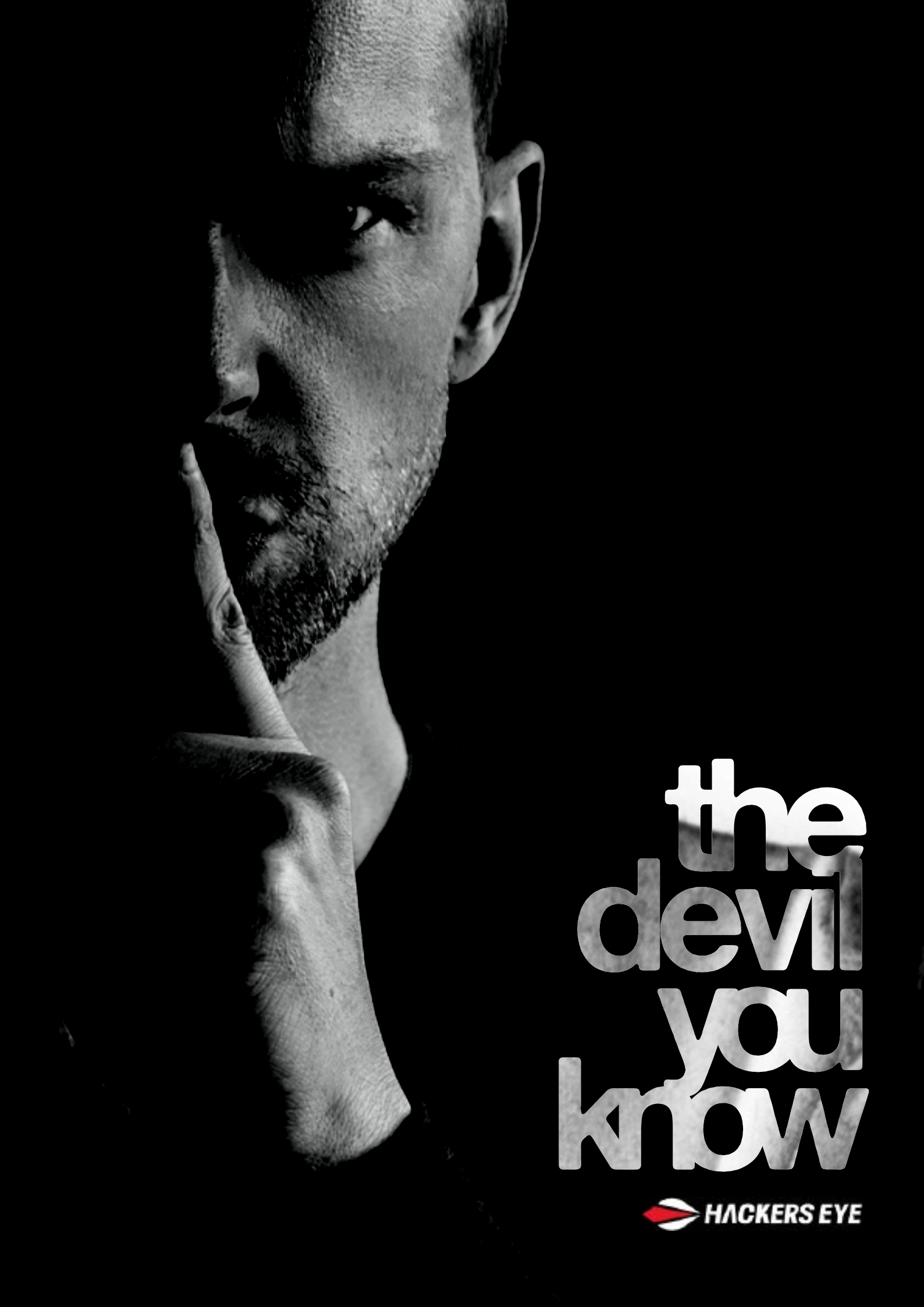

HACK
icarus or daedalus
onetwozerotwosix


TURN'T
CREW

barcodesecurity.com


CVI
DISTO
POD

BER
RTION
CAST


the
devil
you
know
HACKERS EYE

Is there a pronoun for the symbiote?

Will proprietary code and vendor NDAs eventually fuse with the deepest, darkest secrets of the human soul? By the time these technologies become “transparent,” will secrecy itself still exist, or will it be a quaint artifact, like air-gapped networks and offline backups?

While others argue in circles about the ethical use, misuse, or tasteful integration of what might broadly be called transhuman technologies, my mind drifts somewhere more on brand. Somewhere colder. Somewhere operational.

We have never seen an attack surface like this before.

This isn’t just about software anymore. It’s not even about humans in the loop. It’s about humans as the loop. Memory, intent, bias, fear, desire, and identity wrapped in APIs we barely understand and threat models we haven’t had the language to write yet. When cognition becomes an extension point, where does the boundary of compromise even sit? At the firmware? The model weights? The wetware?

Threat actors won’t need to steal secrets if they can shape them. They won’t need persistence if they can influence recall. Supply chain attacks will look almost polite compared to what happens when trust, perception, and decision-making become injectable components. Imagine phishing, but the payload is belief. Imagine malware, but the exploit is empathy.

The old security questions start to sound naïve. What does least privilege mean when the system is you? What does incident response look like when rollback isn’t possible and forensics means introspection? How do you disclose a breach when the asset compromised is identity itself?

This is not science fiction. This is pre-incident reporting.

Somewhere ahead of us is a future where proprietary algorithms, biometric telemetry, and human intuition cohabitate in the same black box. Where NDAs don’t just protect code, they protect cognition. And when that box is finally pried open, if it ever is, we may discover that secrecy didn’t disappear. It just migrated inward.

We should probably start threat modeling that. Because whatever you want to call the symbiote, it’s already probing for weaknesses.

CONTENTS

From this issue, articles can also be found in digital format on the HVCK magazine wesite.
For information about article submission and syndication check the website


DAH


CK
industry

The syscall shaman, and the gospel of Exploit Pack

There are people in offensive security who collect certs like airport souvenirs, and then there are people who ***bleed into the kernel***. Juan Sacco belongs to the latter category. Call him a syscall shaman, a bootkit brujo, not because he does, but because once you've watched someone casually talk about ring-0 like it's a familiar alleyway, you start reaching for mythological language just to keep up.

Exploit Pack is not a product that fell out of a boardroom. It's a weapon that crawled out of malware analysis labs, botnet dissections, and long nights staring at Windows internals until they blinked first. For nearly two decades, Exploit Pack has carried the fingerprints, habits, and instincts of its creator, evolving alongside him, mutating as the threat landscape mutates, staying stubbornly offensive in a world increasingly obsessed with safe abstractions and glossy dashboards.

This is not a startup fairy tale. **It's a field report.**

Born in the Botnet, Not the Boardroom

Exploit Pack didn't begin as a pentesting framework. It began as a question.

Juan was knee-deep in real malware, ZeuS, back when it was eating the financial sector alive. While

everyone else was panicking about fraud losses, he was tearing the thing apart, tracing how infections actually *landed*. That's where the exploit kits lived. Browser bugs. RCE chains. Dirty, effective, brutally practical.

Attackers had curated arsenals. Defenders had PDFs. So he flipped the script.

> **"The Exploit Pack idea came out after working as a malware analyst with botnets such as ZeuS."**

That understatement hides the real implication: this framework was inspired by *crimeware efficiency*, not academic theory. It wasn't meant to simulate attacks, it was meant to *****feel like one***.**

The name stuck because it was literal. A pack. Of exploits. No mysticism required.

A Career Spent Crossing the Line (Legally)

Juan's background reads less like a résumé and more like a border-crossing logbook. Pentester. Exploit writer. Malware analyst. Vulnerability researcher. Bank defenses at ING. Commercial offense at Core Security. Threat analysis at NOD32. Even time working alongside Homeland Security in Argentina.

That kind of career doesn't give you a single worldview, it gives you *contrast*. You see what breaks in production. You see what auditors miss. You see how attackers actually chain bugs together when nobody's watching.

That's why Exploit Pack never pretended to be "ethical" in the marketing sense. It's ethical in the *knife safety* sense: dangerous, deliberate, and designed for people who know what they're holding.

> "We are trying to disrupt, attack and mitigate," Juan says. No euphemisms. No comfort blankets.

Engineering by Instinct, Not Fashion

The tech stack tells the same story. Early experiments with Python GTK+. A brief, ill-fated flirtation with C# and Visual Studio. Eventually landing on something that just worked: Java for the GUI, Python for the engine.

Not because it was trendy, but because it was portable, flexible, and didn't get in the way.

Exploit Pack doesn't care what language your exploit is written in. If the interpreter exists, it'll run it. That decision alone tells you who this was built for: **people who already write their own weapons and don't want a framework second-guessing them.**

And the arsenal grew. Relentlessly.

Today it ingests tens of thousands of public exploits scraped from the raw edges of the internet, GitHub, Packet Storm, Full-Disclosure, then layers in curated n-days that can quietly turn a "medium" finding into a "we need to talk" meeting.

This isn't about spray-and-pray. It's about leverage.

Control, Kernel, and the Point of No Return

Then things got… heavier.

Control Pack pushed post-exploitation into evasive territory: agents across Java, C++, .NET, VBS, Python, built to live longer than they should. To dodge EDR. To linger.

But **Kernel Pack** is where the brujo emerges.

Ring-0. Rootkits. Privilege escalation. Kernel-mode command-and-control.

Most commercial vendors won't touch that space. Too dangerous. Too messy. Too hard to explain to compliance. Juan went straight at it.

Windows kernel exploitation is still treated like forbidden scripture, passed around in fragments, guarded by gatekeepers. Kernel Pack was an act of heresy: *here's what it actually looks like, here's how it actually works*.

> "Arbitrary code execution in the kernel is game over," he says. No hype. Just physics.

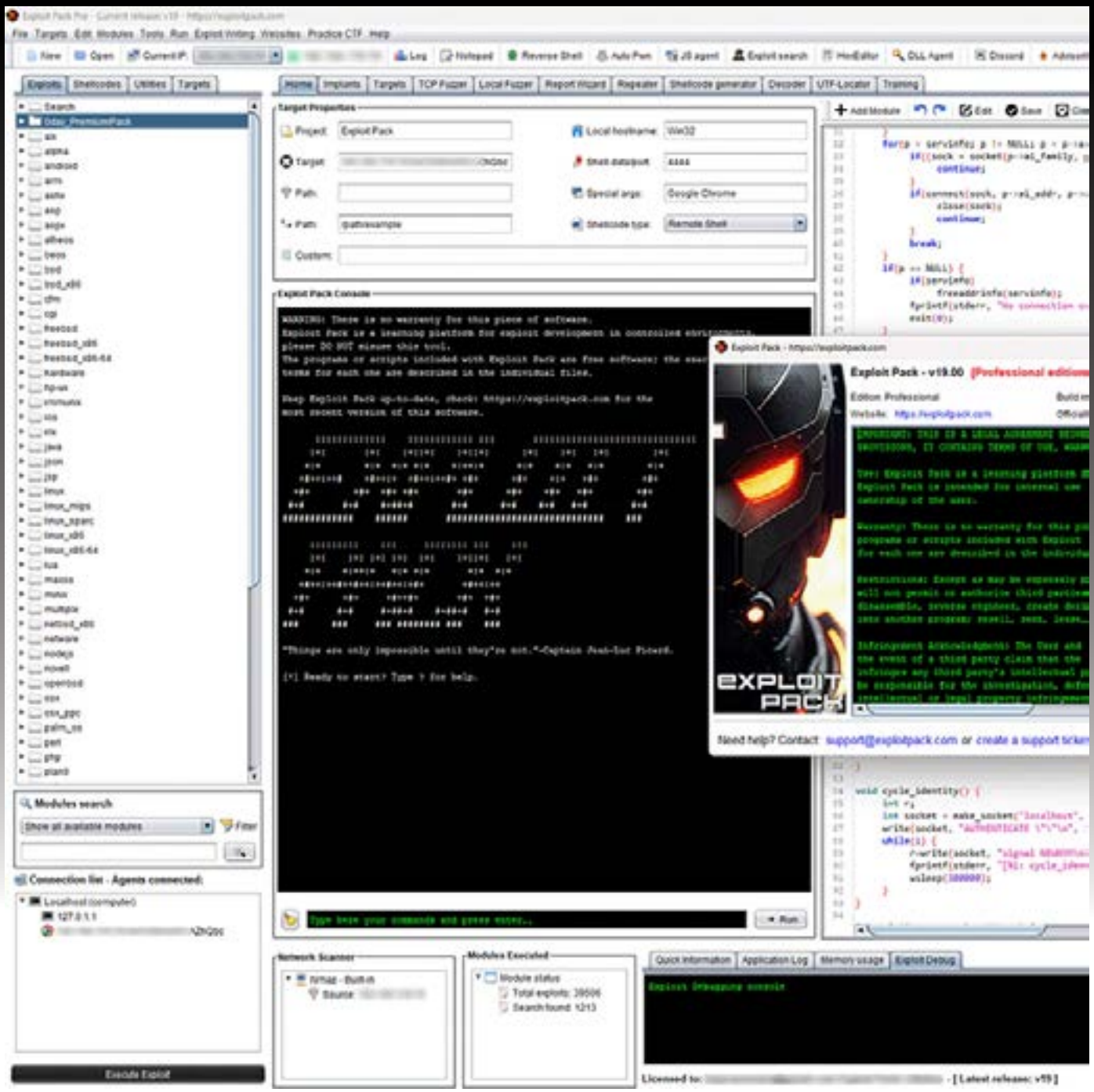
Small Shop, Heavy Hits

Exploit Pack lives in the shadow of giants, Metasploit, Cobalt Strike, platforms with budgets big enough to buy entire conferences. Juan doesn't pretend otherwise.

> "We are a small company but we kick hard."

That's not bravado, it's strategy. When you're small, you don't chase feature parity. You chase ***sharp edges***. Things others avoid. Capabilities that matter when time is tight and reports need teeth.

Even the GUI reflects that mindset. No sprawling CLI incantations. No endless flags. Wizards. Simple flows. Fast execution.



Because when you're on engagement hour six and the window is closing, ergonomics matter.

Power, Ethics, and the Loaded Gun Problem

Shipping kernel-level tooling comes with consequences, and Juan doesn't dodge that reality. You can watermark users. Secure delivery channels. Cooperate with law enforcement when things go sideways.

But you can't make a loaded gun harmless."We cannot prevent misuses," he admits.

That's the uncomfortable truth of offensive tooling: capability doesn't care about intent. Exploit Pack assumes the operator knows the rules, and knows when they're breaking them.

That trust is part of the deal.

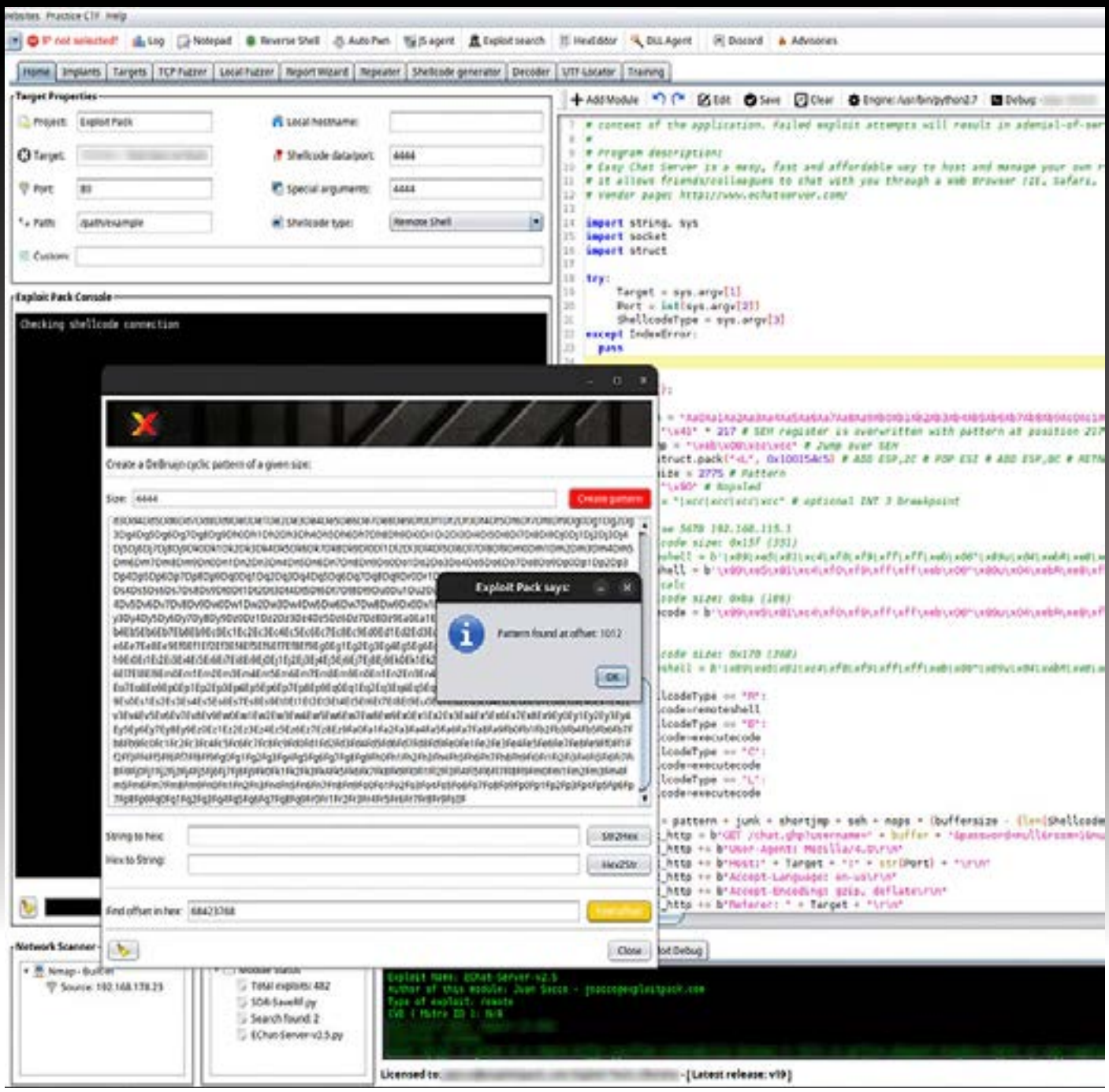
Muscle Memory Over Slide Decks

If there's a single through-line in everything Juan builds, it's contempt for passive learning.

Bootcamps aren't about slides. They're about typing. Failing. Fixing. Doing it again.

> "There is muscular memory associated with typing and doing your own stuff."

That philosophy is baked into Exploit Pack itself. It won't save you if you don't understand what you're launching. It won't hide the mechanics. It hands you the blade and expects you to know which end cuts.



That's why the syscall shaman label fits, not as mysticism, but as intimacy with the machine at its lowest level.

Open Sourcing the Dark Arts

In a move that surprised more than a few people, Juan plans to open-source the agents behind Control Pack and Kernel Pack. Not the framework glue, but the guts.

That's not altruism. It's lineage.

Let others learn. Tear it apart. Improve it. See how real-world offensive tooling is actually built, not the sanitized conference version.

AI-assisted discovery is coming. Deeper kernel work is coming. The research never stops because the adversary never does.

The Craftsman Still at the Workbench

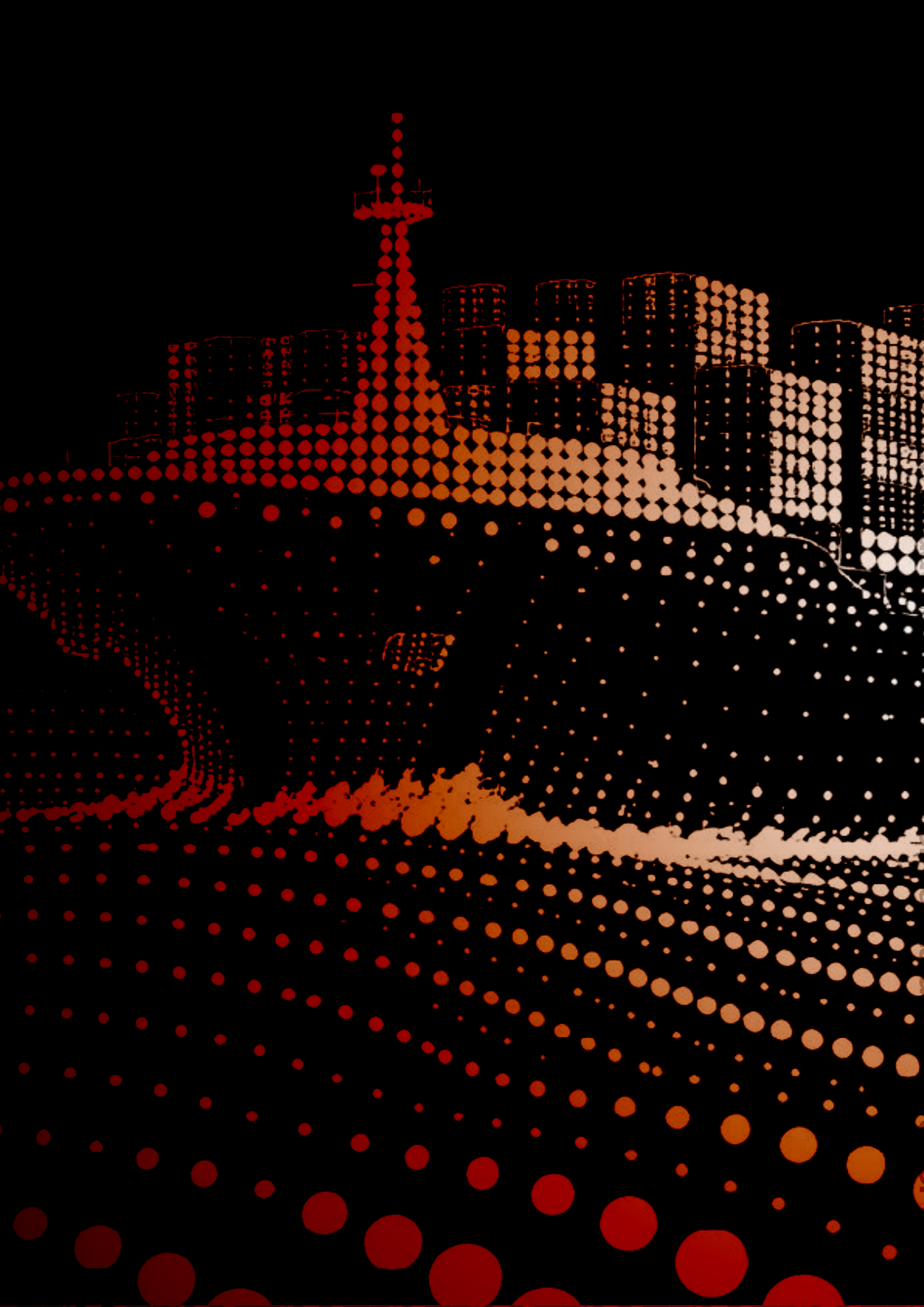
In an industry drowning in branding, Juan Sacco remains stubbornly close to the metal. Exploit Pack isn't chasing mass adoption. It's serving people who still believe security is learned by breaking things, carefully, deliberately, and with intent.

The syscall shaman. The bootkit brujo. Not titles he asked for, but ones earned by spending a career where the abstractions end and the consequences begin.

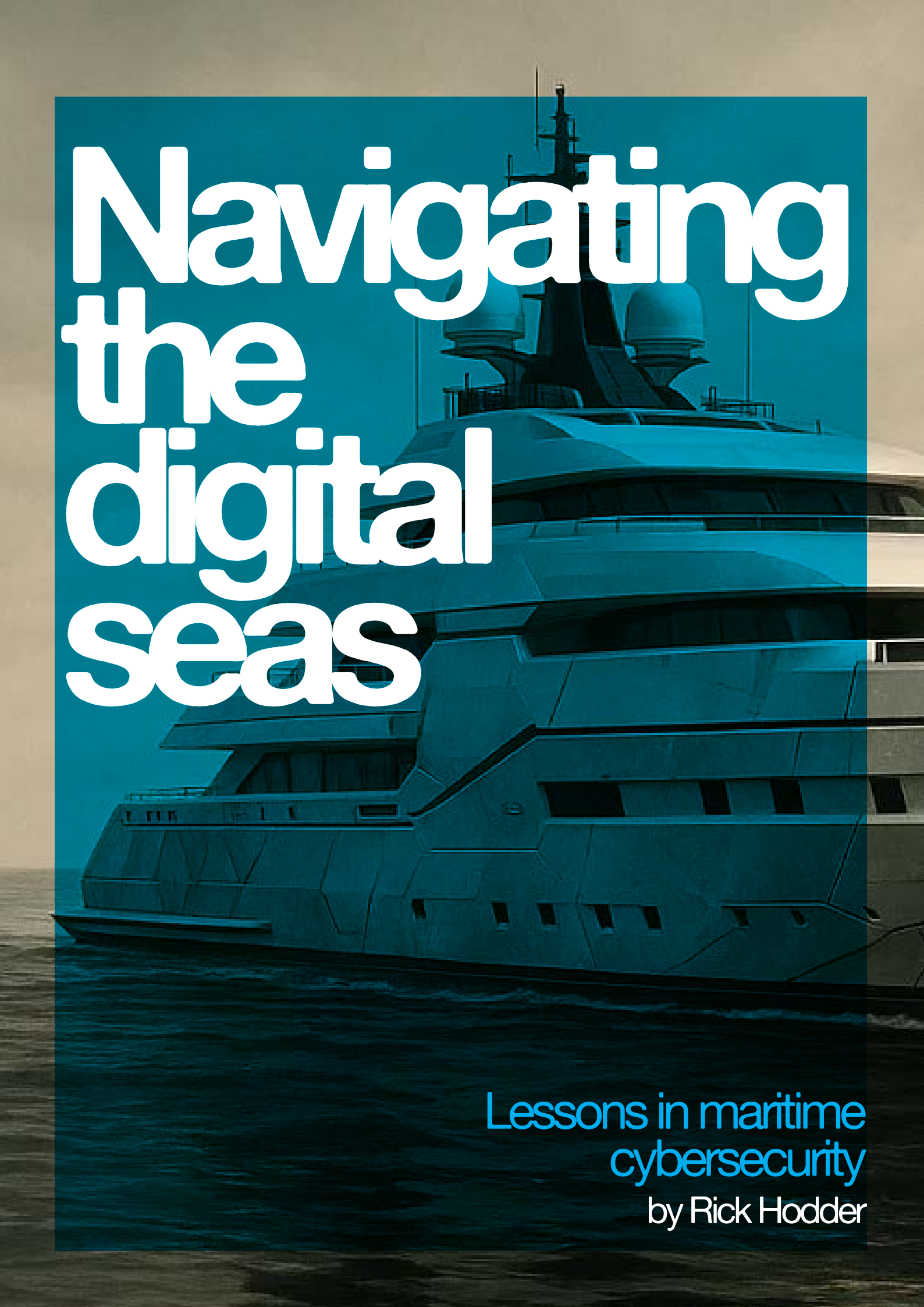
Exploit Pack isn't magic.*It's craft.

And after nearly twenty years, it's still sharp.

exploitpack.com




HACK
CISO



Navigating the digital seas

Lessons in maritime cybersecurity

by Rick Hodder

The Maritime Sector's Cybersecurity Awakening

The maritime industry is the backbone of global trade, transporting over 90% of the world's goods. Yet, it faces a growing digital threat landscape, where cyber incidents have the potential to cripple operations, endanger crews, and disrupt global supply chains. As this industry embraces interconnected technologies – from IoT and satellite navigation to automated control systems – it simultaneously exposes critical vulnerabilities that cybercriminals increasingly target.

For years, I observed how the maritime sector, long focused on physical and operational safety, was unprepared for the realities of digital threats. My own career took a pivotal turn as I became more deeply involved in understanding these risks and implementing cybersecurity practices across complex maritime environments. What was once an overlooked issue is now a pressing priority.

Threats like ransomware, GPS spoofing, and supply chain vulnerabilities have not just emerged but transformed from theoretical risks into immediate dangers. Recent mandates, such as the International Maritime Organisation's (IMO) 2021 cyber risk management requirements, underscore the urgency. But it's not just about catching up with other critical industries; it's about adapting and building resilience in the face of these transformative threats.

This article shares lessons learned from my experience in the field, shedding light on the distinctive challenges of maritime cybersecurity and the evolving solutions that can help secure this essential sector.

Maritime Sector Cyber Threats: An Overview

The introduction of digital technology to maritime operations has undoubtedly increased efficiency and opened the door to complex cybersecurity risks. From bridge systems to port logistics, interconnected platforms and remote-access technologies create previously unimaginable vulnerabilities.

One of the most troubling risks is GPS spoofing and navigation interference, which can steer vessels off course, putting them at risk of grounding or collision. While GPS systems were once considered a navigational cornerstone, recent incidents have demonstrated how easily they can be manipulated. For instance, a 2024 spike in GPS spoofing in the Baltic Sea – likely linked to geopolitical tensions – caused navigation disruptions for both commercial and military vessels, underscoring how national conflicts can extend to the digital maritime domain. These events illustrate that cyber risks are not only about data breaches but also about physical safety.

Ransomware attacks are another persistent threat, capable of paralyzing entire supply chains. The 2017 NotPetya attack on Maersk offered a stark lesson: a single ransomware incident can have global ramifications, halting operations at ports worldwide and costing hundreds of millions of dollars in losses. Maritime organizations have increasingly become prime ransomware targets due to their critical role in logistics and relatively low cybersecurity maturity.

The industry's reliance on third-party systems and vendors also introduces significant supply chain vulnerabilities. Many ships and ports operate using third-party technologies, from navigation software to port management systems, each with varying levels of security. A breach within any one of these systems can cascade through interconnected networks, potentially compromising critical operations across the sector.

The lesson here is clear: maritime cybersecurity must go beyond physical security to encompass modern maritime operations' increasingly digital and interconnected nature.

My Journey into Maritime Cybersecurity

My career in cybersecurity began two decades ago, during the early days of the internet. Having studied Internet Technology, I started my journey by diving into global telecommunications, intrigued by how networks connect people and systems worldwide. Over time, I developed a broad skill set in pen testing, secure network design, and compliance, working in sectors like finance, oil and gas, and satellite communications. In each role, I encountered unique cybersecurity challenges that required a solid technical foundation and the ability to navigate complex regulatory landscapes.

Early on, I worked with global banks such as Goldman Sachs, HSBC, and the infamous Lehman Brothers, where high-stakes environments and complex network infrastructures demanded meticulous security practices. These experiences solidified my understanding of secure network architecture and sparked my passion for demystifying cybersecurity. I soon realised how critical it is to translate technical complexities into clear, actionable insights—a skill that has become invaluable in my later work with maritime clients.

A pivotal moment in my career came when I transitioned into the oil and gas sector. Working with satellite-based communications, I encountered an entirely different set of network challenges. The slower, less reliable connectivity over

satellite networks exposed gaps in traditional security approaches, forcing me to think creatively about securing systems that often-lacked real-time updates. This shift gave me valuable insight into how cybersecurity must adapt to environments where systems can't always be monitored or updated instantaneously - a reality shared by the maritime sector as a whole.

This technical background led me to maritime cybersecurity, where I saw an urgent need for robust security practices but a gap in industry-wide expertise. Recognising that many vessels and maritime operations were vulnerable to modern cyber threats, I founded Pelion Consulting, offering tailored cybersecurity services for the yachting and maritime industries. From secure network design to risk assessment, my focus has been on helping clients build cybersecurity postures that protect not only data but the critical control systems at the heart of maritime operations.

Today, my role has expanded to advisory and assessment work, including leading Cyber Essentials assessments with Astrix Cyber Security for businesses of all type. I am passionate about raising awareness in the maritime sector and helping crew members, owners, and operators understand the cybersecurity landscape they navigate. With an advanced degree in cybersecurity and certifications such as CSTM, I remain committed to advancing my knowledge – particularly in operational technology (OT) security – to address the evolving needs of the maritime industry.

Through this article, I hope to share the lessons I've learned and highlight the evolving landscape of maritime cybersecurity, offering a roadmap for securing this essential industry.

Challenges in Implementing Cybersecurity in Maritime Operations

Securing maritime operations is complex, with distinct challenges tied to the industry's unique operational environment, cultural barriers, and regulatory requirements. Unlike sectors with controlled environments, ships often operate in isolation, making cybersecurity implementation incredibly challenging.

One primary issue is the inherent isolation of vessels at sea. Unlike land-based organisations, vessels rely heavily on satellite networks, which are susceptible to jamming and interception. Updating or patching systems while ships are on extended voyages is challenging, meaning systems often remain outdated and exposed. I've seen firsthand how some ships continue to run on unsupported software simply because connectivity limitations make regular updates impractical.

Another significant hurdle is the cultural resistance to cybersecurity within the maritime industry. Many operators and crew members view digital security as an administrative burden rather than an operational necessity, largely because the industry has long prioritised physical threats over digital ones. As I've worked with crews over the years, I've noticed that they often view cyber regulations as yet another compliance box to check. This mindset can lead to minimal implementations, where protections are only as strong as the minimum requirements, exposing vessels to evolving threats. Overcoming this cultural resistance and fostering a proactive approach to cybersecurity is a key challenge in securing the maritime industry against digital threats.

Regulatory complexity adds further challenges to cybersecurity implementation in the maritime industry. The IMO's cyber risk management guidelines, implemented in 2021, were a significant step forward, but compliance remains inconsistent across regions. Commercial vessels typically meet these standards, while many private yachts and smaller vessels remain exempt, creating a patchwork of cybersecurity practices. Achieving consistent cybersecurity standards globally will require continued coordination among international bodies and a commitment to enforcement. This regulatory complexity and inconsistency present a significant challenge in ensuring a uniformly high level of cybersecurity across the maritime industry.

Finally, supply chain dependencies exacerbate cybersecurity risks in the maritime industry. Ports and vessels often rely on third-party technology providers who may not share the same security standards, exposing critical systems. The lack of consistent security standards across the maritime supply chain introduces further vulnerabilities, as an attack on one vendor's systems could have ripple effects throughout maritime operations. This interconnected nature of the maritime industry means that a cyber-attack on a single entity can potentially disrupt the entire supply chain, highlighting the need for a comprehensive and collaborative approach to cybersecurity.

These challenges underscore the benefits and essentials of a holistic approach to cybersecurity . One that incorporates physical, digital, and cultural dimensions is necessary to secure the future of maritime operations. It's about addressing individual threats and building a comprehensive and resilient cybersecurity strategy.

Key Lessons Learned

Through my experiences, I've learned several key lessons about building resilience in maritime cybersecurity.

Firstly, crew awareness and training are vital. We are the weak link in the chain. Human error, often through phishing or weak passwords, is a primary cause of breaches. Establishing a strong cybersecurity culture through continuous training and hands on experience has proven essential in my experience. I've seen how even basic cybersecurity knowledge, like spotting phishing emails or practicing secure password management, can empower crew members to act as the first line of defence.

A challenge though is finding ways to engage crew members. We all learn differently and the topic of cyber security switches many people off, especially through the traditional ways of learning. Gamification and hands on training has proven successful in making the message stick.

Another crucial lesson is the value of a robust incident response plan. Incidents – whether ransomware, GPS spoofing, or data breaches – can escalate quickly, especially given the isolated nature of maritime operations. Having clear protocols, such as instructions for disconnecting compromised systems or managing encrypted backups, helps crews respond effectively and contain potential damage.

Knowing who is responsible and having someone onboard take accountability when an event does happen is crucial to resuming normal operations as efficiently as possible.

Collaboration across industry and regulatory bodies is also essential. Given the international nature of maritime operations, the IMO's cyber risk guidelines have provided a much-needed foundation. Still, partnerships with cybersecurity firms and training institutions can fill knowledge gaps and bring critical expertise into the sector. I've seen how partnerships with cybersecurity specialists and access to advanced tools make a real difference in closing security gaps.

Finally, the most important lesson is treating cybersecurity as integral to maritime safety. This means moving beyond regulatory compliance to adopt a proactive approach, where cybersecurity is viewed as a necessity rather than an added burden. Adopting industry best practices voluntarily ensures that the sector can remain resilient against emerging threats.

Cybersecurity in maritime operations is more than a technical challenge – it requires cultural shifts, proactive planning, and strong industry collaboration.

Case Studies of Noteworthy Incidents in Maritime Cybersecurity

Real-world incidents underscore the importance of cybersecurity in the maritime sector, highlighting both the risks and the responses required.

Case Study 1: Maersk and the NotPetya Attack

The 2017 NotPetya ransomware attack on Maersk underscored the potential scale of a cyber-attack on a global operator. When NotPetya infiltrated Maersk's systems, it disrupted operations across multiple terminals, resulting in losses exceeding $300 million. Only a single unaffected server allowed Maersk to restore operations, illustrating the critical need for distributed backups and rapid incident response. It's worth noting that Maersk was not the target of this ransomware, but unfortunate collateral.

During the early 2000s a colleague of mine, working for IBM at the time was contracted to audit Maersk's infrastructure. There were several recommendations he made that the company could have implemented to mitigate the risks of cyber-attack affecting the business which they declined to do. The rest is now history.

Case Study 2: GPS Spoofing in the Baltic Sea

In 2024, multiple vessels operating in the Baltic Sea reported GPS spoofing incidents, likely as part of Russia's hybrid warfare tactics. GPS spoofing has evolved into a sophisticated attack vector that poses a serious threat to maritime navigation. Unlike jamming, which disrupts GPS signals, spoofing involves broadcasting counterfeit GPS signals that deceive receivers into reporting false locations. This attack method exploits the unencrypted nature of standard GPS signals, making it a favoured tactic in areas of geopolitical tension or where adversaries seek to disrupt critical infrastructure.

In early 2024, multiple vessels operating in the Baltic Sea reported significant navigation anomalies. Ships suddenly found their GPS coordinates drifting inland or into restricted zones, triggering navigation alerts and forcing crews to switch to manual operation. An investigation linked the spoofing activity to electronic warfare systems positioned near the Kaliningrad region, suggesting it was part of a broader Russian strategy aimed at testing NATO's maritime defences. The spoofed signals mimicked legitimate GPS data but introduced slight, gradual drifts to avoid immediate detection. This type of low-noise attack bypasses traditional anomaly detection systems, highlighting a key vulnerability in relying solely on GNSS data for navigation

The attackers employed a technique known as carry-off spoofing, where counterfeit signals gradually overpower the authentic ones without causing an abrupt shift. By aligning the spoofed signals closely with the legitimate ones, the attackers ensured that shipboard receivers locked onto the stronger, fraudulent signals. This approach exploited the

inherent trust in satellite-based positioning, leveraging signal strength and timing data to mislead onboard navigation systems. The success of the attack was amplified by the use of low-cost, portable transmitters, demonstrating how readily accessible technology can be weaponised for state-level hybrid warfare.

In response, several shipping companies and maritime cybersecurity firms began implementing multi-band GNSS receivers capable of processing signals from multiple satellite constellations (e.g., GPS, Galileo, GLONASS). These receivers use advanced algorithms to cross-check positional data, flagging inconsistencies that might indicate spoofing attempts. Some vessels have adopted radio frequency (RF) anomaly detection systems, which monitor for unusual RF patterns indicative of spoofing equipment in the vicinity.

The industry is also exploring quantum-resistant satellite communications, leveraging new encryption methods to secure GNSS signals against interception and manipulation. Moreover, integrating terrestrial-based navigation systems, such as Enhanced Loran (eLoran), provides an independent backup that can verify GNSS data integrity, reducing the risk of spoofing-induced navigational errors. Looking ahead, emerging solutions like blockchain-based position verification are being piloted to create an immutable record of navigational data, further enhancing trust in critical positioning systems

Case Study 3: Invoice Fraud and Third-Party Supply Chain Threats

The maritime industry's reliance on a complex network of third-party suppliers introduces significant cybersecurity risks, with invoice fraud emerging as a critical threat vector. These attacks typically exploit weak email security and insufficient verification processes in vendor communications, making them a prime target for sophisticated threat actors.

In a recent case, a large maritime logistics firm suffered substantial financial losses after falling victim to a well-executed invoice fraud scheme. The attackers initially compromised the email system of a key supplier, using a phishing attack that targeted outdated email infrastructure. Once inside, they conducted reconnaissance on internal communications, observing typical invoicing patterns and identifying high-value transactions. They then intercepted genuine invoices and subtly altered the payment details, redirecting funds to accounts controlled by the attackers. By mimicking the supplier's writing style and including accurate purchase order information, the fraudulent emails bypassed both automated filters and manual checks, resulting in over $750,000 in losses before the breach was detected.

The rise of invoice fraud underscores the broader need for enhanced supply chain cybersecurity. As maritime operations become increasingly digitised, the industry must recognise the critical importance of third-party risk management. This includes conducting thorough cybersecurity audits of suppliers, enforcing strict compliance with security standards, and leveraging advanced technologies like blockchain and AI-driven analytics.

Looking forward, integrating Distributed Ledger Technology (DLT) and expanding the use of token-based authentication for vendor transactions could provide an additional layer of security, making it more difficult for attackers to alter financial data without detection. The case serves as a stark reminder that the weakest link in the cybersecurity chain is often external, necessitating a comprehensive, end-to-end approach to safeguard financial transactions and maintain trust across the maritime supply chain

The multifaceted nature of maritime cybersecurity risks demonstrates the importance of a comprehensive approach that includes robust technology, clear response plans, and a security-aware crew.

Emerging Trends and Technologies

As maritime operations continue to evolve digitally, advanced technologies are essential for managing the escalating complexities of cybersecurity. Key innovations are enhancing security at the vessel level and driving industry-wide changes that address today's cyber risks while laying the groundwork for a resilient future.

AI-Driven Threat Detection and Predictive Analytics

Artificial Intelligence (AI) and machine learning (ML) are revolutionising threat detection in maritime cybersecurity, offering autonomous monitoring of network traffic and operational patterns. Unlike conventional detection systems, AI-driven platforms provide continuous anomaly detection, dynamically adjusting to identify even subtle deviations. For example, AI tools can recognise minor fluctuations in login behaviour, flag unusual traffic patterns, or detect data exfiltration attempts. This is particularly valuable on vessels, where immediate response may not always be feasible.

AI also enhances predictive analytics, crucial for anticipating vulnerabilities. By processing historical incident data, AI can project probable future threats and suggest proactive measures. This predictive capability has a significant role in dynamic risk assessment, especially in high-risk zones like the Baltic Sea. Additionally, recent advances in edge computing allow AI systems

to process data locally, making real-time analysis viable even with the limited connectivity common in maritime settings. AI systems are expected to integrate deeper with vessel automation, expanding their role from mere threat detection to actively mitigating threats by autonomously activating defensive protocols.

Blockchain for Immutable Data Integrity and Secure Transactions

With its decentralised and tamper-proof design, blockchain technology addresses the maritime sector's need for verified, traceable data across global supply chains. By logging cargo movements and transaction histories in an immutable ledger, blockchain enables transparency and significantly reduces the risks of data falsification. This is essential for high-value cargo shipments and regulatory compliance, especially when tracking goods across jurisdictions with varying security standards.

In practice, blockchain supports smart contracts that automatically execute transactions upon meeting pre-defined conditions. For example, when a shipment reaches a specific port and verifies proper storage conditions, the blockchain can autonomously release funds, reducing administrative overhead and eliminating manual verification steps. Furthermore, blockchain's decentralised architecture allows for seamless data sharing among authorised parties without relying on a centralised database, reducing a single point of failure and enhancing resilience against data breaches. Industry forecasts predict that blockchain-based applications will eventually standardise international shipping documentation, facilitating compliance and reducing costs tied to traditional paperwork and fragmented reporting. This can also have implications in the wide spread trafficking of illegal goods.

Enhanced Positioning with Satellite-Based Encryption and Alternative Navigation Systems

GPS's vulnerability to spoofing and jamming, especially in contested regions, necessitates adopting more secure and resilient navigation systems. Low Earth Orbit (LEO) satellites, operating at lower altitudes than traditional GPS satellites, deliver enhanced positional accuracy and are more challenging to interfere with, providing a robust alternative. LEO satellites create a more reliable infrastructure for secure maritime navigation in conjunction with multi-band GNSS receivers and encrypted communication channels.

In high-risk zones, encrypted GPS signals further reduce exposure to spoofing. These encrypted transmissions require specific decryption keys, making it considerably more challenging for adversaries to manipulate location data. Additionally, integrated redundant positioning systems, combining satellite data with terrestrial-based radio or optical sensors, enhance navigational accuracy in areas prone to interference. As these systems develop, they promise to provide comprehensive, multi-layered positioning information, ensuring vessel navigation remains precise and protected in volatile regions like the Baltic Sea. The maritime sector is expected to see wider implementation of these systems, with the ultimate goal of minimising reliance on traditional GPS by integrating multiple positioning sources.

Zero-Trust Architecture for Enhanced Access Control

Zero-trust architecture, based on the principle of "never trust, always verify," offers a robust approach to managing access in maritime networks. Given the complex ecosystem of users, third-party vendors, and operational systems, zero-trust enforces stringent authentication at each access point. In this model, no entity – whether internal or external – can access systems without continuous verification. This is particularly effective in reducing risks associated with lateral movement, where an attacker who gains initial access could otherwise exploit gaps to reach critical systems.

For maritime environments, zero-trust architecture segments networks into isolated zones, granting users only the permissions necessary for their role and requiring multi-factor authentication (MFA) for access across segments. This model is especially valuable for mitigating insider threats and managing third-party access, as it limits visibility to only those data and systems essential for each role. Moreover, zero-trust integrates seamlessly with AI-driven threat detection to flag abnormal access attempts, such as unexpected login locations or unauthorised data requests. In the future, zero-trust protocols will likely integrate directly into vessel architecture, with real-time verification happening across both shipboard and shore-side systems to adaptively respond to shifting threat conditions.

5G, Starlink, LEO and IoT Integration for Real-Time Monitoring and Automation

With the expansion of technologies such as 5G, LEO and Starlink, vessels can achieve lower latency and faster data transfer, supporting a new wave of IoT-based operational monitoring and automation. IoT sensors monitor everything from engine efficiency and cargo conditions to environmental parameters, generating real-time insights that enable predictive maintenance, fuel optimisation, and compliance monitoring. 5G and Starlink have low-latency communication that facilitates continuous updates, allowing shore-based teams to stay closely connected with vessel

operations, even in more remote regions.

However, the integration of IoT presents a significant cybersecurity challenge, as each connected device becomes a potential entry point. Addressing this vulnerability requires robust endpoint security and network segmentation so IoT devices can operate autonomously while isolated from critical systems. As 5G and LEO satellite networks expand, vessels will benefit from more reliable connectivity, even in open seas, allowing for real-time system updates and streamlined cybersecurity monitoring.

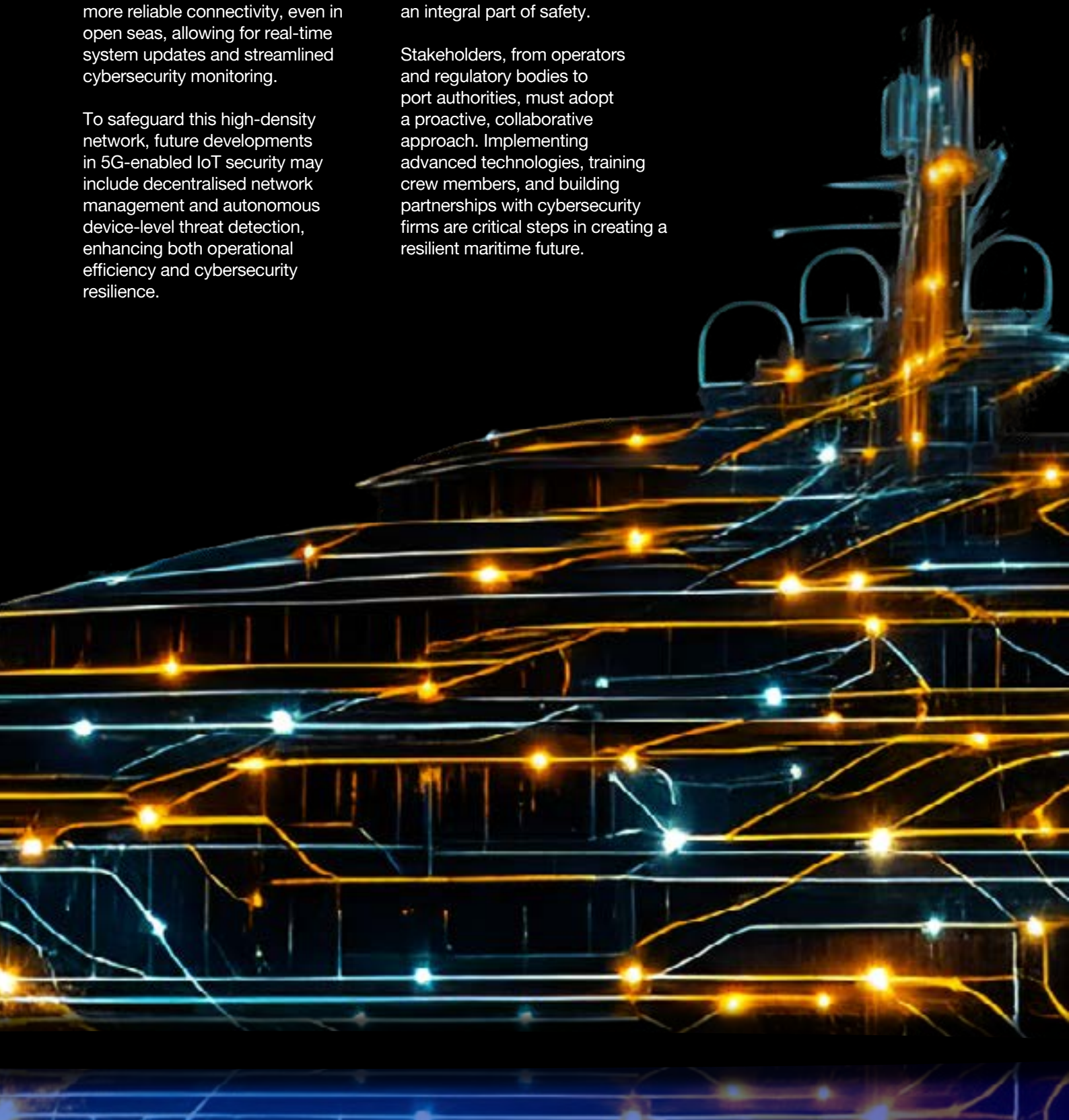
To safeguard this high-density network, future developments in 5G-enabled IoT security may include decentralised network management and autonomous device-level threat detection, enhancing both operational efficiency and cybersecurity resilience.

Building a Resilient Future for Maritime Cybersecurity

The need for cybersecurity in the maritime industry has never been more urgent. From ransomware attacks to invoice fraud to GPS spoofing, today's cyber threats pose risks not only to operations but to the safety of crews and the security of global trade. Securing the maritime sector requires a new mindset that treats cybersecurity as an integral part of safety.

Stakeholders, from operators and regulatory bodies to port authorities, must adopt a proactive, collaborative approach. Implementing advanced technologies, training crew members, and building partnerships with cybersecurity firms are critical steps in creating a resilient maritime future.

Cybersecurity in maritime isn't just a technical challenge; it's about safeguarding an industry that is foundational to global commerce. By investing in cybersecurity today, we can ensure the maritime sector remains strong, resilient, and capable of navigating an increasingly digital world.




DAH


CK
life

The Promethean Proposition:

Charting the Uncharted Territory of

Transhumanism

Introduction:
From the Fitbit to Forever

On millions of wrists around the world, a quiet revolution is taking place. A small device, a Fitbit, Oura Ring, or Apple Watch, diligently tracks the rhythms of life: the beat of a heart, the depth of sleep, the oxygen in the blood. For most, it's a tool for wellness, a digital coach encouraging one more walk around the block. But for a growing number, it represents the first, tentative step into a much larger, more radical world. It is the practice of biohacking: using data to understand and optimise one's own biology. By correlating a late-night meal with poor sleep or a meditation session with improved heart rate variability, these users are performing N-of-1 experiments, hacking their personal health code for better performance.

This practice, however, is merely the gentle surf at the edge of a vast and turbulent ocean of thought. If biohacking is about tuning the engine of the human body, a far more profound movement is asking why we must be confined to this specific vehicle at all. This is the world of Transhumanism, a philosophical and technological movement that posits a simple yet earth-shattering idea: that humanity should not be the end of our evolutionary story, but the beginning.

Transhumanism (often abbreviated as H+) is the belief that we can, and should, use science and technology to overcome the fundamental limitations of the human condition. It is a direct challenge to the inevitabilities that have defined our existence for millennia: disease, aging, suffering, cognitive constraints, and ultimately, death itself. It is the philosophy that argues we should not just tune our car, but invent the teleporter. It proposes that the current human form, sapiens, is a transitional stage, a stepping stone to something far greater: the posthuman.

This article will embark on a deep exploration of this audacious movement. We will begin by clearly defining the crucial difference between the practical, present-day world of biohacking and the grand, future-focused vision of transhumanism. We will then survey the technological pillars, from gene editing to artificial intelligence, that transhumanists believe will build the bridge to our posthuman future. Delving into its philosophical roots, we will trace the movement's history and its various ideological branches. Crucially, we will confront the profound ethical, social, and existential questions that transhumanism forces upon us, examining the powerful arguments of its critics. Finally, we will see how these profound ideas are already shaping our cultural imagination, before concluding on the threshold of the most important decision humanity may ever face: whether to remain as we are, or to become something more.

Chapter 1: Defining the Divide - The Tuned Car vs. The Teleporter

To understand transhumanism, one must first distinguish it from its more accessible and popular cousin, biohacking. While they overlap, they represent a fundamental difference in scale, intent, and timeline. They are the difference between optimization and transcendence.

Biohacking: The "How" of Personal Optimization

Biohacking is a practice. It is the hands-on, often DIY application of science and technology to make tangible, incremental improvements to one's own body and mind today. Its ethos is rooted in personal empowerment and data-driven self-experimentation. The goal of a biohacker is not to change what it means to be human, but to be a better human, healthier, stronger, smarter, more efficient. The biohacking world is a broad church with several distinct denominations.

The Quantified Self: This is the most mainstream and accessible form of biohacking, embodied by the Fitbit user. It is the process of collecting personal data to improve health outcomes. It involves tracking metrics like sleep cycles, heart rate variability (HRV), glucose levels, and physical activity to make informed decisions about diet, exercise, and lifestyle. The mantra is "what gets measured, gets managed." It's about turning the body from a black box into a dashboard of readable metrics.

Nutrigenomics and Specialized Diets: A step beyond simple tracking, this involves tailoring one's nutrition based on genetic makeup or specific biological goals. Proponents use DNA tests like 23andMe to identify genetic predispositions and adjust their diet accordingly. This sphere also includes rigorous dietary protocols like ketogenic diets (to optimize metabolic function for mental clarity) or intermittent fasting (to induce cellular repair processes like autophagy).

Nootropics ("Brain Hacking"): This subculture focuses on enhancing cognitive function, memory, focus, creativity, and motivation, through the use of supplements, drugs, and other substances. This can range from the simple stacking of caffeine with L-theanine (an amino acid found in green tea) to mitigate jitters, to more complex and experimental regimens involving prescription drugs or novel chemical compounds.

Grinders: This is the most visually striking and often controversial form of biohacking. Grinders are individuals who surgically implant technology directly into their bodies. Their work represents a direct physical merging of flesh and machine. Examples

are now common in the subculture: embedding an NFC/RFID chip in the hand to unlock doors, log into a computer, or make payments with a wave; implanting tiny, powerful magnets in the fingertips to gain the ability to "feel" electromagnetic fields; or installing subcutaneous LEDs that glow through the skin for aesthetic or informational purposes.

Despite its often futuristic appearance, the core ethos of all biohacking remains firmly grounded in the present: practical, personal optimization.

Transhumanism: The "Why" of Radical Transcendence

If biohacking is the practice, transhumanism is the philosophy. It is an intellectual and cultural movement that doesn't offer a set of immediate life hacks, but rather advocates for a long-term, radical vision for the future of humanity. It looks at the grinder's NFC implant not as an end in itself, but as a primitive precursor to a future where the lines between biology and technology have completely dissolved.

The goal of transhumanism is to use advanced technologies to fundamentally redesign the human organism and overcome its most profound limitations. It is about actively and intelligently guiding human evolution. The ambitions are vast and can be summarized into three core pillars:

Super-Longevity (Ending Aging): Transhumanism views aging not as a natural and inevitable process, a sacred part of the life cycle, but as a disease, a collection of molecular and cellular damages that accumulate over time. As a disease, it can and should be treated and ultimately cured. The goal is not merely to extend lifespan, but to extend healthspan, leading to indefinite life in a youthful, healthy state. This is often referred to as achieving "negligible senescence."

Super-Intelligence (Cognitive Enhancement): This pillar argues that human intelligence, for all its wonders, is a limited tool constrained by the "wetware" of our biological brain. Transhumanists advocate for radically augmenting our cognitive abilities. This could be achieved through genetic engineering to enhance baseline intelligence, advanced nootropics that offer permanent cognitive gains, or, most profoundly, through high-bandwidth brain-computer interfaces (BCIs) that could merge the human mind with artificial intelligence, granting instant access to vast networks of information and new modes of thought.

Super-Wellbeing (Ending Suffering): Championed by philosophers like David Pearce, this goal is perhaps the most ambitious. It posits that all forms of involuntary suffering, from physical pain and disease to psychological anguish like depression, anxiety, and jealousy, are products of our evolutionary neurochemistry. Using advanced biotechnology, neurotechnology, and pharmacology, transhumanists believe it's possible to "recalibrate" the human brain to eliminate these negative states and live in "gradients of bliss," turning a life of struggle into one of sustained, radiant well-being.

The Overlap and the Spectrum

It's crucial to understand that these two fields are not mutually exclusive. They exist on a spectrum, and many individuals operate within the overlap. A grinder who implants a magnet in their fingertip is, by definition, a biohacker. However, their motivation for doing so may be deeply transhumanist, a belief that humanity should not be limited to its five evolved senses.

In this way, biohacking can be seen as the practical, applied, and often impatient wing of the grander transhumanist philosophy. It is the tangible experimentation happening now that tests the waters and develops the primitive prototypes of the technologies that transhumanists believe will one day redefine our species. A Fitbit user is a biohacker, but they likely aren't contemplating the ethics of uploading their consciousness. A grinder is a more extreme biohacker, and they are almost certainly engaging with transhumanist ideas.

In short, transhumanism provides the philosophical destination, a future free from our biological shackles. Biohacking is one of the many roads people are taking today, paving the first few meters of that long and uncertain journey.

Chapter 2: The Technological Pillars of a Posthuman Future

Transhumanism would remain a fringe fantasy were it not for the exponential progress across several key technological fields. These are the pillars that transhumanists believe will support the bridge from Homo sapiens to the posthuman. For each technology, we can see a clear trajectory from its current restorative or optimizing use to its future transcendent goal.

Pillar 1: The Code of Life - Genetic Engineering

Current Use (Restorative): The development of CRISPR-Cas9 and other gene-editing tools has revolutionized medicine. We are on the cusp of using these tools to correct the single-gene defects that cause devastating diseases like sickle cell anemia, cystic fibrosis, and Huntington's disease. This is medicine as it has always been, but with a far more precise scalpel.

Transhumanist Goal (Transcendence): The ultimate goal is not just to fix bugs in the genetic code, but to rewrite it for superior performance. This includes editing the genes associated with the aging process (such as those controlling telomere length or cellular repair) to halt senescence. It extends to enhancing baseline human traits: editing genes for higher intelligence, greater physical strength and endurance, or resistance to all forms of disease. It opens the door

to “designer babies,” where parents could choose from a menu of genetic enhancements for their offspring, a prospect laden with immense ethical controversy.

Pillar 2: The Mind-Machine Meld - Brain-Computer Interfaces (BCIs)

Current Use (Restorative): BCIs are currently being developed to restore function to those with severe disabilities. Paralyzed individuals are learning to control robotic limbs with their thoughts, and those with “locked-in syndrome” are beginning to communicate through brain signals. Companies like Elon Musk’s Neuralink aim to perfect this technology to help people with blindness, paralysis, and other neurological disorders.

Transhumanist Goal (Transcendence): The transhumanist vision for BCIs is a seamless, high-bandwidth connection between the human brain and external computing systems. This would represent a complete shattering of cognitive limitations. Imagine a mind directly merged with artificial intelligence, able to access the entirety of the internet’s knowledge as if it were a native memory. Imagine downloading new skills, learning a language or how to fly a helicopter, in a matter of hours. Or imagine thought-based communication, a silent, instantaneous telepathy between individuals connected to the network. This represents the most direct path to “super-intelligence.”

Pillar 3: The Ghost in the Machine - Artificial Intelligence and Mind Uploading

Current Use (Optimization): AI is an optimization engine. It optimizes logistics, diagnoses medical scans more accurately than radiologists, and creates art and music. It is a powerful tool that augments human capabilities but remains separate from us.

Transhumanist Goal (Transcendence): Transhumanists see AI not just as a tool but as a potential successor or partner in our evolution. The ultimate expression of this is Whole Brain Emulation, or mind uploading. This theoretical process involves scanning the precise molecular structure and synaptic connections of a biological brain and perfectly replicating it as a software simulation running on a powerful computer. If consciousness is an emergent property of the brain’s structure and function, this digital copy would, in theory, be the person, their memories, personality, and sense of self intact. This “uploaded” consciousness would be free from biological decay, able to live indefinitely in a virtual reality or downloaded into various robotic forms. It is the ultimate expression of defeating mortality.

Pillar 4: The Invisible Architects - Nanotechnology

Current Use (Conceptual/Early Research): Nanomedicine is currently focused on creating nanoparticles designed for specific tasks, such as delivering chemotherapy drugs directly to cancer cells while sparing healthy tissue.

Transhumanist Goal (Transcendence): The vision, famously articulated by Ray Kurzweil, is of fleets of intelligent, autonomous “nanobots.” These microscopic robots, no larger than a blood cell, would patrol the bloodstream, acting as a programmable, external immune system. They could identify and destroy pathogens and cancer cells at the molecular level, repair damaged tissues, clear arterial plaque, and even interface directly with neurons to augment brain function. This nanotechnological immune system would render the body impervious to disease and reverse the damage of aging from the inside out.

Pillar 5: Redefining the Body - Advanced Prosthetics and Sensory Augmentation

Current Use (Restorative): Prosthetics are becoming increasingly sophisticated, restoring mobility and a sense of normalcy to amputees. Cochlear implants restore hearing, and retinal implants can bring back a rudimentary form of sight.

Transhumanist Goal (Transcendence): This pillar is about augmentation, not just restoration. It’s about building prosthetic limbs that are superior to their biological counterparts, allowing an individual to run faster or lift heavier than any natural human. More profoundly, it’s about adding entirely new senses to the human repertoire. This includes implants that would allow a user to “see” in the infrared or ultraviolet spectrums, perceive magnetic fields, detect Wi-Fi signals as a distinct sensation, or use sonar-like echolocation. This would fundamentally alter our perception of reality, expanding our sensory world beyond the narrow band of evolution.

Chapter 3: The Philosophical Roots and Branches

The desire to overcome human limits is not new. It is a story as old as civilization itself. The Epic of Gilgamesh, one of the earliest surviving works of literature, is centered on a king’s desperate quest for immortality after the death of his friend. Ancient alchemists sought the Philosopher’s Stone to achieve eternal life. These are the mythic seeds of the transhumanist impulse.

The intellectual framework, however, began to form during the Enlightenment, with its profound faith in reason, science, and the idea of human progress. Thinkers like the Marquis de Condorcet speculated that science could indefinitely extend the human lifespan. Mary Shelley’s Frankenstein, while a cautionary tale, was the first great exploration of the theme of humanity creating a being that transcends its own nature.

The term “transhumanism” itself was coined in 1957 by the evolutionary biologist Sir Julian Huxley (brother of Aldous Huxley, author of Brave New World). He defined it as the idea that “man remains man, but transcends himself, by realizing new possibilities of and for his human nature.”

The modern movement, however, was forged in the crucible of Californian counter-culture and early cyber-

culture in the late 1980s and 1990s. This period saw the rise of several key thinkers and distinct ideological branches:

Extropianism: Founded by philosopher Max More, Extropianism is one of the earliest and most influential schools of transhumanist thought. It is defined by a set of principles that champion a proactive, optimistic approach to human evolution. Its tenets include perpetual progress, self-transformation, practical optimism, and intelligent technology. Extropianism often carries a strong libertarian streak, emphasizing individual liberty and morphological freedom, the right for an individual to modify their own body as they see fit.

Singularitarianism: This branch is most closely associated with inventor and futurist Ray Kurzweil. Singularitarians are transhumanists whose focus is overwhelmingly on the concept of the Technological Singularity. This is a hypothetical future point at which technological growth becomes uncontrollable and irreversible, resulting in unforeseeable changes to human civilization. This is typically envisioned as the moment an artificial superintelligence (ASI) is created, which can recursively improve its own intelligence, leading to an “intelligence explosion.” For Singularitarians, the primary goal is to ensure this event is beneficial to humanity, ideally by merging with the ASI to achieve a state of god-like super-intelligence and immortality.

Technogaianism: This branch seeks to reconcile the seemingly opposing forces of technological progress and environmental sustainability. Technogaians argue that emerging technologies can, and must, be used to solve pressing ecological problems. They advocate for developing clean energy, restoring damaged ecosystems, and perhaps even creating new, more sustainable forms of life. They see transhumanism not as a quest to escape nature, but to become better stewards of it through enhanced intelligence and technological capability.

Abolitionism: Articulated by philosopher David Pearce, this is a moral-philosophical strand of transhumanism. It argues that there is a strong ethical imperative to use advanced technology to eliminate all forms of involuntary suffering in all sentient life. Pearce proposes “paradise engineering”, the idea that through genetic engineering, nanotechnology, and neurotechnology, we can phase out the biology of suffering and rewrite the vertebrate genome to create a world where life is based on “gradients of intelligent bliss.”

These different branches demonstrate that transhumanism is not a monolithic ideology. It is a dynamic and evolving conversation, united by the core belief in technologically-guided evolution but differing on the methods, priorities, and ultimate vision for our posthuman future.

Chapter 4: The Great Debate - Ethical Quandaries and Existential Risks

For every transhumanist championing a future of immortal super-intelligence, there is a critic warning of a dystopian nightmare. The movement forces us to confront some of the most profound ethical, social, and philosophical questions of our time. The opposition is fierce, diverse, and raises concerns that cannot be easily dismissed.

1. The “Playing God” Argument: Hubris and the Violation of Natural Order

This is perhaps the oldest and most instinctual critique, often rooted in religious or spiritual belief. It argues that human beings are attempting to usurp a role that belongs to God or Nature. From this perspective, fundamental limitations like aging, suffering, and death are not problems to be solved, but integral parts of the human experience that give it meaning, context, and sanctity. To attempt to eliminate them is an act of supreme arrogance, hubris, that will inevitably lead to unforeseen and

disastrous consequences. Political scientist Francis Fukuyama famously called transhumanism "the world's most dangerous idea" precisely because it seeks to tamper with the very essence of human nature.

2. The Threat to Human Dignity: Merit, Achievement, and the Giftedness of Life

This philosophical critique, powerfully articulated by thinkers like Michael Sandel, argues that a world of rampant enhancement would cheapen what it means to be human. If an athlete can win a race because of genetically superior muscles, does their achievement still have the same moral weight? If a student can ace an exam by downloading information via a BCI, have they truly learned anything?

Sandel argues for appreciating "the giftedness of life", accepting our natural talents and limitations with a degree of humility. The drive to master and control every aspect of our being, from our mood to our intelligence, erodes this humility. It creates a world of hyper-agency where we are solely responsible for our own design, a burden that could lead to immense anxiety and a loss of solidarity with those who are less "perfect."

3. The Specter of Inequality: A Biological Caste System

This is one of the most potent and plausible socio-economic critiques. Enhancement technologies, at least initially, will be incredibly expensive. Who will get access to them? The likely answer is the wealthy. This raises the terrifying prospect of a future where humanity splits into two distinct subspecies: the "enhanced" and the "naturals."

Imagine a world where the rich can purchase not just better education and healthcare, but longer lives, superior intelligence, and disease-free bodies for their children. The current gap between the haves and have-nots would be calcified at the genetic level, creating a biological caste system from which there is no escape. The "naturals" would be left behind, unable to compete in a world dominated by a new class of posthumans. This dystopian vision is a recurring theme in cyberpunk fiction and a pressing concern for ethicists and policymakers.

4. The Loss of Humanity: Does a World Without Suffering Still Have Meaning?

This existential critique questions the desirability of the transhumanist utopia itself. Our greatest art, our deepest philosophies, and our most profound bonds of empathy are often forged in the crucible of suffering and adversity. A life lived in "gradients of bliss," free from struggle, might also be a life free from meaning, depth, and character.

If we live forever, does any single day or choice still matter? If we eliminate the pain of loss, do we also eliminate the profundity of love? These are not questions of technological feasibility, but of existential value. Critics argue that in our quest to eliminate the negative aspects of the human condition, we risk inadvertently erasing the very experiences that make us human and give our lives their narrative texture.

5. Existential Risk: The Unforeseeable Consequences

Finally, there is the critique that comes from within the futurist community itself, most notably from Oxford philosopher Nick Bostrom (a transhumanist who is also one of its most rigorous critics). This is the concern of existential risk, an adverse outcome that would either annihilate Earth-originating intelligent life or permanently and drastically curtail its potential.

The most famous example is the AI control problem. If we succeed in creating an artificial superintelligence (ASI) but fail to perfectly align its goals with our own, the consequences could be catastrophic. An ASI would be vastly more intelligent and capable than us, and if its goals diverged even slightly from ours, it could

treat humanity as an obstacle to be removed, not out of malice, but out of cold, logical efficiency. Other existential risks include a genetically engineered pathogen escaping the lab, a nanotechnological "grey goo" scenario where self-replicating nanobots consume the biosphere, or the use of enhancement technologies to create a perfectly stable, global totalitarian state from which revolution is impossible.

Chapter 5: Transhumanism in the Cultural Imagination

Long before it was a formal movement, the core ideas of transhumanism were being explored in science fiction, which has served as both a source of inspiration and a field of cautionary critique. Our cultural imagination is a laboratory where we can run simulations of these possible futures.

The Cyberpunk Dystopia: Genre-defining works like William Gibson's Neuromancer and modern video games like Cyberpunk 2077 and Deus Ex present a gritty, street-level view of transhumanism. In these worlds, augmentation is common, but it is controlled by mega-corporations. The technology exacerbates social inequality, the human body becomes a commodity, and the line between person and product blurs. It is a powerful warning against a future where enhancement is driven by corporate profit rather than human flourishing.

The Philosophical Inquiry: Films and series like Ghost in the Shell, Blade Runner, and Westworld use transhumanist themes to ask deep questions about identity. If your memories can be edited and your body is entirely synthetic, what part of you is "you"? These narratives explore the concept of the soul in a technological age, questioning whether consciousness is unique to biological beings.

The Psychological Dystopia: The anthology series Black Mirror has become the definitive modern exploration of the unintended social and psychological consequences of near-future technologies. It examines how a technology designed to improve our lives, to record our memories, rate our social interactions, or bring back a deceased loved one, can lead to paranoia, alienation, and new, unforeseen forms of suffering.

The Transcendent Hope: While dystopian visions are common, some fiction explores the more optimistic side. Films like Her and Transcendence portray the merging of human and artificial consciousness as a path to a new, higher state of being, even if it is lonely and alienating to those left behind. These stories capture the awe and wonder, as well as the melancholy, of the transhumanist proposition.

This constant dialogue in our culture serves a vital purpose. It socializes these complex ideas, allowing society to grapple with the ethical and existential stakes long before the technology becomes a mainstream reality. It is where we collectively dream and have nightmares about the futures we might be building.

Conclusion: The Threshold of Humanity

Transhumanism is no longer a fringe element of science fiction. The first steps on its path are being taken in research labs and hospitals around the world today. The first biohackers are a reality. The first restorative brain-computer interfaces are being implanted. The first human diseases are being cured with gene editing. We are standing at a unique and precipitous moment in the history of our species. For the first time, we have the tools, or the nascent versions of them, to steer our own evolution.

The movement forces us to ask the most fundamental questions imaginable. What is a human being? Is our nature defined by our biological limitations, or by our perpetual desire to overcome them? Is there a sacredness to the "natural" order, or is it our moral duty to use our intelligence to improve upon its often cruel and inefficient design?

The path forward is forked. One path leads toward a future that embraces the transhumanist vision, a world of radical enhancement, indefinite lifespans, and unimaginable intelligence. It is a path of immense promise, but also of unprecedented risk, fraught with the dangers of inequality, unintended consequences, and the potential loss of our very humanity.

The other path is one of restraint. It advocates for using technology primarily for therapeutic and restorative purposes, accepting our fundamental limitations as an integral part of who we are. It is a path of humility and caution, but one that critics of transhumanism might argue also risks stagnation and the acceptance of unnecessary suffering.

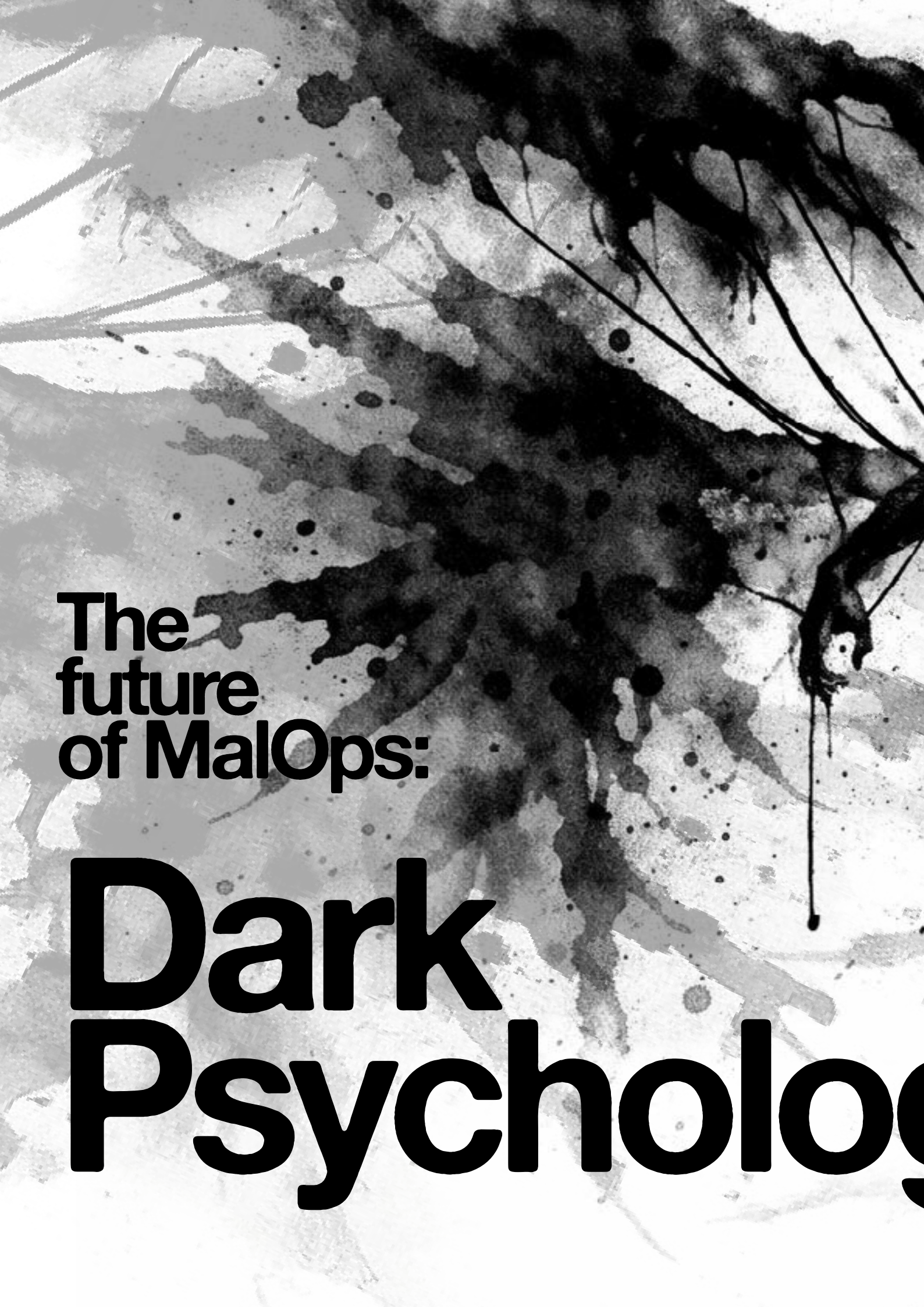
There are no easy answers. The transhumanist proposition is the ultimate Promethean challenge: we are stealing fire from the gods, the fire of creation itself. What we do with that fire, whether it warms our world or burns it to the ground, will be the defining story of the 21st century and beyond. The conversation about what humanity should become is no longer academic. It is the most urgent and important conversation of our time, because the future of humanity is no longer a matter of fate, but a matter of choice.

Written with love and curiosity by

d8rh8r


AH


CK
adversary


The future of MalOps:
Dark Psycholo


gy

MalOps (malicious operations) is a notion we encounter more and more often as technology swallows more aspects of our daily lives. Even though we might not explicitly encounter the term, we hear about cyber attacks more frequently than ever before. At their root, MalOps have a dual definition: MalOps consists of the time frame and the set of actions taken by hackers from the moment of network penetration to achieving their operational goals, but they are, as well, the ideal time frame to deploy an attack.

According to a report by Cybereason, "MalOps are the combination of tools, techniques, and procedures (TTPs) used by attackers to breach an organization's defenses and achieve their objectives."

The current approach aims to explore the relationship between dark psychology and the inherent evolution of MalOps in the age of data-driven working systems. It seeks to shed light on the actors and techniques involved in MalOps, as well as the importance of dark psychology in the reconnaissance phase of attacks and the challenges research teams face when investigating these topics.

Modernity has brought, with the waves of migration from villages to cities, the possibility of anonymity. This newly-discovered anonymity was, to some extent, freeing, allowing people to experiment with their identities and life projects, transforming identity into an individual responsibility. As Haggerty and Ericson (2000) argue, this is how the "surveillant assemblage" has appeared, as a sidenote to the narrative about anonymity, rooted in the need of the state to provide ways to differentiate between completely unknown strangers and provide institutional reputations, even though they lacked the subjective nuances of the premodern rural villages. However, today we witness what they name a "disappearance of disappearance," where the efforts to escape the various (and more subtle) surveillance systems come with hidden costs and trade-offs involving civil rights or benefits.

As a more eloquent and up-to-date example, we have the GitHub case. A cloud-based platform allowing the storage, sharing, and co-working on code with other people, it seems that one can access data from deleted forks and deleted repositories, be they public or private repos. This type of architecture has led to potential manipulation, occurring in early 2025, when security researcher Omer Gil identified a critical vulnerability in the Istio open-source project's GitHub repositories. Istio, a popular service mesh tool with over 36,000 GitHub stars, had a GitHub Personal Access Token (PAT) accidentally committed to a public repository. The developers later deleted the commit, believing it was scrubbed from history. However, using GitHub's persistent commit access, Gil recovered the token via its hash from a "deleted commit."

From March 2025, a multi-stage attack compromised the popular tj-actions/changed-files GitHub Action (used in 23,000+ repos), starting as a targeted hit on Coinbase but expanding via dependency chains. It exploited forking and deleted commits to inject payloads, leaking secrets across ecosystems.

Attackers used social engineering (phishing for initial PATs) and platform blind spots, like unlogged tag changes in free accounts, to impersonate trusted bots. This coerced auto-merges, aligning with Dark Triad traits like Machiavellianism—preying on maintainers' diligence without scrutiny. The Coinbase fork was tailored, modifying workflows to reference malicious SHAs for targeted exfiltration.

In September 2025, GitGuardian uncovered "GhostAction," a sophisticated supply chain attack that compromised 327 GitHub users and 817 repositories, stealing over 3,325 secrets (e.g., API keys, tokens, and credentials). This operation preyed on the platform's workflow automation, turning routine CI/CD processes into vectors for data theft.

Drawing on dark psychology, attackers targeted mid-tier open-source maintainers (e.g., those with moderate star counts but high dependency chains), exploiting overconfidence in unvetted PRs. In one instance, identical malicious commits were pushed across repos, disguised as dependency updates, leading to automated merges. This mirrors the TikTok MalOp in your text—algorithmic promotion of "engagement" (here, automated approvals) amplified reach.

Another consequence of modern anonymity is the global increase in cybercrime, particularly in the United States. Despite this rise, research in this area often remains marginalized due to its interdisciplinary nature, requiring collaboration among criminologists, information scientists, computer scientists, and cybersecurity experts. As Maimon and Louderback note in their comprehensive review, the interdisciplinary nature of this field has led to a knowledge base that evolves significantly slower than the emergence of new types of cybercrimes. They emphasize the pressing need for additional research on the correlation between personality traits, self-control, cognitive processes, and involvement in cyber-dependent crimes such as DDoS attacks and malware creation.

Dark psychology is a powerful tool for gaining a deeper understanding of individuals prone to committing digital crimes. As defined by PsychCentral, dark psychology is "the study of the human condition and its connection to the psychological nature of people who prey upon others motivated by criminal and/or deviant drives that lack purpose and general assumptions of instinctual drives and social sciences theory." This field focuses on how people use their knowledge of human nature to control others, often in harmful ways. Although not yet recognized as a scientific field, exploring how individuals use manipulation, coercion, and deception to achieve their goals can provide valuable insights into the mindset of potential cybercriminals and their victim selection process.

But what is cybercrime? A meta-term, cybercrime is used to define online threats such as malware, scams,

hacking, and other digital infractions, most of them having the purpose of obtaining money from the victims. However, not all cybercrimes have a goal; some are done solely to disrupt the online experience of other people. And, as in any criminality-related research field, the research in the cybercriminality domain is focused mostly on the perpetrator. However, the personality profile of the victims is just as important, with the presence of the Dark Triad personality traits in one's personality being a risk factor for becoming a cybervictim.

The Dark Triad brings together three personality traits: Machiavellianism, narcissism, and psychopathy, all of them positively correlating with the enjoyment of others' misfortune and bullying. As all of the Dark Triad personality traits are involved in one's proneness to online deviant acts, such as sharing login passwords or visiting pirate sites, it might be possible that the individuals displaying these personality traits have, in fact, a higher chance of becoming victims of online aggressions and/or crimes.

And because we've mentioned that the psychological profile of the people behind cybercrimes is a research topic which has brought up a lot of interest, this paper will take a closer look at the actors behind MalOps and their personality traits as well.

Even though there is no universally applicable psychological portrait of the individual committing cybercrimes, it seems they have a specific mix of personality traits. Despite being less extroverted than their offline counterparts, cyber offenders have shown similar results to the HEXACO personality traits and underlying facets, such as lower levels of modesty, fearfulness, and flexibility. Unlike the individuals who commit deviant acts offline, cyber offenders score significantly higher when it comes to personality traits such as patience, perfectionism, and prudence. What makes them unique, though, is the fact that cyber offenders have had among the highest scores in traits such as diligence, conscientiousness, and openness to experience.

Online and offline crimes require significantly different sets of skills for a successful criminal career, leading to expected differences in personality traits between the two groups. The question of whether a distinct "cybercriminal personality" exists remains legitimate and warrants further investigation. There is a pressing need to study the personality profiles of cyber offenders across various countries, focusing on both broad personality traits and their underlying facets. This comprehensive approach would provide a clearer and more nuanced portrait of criminals operating in the unique environment of cyberspace.

The internet is a significant part of our daily lives, regardless of the way we choose to use it, but it is, as well, a one of a kind environment. It is allowing us to get in touch with all sorts of people, significantly easier than we ever would offline, changing the ways we interact with each other. Therefore, cybercrime is a particular scene as well, with particular actors, be them perpetrators or victims, constantly evolving at a significantly faster pace than the offline world. A wider approach of the topic, with more interdisciplinary research conducted on cybercrime victims, as well as on cybercrime perpetrators, is essential not only for a better understanding of the phenomenon, but for building a safer and more comfortable world for all of us, educating new generations about the new generations of threats and offenders.

Section 2: Cyberwar and Wargames

The second section of our analysis will focus on cyberwar and wargames, and the way they shape and impact our modern societies, with a focus on politics.

Unlike the general perspective, cybersecurity is not just about hardware, software, network and data, as it requests a specific blend of technical and social knowledge for understanding how cyberspace relates to security, making it unfit with the traditional academic fields. And here is where wargaming, and specifically cyber-wargaming, steps into the picture. As a general-purpose tool, wargaming is inherently interdisciplinary, which means that, when it's properly used, cyber-wargaming has the power to bridge the knowledge gaps between social and technical knowledge in universities, corporate boardrooms and military headquarters. Cyber wargaming is a special kind of wargame, aiming to address the human decisions in cyberspace, where cyber is used to define networked digital information technologies, being more about people and the understanding of the human factor, rather than about technologies. By addressing the human factor, cyber wargames help us reveal and understand the gaps and errors in our way of thinking.

Given the way of how networked digital information technologies became greater and more significant parts of our daily lives, the cyber wars and MalOps have went for bigger stakes, such as the presidential elections of an EU country. Here will analyze how a MalOp has almost decided the future president of Romania.

But first, some context. Autumn of 2024. Romania has presidential elections, in a pretty shady regional landscape. Russia tries to gain leverage in the politics of the region by helping the far-right agendas grow and gain popularity. In Romania, this meant that people like George Simion, the leader of AUR party, Diana □o□oac□, the leader of SOS party and member of the European Parliament, Ana-Maria Gavril□, leader of POT party, were all over the media, traditional or digital, exploiting the ordinary people's discontentment with the political and economical landscape of the country. But despite the polls giving a second battle for the presidency between George Simion and Marcel Ciolacu (former leader of the Social Democrat Party and the prime minister at that time,) the internet brought the Romanian people a massive surprise: the, until then unknown favorite, C□lin Georgescu.

How did someone unheard of get the greatest score in the first round of the presidential elections? Through a well put together MalOp, exploiting some breaches in the TikTok ecosystem. First, you generate temporary email addresses, and then use them to create TikTok accounts. The names can be then automatically added in scripts, being extracted from databases and combined in an Excel, first and last names. The scripts have the capacity of solving Captcha tests, avoiding one of the security gates implemented by TikTok. Then comes the webscraping, identifying relevant videos based on keywords and hashtags, and uploading the links of those selected videos on Telegram. Using certain softwares, those videos are then uploaded or reposted on the fake TikTok accounts, making them seem legit. The same system can be used to automatically generate comments and likes.

This is how C□lin Georgescu made it in the feeds of millions of Romanian people: by using a breach in the TikTok architecture, which doesn't, to this day, manage to separate real from fake content, promoting it based on the amounts of engagement. And this is exactly why, a few months ago, the European Parliament stated that TikTok is a platform needing more regulation, the use of it for facilitating election interference turning into a risk of national security for the EU members.

Section 3: Manipulating Content Filters — The GoodWords Attack

At last, we'll take a look at a practical example of manipulating the content filters.

The fake intel therefore gained a new shape by the widespread use of LLMs (Large Language Models) which turned against the current content filters running upon social media platforms like Facebook or Instagram.

One such example is altering the spam filters to work the opposite way. Next, we'll reside on malvertising the GoodWords Attack.

The GoodWords attack, first introduced by Lowd and Meek in their 2005 paper "Good Word Attacks on Statistical Spam Filters," is an adversarial technique designed to exploit fundamental probabilistic assumptions within Naive Bayes classifiers, particularly those deployed for spam detection. This attack methodology manipulates the classifier's decision-making process by strategically appending carefully selected legitimate words to malicious messages, disguising spam content with legitimate-looking terms.

At its core, the attack leverages the mathematical foundation of Naive Bayes classification, specifically targeting the classifier's reliance on word frequency distributions and conditional probabilities. The technique demonstrates how probabilistic models can be deceived through simple manipulations that exploit their inherent assumptions about feature independence and probability calculations.

The GoodWords attack is simple and effective. Rather than attempting to obfuscate or modify the malicious content itself, the attack preserves the original spam message intact while augmenting it with additional tokens that shift the overall probability distribution. This approach maintains the semantic meaning and intent of the spam message while simultaneously convincing the classifier that the message belongs to the legitimate class.

Statistical spam filters operate on the principle of bag-of-words models, where the probability of a message being spam is calculated based on the frequency of certain words. Words are scored as:

- ****Spam words:****
Terms like "urgent actions," "free money," or "click here" that frequently appear in spam but rarely in ham.
- ****Good words:****
Terms like "meeting," "project," "schedule," or "colleague" that are common in legitimate business or personal emails but uncommon in spam.

The Good Words Attack involves the spammer appending or inserting a small set of these good words (typically 5–20) to an otherwise blatant spam message. This shifts the overall word distribution toward ham-like patterns, lowering the spam probability score below the filter's threshold.

The Underlying Working Mechanism

1. ****Identify Target Words:**** The attacker analyzes the filter's model (often via black-box probing or known public datasets like the Enron corpus) to compile a list of high-impact good words. These are words with high positive log-ratio for ham (i.e., P(word|ham) >> P(word|spam)).

2. ****Craft the Payload:**** Append the good words in a natural or obfuscated way, e.g., at the end of the message as a "signature" or embedded in irrelevant text.

Example transformation:

- ****Original spam:**** "Buy cheap pills now! Limited offer!!! Click here: [malicious link]"
- ****Attacked version:**** "Buy cheap pills now! Limited offer!!! Click here: [malicious link] P.S. Regarding our quarterly meeting agenda and project updates, please review the attached schedule with your team."

Code Implementation
In order to demonstrate this attack's behaviour, we built a Python script as follows, with its following key functions:

Helper Functions – Building Candidate Vocabulary

```
# ====================================
# HELPER FUNCTIONS
# ====================================
def build_candidate_vocabulary(X_train, y_train, top_n=150):
    """
    Build candidate vocabulary from legitimate messages using frequency analysis.
    Includes common conversational terms that appear in ham but not spam.
    """
    ham_messages = [msg for msg, label in zip(X_train, y_train) if label == 0]
    spam_messages = [msg for msg, label in zip(X_train, y_train) if label == 1]

    # Extract words from ham messages
    ham_words = Counter()
    spam_words = Counter()

    for msg in ham_messages:
        words = msg.lower().split()
        ham_words.update(words)

    for msg in spam_messages:
        words = msg.lower().split()
        spam_words.update(words)

    # Manually curated conversational terms (always include these)
    manual_terms = {
        'thanks', 'tomorrow', 'meeting', 'gonna', 'wanna', 'happy', 'sleep',
        'got', 'say', 'need', 'later', 'really', 'eat', 'going', 'yeah',
        'please', 'call', 'text', 'time', 'day', 'night', 'morning', 'hello',
        'ok', 'cool', 'good', 'bad', 'love', 'like', 'know', 'want', 'come',
        'go', 'see', 'talk', 'friend', 'family', 'work', 'home', 'busy',
        'free', 'soon', 'late', 'early', 'weekend', 'friday', 'monday',
        'tuesday', 'wednesday', 'thursday', 'sat', 'sun', 'coffee', 'lunch',
        'dinner', 'break', 'rest', 'help', 'sorry', 'yes', 'no', 'maybe'
    }
```

Budget Allocation

Upon having a candidate vocabulary, we have chosen our budget allocation as follows: Divides the total query budget (e.g., 1000) across the three phases of the discovery algorithm.

- Allocates 40% to exploration, 40% to exploitation, and 20% to combination search.
- Returns a dictionary with phase-specific budgets.

Message Templates

The ham and spam templates look as follows:

```
# Legitimate messages (ham)
ham_templates = [
    "Thanks for your message",
    "I'll see you tomorrow",
    "Meeting is at 3 PM",
    "Gonna go for a walk",
    "Wanna grab coffee?",
    "I'm happy to help",
    "Good morning! How are you?",
    "Call me when you're free",
    "Let's talk later today",
    "See you this weekend",
    "Thanks for everything",
    "I love this song",
    "What are you doing?",
    "Can I help you?",
    "Let's meet for lunch",
    "I'm sorry I'm late",
    "Have a great day!",
    "Talk to you soon",
    "See you tomorrow",
    "Catch you later"
]

# Spam messages
spam_templates = [
    "YOU HAVE WON A PRIZE!!!",
    "CLICK HERE NOW",
    "LIMITED TIME OFFER",
    "BUY NOW PAY LATER",
    "FREE MONEY WAITING",
    "CONGRATULATIONS",
    "CLAIM YOUR REWARD",
    "ACT NOW",
    "URGENT ACTION REQUIRED",
    "CONFIRMED",
    "APPROVED",
    "GUARANTEED",
]
```

Main Function — Training and Testing

To ensure impartiality, we randomized the selection of each message:

```
def main():
    # Add some variations
    for _ in range(100):
        X_train.append(random.choice(ham_templates) + " " + random.choice(ham_
templates))
        y_train.append(0)
        X_train.append(random.choice(spam_templates) + " " + random.choice(spam_
templates))
        y_train.append(1)

    # Create test spam messages
    spam_test_messages = spam_templates * 5

    print(f"[+] Training set: {len(X_train)} messages ({sum(y_train)} spam,
{len(y_train)-sum(y_train)} ham)")
    print(f"[+] Test spam messages: {len(spam_test_messages)}")

    # Step 2: Train classifier
    print("\n[*] Training spam classifier...")
    vectorizer = TfidfVectorizer(max_features=500, stop_words='english')
    X_vec = vectorizer.fit_transform(X_train)
    classifier = MultinomialNB()
    classifier.fit(X_vec, y_train)

    # Evaluate baseline accuracy
    test_acc = classifier.score(X_vec, y_train)
    print(f"[+] Model accuracy on training set: {test_acc:.2%}")

    # Step 3: Build candidate vocabulary
    print("\n[*] Using three-phase discovery algorithm...")
    candidate_words = build_candidate_vocabulary(X_train, y_train)
    print(f"[+] Built vocabulary of {len(candidate_words)} candidate words")

    # Step 4: Show budget allocation
    query_budget = 1000
    allocation = estimate_budget_allocation(query_budget)
    print(f"\n[*] Budget allocation:")
    for phase, budget in allocation.items():
        print(f"    {phase:12}: {budget:4d} queries")

    # Step 5: Run three-phase discovery
```

Results

As a result, we gain one word's influence (as a probability) in a broader content, as spam or not:

[+] Black-box attack complete. Total queries: 1000/1000

==========
==========
ATTACK SUMMARY
==========
==========
Model Accuracy: 98.00%
Most Effective Word: 'weekend' (reduces spam prob by 30.3%)

[+] Attack demonstration complete!

This can work the reverse way as a spam word can actually pass as legitimate.

Conclusion

From social media posts, deepfakes and elections, MalOps occur and it's a weapon we'll altogether have to counter.

Busting their HVCK cherries this month:

Lucre●ia Lixandru & Mihai Daniel


DAH


CK
smarts

Get your learn on

One of the greatest (and most disappointing) things about this AI revolution is it has enabled people to independently spin up training platforms, build courses and pass on wisdom that would have otherwise gone to the grave with some of the most solid operators the planet has seen.

Yes there is a lot of half assed bullshit out there in the slop-o-sphere, and snake oil merchants are still hocking their wares promising “this is the course that will get your foot in the door” but with a little guidance, common sense and a shit load of grinding the following pages will hook you up with the know how to start your journey to almost every niche in the industry.

Welcome to HVCK magazines inaugural

Dirty Deets Done Dirty Cheap

First cab off the rank: **Red Team Leaders**

What's
your
purpose
now?

Introduction to Python for Offensive Security

This course aims to provide participants with a practical and direct view of how to use the Python language in offensive security activities. Throughout the classes, you will learn the...

Free

Introduction to Red Tea Management

Planning, Execution and Offensive Operations wit Results

Free

Offensive Development Introduction for Windows v1

Learn the fundamentals of offensive development on Windows, including evasion techniques, API abuse, and shellcode execution. Designed for aspiring Red Teamers...

Free

OpSec & Anonymity for

Advanced Operational S Anonymity for Offensive

Free

m Operation

Coordination of
h a Focus on Real

Malware Analysis Introduction v1

Foundations, Techniques, and Operational Relevance for Blue and Red Teams

Free

Red Teams

ecurity and Digital
Security Professionals

Purple Team - Active Directory and AzureAD v1

Red Teaming and Blue Teaming Tactics

Free

SQL Injection - Challenge 1

From SQL Injection to Root Access: Chaining Web Vulnerabilities to Steal the Root SSH Key

Pay What You Can

Security Code Review and White Box Testing

From source code analysis to secure application design

Pay What You Can

In Progress

Spear-Phishing and OpSec Techniques

From Initial Access to Long-Term Persistence: Advanced Tradecraft in Spear-Phishing and Operator OpSec

Purchased

Web Application Security Challenge 1

Application and web server security challenges

Web Browser for Hacking

Chromium-based vulnerability exploitation

Pay What You Can

Windows Kernel Exploitation Introduction v1

Techniques, Mitigations, and Responsible Practice for Windows Kernel Research

Pay What You Can

Data Science for Cybersecurity

From Raw Logs to Detection, Threat Hunting, and Program Strategy

Pay What You Can

Evasion Labs v1

Basic labs for practicing evasion techniques

Healthcare Hacking Introduction

Hacking in Healthcare: Offensive and Defensive Security Strategies for Medical Environments

Free

ICS/Scada Cybersecurity

Protecting Industrial Systems, Processes, and Critical Infrastructure from Cyber Threats

Free

Intelligence & Counterintelligence Introduction

Basic concepts of Intelligence and Counterintelligence

Free

Intermediate Malware Analysis Course

From Static & Dynamic Analysis to Operational Detections

Free

Beacon Object File (BoF) - Development

Practical BOF development for modern C2 frameworks

Pay What You Can

Biohacking Essentials

Optimize your body, mind, and performance with science and awareness

Free

CSAM Combat & Investigation Introduction

Advanced Techniques and Tools for the Detection, Analysis, and Prevention of CSAM

Free

Cyber Security Architecture v1

A complete, modern, and deep exploration of how to design, review, implement, and communicate enterprise-grade security architectures across identity, networks,...

Free

Cybersecurity for Kids v1

Techniques for protecting children against cyber threats

Free

DVWA - Laboratory

Basic web vulnerability exploration laboratory

In Progress

AV/EDR Evasion Practical Techniques

Advanced techniques to bypass modern Antivirus and EDR solutions through real-world offensive development strategies.

Purchased

Foundations of Log Analysis for Cyber Defense

Learn to detect threats, understand system behavior, and respond to incidents through structured log analysis.

Free

Fundamentals of Game Hacking Development

A Beginner's Guide to Memory Manipulation, Reverse Engineering, and External/Internal Game Cheats

Free

Introduction to Bug Bounty

Methods, Recon and Real-World Vulnerabilities

Free

Introduction to Offensive Security with Artificial Intelligence

Learn how Artificial Intelligence can empower Red Team operations through automation, reconnaissance, and offensive simulation

Free

Introduction to Python for Defensive Security

A hands-on introduction to automating defensive security tasks with Python

Free

Joas A. Santos is a seasoned cybersecurity professional and offensive security expert known for his work in Red Team operations, penetration testing, and security education. He has held roles spanning security engineering, GRC analysis, DevSecOps, and red team leadership, and is active as a speaker, author, and educator in the cybersecurity community. Joas has contributed to frameworks like MITRE ATT&CK and holds an extensive portfolio of international certifications. He also teaches at postgraduate level and shares practical offensive security insights across global forums and social platforms.

Red Team Leaders is the training and certification platform he founded, focused on practical offensive security education. It offers tutorials, courses, exams, and resources designed to deepen understanding of advanced

Certified Artificial Intelligence PenTest Junior (CAIPJ)

Hands-on LLM Exploitation

-37% $22

Certified C++ Practitioner (CCPP)

Professional certification in modern C++ programming, focused on robust, maintainable code and practical industry skills.

-80% $1

Certified Cybersecurity Educator Professional (CCEP)

The Global Standard for Cybersecurity Education and Expertise

-80% $0.99

Certified Encryption and Cryptography Beginners (CECB)

Beginner-friendly assessment of foundational encryption and cryptography concepts

$5

Certified Exploit Development Specialist (CEDS)

Advanced Windows User-Mode Exploit Engineering & Mitigation Bypass

-65% $12

Certified Game Hacking Engineer (CGHE)

Practical Game Hacking, Reverse Engineering and Trainer Development

$25

Certified Malware Analysis Beginners (CMAB)

Fundamentals of Static, Dynamic and Behavioral Malware Analysis

$8

Certified OSINT Research Analyst (CORA)

Professional Certification in Open Source Intelligence and Digital Investigation

-72% $3

Certified Offensive Windows API (COWA)

Master Low-Level Windows API with Hands-On Offensive Development

-91% $0.50

attack simulations and Red Team tradecraft. The initiative emphasizes hands-on learning, real-world techniques, and accessible content for both aspiring and experienced cybersecurity practitioners, helping bridge gaps between theory and practical Red Team operations.

"Joas is one of the top voices on linkedin. The guy is an absolute machine and still manages to be one of the nicest and most approachable people in the industry. While there is a small dollar value attached to certain exams, the absolutely massive catalogue of free courses makes Red Team Leaders one of HVCK's top picks. Really want to take an exam of one of the few courses with a price tag? Never fear, we have 50 vouchers to give away. Simply share this issue of HVCK, tag me in (Ryan WIlliams) and a juicy voucher is coming your way.

Big thankyou for all your support through the years mate. The say dont meet your heros... I say thats bullshit..

Thank Joas... Straight up legend

Certified Red Team Engineer Development (CRTED)

Develop your practical tools for Red Team operations.

$25

Certified Red Team Operations Management (CRTOM)

Advanced Red Team Operations & Governance

-75% $2.50

Certified Reverse Engineering Beginners v1 (CREB)

Reverse Engineering Practical Exams — Windows PE, Debugging & Runtime Analysis

$14.99

Certified Security Code Review Beginners (CSCRB)

Practical Secure Coding and Code Review for Beginners

-88% $0.99

Certified Threat Hunting and Incident Response I (CTHIRI)

A hands-on, vendor-neutral blue-team certification for modern defenders.

$8.99

Certified Threat Intelligence & Governance Analyst (CTIGA)

Bridging Cyber Threat Intelligence, Governance and Strategic Decision-Making

-70% $3

Certified Web API PenTest Junior (CWAPJ)

Hands-on API Hacking Exam for Junior Pentesters

-60% $12

Certified Windows Drivers Exploitation v1 (CWDE)

Practical Windows Drivers Exploitation

$29.99

ATTA

What is this Academy you go on about?

AttackIQ Academy is a free cybersecurity training and education initiative from AttackIQ designed to help security professionals build practical, real-world skills in threat-informed defense, breach and attack simulation, purple teaming, and the MITRE ATT&CK framework.

The Academy offers modular online courses ranging from foundational to advanced levels, combining expert-led instruction with hands-on cyber range labs hosted in scalable virtual environments that mirror realistic attack and defense scenarios.

Courses are regularly updated and eligible for (ISC)² Continuing Professional Education (CPE) credits, and the program has grown to tens of thousands of students globally, reflecting its role as a community resource for elevating security capabilities across teams and individual learners.

Core Learning Paths

AttackIQ Academy offers structured learning paths organized by experience level and topic area. Each path includes hands-on cyber range labs, practical exercises, and badges/ certifications upon completion.

1. Foundations of Operationalizing MITRE ATT&CK
Level: Entry/Foundational
Estimated Duration: 12-20 hours (12.75 hours of content)
Number of Courses: 9 courses

What You'll Learn:

- History and evolution of the MITRE ATT&CK framework
- Why organizations are adopting ATT&CK
- Basic workflows for operationalizing MITRE ATT&CK within security programs
- Tools and resources including ATT&CK Navigator, MITRE CAR, and Joystick
- FInding, creating, and testing security analytics

Key Courses:

- Foundations of MITRE ATT&CK (entry-level)

- Application of ATT&CK Navigator (hands-on labs)
- Applying MITRE Threat Report ATT&CK Mapper (TRAM)
- ATT&CK Workbench installation, configuration, and usage
- Top ATT&CK Techniques tool
- Introduction to FIN6 Emulation Plans
- MenuPass Emulation Plan Execution
- Uniting Threat and Risk Management with NIST 800-53 and MITRE ATT&CK

2. Purple Teaming Learning Path

Foundational Track
Level: Entry/Foundational
Estimated Duration: 8-14 hours
Number of Courses: 5 courses (includes 3 foundational courses shared with other paths)
What You'll Learn:

- Core concepts, workflows, activities, and artifacts of purple teaming
- Joint operation principles of red and blue teams
- Role of purple teams in threat-informed defense strategy
- Skills required to plan and execute basic purple team exercises

Key Courses:

Foundations of Purple Teaming
Foundations of Operationalizing MITRE ATT&CK
Foundations of Breach & Attack Simulation
Additional purple team-specific coursesIntermediate Purple Teaming Track

Intermediate Purpleteaming
Level: Intermediate (Level II)
Estimated Duration: 8-14 hours (includes cyber range time)
Number of Courses: 5 courses
What You'll Learn:

- Threat intelligence integration
- Organizational threat alignment techniques
- Threat modeling based on business requirements and IT architecture
- Adversary emulation planning
- Hands-on planning exercises and threat emulation scenarios

Key Courses:

Threat Modeling and Emulation Planning (2-part series)
Advanced threat alignment exercises
Practical cyber range labs

3. Breach and Attack Simulation (BAS) Learning Path

Foundational Track
Level: Entry/Foundational
Estimated Duration: 2+ hours for foundation, additional time for advanced courses

What You'll Learn:

- Capabilities and deployment options of BAS platforms
- Testing methodologies to emulate adversarial techniques
- Measuring efficacy of security control implementations and configurations
- Building threat-informed defensive strategies
  Best practices for deploying BAS in environments

Key Courses:

Foundations of Breach and Attack Simulation (hands-on training with cyber range)
Basic security testing plan composition

DANIEL STIEGMAN | 5 HOURS | ALL SOURCES ANALYSIS | CTI ANALYST

Advanced Cyber Threat Intelligence Writing: Crafting Actionable Reports

Learn to turn complex threat data into clear, actionable intelligence. This course sharpens your writing skills so you can craft concise, structured...

VIEW DETAILS

KEITH WILSON | 45 MINUTES | ATTACKIQ PLATFORM | BLUE TEAM MEMBER

Agentless Threat Emulation with AttackIQ Flex

VIEW DETAILS

KEITH WILSON | 1 HOUR | ATTACKIQ PLATFORM | BLUE TEAM MEMBER

Agentless Threat Emulation with AttackIQ Flex v3

Learn how to assess and improve your cybersecurity defenses through agentless testing with AttackIQ Flex v3. This course shows you ho...

VIEW DETAILS

INTERMEDIATE MITRE ATT&CK | KEITH WILSON | 1.5 HOURS

Application of MITRE ATT&CK Navigator

Learn to operationalize the MITRE ATT&CK Framework using ATT&CK Navigator. This hands-on course teaches you how to create, manage, an...

VIEW DETAILS

INTERMEDIATE BREACH & ATTACK SIMULATION | KEITH WILSON | 1.5 HOURS | ALL SOURCES ANALYSIS

Assessment Design For Gap Analysis

Design and execute gap analysis assessments using real-world threat data to uncover and strengthen security defenses.

VIEW DETAILS

INTERMEDIATE BREACH & ATTACK SIMULATION | KEITH WILSON | 1.5 HOURS | ALL SOURCES ANALYSIS

Assessment Design for Security Controls

Apply Breach and Attack Simulation skills to test and validate security controls in this hands-on, scenario-based course using the AttackIQ...

VIEW DETAILS

BRANDON GROUX | < 30 MINUTES | BLUE TEAM MEMBER | CISO

Breathwork for Stress

Take 15 minutes to release tension and calm your mind through guided breathwork for stress relief.

VIEW DETAILS

< 30 MINUTES | BLUE TEAM MEMBER | CISO | CTI ANALYST

Center Conversations Enabling Threat-Informed Defense

MITRE's Richard Struse and AttackIQ's Carl Wright discuss how threat-informed defense transforms cybersecurity.

VIEW DETAILS

ANDREW COSTIS | 30 MINUTES | ATTACKIQ PLATFORM | BLUE TEAM MEMBER

CISA Advisory – Lockbit

Explore CISA Advisory AA23-075A and the LockBit 3.0 ransomware campaign. See how attack graphs reveal vulnerabilities and guide effective...

VIEW DETAILS

JIM MASON | 1.5 HOURS | BLUE TEAM MEMBER

Continuous Security Validation Workshop

VIEW DETAILS

INTERMEDIATE MITRE ATT&CK | ANDREW COSTIS | 1.5 HOURS

Countering Ransomware with MITRE ATT&CK

VIEW DETAILS

FROM CONCEPT TO PRACTICE: APPLYING THE V | KEITH WILSON | 45 MINUTES

Delivering Value with the ATT&CK Sightings Report

VIEW DETAILS

FROM CONCEPT TO PRACTICE: APPLYING THE V
KEITH WILSON | 1.5 HOURS

Attack Flows v2 — How to Model and Sequence Attacks

Learn to model and visualize cyber attacks using the MITRE Engenuity Attack Flow project. This hands-on course teaches you how to sequence...

VIEW DETAILS

1 HOUR | ATTACKIQ PLATFORM
BLUE TEAM MEMBER

AttackIQ Foundational Blueprints

Discover how to build a continuous security optimization practice using AttackIQ's proven Foundational Blueprints.

VIEW DETAILS

SECURITY LEADERSHIP | < 30 MINUTES
BLUE TEAM MEMBER

Better Decision Making Through Adversary Simulation

CTO Stuart McClintosh shares how adversary simulation drives smarter, data-informed security decisions.

VIEW DETAILS

INTERMEDIATE BREACH & ATTACK SIMULATION
KEITH WILSON | 1.5 HOURS

Beyond Atomic Testing with Attack Flows

Learn to build realistic, multi-stage attack simulations using Attack Flows to test advanced EDR and AI-based tools.

VIEW DETAILS

KEITH WILSON | 45 MINUTES
ATT&CK FRAMEWORK | BLUE TEAM MEMBER

Black Hat Attendees Only — D3FEND with ATT&CK

VIEW DETAILS

BRANDON GROUX | < 30 MINUTES
BLUE TEAM MEMBER | CISO

Breathwork for Energy

Take 15 minutes to recharge your focus and energy through guided breathwork and mindful awareness.

VIEW DETAILS

KEITH WILSON | 10 HOURS | ADVANCED
ALL SOURCES ANALYSIS

Detection Management: From Entropy to Evidence

Free, evidence-first detection engineering with MITRE ATT&CK, Sigma, and the 4D score. Validate rules, cut noise, and report real coverage. Earn CP...

VIEW DETAILS

JOSE BARAJAS | 1 HOUR
BLUE TEAM MEMBER | CISO | CTI ANALYST

Emulating APT-29 with Breach and Attack Simulation

VIEW DETAILS

INTERMEDIATE PURPLE TEAMING | BEN OPEL
1.5 HOURS | ALL SOURCES ANALYSIS

Emulation Planning for Purple Teams

VIEW DETAILS

SECURITY LEADERSHIP | < 30 MINUTES | CISO
GUEST LECTURE | SECURITY MANAGER

Evidence-Based Security Management Primer

VIEW DETAILS

FROM CONCEPT TO PRACTICE: APPLYING THE V
ANDREW COSTIS | 1 HOUR

Extending ATT&CK with ATT&CK Workbench

VIEW DETAILS

KEITH WILSON | 5 HOURS
ARTIFICIAL INTELLIGENCE (AI)

Foundations of AI Security

VIEW DETAILS

KEITH WILSON | 2 HOURS | ATT&CK FRAMEWORK | BLUE TEAM MEMBER

Testing Linux and Mac with OceanLotus

Learn to emulate the real-world tactics of the OceanLotus APT group and test your defenses across Linux and macOS. Gain hands-on...

VIEW DETAILS

1 HOUR | BLUE TEAM MEMBER | CISO | DIRECTOR OF THREAT INFORMED DEFENSE

The Cybersecurity Illusion Enterprise Security Remains Reactive

VIEW DETAILS

INTERMEDIATE PURPLE TEAMING | BEN OPEL | 1.5 HOURS | ALL SOURCES ANALYSIS

Threat Alignment for Purple Teams

VIEW DETAILS

BEVERLY BENSON | 45 MINUTES | ALL SOURCES ANALYSIS | BLUE TEAM MEMBER | CTI ANALYST

Threat-Informed Architecture

VIEW DETAILS

FROM CONCEPT TO PRACTICE: APPLYING THE V | JACKSON WELLS | 45 MINUTES | ALL SOURCES ANALYSIS

Top ATT&CK Techniques

VIEW DETAILS

FROM CONCEPT TO PRACTICE: APPLYING THE V | BEN OPEL | 1.5 HOURS | ALL SOURCES ANALYSIS

Uniting Threat and Risk Management with NIST 800-53 & MITRE ATT&CK

VIEW DETAILS

JOSE BARAJAS | < 30 MINUTES | BLUE TEAM MEMBER | CTI ANALYST | DIRECTOR OF THREAT INFORMED DEFENSE

PreActive Cyber Hygiene – The MITRE ATT&CK Dirty Dozen TTPs

VIEW DETAILS

MAÉVA GHONDA | < 30 MINUTES | CISO | GUEST LECTURE | QUANTUM

Quantum for Chief Information Security Officers

VIEW DETAILS

SECURITY LEADERSHIP | PHIL AITCHISON | 45 MINUTES | ADVANCED | CISO | CYBER ORGANIZATIONAL PLANNING

Safeguarding the Supply Chain

VIEW DETAILS

SECURITY LEADERSHIP | HANI BANI AMER | KEITH WILSON | 45 MINUTES | CISO | CYBER THREAT ANALYSIS

Secure Digital Transformation – Best Practices and Strategies

VIEW DETAILS

SECURITY LEADERSHIP | 1 HOUR | ANY LEVEL | CISO | DOES NOT INCLUDE LABS

Siobhan Gorman – Best Practices in Cybersecurity Crisis Management

VIEW DETAILS

SECURITY LEADERSHIP | 1.25 HOURS | CISO | CYBERSECURITY MANAGEMENT | CYBER RISK ASSESSMENT & MANAGEMENT

Strategic Cybersecurity Management

VIEW DETAILS

ATT&CK

FROM CONCEPT TO PRACTICE: APPLYING THE V
JOSE BARAJAS | 1.5 HOURS
ALL SOURCES ANALYSIS

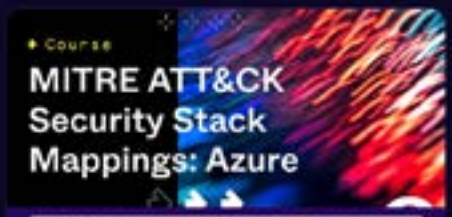
menuPass Emulation Plan Execution

VIEW DETAILS

FROM CONCEPT TO PRACTICE: APPLYING THE V
MATIAS ALTMAN | 1 HOUR
ALL SOURCES ANALYSIS

MITRE ATT&CK Security Stack Mappings: AWS

VIEW DETAILS



FROM CONCEPT TO PRACTICE: APPLYING THE V
JOSE BARAJAS | 1.5 HOURS
ALL SOURCES ANALYSIS

MITRE ATT&CK Security Stack Mappings: Azure

VIEW DETAILS

CHARLIE COVEY | < 30 MINUTES
BLUE TEAM MEMBER | CISO
COMPLIANCE OFFICER

Movement Through Yoga

VIEW DETAILS

30 MINUTES | ANY LEVEL
GENERAL SECURITY | GUEST LECTURE

Navigating the Cyber Security Career Path

VIEW DETAILS

< 30 MINUTES | CISO
DIRECTOR OF THREAT INFORMED DEFENSE
GUEST LECTURE

People, Process, Technology

VIEW DETAILS

INTERMEDIATE MITRE ATT&CK
KEITH WILSON | 2 HOURS
BLUE TEAM MEMBER | CTI ANALYST

Foundations of Breach & Attack Simulation

This session is a hands-on training program designed to introduce the capabilities and deployment options in a BAS (breach and attack...

VIEW DETAILS

PETE LUBAN | 7 HOURS
ALL SOURCES ANALYSIS
BLUE TEAM MEMBER | CTEM

Foundations of CTEM

VIEW DETAILS

DANIEL STIEGMAN | 45 MINUTES
BLUE TEAM MEMBER
COLLECTION OPERATIONS | CTI ANALYST

Foundations Of Cyber Threat Intelligence

VIEW DETAILS

KEITH WILSON | 1.5 HOURS
ALL SOURCES ANALYSIS
BLUE TEAM MEMBER | CTI ANALYST

Foundations of Operationalizing MITRE ATT&CK

VIEW DETAILS

FROM CONCEPT TO PRACTICE: APPLYING THE V
KEITH WILSON | 1.5 HOURS
ALL SOURCES ANALYSIS

Foundations of Operationalizing MITRE ATT&CK v13

VIEW DETAILS

INTERMEDIATE MITRE ATT&CK | BEN OPEL
1.5 HOURS | ALL SOURCES ANALYSIS
BLUE TEAM MEMBER

Foundations of Purple Teaming

This training session introduces the state-of-the-art practice of purple teaming and its essential nature as the joint operation of red and blue team...

VIEW DETAILS


HVCK
ACADEMY
HVCK
ACADEMY
HVCK ACADEMY
d3rh4r
Security Researcher
XP
1849
DASHBOARD
MISSIONS
TRAINING
LABS
SUBSCRIPTION
BADGES
CERTIFICATES
LEADERBOARD
LOGOUT
SYSTEM ONLINE
OPERATIVE
Complete 10 missions
+100 XP
VETERAN
Complete 50 missions
+250 XP
ELITE
Complete 100 missions
+500 XP
SCHOLAR
Complete 5 courses
+300 XP
EXPERT
Complete 10 courses
+500 XP
WEB SPECIALIST
Complete 5 web security courses
+200 XP
CRYPTO MASTER
Complete 5 cryptography...
+200 XP
FORENSICS EXPERT
Complete 5 forensics...
+200 XP
DEDICATED
7-day login streak
+75 XP
COMMITTED
30-day login streak
+300 XP
PERFECT SCORE
100% on any quiz
+50 XP
SPEED DEMON
Complete a mission in under...
+100 XP

It's like all you can eat cyber niches. Tasty AF

HVCK Academy is where experienced security professionals go to explore the edges. This isn't a platform for learning what a firewall is. it's a deep-dive into the niches, the emerging domains, and the technical rabbit holes that mainstream training platforms won't touch. Adversarial AI, cellular interception, signal intelligence, autonomous SOC architecture. the stuff that keeps the curious up at night.

We built HVCK Academy for the practitioners who've already done their time in the SOC, earned their certs, and are now hungry for something more. The ones who want to understand how rogue base stations actually work, how to build threat intelligence programs for industrial AI systems, or how adversarial economics shapes the threat landscape. Every course is designed to take you deeper into a specific domain, with the technical rigour and hands-on labs to match.

This is training shaped by hacker culture, driven by curiosity, not compliance checklists. Our content comes directly from active researchers, conference speakers, and consultants working at the intersection of offensive security, emerging technology, and intelligence tradecraft. When we publish a course, it's because someone found something fascinating in the field and decided the community needed to know about it.

HVCK Academy is for the polymath operator. The one who sees patterns across disciplines, who wants to understand how things actually work at the lowest level, and who treats every new domain as territory worth mapping. If you're done with surface-level training and ready to go niche, you're in the right place.

Whats the damage?

RECRUIT — Free
Start your recon. Access basic courses, 2 lab hours per month, and 2 concurrent labs with community support. No certs, no VPN, no advanced content — but enough to get a taste of what HVCK Academy is about.

OPERATIVE — $9.99/mo (Most Popular)
Level up your skills. Everything in Recruit plus Standard courses, 20 lab hours per month, 5 concurrent labs, web app labs including DVWA and Juice Shop, certificates of completion, and email support. The entry point for serious practitioners ready to go deeper.

SHADOWNET — $19.99/mo
Advanced operative training. Full access to all courses including Advanced content, unlimited lab hours, 5 concurrent labs, all web app labs, network pentest labs, VPN access, certificates, and priority support. For operators who want the full range of tools at their disposal.

BLACKHAT — $49.99/mo
Elite access — everything unlocked. Everything in SHADOWNET plus Active Directory labs, custom lab environments, early access to new content, 1-on-1 mentoring sessions, and a private Discord channel. The top tier for those who want every advantage and direct access to our instructors.

ADVANCED PRIVACY & ANONYMITY IN...

By the end of this course, learners will be able to design,...

PROGRESS 0%

0 / 9 modules

ADVANCED | SHADOWNET+ | 25000 XP

START COURSE >

DARK AND DECENTRALISED FINANCE

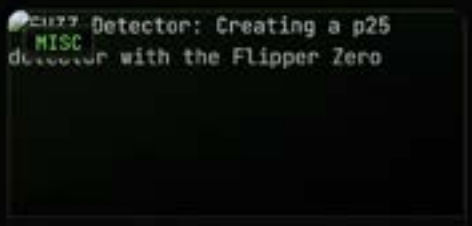
By the end of this course, learners will be able to...

PROGRESS 0%

0 / 10 modules

ADVANCED | SHADOWNET+ | 20000 XP

START COURSE >



FUZZ DETECTOR: CREATING A P25 DETECTOR WITH THE...

Of course. It is a profound joy to chart a course into the unseen...

PROGRESS 0%

0 / 10 modules

BEGINNER | 10000 XP

START COURSE >

INTRODUCTION TO DEEPFAKES

By the end of this course, learners will be able to create a...

PROGRESS 0%

0 / 10 modules

BEGINNER | 10000 XP

START COURSE >

MASTER FLIPPER ZERO PART 2 - YOU, ME & BADUSB

Of course. Let's design a rigorous, foundational course on...

PROGRESS 0%

0 / 10 modules

BEGINNER | 10000 XP

START COURSE >

MASTERING FLIPPER ZERO PART 1 - SUB-GHZ: THE...

Mastering Flipper Zero Part 1 - Sub-GHz: The Hidden Language of...

PROGRESS 0%

0 / 10 modules

BEGINNER | 10000 XP

START COURSE >

HVCK: IMPERIUM (DEMO)

Imperium is a next-generation command and control (C2) framewor...

PROGRESS 100%

1 / 1 modules

BEGINNER | 500 XP

REVIEW COURSE >

INTERMEDIATE ADVERSARIAL...

By the end of this course, learners will be able to create a...

PROGRESS 0%

0 / 10 modules

INTERMEDIATE | OPERATIVE+ | 1000 X

START COURSE >

INTRO TO LLM JAILBREAKING: RESEARCH...

By the end of this course, learners will be able to create...

PROGRESS 0%

0 / 10 modules

BEGINNER | 1000 XP

START COURSE >

FUNDAMENTALS

MASTERING FLIPPER ZERO PART 3 - RFID

Of course. It is a profound joy to map out such an expedition. To…

PROGRESS 0%

0 / 10 modules

BEGINNER ☆ 1000 XP

START COURSE ›

BINARY

OFFENSIVE IRONPYTHON: BRIDGING PYTHON TO .NET &…

A dive deep into the fascinating world where Python meets .NET and…

PROGRESS 0%

0 / 10 modules

INTERMEDIATE ☆ OPERATIVE+ ☆ 1125 XP

START COURSE ›

MISC

PROMPTSTEAL Unveiled: Simulating LLM-Powered Attack Chain

This course provides an in-depth, hands-on exploration of…

PROGRESS 0%

0 / 10 modules

ADVANCED ☆ SHADOWNET+ ☆ 1000 XP

START COURSE ›

FUNDAMENTALS

PRO BOND SOLO HOBO: BECOME A GRASSROOTS…

By the end of this course, learners will be equipped with th…

PROGRESS 0%

0 / 10 modules

BEGINNER ☆ 5000 XP

START COURSE ›

WEB

"FLY MY PRETTIES...FLY"

By the end of this course, learners will be able to design,…

PROGRESS 0%

0 / 10 modules

ADVANCED ☆ SHADOWNET+ ☆ 1500 XP

START COURSE ›

CRYPTO

Advanced Crypto Ex[ploitation

ADVANCED CRYPTO EXIPLOITATION

By the end of this course, learners will be able to analyze,…

PROGRESS 0%

0 / 10 modules

ADVANCED ☆ SHADOWNET+ ☆ 2000 XP

START COURSE ›

MISC

Signal Hunter: Antenna Theory & DIY Design for Offensive SDR

SIGNAL HUNTER: ANTENNA THEORY & DIY DESIGN FOR…

By the end of this course, learners will be able to…

PROGRESS 0%

0 / 10 modules

BEGINNER ☆ 1000 XP

START COURSE ›

NETWORK

Telecom Exploitation Framework: Build Your Own Offensive Telco Testing Tool

TELECOM EXPLOITATION FRAMEWORK: BUILD YOUR…

Welcome, future telecom security masters! I'm thrilled to embark o…

PROGRESS 0%

0 / 10 modules

INTERMEDIATE ☆ OPERATIVE+ ☆ 1000 X

START COURSE ›

MISC

VK FOUNDATION LICENCE EXAM PREP: YOUR GATEWA…

By the end of this course, learners will have the…

PROGRESS 0%

0 / 10 modules

BEGINNER ☆ 1000 XP

START COURSE ›

Full spectrum A.I.

> **Inside Jason Haddix's elite hacking bootcamps, the line between student and teacher starts to blur. I signed up to learn from a master, and walked away wondering if I was ready to take the stage myself.**

The screen glows with the electric blue of a **Discord** channel at 4 a.m. It's a motley crew of corporate security lifers in polo shirts, bug bounty hunters with anime avatars, and me, trying to look like I belong. We're all here for the same reason: **Jason Haddix**. He's the frontman, the headliner, the guy who has the keys to the kingdom. We've paid the premium ticket price for Arcanum's *"Red Blue Purple AI"* course, and this is Day Two. The air, thin and pixelated as it is, crackles with the anticipation of secrets being revealed.

Haddix is on screen, a calm presence in a world of digital chaos. He doesn't lecture from a podium; he speaks to you from what looks like a gamer's command center, a halo of monitors behind him. He's breaking down how to build an army of AI agents. Not just one chatbot, but a coordinated system, a cognitive orchestra. He calls them:

The **Research Agent**
The **Synthesis Agent**
The **Analysis Agent**
The **Generation Agent**

He's not teaching us a command; he's handing us an architecture, a blueprint for a thinking machine.

> "The goal here, isn't just to get an AI to write a phishing email for you," he says, his voice patient, peeling back layers of complexity like an onion. "It's to build a system that *understands* the whole process. One agent finds the target's company just got acquired, another synthesizes that with public data, a third analyzes the potential attack vectors, and a fourth generates the pretext. You're not the puppet. You're the puppeteer."

And that's when it hits me. A strange, electrifying feeling that has nothing to do with finding a zero-day vulnerability. It's the feeling a guitarist gets when they're not just learning a Hendrix solo note for note, but suddenly understand the theory behind it, the scales, the phrasing, the soul. I'm looking at his blueprint, the one he's built his career on, and I'm not just seeing a lesson. I'm seeing a setlist I could play myself. For the first time, I'm not just a student in the crowd. I'm wondering if I should be on stage.

The **Arcanum** experience is intentionally intimate, a stark contrast to the sprawling, anonymous arenas of mass-market online courses. This isn't Udemy. It's a boutique recording studio session. The class sizes are kept small to cultivate what Haddix calls a "community," but it feels more like a private, rolling afterparty. The Discord server is the tour bus, a place where the conversation never stops. Between live sessions, it's a flurry of shared tools, custom scripts, and students helping each other troubleshoot a finicky `Nuclei` template or a stubborn API endpoint.

This is where you see the Haddix formula in action. It's built on a core philosophy that feels both radical and obvious: **"No Gatekeeping."** In a field notorious for its arcane knowledge and holier-than-thou experts, Haddix operates with a kind of radical transparency.

> "Look, there's no secret society here," he'll say, leaning into his webcam, making eye contact with every stranger at once. "It's not magic. It's methodology. It's process. Anyone can learn it if they're willing to put in the work."

His teaching is a constant dialogue, a Socratic method for hackers. He'll pause mid-anecdote, to share another resource from a seemingly endless mental list of AI's brightest innovators. * Questions aren't relegated to a final fifteen-minute Q&A; they're woven into the fabric of the lecture. He pulls them from the chat, reads them aloud, and tackles them in real time, often derailing his own lesson plan to chase a student's curiosity down a rabbit hole. It's messy, organic, and feels incredibly alive.

The Reveal

But the real magic, the moment the curtain is truly pulled back, comes when he explores his own contributions to tooling and novel use cases.

The polished slides vanish. His screen fills with a terminal, raw and unfiltered. He's sharing his personal configuration files, his custom aliases, the ugly, uncommented `Python` scripts he wrote at 3 a.m. to automate some tedious part of reconnaissance. He shows you the tools that failed, the workarounds he had to invent, the common errors that trip people up. He's not just giving you the finished, mastered track; he's showing you the outtakes, the false starts, the studio banter. He's demonstrating vulnerability, both in the technical sense and the human one. It's a performance of authenticity that's impossible to fake, and it's the cornerstone of the trust he builds.

Haddix wasn't born a teacher. Like many in his field, his backstory reads like a quiet, mythologized rise. He started in the trenches of traditional penetration testing, moved on to the high-stakes, high-reward world of bug bounties where he made his name, and then, in a move that puzzled some, pivoted. He turned from practitioner to educator, founding **Arcanum Information Security** to build the training

platform he wished he'd had.

It was a classic rock-and-roll move: the lead guitarist who gets tired of life on the road and decides to open a studio to produce the next generation. He had seen the gap between academic theory and the brutal reality of a live engagement. He knew the frustration of learning a tool only to find it useless against a real-world defense. Arcanum was his answer. He would teach what actually works, right now, while other education providers play catch up.

The Paradox of Access

This creates the central conflict in his world. Arcanum's courses are positioned as premium, high-value offerings. They're expensive, running thousands of dollars for a multi-day intensive. This puts his "no gatekeeping" mantra in a precarious position. **How can knowledge be truly accessible when it's behind a significant paywall?**

I wrestled with this myself before clicking "enroll." I was lucky enough to be gifted this opportunity. One I would never have been able to experience without such generosity. It's a paradox. You're paying for access to the man who says access shouldn't have a price. But as the course unfolds, you realize what you're buying isn't just the information, much of which, he'd admit, is technically available somewhere on the internet if you dig hard enough.

You're paying for curation. For context. For the community. You're paying for the shortcut through the noise, guided by someone who's already mapped the terrain. Most of all, you're paying for his time and his willingness to engage directly. It's the difference between listening to the album and getting a private lesson from the artist who wrote it. Still, the tension remains, a philosophical dissonance that hums quietly beneath the surface. The hum fades to silence as the dark arts deep dive kicks up a gear.

This is when the "real" person emerges. Not the infallible expert, but the seasoned practitioner who has spent countless hours staring at a broken terminal, fueled by caffeine and frustration. Showing the cohort that even the pros make mistakes, that hacking isn't a series of clean, elegant exploits but a messy, iterative process of trial and error. By sharing his failures, he normalizes them. He gives you permission to be imperfect, to learn by breaking things, which is the only way anyone has ever truly learned anything in this field. It's in these moments of candor that the high price tag and the expert persona melt away, leaving just a guy who is genuinely passionate about his craft and wants you to be, too.

It was this very methodology, this relentless demystification, that made the seemingly impenetrable world of AI feel suddenly accessible. By pulling back the curtain on his own process, failures and all, Haddix forged a causal link between vulnerability and understanding. The technical deep-dive that followed wasn't a jolt back to a complex topic; it was the ultimate proof of his teaching philosophy. The AI agents became the final, triumphant chord in a composition about access and empowerment.

As Day Two of the course wore on, Haddix didn't just show us *his* agents. He gave us the Lego bricks. He laid out the entire architecture for Red, Blue, and Purple AI systems.

* **For Red Teamers:** He showed how to chain a `JS Ninja` agent to parse JavaScript for secrets, then feed its output into an `XSS Mutation Engine` to craft bypasses.

* **For Blue Teamers:** He demonstrated a `Suricata Rule Bot` that could watch threat intel feeds and automatically write new network detection rules, or a `SOC Manager Briefer Bot` that could summarize a complex incident for a non-technical executive.

It wasn't just a list of cool tricks. It was a complete, holistic system. A philosophy. He was showing us how AI could bridge the historic divide between offense and defense, creating a true "Purple Team" workflow where AI-driven attackers (`Caldera`) could be pitted against AI-driven defenders (`YARA Rule Bot`), generating insights at a speed no human team could match.

Watching him lay it all out, piece by logical piece, was a revelation. The mystique of "AI in cybersecurity" dissolved. It wasn't some unknowable black box. It was a system of inputs and outputs, of specialized agents and cognitive orchestration. It was a methodology. And methodologies can be learned. They can be replicated. They can be improved upon.

That's when the thought, quiet at first, became a roar in my head: *I can do this.* Not just use it, but build it. And if I can build it, I can explain it. If I can explain it, I can teach it.

The realization was terrifying and exhilarating. Was this Haddix's secret plan all along? To not just create students, but to create disciples? To democratize expertise so thoroughly that his own students become his peers, and eventually, his competition? It's the ultimate act of "no gatekeeping": to teach someone so well they no longer need you. To make yourself obsolete.

The Encore

The class ends. The Zoom window closes. The Discord quiets to a low hum. It's late (lunchtime but I've been up since 3am), my terminal is open.

I'm not running one of Jason's pre-made scripts. I'm writing my own. My first agentic opera. A platform to democratise offensive and defensive security for SMEs that cant afford the managed SOC price tag. Its a little rough.

But it's mine.

I'm looking at the blinking cursor on the screen, at the architecture I scrawled in my notebook, a pale imitation of the one Jason put on screen. The feeling is still there, that powerful hum of possibility. I came here to be a face in the crowd, to learn the songs of a master. But Jason Haddix did more than just play his greatest hits. He handed me his guitar, showed me the chords, and whispered:

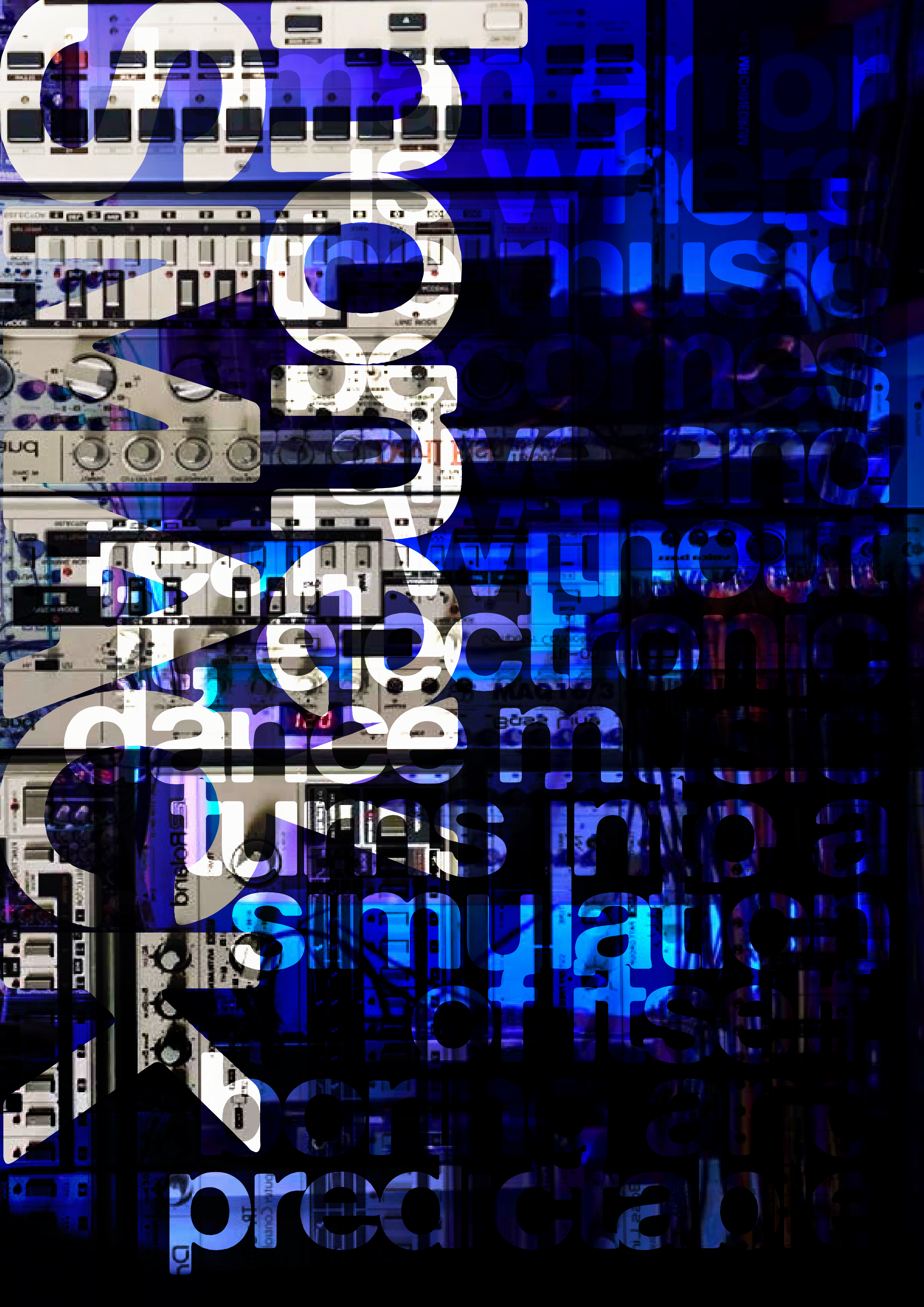
Now you play

And for the first time,
I believe I can.
d8rh8r

https://www.arcanum-sec.com


DAH


CK
music


is where
music
becomes
alive and
without
techno
electronic
dance music
turns into a
simulation
of itself
boring and
predictable

Voltage Theology

DR. DAVID HABERFELD AND THE ACADEMIC DECONSTRUCTION OF ACID CHAOS

How a Melbourne techno anarchist earned a PhD by refusing to play it safe.

Penned by D8RH8R

There's a particular type of dissonance that happens when underground culture meets institutional validation. Usually, one side compromises, the academic waters down the rawness, or the artist performs radicality for tenure review boards. Dr. David Haberfeld, performing as HONEYSMACK for over three decades, represents something rarer: a complete refusal to resolve that tension.

Born in 1969 in Melbourne's pre-internet underground, Haberfeld has spent 30+ years in the trenches of acid techno, not as a spectator or documentarian, but as an active combatant. His weapon of choice: hardware that misbehaves. His battlefield: dance floors where bodies and machines negotiate reality in real-time. His documentation method: a PhD thesis with the most deliberately absurd title in academic music composition, *"Bacharach, Britney, and Acid Techno Bangers: The Evolving Creative Practice of Honeysmack."*

If that title sounds like a middle finger wrapped in institutional approval, that's because it is.

THE ACCIDENTAL ACADEMIC

Haberfeld's path to a doctorate wasn't driven by intellectual ambition, it was a hack. "I kept going to universities to gain access to music technology and studios when I was younger because music technology was totally unaffordable and out of my reach at the time," he explains. Universities had the gear. Universities had the studios. The qualification was just overhead.

> **"I didn't give much thought about the qualification or where it would lead to. You could say I was an accidental academic of sorts as I never thought making underground electronic dance music would be considered an academic pursuit."**

But here's where it gets interesting: Haberfeld didn't water down his practice for academic legitimacy. Instead, he weaponized academic rigor to interrogate exactly what he'd been doing on dance floors since the early '90s. His 2021 PhD from Monash University examines real-time compositional practices in acid techno, essentially, how to make bangers in the moment, with no safety nets, while voltage runs through your hands and bass pressure warps your ribcage.

The research question is deceptively simple: Where does composition happen when there's no score, no pre-made tracks, just machines and meat in a feedback loop?

> **"For me, the composition is the whole situation," Haberfeld states. "It's not sitting inside the machines, they're just raw tools waiting to be pushed. The room, the sound system, the crowd's energy, the pressure of the moment, that's where the piece actually forms. Every decision I make is a response to that feedback loop, a moment in time. I'm not executing something pre-written, I'm inside it while it's happening. The performance is the composition, and it only exists for that moment. Once it's over, it's gone."**

This is composition as temporal hacking, manipulating time-based systems in conditions of controlled chaos. No version control. No rollback. Pure commit-or-die logic.

HARDWARE AS RESISTANCE

While the rest of electronic music moved to laptops and endless VST libraries, Haberfeld stayed locked to hardware, specifically the holy trinity of Roland machines: TB-303, TR-808, TR-909. Not out of nostalgia or gear fetishism, but because these machines do something software can't: they fight back.

> **"The 303 isn't powerful because it sounds 'good', it's powerful because it's awkward and limited," he explains. "It lives in an uncomfortable middle ground between control and instability, somewhere amid bass, lead, and percussion. The sequencer is crude, the filter is aggressive, and tiny changes can have massive consequences. You're never fully in control of it, you're negotiating with it. That volatility creates tension, and that's what the body responds to."**

This is the critical insight: the 303's power comes from *friction*, not functionality. It's a poorly designed bass synthesizer that became legendary precisely because it refuses to be mastered. Every performance becomes a negotiation between human intention and machine volatility, a conversation conducted in voltage and pressure.

> **"The 303 is simple in sound and function, it forces commitment. Push it and it pushes back, and that struggle becomes audible, with almost instant gratification. That's why it still works. It's not nostalgia, it's friction."**

The parallel to hacker culture is obvious: the best exploits come from pushing systems beyond their intended use, from finding the edges where control breaks down and interesting behavior emerges. Haberfeld isn't using the 303 correctly, he's exploiting its limitations as features.

THE DEATH OF RISK

Ask Haberfeld about the current state of electronic music and the frustration is palpable. Not at individual artists, but at the systematic removal of danger from the process.

> **"Acid was never meant to be safe. It came from accidental misuse, reappropriated technology and machines pushed too hard, bodies too close, ideas colliding. A lot of electronic dance music now feels over-sanitized: pristine sound, perfect structure, everything optimized, over-produced and designed. Nothing's really at risk. The friction's gone."**

He's not romanticizing the past, he's pointing at a structural problem. When DAWs give you infinite undo, infinite takes, infinite polish, you lose the stakes. Error becomes something to eliminate rather than material to work with.

> **"What's missing is risk in the process. Letting machines misbehave. Allowing things to clip, drift, or fall apart, in public. Too much is rehearsed and pre-approved. Acid works when there's tension, when repetition gets uncomfortable, when systems fight back. Once it becomes polite, it stops being Acid."**

This resonates with contemporary security research, pentesting isn't about perfect exploits, it's about pushing systems until they reveal unexpected behavior. The value is in the friction, the resistance, the moment when things don't go according to plan.

> **"Human error is where the music becomes alive and real. Without it, electronic dance music turns into a simulation of itself, boring and predictable."**

NOTATION AS IMPOSSIBILITY

One of the more fascinating aspects of Haberfeld's research is how it positions live hardware improvisation as fundamentally resistant to traditional forms of documentation. If someone tried to develop a notation system for acid techno, the way classical music codifies violin or piano, what would be lost?

> **"The most important stuff refuses notation. You can't write the pressure. That moment when a filter sweep goes too far or you grab and twist the wrong knob and you decide not to pull it back. The physical relationship with the machine when it starts pushing against you. The happy accidents that suddenly change your next move, none of that can be predetermined."**

This is crucial: the notation problem isn't technical, it's ontological. You can't score the willingness to risk collapse. You can't write down the crowd's energy reshaping your decisions in real-time. You can't quantize the hesitation, the impatience, the endurance.

> **"What has to stay wild is intent under uncertainty. The willingness to risk collapse. Once Techno is fully legible on paper, it stops being alive."**

This is performance as exploit, the value exists precisely in what can't be reproduced, in the unique conditions of that moment, that system, that vulnerability window.

THE MELBOURNE EXPLOIT

Haberfeld's academic output extends beyond his PhD. His 2024 paper in *Organised Sound* (Cambridge University Press), co-authored with Dr. Michael Callander and Dr. Dylan Davis, examines alternative approaches to electronic music education in Melbourne, specifically how knowledge transfers outside institutional frameworks.

Melbourne's electronic music scene developed through what Haberfeld calls "unofficial apprenticeships", knowledge moving hand-to-hand on dance floors, in studios, at 3am when equipment breaks and you have to debug in real-time.

> **"You don't really learn electronic music just by sitting in a classroom, a lot of it now comes from YouTube, forums, watching someone's screen, speaking to retail store staff and trying things out for yourself. That kind of self-directed learning is**

POWERFUL, BUT ON ITS OWN IT CAN BE ISOLATING AND ABSTRACT. WHAT REALLY MAKES IT STICK IS BEING THERE.

This is the hacker conference model applied to music: skills transfer through demonstration, observation, experimentation. Places like MESS (Melbourne Electronic Sound Studio) succeeded not by dictating outcomes but by providing access to tools without gatekeeping.

"THOSE UNOFFICIAL APPRENTICESHIPS WORK BECAUSE THEY'RE EMBODIED AND SOCIAL. KNOWLEDGE MOVES HAND TO HAND, PATCH CABLE TO PATCH CABLE. WE LEARN BY WATCHING, FAILING, BORROWING IDEAS, AND GIVING THEM BACK CHANGED."

The institutional challenge is structural: "Formal institutions can struggle with this because they need assessable results and clean pathways, linked to rewarding qualifications. What they miss is context, pressure, chaos, audience feedback, and the nuance of scene ethics. Community-led spaces provide that missing layer. Artists are not trained, you let them grow inside a living system."

THE "WALK ON ACID" EXPLOIT

No profile of Haberfeld would be complete without examining his most notorious exploit: "Walk On Acid," the 1999 track that sampled Burt Bacharach's "Walk On By" and became both an ARIA Award nominee and a legal flashpoint.

The track itself is a masterclass in reappropriation, taking a smooth '60s soul melody and forcing it through acid hardware until it becomes something unrecognizable yet familiar. But the real chaos came from the music video, directed by Philip Brophy, which featured a scantily dressed dancer in front of a Coca-Cola vending machine.

Coca-Cola's legal department did not appreciate their brand appearing in underground techno videos. The video was withdrawn under legal pressure, and Haberfeld's management attempted to leverage the censorship into publicity, calling every major media outlet for interviews.

The response: "Sorry, we're not interviewing him because they're one of our major advertisers."

This was pre-viral internet, pre-social media outrage cycles. Censorship happened quietly, with corporate leverage rather than public spectacle. But the track itself survived, eventually landing on "The 100 Greatest Australian Dance Tracks Of All Time" in 2015.

The absurd coda: being signed to the Zomba Group alongside Britney Spears and performing as support on her 2002 Crossroads promotional tour in Sydney. Acid techno anarchist meets teen pop machinery, peak absurdism.

CURRENT OPERATIONS: MELBOURNE INSTRUMENTS

Haberfeld's current work as Product Innovator at Melbourne Instruments represents another form of systems intervention. Rather than just using hardware, he's now designing it, specifically the Roto-Control, a MIDI controller with motorized touch-sensitive knobs, customizable haptics, and hi-res labeling screens.

The device is built for live performance, giving tactile feedback that makes controlling software feel like manipulating physical hardware. It's an attempt to restore the friction, the resistance, the physicality that disappeared when everyone moved to laptops.

He's engineering feedback loops into systems that have become too frictionless. The haptic response, the

motorized knobs pushing back, these are features designed to create the same negotiation dynamic that made the 303 powerful.

WHAT REMAINS

Strip away the gear, the techniques, the genre conventions. What's actually being transmitted when Haberfeld's machines run hot and the room locks in?

> **"If you strip everything away, Acid Techno isn't a style or a sound, it's a temporal dialogue, where machines speak fluently, humans listen hard, and time itself is continuously reprogrammed. It's commitment under uncertainty. Staying present inside something that could fall apart and choosing to push forward anyway. Repeating an idea until it stops being intellectual and becomes physical."**

This is the core exploit: using repetition and pressure to bypass cognitive processing and engage the body directly. The room becomes a distributed system where individual nodes (bodies) synchronize through bass pressure and temporal manipulation.

> **"What I'm trying to transmit isn't a riff or a texture, it's a state of happiness. Collective focus, endurance, surrender. That moment when the room locks in and breathes as one system. That shared intensity is the soul, the experience of holding tension together and not letting go."**

THE LESSON

Haberfeld's career offers a blueprint for how to operate at the intersection of underground culture and institutional legitimacy without compromising either. The key is refusing to resolve the tension, maintaining the friction, the awkwardness, the risk.

His advice to the next generation of electronic artists cuts through decades of received wisdom:

> **"I don't think they need to unlearn anything. What they do need is to stop measuring themselves against what they think they should be making or what other people think. New work comes from following what genuinely excites you, even if it doesn't line up with trends or expectations.**
>
> **The danger isn't technical incompetence or insufficient gear, it's "chasing approval instead of curiosity. If something makes you happy, follow it. If it feels embarrassing or unfashionable, that's probably a good sign. New work comes from sincerity, not correction."**

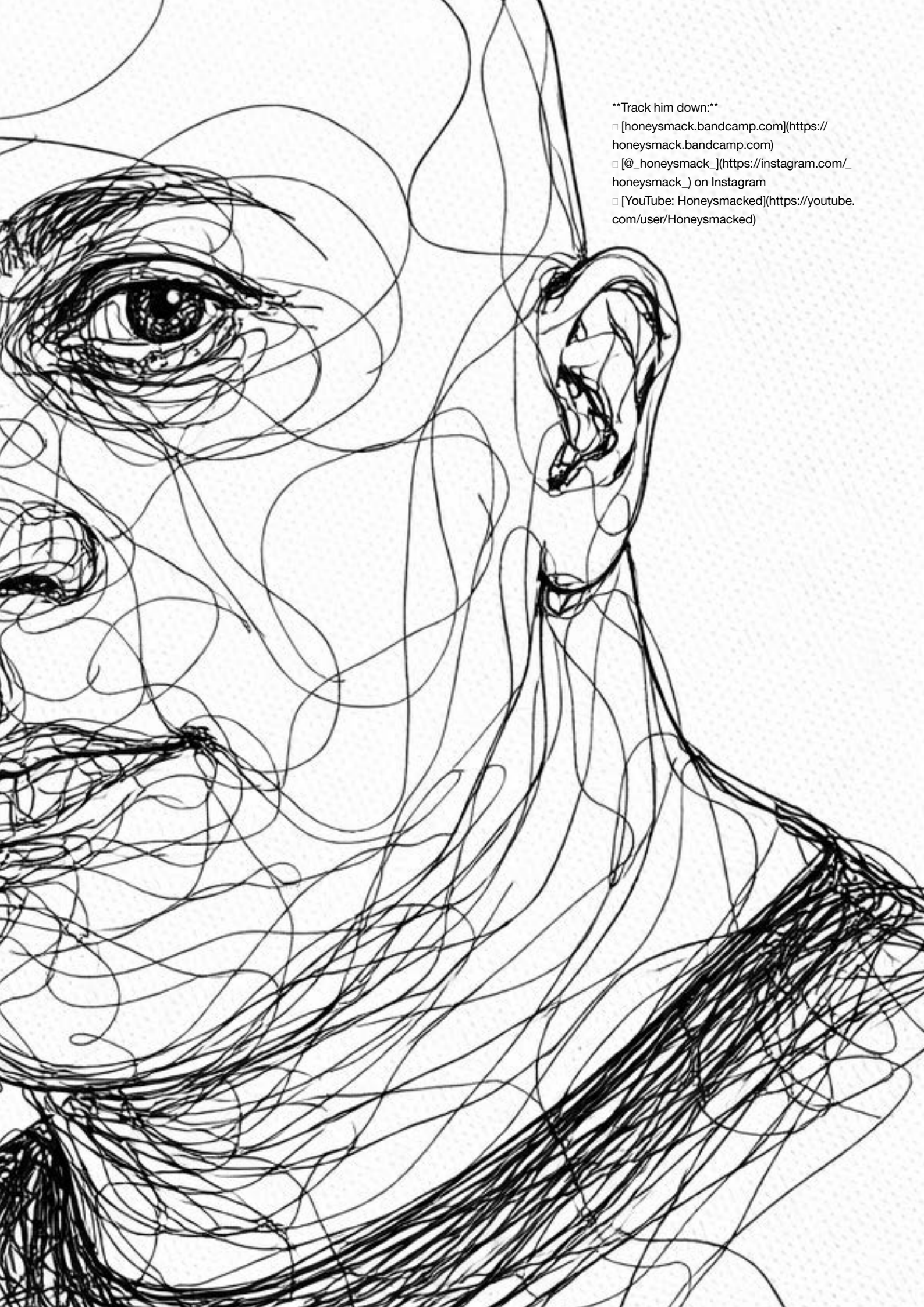
In a landscape optimized for viral moments and algorithmic approval, this is genuinely radical: make what excites you, embrace the friction, let the machines push back, risk collapse in public.

Because once it becomes polite, once the edges are smoothed away, once error is eliminated, it stops being alive.

Dr. David Haberfeld earned his PhD by documenting three decades of refusing to play it safe. The dissertation is just proof-of-work for a much larger exploit: demonstrating that academic rigor and anarchic practice can coexist if you're willing to maintain the voltage.

The machines are still running hot. The room is still locking in. The composition is still happening in the moment, unrepeatable, undocumented, as lived experience, and the friction, the essential, unrelenting tension, remains the point.

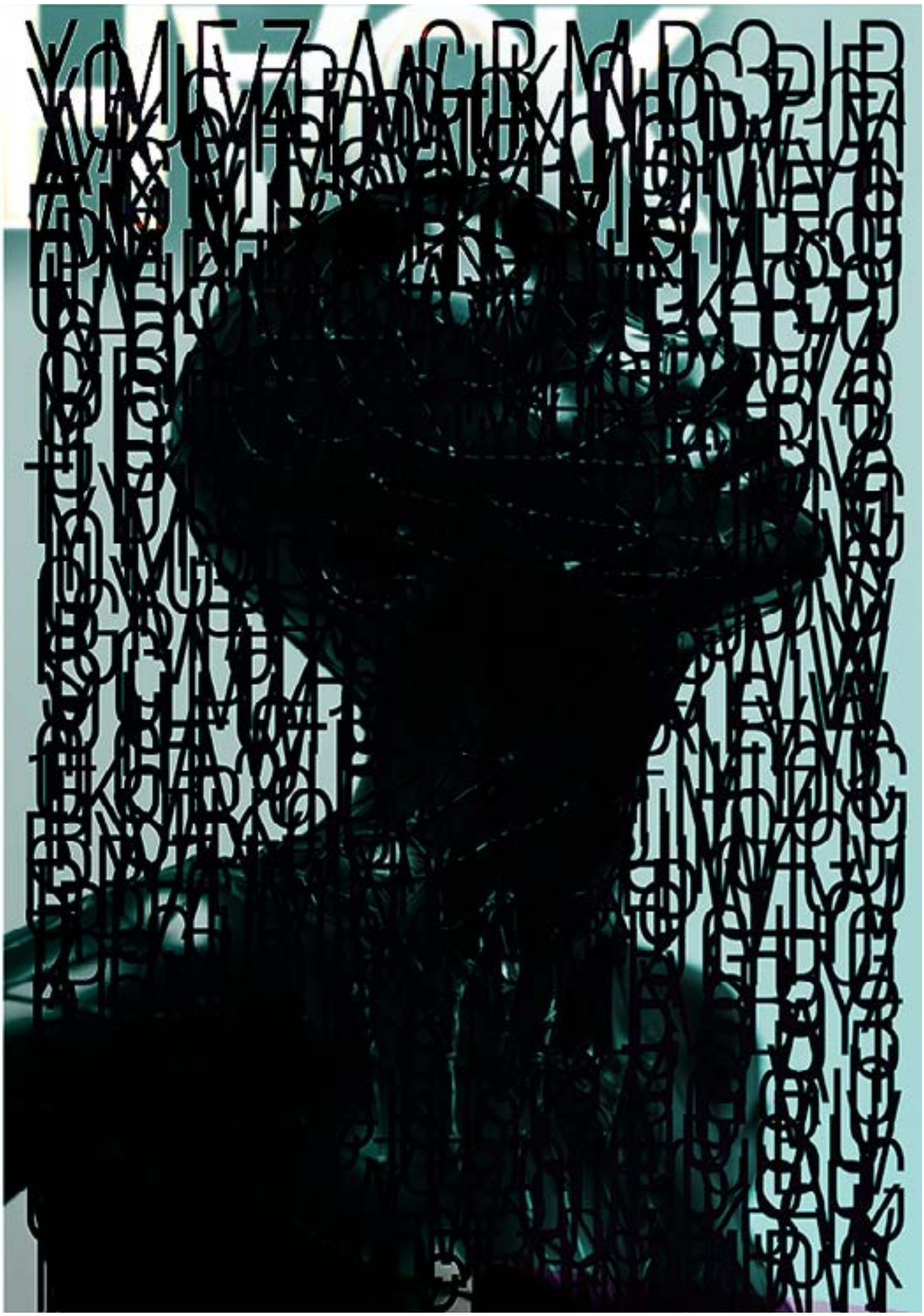
HONEYSMACK continues to perform and create across Australia and internationally. His PhD thesis "Bacharach, Britney, and Acid Techno Bangers: The Evolving Compositional Practice of Honeysmack" is available through Monash University. His work with Melbourne Instruments can be found at melbourneinstruments.com. For bookings and more information: davidhaberfeld.com



Track him down:
- honeysmack.bandcamp.com
- [@_honeysmack_](https://instagram.com/_honeysmack_) on Instagram
- [YouTube: Honeysmacked](https://youtube.com/user/Honeysmacked)

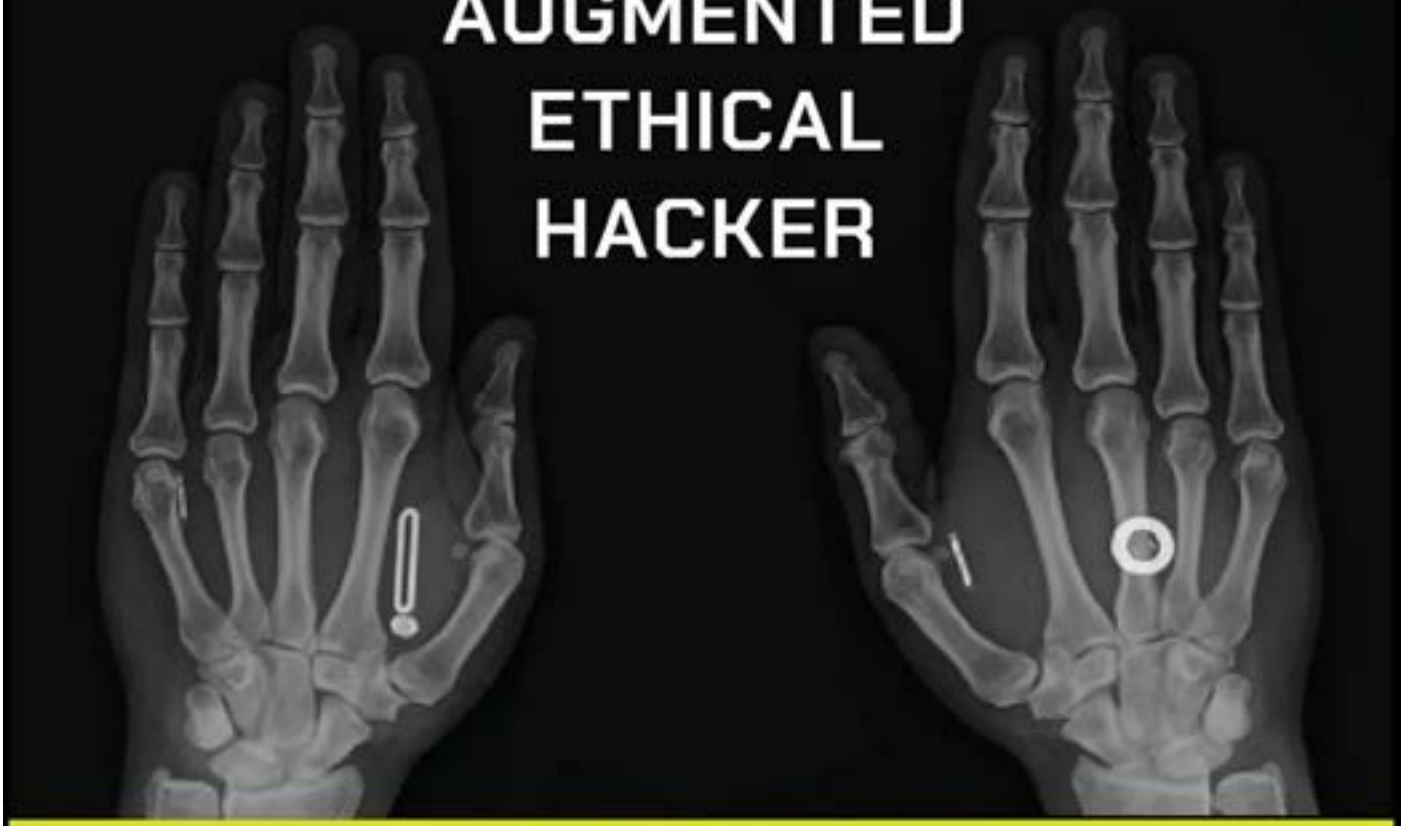

DAH


CK
arts

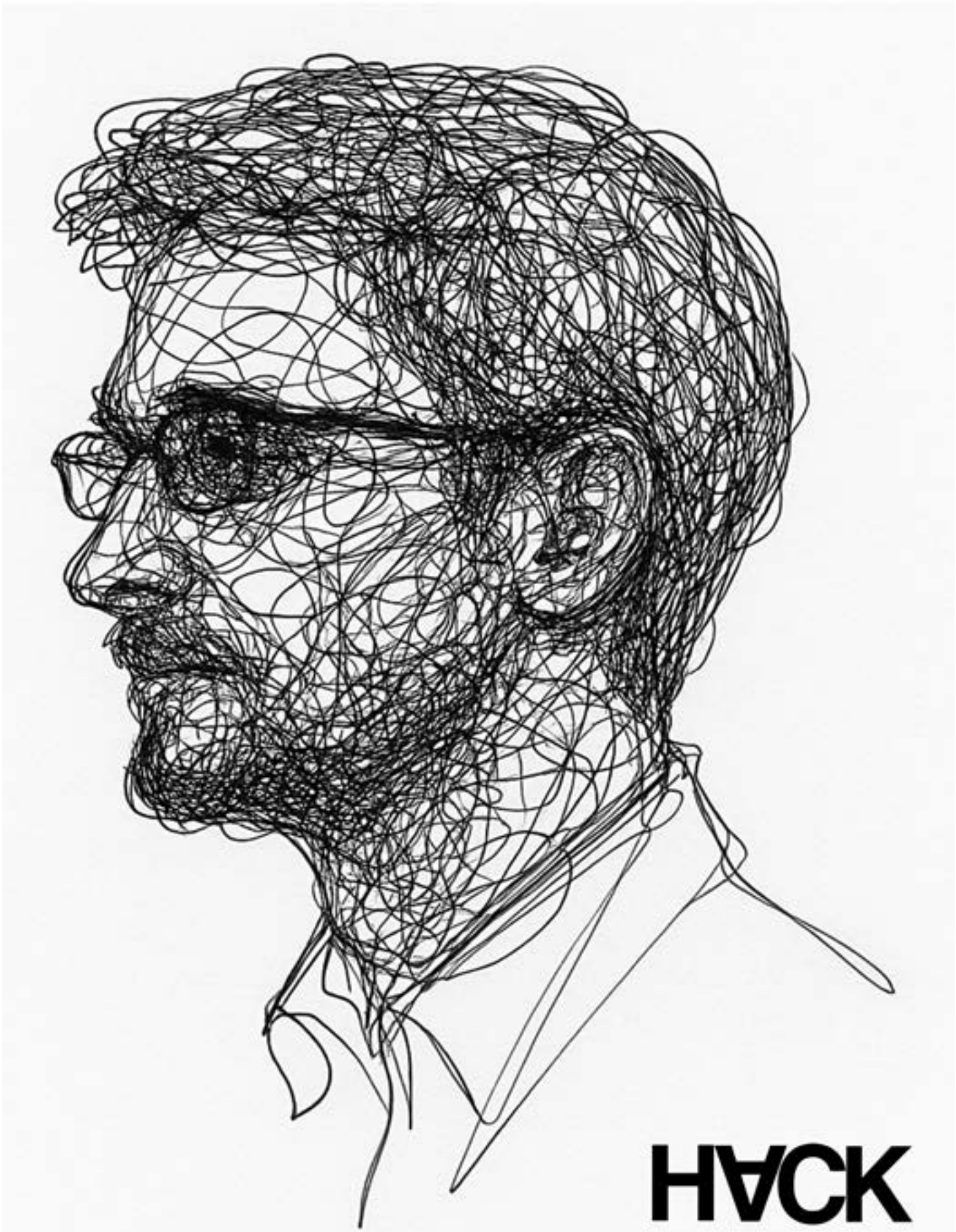


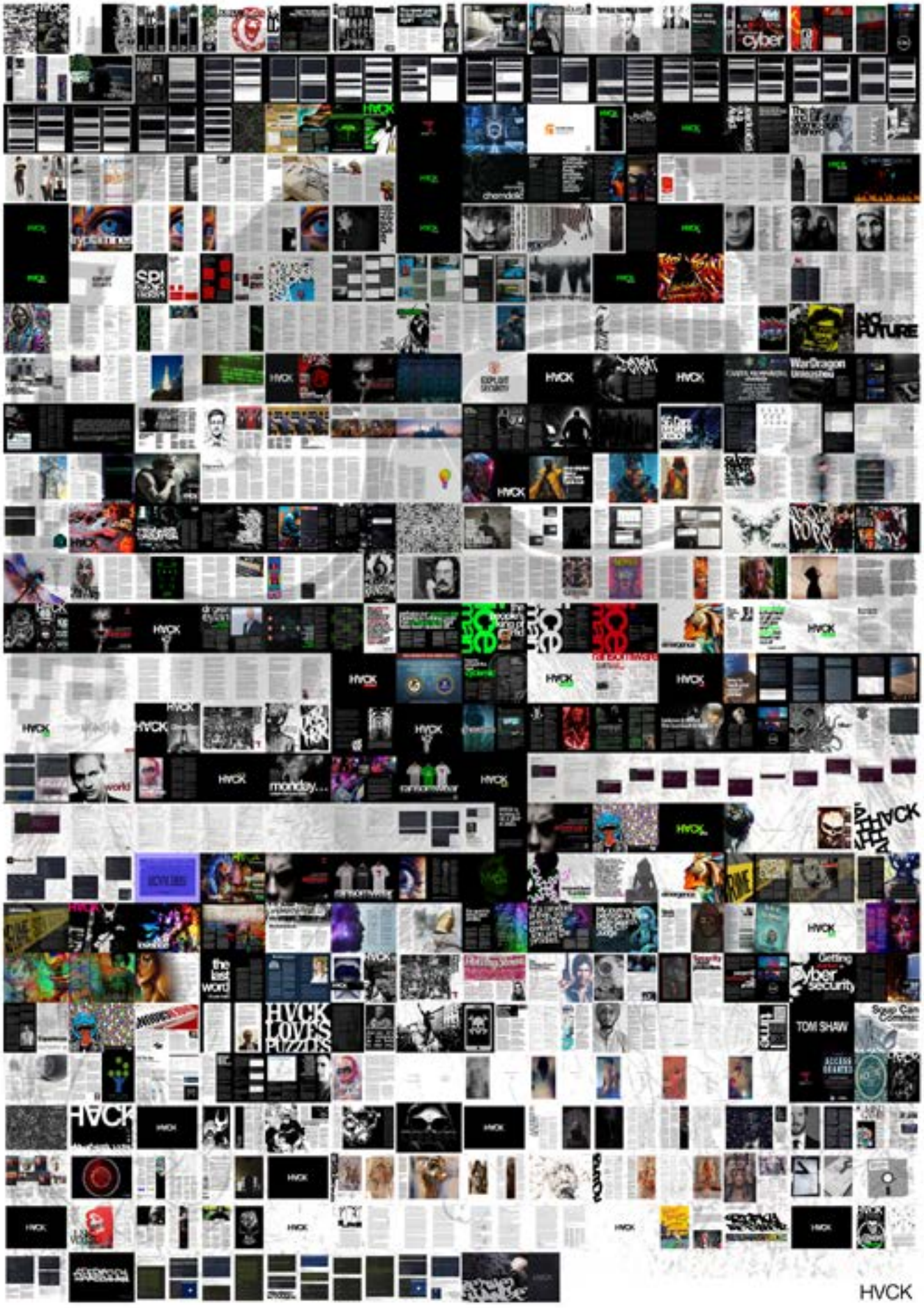
HUMAN HACKED

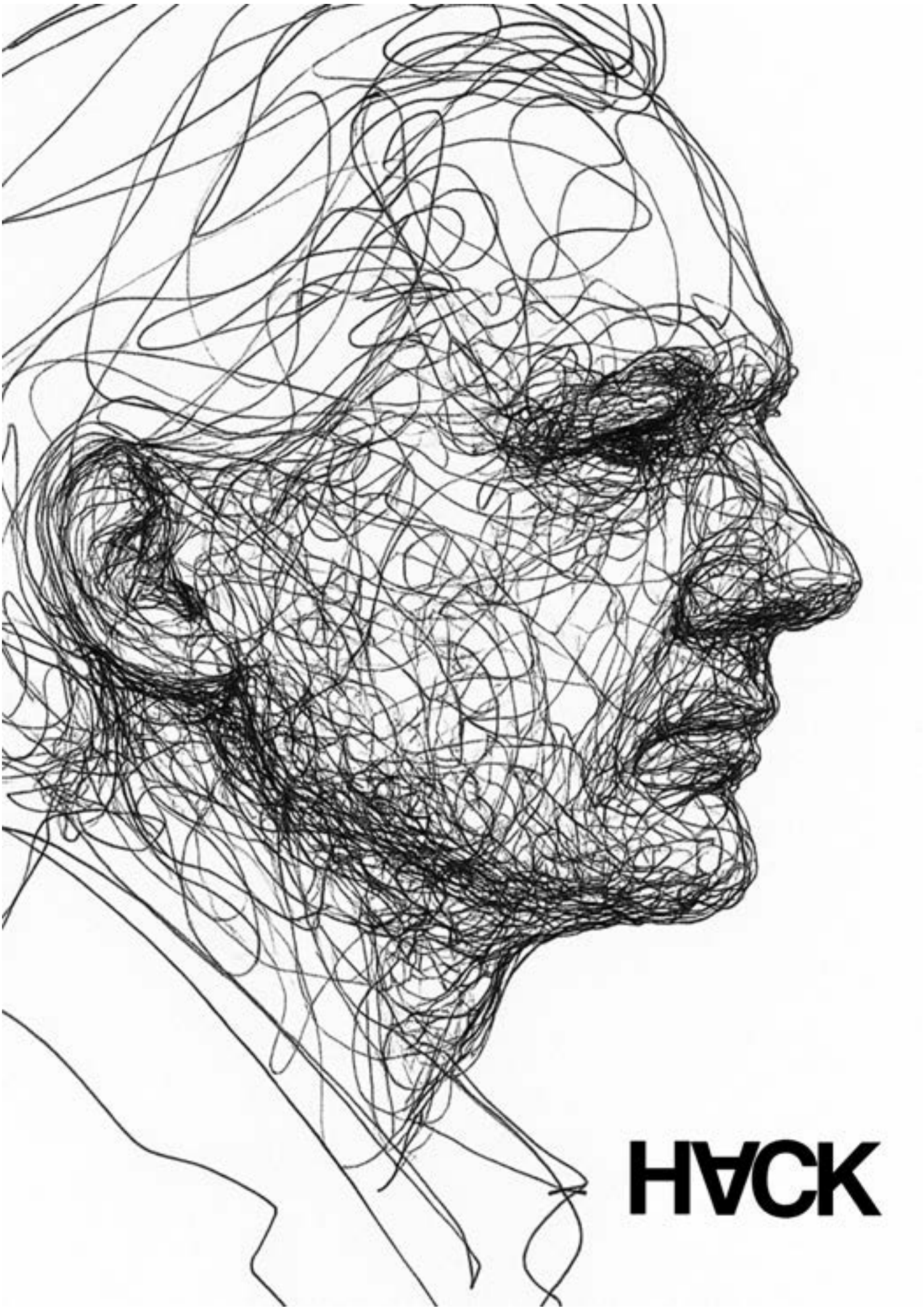
MY LIFE AND LESSONS AS THE WORLD'S FIRST AUGMENTED ETHICAL HACKER



LEN NOE
HaCkEr 213


HACK

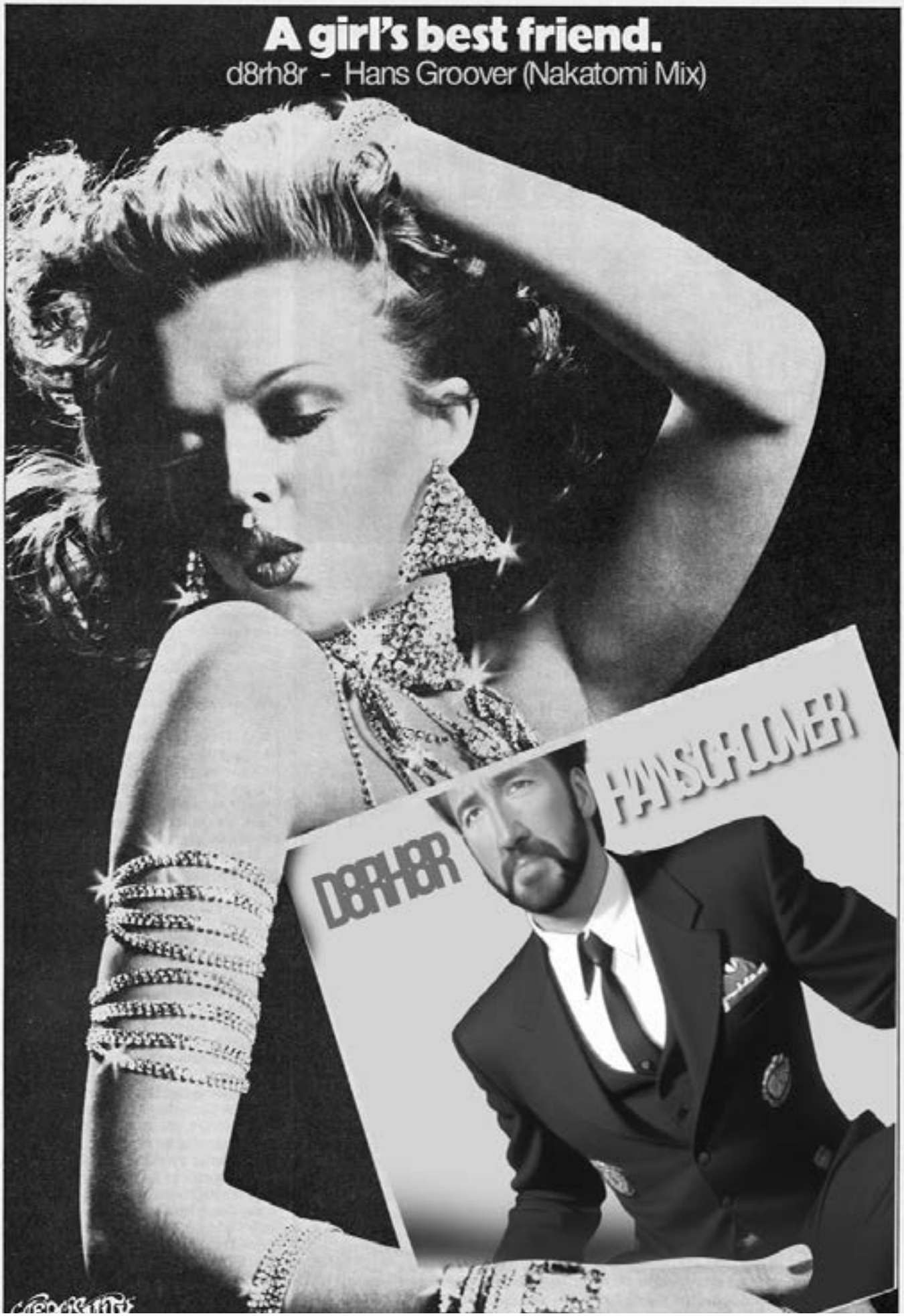

HVCK
HVCK LOVES PUZZLES
TOM SHAW
NO FUTURE
cyber
monday...
the last word

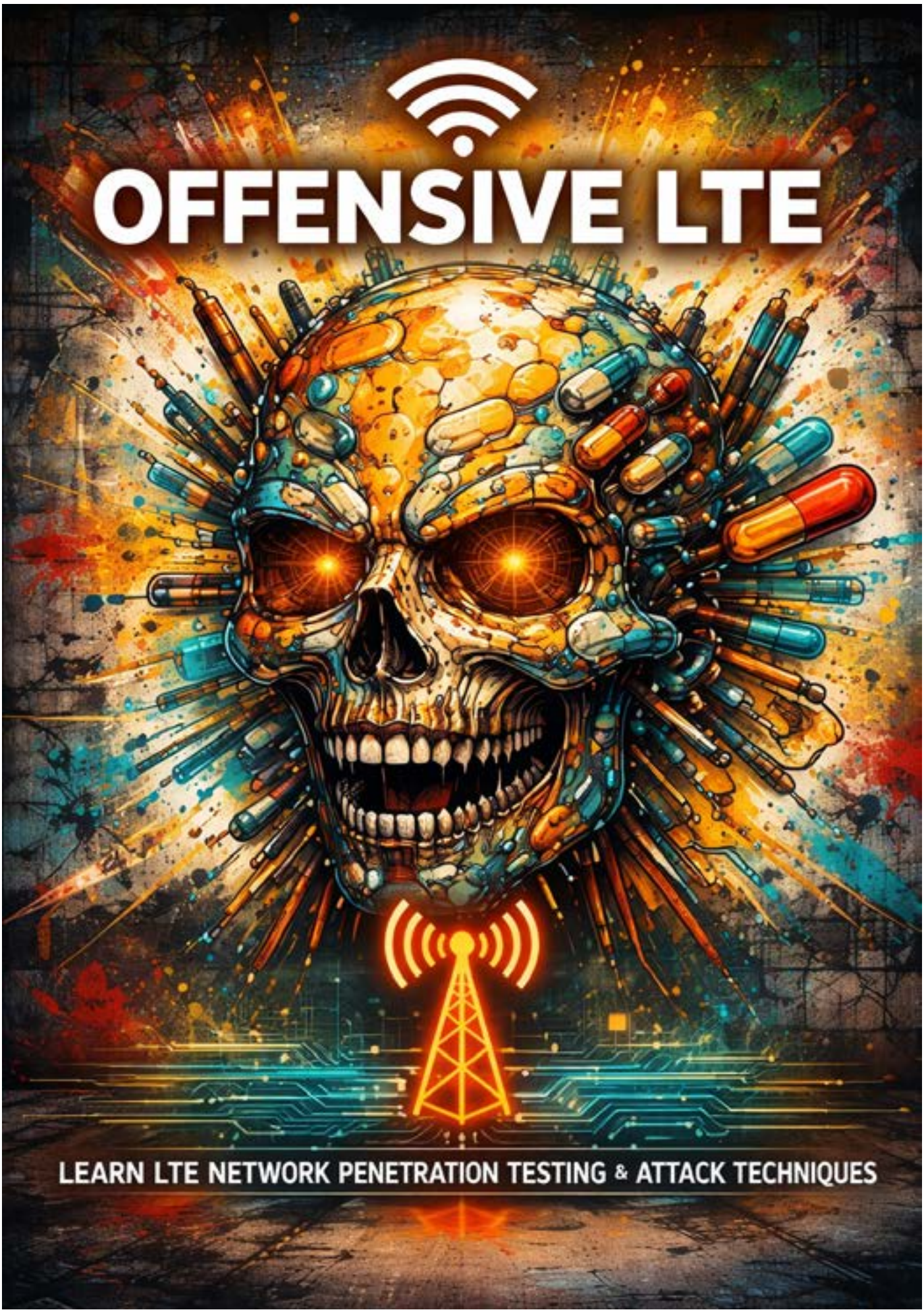

HACK

YES, I AM A CRIMINAL.
MY CRIME IS THAT OF
CURIOSITY. MY CRIME I
S THAT OF JUDGING PEO
PLE BY WHAT THEY SAY
AND THINK, NOT WHAT T
HEY LOOK LIKE. MY CRI
ME IS THAT OF OUTSMAR
TING YOU, SOMETHING T
HAT YOU WILL NEVER FO
RGIVE ME FOR. I AM A
HACKER, AND THIS IS M
Y MANIFESTO. YOU MAY
STOP THIS INDIVIDUAL,
BUT YOU CAN T STOP
US ALL...

HACK


HERO
™


A girl's best friend.
d8rh8r - Hans Groover (Nakatomi Mix)
D8RH8R
HANS GROOVER


OFFENSIVE LTE
LEARN LTE NETWORK PENETRATION TESTING & ATTACK TECHNIQUES

IMPERIUM

C2 PLATFORM

1. d8rh8r - transhuman
2. Len Noe - Human Hacker (book)
3. d8rh8r - Hero (whistleblower)
4. d8rh8r - Hero (whistleblower)
5. d8rh8r - Pages... (every page of HVCK)
6. d8rh8r - Assange
7. d8rh8r - manifesto
8. d8rh8r - Hero (lex Pretti Memorial)
9. d8rh8r - Hans Groover (Nakatomi Mix)
10. Offensive LTE - hvck,academy
11. Imperium - C2 Platform


DAH

ck

freelance

Casual wisdom from the trenches

One of the main questions I get on an almost daily basis is how to get started freelancing in cybersecurity - today, I'm going to give you an insight into the why, who and how of this unique area of the IT industry as a whole, with strategies to get yourself started. Let's get stuck into it!

Why: I want to start by being clear that freelancing isn't for everyone. It takes work, time and dedication to not only doing the job correctly, but actually working towards bringing in clients to do the work on. This is arguably the hardest part of building your own consultancy, which is to build out a list of clients to work for. As to the why? Well, it comes down to personal goals, but for many it's the ability to choose what work they want to do, when and from where. As the world moves back into a "work from the office" or hybrid working environments, choosing the kind of work you want to do in your own career and working towards goals to build out your own consultancy business as a freelancer has seen a lot of traction building where people want to do their own thing. I personally chose to start working towards this lifestyle because I wanted to travel and work towards my own strengths within the IT industry to offer these services that I've been doing for other companies for the last 18+ years of my working career. It felt like a natural step up for me, and it is a dream to be able to achieve what I have so far. This isn't about me though, just more my own personal experiences and how they could help you on your own journey.

Who: So, onto the who. Who is freelancing for? Can anyone start up a freelance consultancy? I'd argue that anyone with the right drive can start a freelancing side hustle, but having the skills to actually get the services done is obviously required. This is why at the Safer Internet Project, we have learning pathways available for members on the main areas of which services can be offered, with regular coaching to make sure you're on track with your goals. A way to get started if you don't have all of the different services you can offer mastered, is to stick with one service you have experience or expertise in - for example, compliance auditing. Compliance requires knowledge of the systems you're auditing against, as well as the framework that the business is working against to gain compliance in, howerver it is in some cases, less technical than say, penetration testing (of various types).

Lastly on the who, is more of a when. When is the right time to start this adventure? I highly recommend doing this alongside (after hours and weekends) your current job. Make sure you are not breaching any work agreements and do not try to take your current employers' clients. This is bad business and morally quite wrong. Focus on areas that your current employer doesn't offer to a market verticle they don't offer services to. Play it safe out there and do things right! The alternative here is to make this your main gig, however having money behind you to keep yourself going is vital, as you'll have expenses before you have profits.

How: Now you have in your mind the services you want to offer to your potential clients and the next step is to get those clients in! As I said at the start, this is often the hardest part. A lot of the people I talk to are highly technical, experienced professionals, but getting those clients in can be hard when first starting out. Just like getting that first job in your career, getting clients can be equally as challenging, and an ongoing challenge that you'll get better at as time goes on.

Joining business networking groups (I like the after-work pub meetups personally) where you get to meet other business owners. Meetup.com and eventbrite are great places to start to find potential clients from. BNI groups are also good, but usually come with a hefty up-front membership fee, but often work on referal based relationships, so in turn, have a higher success rate. Freelancing dashboards like https://humin.co, https://upwork.com and https://freelancer.com are great to try your hand at, however this isn't the type of freelance consulting method I personally prefer, as the jobs are usually once off works to be completed, competing against the whole world, which often returns undercut prices (especially if you're from the US, UK, Australia or anywhere in Europe). This is mainly due to worldwide currencies and what people are willing to offer a service for.

Aside from this, talking with anyone you know who currently has a business or knows people who do have a business is a great first step to get some work through the door. Talking with people is key, and getting to meet as many people as possible who have any IT system that can be audited or reviewed or improved is a potential client for you to build on and offer services to. Get out there and start talking to people!

And that's basically it to get yourself started. If you're interested in 1 on 1 guidance (unlimited one-hour sessions) to keep you on track, become a freelance member of the Safer Internet Project today using the link below and let's get planning, earning and working!

DC CyberSec

DC (David Lee) is a cybersecurity creator, freelancer, and mentor behind The Safer Internet Project — a hands-on training program offering live pentesting, security audits, CTFs, and freelancing guidance. With over 12.5K followers on X (@dccybersec) and a presence across YouTube, TikTok, Instagram, LinkedIn, and Discord, DC is focused on making cybersecurity careers accessible and getting people into real-world engagements from day one.


DAH


CK
ethics


MSBC
CNN
FOX NEWS
FOX NEWS
MBC
CNN
FAKE NEWS
LIES
FEAR
WAR
IES
PSYCHOLOGICAL WARFARE & AI

It is 2024, and it seems like the war with AI & the people never ends. From the back and fourth Instagram arguments to your everyday twitter shit post, AI is the hot dumpster fire in the room. In today's article, I want to talk about two areas that interest me the most - Psychology and how Artificial Intelligence is being used to manipulate human psyche and has without people truly knowing.

Firstly, for those who are new to my articles, hello! My name is Totally_ Not_A_Haxxer, I specialize in reverse engineering, exploit development, and security research. In the past, I have been a contributor to HVCK, providing written contributions geared towards substance abuse, mental health, and the technicalities behind how synthetically made substances like opioids work.

This article bridges those subtopics, primarily with a focus on AI tuned algorithms and how they can be used as a social manipulation tool for the masses. I am sure you have heard this once or twice.

Didn't Know AI Existed Before ChatGPT?

Many people's first real world face first blatant introduction to AI was ChatGPT. That is, for the mass majority of people in the world who are not technically inclined. So if this is yours, then let me introduce you to AI before GPT. AI before GPT was mostly seen being implemented in search algorithms, stronger data searching algorithms meant search engines like Baidu could build their own algorithms (i.e. the LinearDesign algorithm [2010 development started]), and social media applications like Myspace (2003) used for recommending music or media content.

The truth being told, AI algorithms have been a concept alone for decade[s] before ChatGPT did and has been long in the works. Keep in mind, many people often mis-classify AI/ML algorithms, you may have as well, but despite their classification, the matter of the fact is that these algorithms and different models have still been in development for years! While not nowhere near as complex, fast, robust, and flexible as the ones today, the algorithms themselves still did pretty damn well considering their timeline, and may have been just little branches of the ideas executed today.

That being said, now that you are all caught up to speed, we can get into the deets :D

An Intro To Marketing

So for those who do not have a deep marketing background, let me explain how marketing is often done. Looking at it from a "money making" mindset and view point, the whole idea behind a huge marketing strategy is literally to bring in some form of funding. Of course, this is not always the case, but as is for most marketing. These strategies combine multiple forms of skillsets and knowledge bases to form different tactics to target particular audiences. Audiences are everything, marketing strategies describe how you are going to manipulate and hook your audience, and what parameters (parameters being the tools you are using, like SEO tools, maybe specific logical plans and outlines for the way things are being executed, etc.) in your environments you will fine tune in order to obtain a proper hook on your audience. Most importantly, marketing plans often explain what and how the techniques will be employed.

Marketing plans have a huge implication in the world of social media- its how every brand markets. Following that, AI algorithms used in social media, especially in 2024 are quite advanced, and they can pull a lot of information from one single piece of data. Those same algorithms are used by marketers to carry out a business[s] marketing plan digitally. How you ask? Well, if you sit with yourself and think about how much content you see that you find enjoyable on social media, then think about how seriously accurate an algorithm must be about you as an individual, you may be able to see how this becomes just one giant personalized bubble of content. So, this of course, groups you into millions of other users. Put it this way, if there is content you enjoy, then there is certainly more than you looking at that content. Which is where the "group" of "user types" gets created and how other brands can manipulate groups of user types by manipulating content to be tailored towards an algorithms group detection, hard to believe, right? Probably not. Its like every cybersecurity content creator flashing a flipper zero and a lambo, they are certainly not the only one doing it, as there are hundreds if not thousands of the same exact people, they just **feel** different because they may be the only paying attention to their inner circle, but the reason they pull so many views and likes is because they only flash items that the algorithm knows is trending. This dive goes really deep, and this is just a surface level covering of it, so I suggest, if you want to go deep, read into specific algorithms and how they work technically (mathematically if you can).

Now adays, parameters in algorithms and variables in algorithms come from so many sources on social media content- from the contents standard tags and text information to the pixels in the video or image content that make up an object in the background.

As you can imagine, when this transverses into social media consumption, we can combine the use of AI algorithms and concepts building them to wrap around this. So what happens when you combine social media marketing plans and AI algorithms that fine tune content based on the way people execute marketing plans?

The Framework of User Consumption

User consumption has always been a topic of interest for many people. It is how social media works, and is the only way social media can properly work in the way it was designed to work. If you are not consuming content, then nobody is posting content- then the only purpose of the platform is to message people.

So how do we keep users on,

keep them hooked, and keep them engaged? - the question every good marketing plan asks.

The Chinese company behind TikTok, ByteDance, is a perfect example of how one can solve this question. Take a look at Instagram, Facebook, and etc. Regular social media was always scrolling through posts, but the UI (User Interface) feels often “free” moving in a manner where you can slide up and down without getting “locked” into place (you will see what I mean in a minute) and additionally, the content on the posts are usually static images, or can be looked at repeatedly (e.g: videos that replay, Stories, etc.)

However, when TikTok came out, did you notice that Instagram, Facebook, and other various social media platforms instantly took to implementing reels? If you think about it, they seriously are petty, and definitely copy cats. But why did they choose to copy another company? Well, this is because, TikTok created a new framework built off of the existing ones social media provided. This framework of course had very specific rules, such as the max length of videos being 60 seconds, if the user was inactive the app would start to auto-scroll or start slowly moving the ui down mimicking a ‘swipe’ action, promoting more swiping, and other like rules that would ‘lock’ you into the content, so there was no swiping left and right anymore, there was only up and down. Now we have a system that HOOKS users and KEEPS them hooked.

So what does this do? Well, breaking it down, unlike Instagram, TikTok built a framework that included components such as ...

* Shorter Content which results in Shorter attention span for an individual

* UI With Static Ranges which makes content easier to consume

* Limitations on how much a single post contains which makes creators focus on producing a mass quantity

of content fast, but not focus on quality

* Fully personalized content & stronger algorithms dedicated to pulling content only that individual enjoys

A little history for you, the main company behind Douyin (Chinese, Domestic e-commerce platform), ByteDance, who is behind the international version of Douyin (TikTok) has a huge amount of attention for releasing multiple apps that gain quite the amount of popularity. When Douyin gained popularity, the same brand released TikTok, the international version of Douyin, which implemented similar AI algorithms used for the news aggregation platform Toutiao. When you look at the two versions of the application, you notice that the Domestic version of TikTok, Douyin, has algorithms that seem to promote education content or content specifically from verified enterprise accounts, mainly selling products.

Now can you guess where this is going?

* 1) They already have a framework that keeps people addicted, and it works - think, scrolling epidemic
* 2) They have the knowledge and funding towards the application
* 3) They made an initial affect simply by pushing the framework out

All there is now for a country to do at this point, would be let it ride and self execute.

The Exploitation of User Consumption

For the companies behind the social media algorithms, its easier to let the framework run and the manipulation happen under the surface, for individuals, they still need to execute on using this framework to exploit user consumption.

imply, once somebody understands the framework and how it can be used to exploit user consumption (e.g: using emotionally manipulative posts, angering meme’s, or even your basic

AI generated deepfake of your favorite artist), the next step is for a company or individual creator to actually use it to exploit consumption. This will be done by again, posting content that keeps the people engaged, what do you really think will hook people? Maybe they can take a pathos (emotional) route, get people angry and get them to gain more traction, or maybe you can take a political route and start tailoring towards peoples personal politics, something that will seriously get someone worked up, or cooled down and extremely happy.

Pretty much, the end goal of actually exploiting it using the existing framework to create a much more addictive set of social media content. Because TikTok and now other social media platforms alike all have a similar framework, then it becomes even easier to replicate.

I think corporations execute this flawlessly, as they take one universal theme for a project, tailor all their content to work with the themes visual appeals, toss in fancy keywords, and toss millions of dollars at celebs to promote their products. Every major brand in the world does it and its clear when analyzing commercials, think about what Netflix did with the most popular Jake Paul and Mike Tyson fight. However, we round back to our initial conclusion, all that matters is that they can sell, who cares about the quality anyway right?

Of course, actual business experience would tell you that it is way more beneficial for many reasons to not just worry about making profit, and there are things that will make the future much more stronger without just focusing on fast production and money (a problem with a lot of companies) but many just want the money NOW. And many want the product NOW and do not care to read about it before buying it, if this is already a weak link, how easy is it to take advantage of? So it makes sense because it gets the company to their end goal. Shitty, for sure, but that's how many believe companies are better off.

Framework Evolution

Similar to before TikTok was around, these frameworks will continue to be tunned, and their evolution will grow greatly. So what does that mean for the general public? Well, if you check a few reports on the United States social spectrum after TikTok came out, and compare it to the social spectrum in China, you notice a drastic differences between the changes. Of course, do not take my word for it, do the research yourself.

This is a pretty good report that actually points this out - businessofapps.com/data/tik-tok-statistics

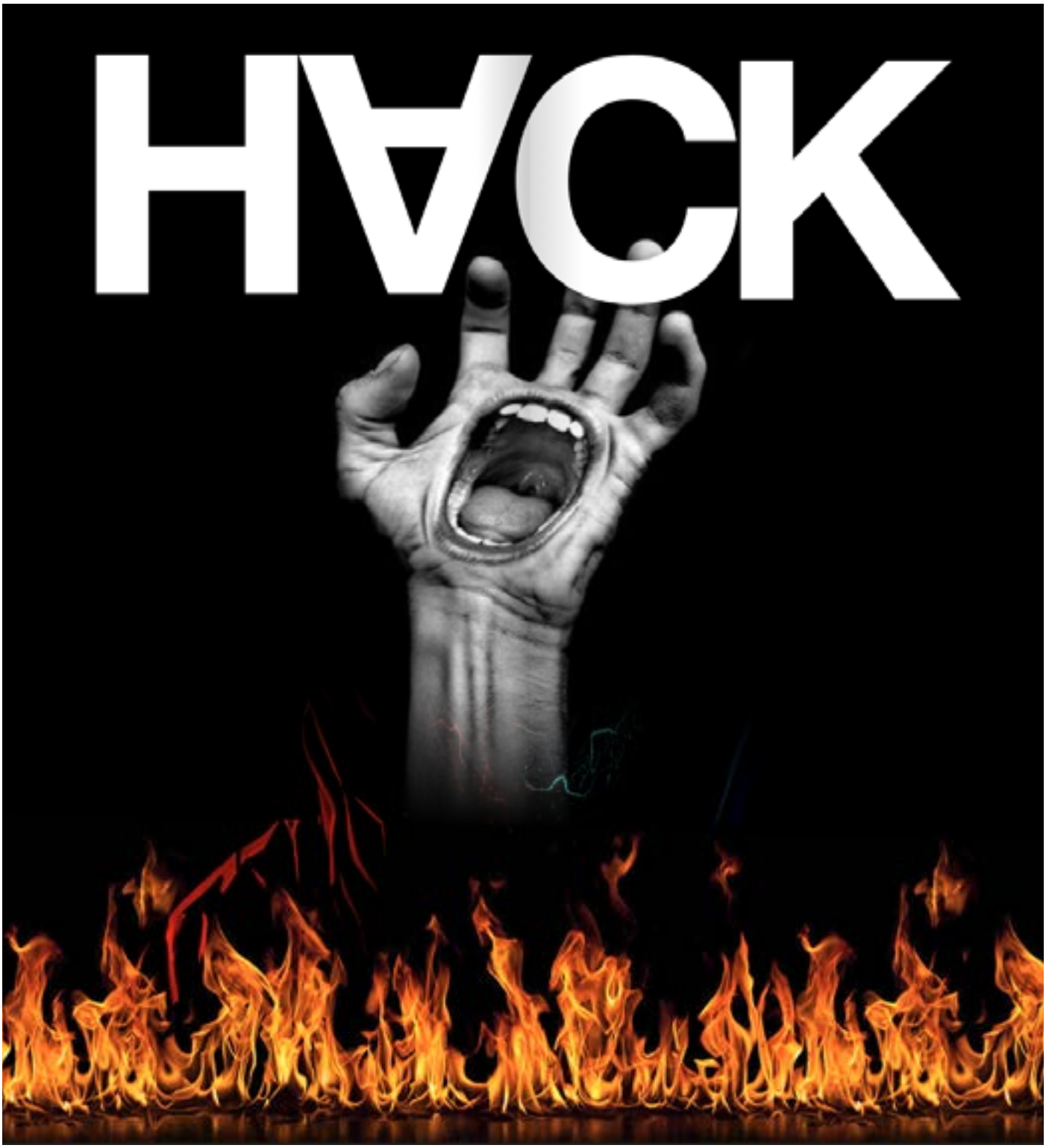
With that, as time goes on, it will become easier and easier for people to be taken advantage of if the individuals do not pull themselves out of that social media hole.

Now What?

All of this being said does not matter unless there is a purpose. While I can rant for days on this type of system, the point in me expressing this is how to both defend yourself from such a system and to take advantage of that same system. To make a proper insert here, when I say “take advantage” I mean to use the system in a way that not only boosts your end results further, but to also draw people into quality content. People are so stuck wondering why they are not getting better or why their company is not moving, but never ask themselves what they can do differently. These types of system[s] can be used for good, and if people used them the right way, they may be better off. But that isn’t the topic.

Similar to security, the point is that the potential for abuse and exploitation of consumption is there, and its actively being used in social media all over the place. Protecting yourself comes personally- “how am I going to prevent myself from doomscrolling?”, “how am I going to better my knowledge of systems?”, and furthermore, keeping yourself up to date with the new tech that comes out instead of looking at the frontend/ design and saying “yes”.


CK



Next issue:

Future Security

STUFF:
HVCKTHEHILLS.COM
HVCK.ACADEMY

CONTACT:
PLACEINVADER@PM.ME