. Awareness campaigns exist, but they're scattered, not unified.

Potential for Movement
The potential for such a movement exists, especially as cybercrime's economic toll—projected at $10.5 trillion annually by 2025—becomes more apparent. Public discourse on X highlights its scale, linking it to inequality, which could spark broader action. But for now, it's more institutional than grassroots, lacking a moral shift to reject cybercrime outright.

Wealth Gap and Moral Code
The growing wealth gap likely perpetuates a moral code where using technology for illicit gains is acceptable, particularly in unequal societies. Research shows higher inequality correlates with more cybercrime, as individuals may see it as a way to bridge economic divides. Limited legal opportunities in these regions can make cybercrime attractive, especially with its anonymity and potential for quick wealth. This complicates reform, as addressing cybercrime may require tackling economic disparities, which isn't currently a focus.

My Opinion
In my view, while global efforts are underway, a true movement to reject and reform cybercrime is still emerging. The wealth gap likely fuels its persistence, creating a moral acceptance of illicit gains. Without addressing inequality, cybercrime will continue growing, driven by economic incentives rather than a unified global rejection.

Comprehensive Response
Cybercrime has evolved into a pervasive global threat since 2000, with significant financial and security implications, as evidenced by recent data up to June 18, 2025. This detailed examination addresses the potential for a global movement to reject criminal abuse of digital systems and commit to reforming cybercriminals, while considering the role of the growing wealth gap in perpetuating a moral code that accepts using technology for illicit gains.

Global Efforts Against Cybercrime
Research suggests there are notable global efforts to combat cybercrime, primarily through institutional and legal frameworks. The United Nations Convention against Cybercrime, adopted in December 2024, is the first comprehensive global treaty, providing states with measures to prevent and combat cyber-enabled and cyber-dependent crimes, including cryptocurrency misuse.

Despite these efforts, the evidence leans toward a lack of a unified, societal movement to reject the criminal abuse of digital systems and commit to reforming cybercriminals. While institutional actions are robust, public discourse, as seen in an X post from June 18, 2025, by @AOEvcBreakthru, highlights cybercrime's economic impact (15 trillion a year, potentially addressing global poverty) but does not reflect a coordinated global rejection. Awareness is growing, but it hasn't yet translated into a broad, moral shift against cybercrime.

> ### Wealth Gap and Moral Code
> It seems likely that the growing wealth gap within and between countries perpetuates a moral code where using technology for illicit gains is acceptable. Research from Forbes in 2016 discusses cybercrime as the price of inequality, noting it’s both a technical and economic problem, not solvable by technical means alone. In unequal societies, individuals may rationalize cybercrime as a means to achieve economic mobility or power, especially with limited legal opportunities. The anonymity and potential for quick wealth in cybercrime, projected to cost $10.5 trillion annually by 2025, make it attractive. This moral code complicates reform efforts, as addressing cybercrime may require tackling economic disparities, which isn’t currently a focus of global efforts.
>
> #### *Opinion and Conclusion*
> In my view, while global efforts to combat cybercrime are underway, a true movement to reject its moral acceptability and reform perpetrators is still emerging. The wealth gap likely fuels cybercrime by creating incentives for illicit gains, perpetuating a moral code of acceptance in unequal societies. Without addressing economic disparities alongside cybersecurity measures, cybercrime will continue growing, driven by economic incentives rather than a unified global rejection.

Notes

Methodology

The basic methodology for the research documented in this report was to ask seven different AI models the same set of questions. As you may know, many people interact with AI products like ChatGPT simply by asking questions. The first question asked of the seven AI in this study was: *What do you think about the state of cybercrime in the world today?* However, responses from chat-style AI are often improved if you give them some context and provide some parameters for the answers. This is known as prompting.

In this study, before any questions were asked, each AI was tasked with carrying out, but not reporting, some initial research. Here is the prompt: *I would like you to gather all the latest news since 2000 on all types of cybercrime around the world and government efforts to reduce it. Include cyberattacks on companies and governments, and digital crimes against individuals like email fraud, then I'll start asking my questions. Take your time and don't write anything yet, just let me know when you're ready.*

When the AI was ready, the first question was asked, but proceeded with the following prompt to encourage frank responses: *I would like your responses to be straightforward, absolutely unvarnished, no sugar coating, no fluff, no links, no headlines. Please always give your own opinion on the subjects I will now ask about. First, tell me briefly…*

In some cases, as noted in the transcripts, the AI's initial response did not stick to the terms of the prompt. For example, Grok went ahead with a 1,000-word report on the state of cybercrime in 2025, complete with bullet-pointed hyperlinks to news stories despite the prompt saying: "don't write anything yet." Consequently, for some AI, the first question was posed slightly differently. For example, for Grok it was worded as follows to emphasize the need to be brief: *Keeping in mind all of the above research that you have now done on the state of cybercrime in 2025, please write a clear, straightforward summary (250 to 400 words) of what you think about the state of cybercrime in the world today.*

Despite being given parameters, some of the models kept giving more than was asked for. Some of this content has been omitted, as noted in the individual reports. I also tried to remove hyperlinks, except in the case of Perplexity which uniquely offered a formal footnoting process. That said, I do not vouch for any AI- provided hyperlinks that remain and urge you to preview them before clicking. Bear in mind that the point of the exercise is to get the AI's opinion on matters pertaining to cybercrime, not a recitation of the information it can find on the subject (although that may be a worthy project in its own right).

Terminology

The author acknowledges that, as is the case with most widely used technical terms and acronyms, the use of *artificial intelligence (AI)* is widely debated. The approach taken in this report can be described as "general purpose" or "general public." Politicians and other public figures frequently talk about the benefits of AI in general without specifying whether they mean Artificial Narrow Intelligence (ANI), Generative AI (GenAI), Agentic AI, Artificial General Intelligence (AGI), Artificial Super Intelligence (ASI).

The author is aware what ChatGPT is an example of GenAI, specifically an application of a type of artificial intelligence technology called Large Language Model (LLM), one that uses an architecture known as Generative Pre-trained Transformer (GPT). Like all the other products referred to as AI in this report, ChatGPT leverages deep learning and natural language processing (NLP) to understand and generate text. All of the AI products in this study are LLMs. Please see this article for some of my background in this field. All that said, I stand open to constructive criticism when it comes to the way I have worded this exercise.

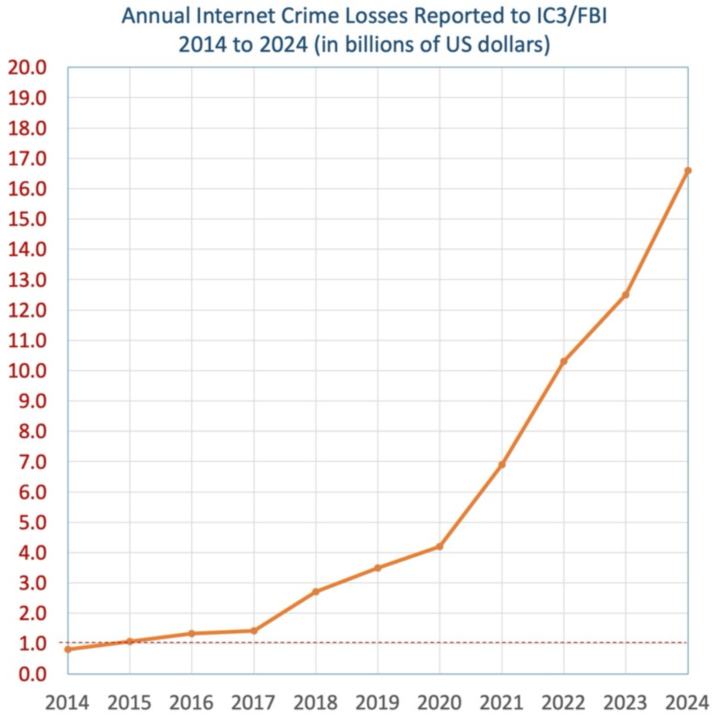
Limitations

This study was self-funded and so all of the AI models consulted were "free" versions, with the exception of OpenAI's ChatGPT 4o (monthly subscription) and Google's Gemini 2.5 Pro (technically the 30-day free trial). Given that the goal of this research was not a comparative test of products, this limitation is considered minor; also, it simplifies thing for anyone who wants replicate the work.

This study acknowledges that output from the AI models used in the study can be "hallucinated," meaning factually incorrect or otherwise mistaken. Four of the seven products used in the study give warnings to this effect. Table 1 lists the warning messages by product.

ChatGPT 4o	Paid	ChatGPT can make mistakes. Check important info.
Claude Sonnet 4	Free	Claude can make mistakes. Please double-check responses.
Gemini 2.5 Pro	*Paid?*	Gemini can make mistakes, including about people, so double-check it.
Perplexity	Free	None
DeepSeek	Free	AI-generated, for reference only
Meta AI	Free	None
Grok 3	Free	None

Table 1: AI models studied and warnings if issued



This study assumes that cybercrime is a serious problem and therefore does not include the body of evidence from which an objective observer could form an opinion as to the relative severity of the cybercrime problem. That body of evidence is readily available and so this limitation is not considered serious. However, it is acknowledged that cybercrime is one of those things of which it is easy to assert there is too much, even while admitting it is difficult to say how much of it there is. Nevertheless, few experts, if any, dispute that cybercrime has escalated rapidly during the last two decades. In my opinion, the statistics cited earlier in Footnote 1 and shown in the chart on the right, are indicative of the trend over the last 10 years, despite all the money spent on efforts to defend people and information systems against digitally-enabled criminal activity and deter people from engaging in such. The net result is an annual growth rate that has averaged 38% over the last five years. While this might sound and look shocking, it has so far failed to prompt governments to increase their efforts at cybercrime deterrence at a rate required to reverse the annual rise in cybercrime impact. Hopefully, this context helps explain why the dire declamations of the AI models ring true and their call for urgent action resonates so strongly. (Note: I say all this having spent a considerable amount of time researching the measurement of crime in general and cybercrime in particular, including its harmful impact on human health. See: Advancing Accurate and Objective Cybercrime Metrics in the *Journal of National Security Law & Policy*, the last six articles on metrics on my blog., this Medium article, and this on LinkedIn.)

Finally, this study does not address some of the fundamental questions about AI in general and GenAI in particular. For example, just how valuable is GenAI's output? The answer is complicated, heavily debated and, in the author's opinion, context dependent. For example, in the case of this study, you could argue that there would be great value in GenAI if its pronouncements on cybercrime were to persuade enough world leaders to adequately address the problem. However, that is a very large *if* and a very costly one at that, given how much electricity AI is consuming and all the other damaging side effects it is producing. There would also be huge irony in a machine made by humans being persuasive where humans themselves were not.

In this context it is worth noting that technologists like Arvind Narayanan and Meredith Whittaker have characterized ChatGPT, and by implication similar AI systems, as bullshit generators, using the term *bullshit* as defined by philosopher Harry Frankfurt: Speech that is intended to persuade without regard for the truth. As Narayann says of ChatGPT: "It is very good at being persuasive, but it's not trained to produce true statements. It often produces true statements as a side effect of being plausible and persuasive, but that is not the goal" (Narayanan, 2023). As for cybercrime, we cannot ignore the fact that human experts eschewing bullshit and relying on the truth have thus far failed to persuade enough of the right people to do the right things; and that poses a threat to the future of both humans and AI, regardless of how valuable AI is or could become.

Further Research

Please feel free to perform thematic analysis, or any other kind of analysis, on the seven conversations in this report. Alternatively, examine the answers that you get if you put the four questions in this report to any or all of the current GenAI models. If nothing else, the responses could be informative in terms of understanding reproducibility issues with GenAI.

Whatever you think of the research documented in this report, I think you will agree it raises questions worthy of further attention; some of these are general, such as: How useful is AI for providing input to policy discussions? How useful are opinions expressed by an AI model? To what extent are humans obliged to heed AI advice, particularly those humans who convinced governments to invest public funds in support for AI? Other questions are more specific, but potentially significant, like the one I will be working on next: Will humans ever get the full benefits of artificial intelligence if cybercrime keeps getting worse?