A PANOPTICPROTOCOL COMMUNITY GUIDE

The Lazarus Heist

Geoff White's Files on North Korea's Cyber-Army, in Plain English — Plus the Second Look

10 CASE FILES | PLAIN ENGLISH | UPDATED 2026

A country that ran out of money built an army to steal it. This book is the story of how a starving, sanctioned state taught itself to rob banks with a keyboard — and of the ordinary people who paid for it.

We've rebuilt the book as case files: the motive, seven operations, the escalation, the verdict. Each file ends with **the Second Look** — what happened after White closed the manuscript in 2021 — and the lesson it leaves for anyone holding crypto today.

A companion, not a replacement — if a case hooks you, buy the book.

Contents

> *Complete edition — the whole book in plain English, plus five years the book never saw. A companion, not a replacement: buy the book. Educational only. NFA. DYOR.*

CASE FILE 00

The Country That Ran Out of Money

Why a nuclear state started robbing banks. Covers the Introduction and Chapters 2–3.

SUBJECT: THE DPRK ECONOMY · **YEARS:** 1948–2006 · **STATUS:** CRIME AS STATE POLICY

Most cyber-powers hack for secrets. North Korea hacks for cash — and White's opening argument is that you cannot understand the hacking until you understand the bankruptcy behind it. A state founded in 1948 locked itself into what he calls a series of **ratchet effects**: a war it could neither win nor concede, an ideology of self-reliance that forbade help, and an isolation so total that each year the outside world pulled further ahead.

The bill came due in the 1990s. Soviet subsidies stopped, the rivers silted and flooded, and the food system collapsed. Estimates of the dead run from 240,000 to three million. Jihyun Park, who escaped and now lives in England, remembers catching dragonflies with her classmates and eating the bodies. She remembers her first corpse: a thirteen-year-old student of hers who had wanted to be a doctor. Nobody said "famine." People said the dead *had an illness*.

US analyst David Asher spent years on one question: with a decade-long trade deficit and near-total bankruptcy, *where did they get the money?* His answer became the Illicit Activities Initiative — and the answer was crime, run as a department of state. Counterfeit Viagra, counterfeit cigarettes, methamphetamine, and above all the **"superdollar"**: a forged $100 bill so good that when an undercover FBI agent sent a sample for analysis, the lab said it was real. Fifteen years of investigation, an FBI sting staged as a wedding on a yacht, fifty-nine arrests from China, Taiwan, Canada and the US — and not one North Korean among them. The usual explanation: the North Koreans allowed to travel are government workers, and they carry diplomatic immunity.

The Second Look: around 2006 the superdollars faded. Not because the policy changed, but because the medium did. Money was moving online, and a state already organised around illicit revenue simply followed it. Everything in the following files is the superdollar operation rebuilt for the internet — same structure, same deniability, vastly better margins.

WHAT IT MEANS FOR YOU

1. **This attacker is not a gang, it's a budget line.** It cannot be deterred by making theft unprofitable, because the alternative isn't a different job — it's national insolvency.
2. **Deniability was designed in from the start.** Diplomatic passports then, front companies and borrowed identities now. Attribution has always been the weak point, and they know it.

> **BOTTOM LINE**
>
> *A state that cannot earn money legally will build something that takes it. That something is now pointed at crypto.*

CASE FILE 01

Dark Seoul: Rehearsal on the Neighbour

Where the group learned to destroy, and learned to wear masks. Covers Chapter 4.

TARGET: SOUTH KOREAN BANKS & BROADCASTERS
YEAR: 2013 · **DAMAGE:** 32,000 MACHINES

At 2 p.m. on Wednesday 20 March 2013, thirty-two thousand computers across two of South Korea's largest banks and its three biggest broadcasters went dark at the same moment. The malware went for the **Master Boot Record** — the instruction that tells a machine where to find its own operating system. No MBR, no computer. ATMs and online banking failed; systems had to be rebuilt one machine at a time.

Two things made analysts sit up. First, the escalation: military strategy talks about five options against an enemy — deny, degrade, disrupt, deceive, destroy — and the attackers had jumped straight to the last one. Second, the masks. A phone company's homepage was defaced with red-eyed skulls signed **"Whois Team."** A day later a group calling itself the **NewRomantic Cyber Army Team** claimed the bank attacks. Neither name had ever existed before, or has been seen since. Investigators later found the code linked them — and linked both to the same operation. Anonymous was rampaging across the internet that year, and the false flags were built to hide inside that noise.

The attribution came from North Korean IP addresses in the code — weak evidence in most countries, unusually strong here, because no commercial VPN offers you a North Korean exit. And the toolset traced back to 2009, to malware that had been quietly harvesting intelligence on South Korea's armed forces. The attackers could have wiped those military machines too. They chose not to.

The Second Look: the restraint is the finding. Thirteen years on, North Korea's viruses sit inside systems they have never detonated. Former ambassador Thae Yong Ho's summary still holds: in peacetime the hackers earn; in wartime the same access becomes a weapon. Every heist in this guide is also a rehearsal.

WHAT IT MEANS FOR YOU

1. **The group hides behind invented brands.** A hack claimed by a hacktivist collective you've never heard of is not evidence of who did it. It's often evidence of who wants you to look elsewhere.
2. **Wiper malware has no ransom and no recovery.** Backups that live on the same network are not backups. This is the attack pattern that offline, immutable copies exist for.

> **BOTTOM LINE**
>
> *They practised on the neighbour first — and the world called it a local story.*

CASE FILE 02

Hacking Hollywood

A comedy about Kim Jong Un, 38 million stolen files, and the fastest public attribution in the history of cyber-attacks. Covers Chapters 5–6.

TARGET: SONY PICTURES ENTERTAINMENT · **YEAR:** 2014 · **ENTRY:** ONE PHISHING LINK

On 25 September 2014 someone calling himself "Nathan Gonsalez" sent a Sony employee a link to some video files for a marketing campaign. Somebody downloaded them. The attackers then spent two months moving quietly from machine to machine before triggering everything at once on 24 November. Badges stopped working. Eight thousand machines had to be pulled off the network. Six weeks later the café on the lot still couldn't take a card. Staff queued in the car park for paper pay cheques.

What followed was not a hack so much as a media campaign. The attackers, calling themselves the **Guardians of Peace**, had taken an estimated **38 million files** and released them to journalists in eight timed stages — unreleased films first to build an audience, then salaries, then 5,000 of co-chair Amy Pascal's emails. They picked hungry mid-size outlets that would break the stories the big networks would then chase. On 16 December they invoked 9/11 against any cinema showing the film; the chains pulled it, and on 19 December President Obama said publicly that North Korea had done it — never, White notes, had a major world leader been so quick to blame another country for a specific cyber-attack.

The people who paid weren't the executives. Employee Celina Chavanette found her offer letter, her salary and her Social Security number online: *"I'm paying for it forever."* Amy Heller, laid off seven months before the breach, found an internal report about a missing $90 ergonomic mouse filed under "property crime" — enough, in an industry where people google you, to end a career.

The Second Look: former NSA analyst Priscilla Moriuchi's verdict is the one that aged best. The world read the attack as a bizarre overreaction to a stupid film and downgraded the threat. What it should have read was the tradecraft: a team that understood the American news cycle well enough to know that *executives' embarrassing emails* were the payload, not the films. Everything since has run on that same skill — reading the target's culture better than the target expects.

WHAT IT MEANS FOR YOU

1. **One person clicking one link ended a company's network.** Every case in this book starts the same way. There is no second lesson here.
2. **Stolen data doesn't expire.** Sony's staff are still living with 2014. Assume anything you put in a corporate system is permanent and potentially public.

> **BOTTOM LINE**
>
> *They didn't just break the network. They understood the audience.*

CASE FILE 03

The Billion-Dollar Bank Job

A year inside a central bank, a sabotaged printer, and the calendar that nearly bought them a billion dollars. Covers Chapters 7–8.

TARGET: BANGLADESH BANK · **YEAR:** 2016 ·
ATTEMPTED: $951M · **TAKEN:** $101M

On 29 January 2015 a polite email from "Rasel Ahlam" reached staff at Bangladesh Bank and other Dhaka institutions, asking them to download a CV. Someone did. Exactly one year later — 29 January 2016 — the attackers finally reached the terminal running **SWIFT**, the messaging system banks use to move money. They replaced two bytes in the software with instructions that do nothing, so a check that should have said "no" now always said "yes" — and they rewired the printer that produced the paper records so it received only blank pages.

Then they used the calendar. The transfers began at 8.36 p.m. Dhaka time on Thursday 4 February — thirty-three minutes after the duty manager went home, and 9.36 a.m. in New York. Bangladesh's weekend is Friday–Saturday; New York's is Saturday–Sunday; and Monday 8 February was the first day of Lunar New Year in Manila. Three calendars, stacked, bought them a five-day head start. Thirty-five requests went out for **$951m** — almost the entire account.

What stopped them was luck. The Manila branch they had chosen sat on **Jupiter Street**, and "Jupiter" is also the name of a sanctioned Iranian vessel. The word tripped the Fed's automated screening, a staffer reviewed the whole batch, and thirty transfers were held. Five got through: **$101m**. White's warning against the heist-movie version is the chapter's real argument — the hackers were not omnipotent, they were *"a burglar dropped into the middle of a dark house with a weak torch,"* and they sat there for a year without being caught.

The Second Look: the FBI charged Park Jin Hyok in 2018 and added Jon Chang Hyok and Kim Il in 2021, alleging attempts on over $1.2bn from banks across Asia, Africa, Europe and Latin America. None has ever been arrested. Meanwhile the tactic migrated: the SWIFT terminal of 2016 is the exchange hot wallet of today, and the year-long patient dwell is still the signature.

WHAT IT MEANS FOR YOU

1. **Patience is the tell.** Serious attackers wait a year. If your only detection is "did something happen today," you will miss them.
2. **Both backups failed together.** The digital ledger and the paper printout were the same control twice. Real redundancy means a copy the attacker cannot reach from inside.

> **BOTTOM LINE**
>
> *A coincidence saved 90% of the money. Not a control. A coincidence.*

CASE FILE 04

The Getaway: Casinos, Cash and a Typo

Stealing the money was the easy part. Covers Chapters 9–12.

ROUTE: MANILA & COLOMBO · **YEAR:** 2016 · **RECOVERED:** A FRACTION

Of the $101m, **$81m** landed in four accounts at an RCBC branch on Jupiter Street, opened nine months earlier with forged licences by holders who all claimed the same job title and salary. The branch CCTV had failed the day before the money arrived and was repaired the Tuesday after. By the time the bank froze the accounts, **$68,335** remained of $81m.

The money became cash — half a billion pesos, about 500kg, the weight of a grand piano — collected by two Chinese men with a van. Thirty million dollars went to a man named Weikang Xu, who left the country and has never been seen again. The rest went to the **Solaire** and **Midas** casinos, where Philippine law then exempted casinos from anti-money-laundering rules. Dozens of gamblers sat in private junket rooms for *weeks*, playing baccarat with balanced bets to recover roughly 90 cents on the dollar, while the story ran on the front pages around them and nobody stopped them.

The fifth transfer went to Sri Lanka — **$20m** to a small charity, the Shalika Foundation, for a dairy farm that had never been built and that the charity's own website costed at under $1m — backed by a forged letter from Japan's aid agency in which "electrification" was misspelt. A bank clerk noticed the payee read **"Shalika Fundation."** The money went back. White's uncomfortable observation: of everyone caught in this machine, the two convicted or ruined were both women — a branch manager and a charity director — while the men who moved the cash vanished.

The Second Look: this file is why crypto matters to the story. Laundering $51m took a corrupt branch manager, a money changer, two couriers, several dozen gamblers and several weeks. In 2017 the same group laundered the WannaCry ransom in under 48 hours with no humans at all. Everything after this page is the group escaping the hardest part of its own business.

WHAT IT MEANS FOR YOU

1. **Moving stolen money is harder than stealing it.** That is why every recovery effort targets the exit, and why exchanges freeze funds fast or never.
2. **Middlemen carry the legal risk.** The people who "just helped with a transfer" got the sentences. Never move funds for someone whose source you cannot verify.

> **BOTTOM LINE**
>
> *A spelling mistake saved $20m. That is how thin the margins of this business really are.*

CASE FILE 05

WannaCry

A stolen NSA weapon, 230,000 machines, 7,000 cancelled NHS appointments — and a ransom that barely paid for a car. Covers Chapter 13.

DATE: 12 MAY 2017 · **SPREAD:** 150 COUNTRIES · **DAMAGE:** $4–8BN

Patrick Ward, forty-seven, had waited two years for open-heart surgery. Minutes before it began, his surgeon told him the hospital's computers were gone and the operation was cancelled. Across England, a third of the organisations running NHS hospitals were infected or had to disconnect. Almost **7,000 appointments** were cancelled, more than a hundred of them urgent cancer cases.

What made WannaCry different was that it spread itself. Bolted onto ordinary ransomware were **EternalBlue** and **DoublePulsar** — exploits built by the US National Security Agency, which had known about the underlying Windows flaw since 2012 and kept it, until a group called the Shadow Brokers stole them and dumped them publicly in April 2017. Microsoft had shipped a fix. It wasn't compulsory. Millions of machines were sitting ducks. As one NCA official put it: a crude bit of ransomware attached to a weapons-grade exploit.

It was stopped by a 22-year-old in Devon. Marcus Hutchins, dissecting the code after lunch at the chip shop, noticed the virus checked whether a particular unregistered domain existed and shut down if it did. He bought it for under £10. Infections stopped within seconds. It was a developer's safety brake that nobody had removed — one of several signs the thing was shipped unfinished. Another: instead of a fresh wallet per victim, the code held just **three Bitcoin addresses**.

The Second Look: the ransom take was a few hundred thousand dollars — a catastrophe by ransomware standards. White's argument is that profit was never the point. On 3 August 2017 all three wallets were emptied within minutes, tumbled through dozens of addresses and dropped into an exchange, where the trail died. Against months of vans and junket rooms in Manila, this took under 48 hours and no accomplices. WannaCry looks like a failure. It was a laundering rehearsal — and the skill it proved is the one now used on every crypto heist in File 08.

WHAT IT MEANS FOR YOU

1. **Patching is not admin work.** The fix existed for months. Everything that followed was optional.
2. **Judge an operation by what it taught the attacker, not what it earned.** A "failed" hack that proves a new laundering route is a win for them.

> **BOTTOM LINE**
>
> *The world called it a botched robbery. It was a successful dress rehearsal.*

CASE FILE 06

Old Tricks, New Money

The fake trading app, the fake recruiter, the fake company — the crypto playbook, written in 2018. Covers Chapter 14.

TARGETS: EXCHANGES & INDIVIDUALS · **YEARS:** 2017–2020 · **TOTAL:** ~$1.3BN

On 4 December 2017 a phishing email reached the Slovenian mining marketplace **NiceHash**. Two days later, Bitcoin worth **$75m** was gone — *"the largest theft in the history of Slovenia,"* as its product manager put it. NiceHash repaid every customer out of future profits. It was the beginning of a run that, valued at the moment of each theft, added up to roughly **$1.3bn** across dozens of targets.

Three techniques appear here that you will still meet today, unchanged. The first is the **fake trading application**: Celas Trade Pro launched in May 2018 with a slick site displaying the logos of four antivirus firms it had never spoken to. The download was real trading software with malware inside, aimed at your wallet. Kaspersky exposed it, so it came back as WorldBit-Bot, then iCryptoFx, Union Crypto Trader, Kupay Wallet, CoinGo Trade, JMT Trader, Dorusio, CryptoNeuro Trader and Ants2Whale — same platform, new paint. Researchers named the family **AppleJeus**.

The second is the **fake job offer**. Researchers found the group studying targets on LinkedIn, writing a bespoke job spec for a role at a rival firm, and attaching an application form that claimed to be protected by European data-protection rules and asked you to "enable content." Clicking installed a backdoor. The same campaign was running in around twenty countries at once. The third is the **fake company**: Marine Chain, a tokenised shipping venture registered in Hong Kong in April 2018, with real hired professionals and four law firms — exposed by an anonymous Reddit user whose only post it ever was. The founder vanished that July.

The Second Look: nothing in this chapter has been retired. The fake app became the fake video-call installer; the LinkedIn job spec became the malicious "coding challenge" repository. Chainalysis puts DPRK-attributed crypto theft at roughly **$6.75bn** since 2016 — the $1.3bn White reported is now under a fifth of the running total.

WHAT IT MEANS FOR YOU

1. **Treat every downloaded trading app as hostile until proven otherwise.** Antivirus logos on a website prove nothing — the originals were used without permission.
2. **An unexpectedly perfect job offer is an attack pattern.** Especially one that arrives with a document, a repo or an installer attached.

> **BOTTOM LINE**
>
> *The 2018 playbook never needed replacing. It only needed better production values.*

CASE FILE 07

Going Back for More

Cash machines in twenty-nine countries, an Instagram millionaire, and why prosecutors indict people they can never arrest. Covers Chapters 1 and 15.

TARGETS: BANKS IN INDIA, PAKISTAN, MALTA
YEARS: 2018–2019 · **TAKEN:** ~$17M

At 3 p.m. on Saturday 11 August 2018, a taxi driver from Mumbai, a pharmacist from Pune and dozens of others fanned out across the Indian city of Kolhapur with stacks of bank cards. By 10 p.m. it was over. Worldwide, in **twenty-nine countries**, more than **$11m** came out of cash machines in **12,000 transactions** inside two hours and thirteen minutes. The mules were paid up to $500 in a country where the average annual income is under $2,000. The bank they had broken — Cosmos Co-Operative, India's second-oldest — had been compromised since September 2017 through phishing emails, giving the attackers control of the system that approves ATM withdrawals. Two months later they did it again to BankIslami in Pakistan for **$6.1m**.

What makes this file useful is who else it catches. The cards and the runner network came from **"Big Boss"** — Ghaleb Alaumary, a Canadian in Ontario, later sentenced to eleven years eight months. His contact was **Ramon Abbas**, "Hushpuppi," a Dubai Instagram influencer with 2.3 million followers and a flat in the Palazzo Versace. After the pair hit the Bank of Valletta in February 2019, launderers went shopping at Harrods and Selfridges for Rolexes, a Jaguar and an Audi.

The North Koreans, as always, walked. White's answer to "why indict people you can never try" is the most practical idea in the book: an indictment is a **demolition order**. The 179-page complaint against Park Jin Hyok listed his email accounts, his social profiles, his viruses and his tactics; later filings listed hundreds of Bitcoin wallets. Publishing it burns the infrastructure and builds a coalition of victims — Bangladesh, Pakistan, Sri Lanka, the Philippines, Slovenia and more.

The Second Look: the strategy has held. Since 2022 the FBI has published wallet lists within days of each major theft, and by 2025 that had become the standard first move — fifty Ethereum addresses were named five days after the Bybit hack. Nobody expects a trial. The point is to make the money harder to spend.

WHAT IT MEANS FOR YOU

1. **The state supplies the hack; organised crime supplies the hands.** Which is why the people who get caught are almost always the local helpers.
2. **Published wallet lists are a tool you can use.** When an exchange or analytics firm flags addresses, that flag propagates. It is the main reason stolen funds go stale.

> **BOTTOM LINE**
>
> *You cannot arrest them. You can make their money radioactive.*

CASE FILE 08

Everything the Book Didn’t Live to See

White closed the manuscript in 2021. Then the group became the largest crypto thief in history.

PERIOD: 2022–2026 · **SOURCE:** CHAINALYSIS, ELLIPTIC, TRM, FBI

The book’s final tally was $1.3bn. Chainalysis now puts the cumulative figure at roughly **$6.75bn** since 2016, with **$2.02bn stolen in 2025 alone**; CertiK counts 263 separate incidents. Estimators differ materially on earlier years — treat every annual figure as an estimate.

DATE	TARGET	TAKEN
Mar 2022	Ronin Bridge (Axie Infinity)	**~$620m**
Jun 2022	Harmony Horizon Bridge	**~$100m**
Jun 2023	Atomic Wallet	**>$100m**
May 2024	DMM Bitcoin	**$308m**
Jul 2024	WazirX	**$235m**
Feb 2025	Bybit	**~$1.5bn**
Apr 2026	Drift Protocol	**~$285m**
Apr 2026	KelpDAO / rsETH bridge	**~$290m**

Bybit is the one to understand. On 21 February 2025 roughly $1.5bn in ETH left the exchange — the largest theft in the asset class. Bybit itself was never breached. A developer at Safe{Wallet}, its multisig provider, was socially engineered into running a malicious project; from that laptop the attackers swapped one JavaScript file for a version that activated only for Bybit’s cold wallet, then restored the clean file two minutes after it fired. Eighteen months and a US court injunction later, Bybit has recovered or frozen about **5%**.

What changed, and what didn’t. Blender, Sinbad and eXch were each shut down and each replaced; a US appeals court struck down the Tornado Cash sanctions in November 2024, Treasury delisted the mixer in March 2025, and it remains in use. The durable pattern is the entry point: as Elliptic puts it, the initial compromise is now *overwhelmingly human*.

WHAT IT MEANS FOR YOU

1. **The attack is upstream of you.** Bybit’s users did nothing wrong. Judge a platform by its key management and its suppliers.
2. **Recovery rates are terrible.** Ronin ~10%, Bybit ~5%. Custody is the control; recovery is not.

> **BOTTOM LINE**
>
> *The book ends at $1.3bn. That total is now five times larger — and the method has not changed.*

CASE FILE 09

The Job Offer

The single most likely way this story reaches you personally.

PERIOD: 2022–2026 · **SOURCE:** DOJ, MICROSOFT, UNIT 42, ESET

The chapter White never wrote runs in two directions, and they are the same programme. In one, North Korean operatives *apply* for your job. In the other, they *offer* you one.

The workers. The Multilateral Sanctions Monitoring Team — the body formed after Russia vetoed the UN Panel of Experts out of existence in 2024 — estimates **1,000–2,000** DPRK IT workers placed abroad in at least eight countries, earning **$350–800m in 2024**, roughly half of it remitted home. They use stolen identities, AI-written profiles, and a US-based facilitator who hosts the company laptop in a "laptop farm" so the login looks domestic. In July 2025 Christina Chapman was sentenced to 8½ years for running one: **309 US companies**, 68 stolen identities, $17.1m generated. In June 2025 four DPRK nationals were charged with stealing over $900,000 in crypto *from the employers who hired them*. Eleven governments warned in July 2026 that AI is now used across the whole cycle — including manipulated video during interviews.

The offers. Palo Alto's Unit 42 named it **Contagious Interview**: a recruiter approaches on LinkedIn or Telegram, a technical interview is arranged, and at some point you are asked to run something — clone this repo, install this package, fix your camera by pasting this command. The payloads (BeaverTail, InvisibleFerret, OtterCookie) hunt browser credentials and dozens of wallet extensions. ESET found the malicious code hidden in comments positioned outside the visible editor window, so glancing at the file proves nothing. Kaspersky documented approaches to executives and VCs using *real recorded video of previous victims* to make the call look genuine, and a 30-minute deadline on the coding task to stop you thinking.

This is not a side channel. It is the main one: the DMM Bitcoin theft of $308m began with a fake recruiter sending a Python "pre-employment test" to an employee at a wallet-software supplier.

WHAT IT MEANS FOR YOU

1. **Treat every *npm install* from a recruiter as remote code execution.** Because that is exactly what it is.
2. **Never run an interview task on a machine holding keys.** Separate device, or a throwaway VM. No wallets, no seed, no production credentials.
3. **No legitimate employer asks you to paste a shell command to fix your camera.** That prompt is the attack, every time.

> **BOTTOM LINE**
>
> *The state that robbed a central bank now sends job offers. Yours is a plausible target.*

FIELD MANUAL

What It Means for Your Wallet

The practical residue of ten case files — for people who hold crypto and work in tech.

AUDIENCE: EVERY CRYPTO USER · **SOURCE:** FILES 00–09

You are not a central bank. You are still in scope — because the entry point in nearly every case in this book was one ordinary person with an inbox. The rules the files teach:

1. **The recruiter is the threat model now** (files 06, 09). Unsolicited role, generous salary, a repo or installer in the process. Verify the company through its own official channels, never a link the "recruiter" gives you.
2. **Keys never touch a machine that runs other people's code** (files 08, 09). A hardware wallet on a laptop where you also test strangers' repositories is not cold storage. Separate the devices.
3. **Never paste a command you don't understand** (file 09). Camera errors, "SDK updates," driver fixes — the fake error *is* the delivery mechanism.
4. **Judge a platform by its suppliers** (file 08). Bybit lost $1.5bn without being breached. Ask who signs, how many signers, and who else can touch the code you trust.
5. **Assume recovery is zero** (files 04, 08). Ronin returned about 10%, Bybit about 5%. Self-custody what you cannot afford to lose, and treat any exchange balance as a promise.
6. **Patch, and turn on automatic updates** (file 05). WannaCry's fix was months old. Every unpatched machine that day was a choice someone made.
7. **Slow down when someone imposes a deadline** (files 02, 09). Thirty-minute coding tests, urgent transfers, expiring offers. Manufactured urgency is the oldest tool in the book and still the most effective.
8. **Backups must be offline** (files 01, 05). Wipers and ransomware both destroy anything they can reach. If your backup is reachable from the infected machine, you do not have one.

> **BOTTOM LINE**
>
> *A nuclear state with no money has decided your inbox is a revenue stream. Act accordingly.*

THE VERDICT

The Book, Weighed

Published 2022 — graded against what followed.

AUTHOR: GEOFF WHITE, INVESTIGATIVE JOURNALIST
GRADE: ESSENTIAL, WITH AN ASTERISK

The best available account of how a state turned itself into a criminal enterprise — and the only one that keeps its eye on the people it cost. The scoreboard:

- ✓ **It explains the motive, not just the method** — the famine, the ratchet effects, the superdollars. Without those chapters the hacking reads as villainy; with them it reads as economics.
- ✓ **Its central warning aged perfectly** — that laundering, not hacking, is the constraint, and that the group was learning to remove it. Everything since 2022 has proved it right.
- ✓ **It gives the victims real pages** — the Sony employee still living with an exposed Social Security number, the Bangladeshi farmers' money, the cancelled heart operation. Journalism, not thriller.
- ✓ **It is honest about attribution** — including White's own warning that "Park Jin Hyok" may itself be the last layer of the doll. Rare intellectual discipline in this genre.
- × **The crypto material is the thinnest part, and the most overtaken** — it ends around 2020, before Ronin, DMM, Bybit and the entire IT-worker scheme. Files 08 and 09 exist because of this gap.
- × **The reader is left with awareness, not a method** — the closing call to be "the last line of defence" is correct and unactionable. See our Field Manual on the previous page.

Final grade: the essential companion to *Tracers in the Dark*. Greenberg wrote the hunters; White wrote the hunted. Read Greenberg to learn that the ledger convicts, then read White to see who builds an economy on top of it anyway. Buy the book for the case files — come to us for the five years it never saw.

> **BOTTOM LINE**
>
> *White documented a bank robbery crew. Since he closed the manuscript, they became the largest crypto thief in history.*