The Dramaturgy of Cyber-Clout: A Sociological and Algorithmic Analysis of Performative Professionalism and Engagement Hacking on LinkedIn

Brendan G. Atamyanov-Craven

12 April 2026

Abstract

The contemporary professional networking ecosystem, epitomized by LinkedIn, functions as an algorithmic panopticon that mandates the continuous performance of professional identity. Within the cybersecurity industry, a discipline fundamentally anchored in the doctrine of zero-trust, rigorous authentication, and extreme skepticism, a profound sociological paradox has emerged. A significant cohort of cybersecurity professionals engages in a highly orchestrated, fundamentally inauthentic clout economy driven by vanity metrics, algorithmic sycophancy, and manufactured narratives. This research paper provides an evidence-based, analytic, cynical investigation into the mechanics of "influence-hacking" on LinkedIn. Through deconstruction of tactical methodologies such as algorithmic engagement pods, the syntactic phenomenon of "broetry," the deployment of weaponized rage-baiting, and the curation of the heroic struggle narrative, this analysis exposes the underlying psychological drivers forcing technical professionals into an unwinnable game of status. Furthermore, this report unpacks the macroeconomic pressures worsening this behaviour, specifically the publicized myth of the cybersecurity skills gap contrasted against the hyper-saturated entry-level market. Through an efficacy audit and content analysis, this article ultimately determines that the hyper-optimization of personal branding generates an insular clout bubble that rarely translates into tangible career advancement.

1 Introduction

In the modern enterprise landscape, participation in digital networking platforms has transitioned from an optional career strategy to a mandatory occupational requirement. LinkedIn operates as the primary nexus for this digital professionalism, commanding the attention of over one billion global users.[1] While the platform purports to facilitate organic networking and meritocratic talent discovery, its underlying architecture is driven by an attention economy that systematically prioritizes viral velocity and continuous user engagement over factual accuracy or technical depth.

Nowhere is the cognitive dissonance of this platform architecture more glaringly apparent than within the cybersecurity sector. The cybersecurity profession is ontologically rooted in paranoia; it relies on frameworks such as zero-trust, which dictate that no entity, internal or external, should be granted access without continuous and controlled

authentication.[13] Security professionals are trained to hunt for anomalies, dismantle phishing lures, identify social engineering vectors, and assume that every piece of digital information is potentially compromised.[13] Yet, when these same professionals log onto LinkedIn, many seamlessly integrate into a high-trust, low-verification theater of performative sycophancy. They participate in an unchecked clout economy where individuals with minimal technical acumen can manufacture massive audiences through the strategic manipulation of the platform's content algorithms.

This performative culture serves as a powerful psychological diagnostic tool, revealing deep-seated insecurities, intense occupational burnout, and structural failures within the industry's talent pipeline.[9] To navigate the algorithm, to achieve visibility, practitioners are strongly incentivized to participate in an ecosystem of influence-hacking. The resulting environment is one of performative professionalism, where the mundane, repetitive realities of IT security are transmuted into epic, digestible sagas of leadership and technological heroism.[9]

This investigation seeks to dissect this phenomenon. By applying established sociological theories of identity management alongside an analysis of LinkedIn's 2025 and 2026 algorithmic updates, this report will decode the methods, motivations, and actual market efficacy of clout-manufacturing in the cybersecurity space. The objective is to demonstrate how a platform designed to connect professionals has instead birthed a sub-economy of digital charlatans and exhausted engineers forced to play a game fundamentally at odds with the core tenets of their profession.

2 Theoretical Framework

To critically analyze the behavioural anomalies exhibited by cybersecurity professionals on LinkedIn, it is necessary to anchor the analysis in established sociological and psychological frameworks. The seemingly irrational pursuit of digital validation can be decoded through the dual lenses of Erving Goffman's dramaturgical theory and Will Storr's evolutionary psychology of status-seeking.

2.1 Erving Goffman's Dramaturgical Theory

The foundational text for understanding performative identity is sociologist Erving Goffman's 1959 work, *The Presentation of Self in Everyday Life*. Goffman posited that all human social interaction is inherently theatrical. Individuals function as actors engaged in "impression management," carefully curating their behaviours, speech, and appearance to project a specific, idealized persona to an audience.[2][11]

Goffman's framework divides human behaviour into two distinct spatial metaphors: the "front stage" and the "back stage." The back stage is the realm of authenticity. It is where the actor can drop the facade, express doubt, rehearse their lines, and perform the messy, invisible labour required to maintain their existence. In the context of cybersecurity, the back stage consists of the highly stressful, repetitive, and deeply unglamorous reality of the job: parsing endless, poorly formatted logs in a Security Operations Center (SOC), arguing with executives over inadequate security budgets, managing chronic alert fatigue, and patching legacy infrastructure that routinely fails.

Conversely, LinkedIn represents the ultimate, hyper-surveilled "front stage." In this socialized digital space, the messy realities of the back stage must be entirely sanitized. The platform demands a cohesive narrative of relentless success, constant "upskilling,"

and visionary thought leadership.[10] Social media platforms function as distributed systems that amplify impression management to an extreme degree, creating an environment that rewards polished artificiality over sincere technical discourse. As ThoughtCo notes, when others are watching, individuals conform to expected norms, whereas backstage they can be their true selves free from such rules.[2]

For the cybersecurity professional, the friction between the back stage and the front stage is particularly violent. The nature of security work is defensive and intrinsically invisible; a highly successful day in cybersecurity is defined entirely by a non-event (a breach did not occur, a server did not crash, data was not exfiltrated). Because invisible preventative labour cannot be easily monetized, quantified, or celebrated on a platform driven by visible achievements and engagement metrics, practitioners are forced to manufacture visible content to signal their competence to the market.[2][11] The transition from the SOC to the LinkedIn feed requires a total translation of technical reality into algorithmic theater.

2.2 Will Storr's Game of Status

While sociology explains *how* professionals perform, evolutionary psychology explains *why* they endure the exhaustion of maintaining this facade. Drawing upon the theoretical frameworks detailed in Will Storr's *The Status Game*, human beings are evolutionarily hardwired to seek and measure status within their chosen tribes. Achieving high status correlates directly with survival, access to resources, and psychological well-being, while the perception of low status triggers profound anxiety. As Storr's analysis puts it, striving for status is "a fundamental rule of human life"; pursuing status improves one's access to food, mates, safety, and other survival-related benefits.[14]

In a traditional, localized tribal structure, status was awarded based on tangible contributions to the community's survival. In the hyper-connected digital economy, the market has democratized and fundamentally altered the status game. LinkedIn gamifies professional status through highly visible, quantifiable metrics: follower counts, post impressions, connection numbers, and badges such as the "Top Voice" designation. Because the actual technical competence of a cybersecurity engineer cannot be easily assessed by a non-technical audience, these vanity metrics become proxy indicators of authority.[14][12] The status game becomes toxic when the pursuit of the metric entirely supersedes the pursuit of actual mastery. Professionals who recognize the hollowness of the game are nonetheless forced to play it, leading to a dissonance as they sacrifice their authentic personal identities to feed the algorithm.

3 The Macroeconomy

The rampant clout-chasing observed on LinkedIn is a direct behavioural response to a specific macroeconomic paradox defining the global cybersecurity industry. This paradox is the juxtaposition of the heavily marketed "skills gap" narrative against the hypercompetitive, impenetrable reality of the entry-level job market.

3.1 The Marketing of the Skills Gap Myth

For the better part of a decade, industry consortiums, educational institutions, cybersecurity vendors, and even government agencies have relentlessly promoted the existence of

a massive, existential skills gap. Data frequently cited from sources such as the Fortinet 2024 and 2025 Cybersecurity Skills Gap Reports, alongside ISC2 workforce studies, indicates a global shortage of nearly 4 to 4.8 million cybersecurity professionals.[7] This narrative asserts that demand vastly outstrips supply, suggesting an industry desperate for any available talent to defend against increasingly sophisticated AI-driven threats and ransomware syndicates.

This narrative is constantly regurgitated across LinkedIn by executives, thought leaders, and software vendors, creating an environment of perceived limitless opportunity. However, an examination of hiring data reveals that this narrative deliberately obscures a grim reality. The alleged talent shortage exists almost exclusively at the senior and specialized engineering levels; roles requiring five to ten years of hands-on experience with complex enterprise network architecture, cloud infrastructure, cryptography, and advanced incident response.

At the entry-level, the market is experiencing severe saturation rather than shortage. A single junior SOC analyst position, or an entry-level Governance, Risk, and Compliance (GRC) role, routinely attracts hundreds or thousands of applicants within hours of being posted.[8] Cybersecurity is fundamentally not an entry-level discipline; it traditionally requires foundational expertise in systems administration, network engineering, or helpdesk support before a practitioner can effectively secure those systems.

To illustrate the stark divide between the manufactured narrative and the actual hiring landscape, the following table details the conflicting pressures driving applicant behaviour:

Industry Dimension	**Marketed Narrative**	**Hiring Reality**
Talent Availability	A catastrophic shortage of 4.8 million workers; companies are desperate for warm bodies to fill seats.[7]	Massive saturation at the entry-level; the shortage only applies to highly experienced senior architects and engineers.[8]
Path to Entry	Bootcamps, job simulations, and simple certifications guarantee a rapid, six-figure career pivot into cybersecurity.	Cybersecurity is a mid-career transition requiring years of prior foundational IT/networking experience.
Value of "Transferable Skills"	Soft skills and unrelated career experience (e.g., retail, sales) easily translate to GRC or security roles.	Employers strictly filter for verifiable technical experience; transferable skills carry zero weight against hands-on IT experience.
Hiring Budgets	Endless capital available to secure digital assets against advanced persistent threats.	37% of teams report budget cuts, 40% experience hiring freezes, and 39% cite lack of budget as the real reason roles remain unfilled.[9]

Table 1: Narrative vs. Reality regarding the Cybersecurity Skills Gap

3.2 The Influencer Sub-Economy and Manufactured Hope

This severe dissonance between the publicized talent shortage and the reality of the entry-level market has birthed a highly lucrative, parasitic sub-economy of LinkedIn influencers. These individuals, often possessing minimal operational security experience, exploit the desperation of career-switchers, students, and recent graduates by peddling false hope masked by performative expertise.

A common manifestation of this grift is the aggressive promotion of GRC roles. Influencers continually frame GRC as an easy, non-technical backdoor into the cybersecurity industry. They leverage engagement hacking to push this narrative to viral status, amassing massive, anxious followings. Once their perceived authority is established via vanity metrics, the monetization phase begins: they sell exorbitant, proprietary online courses, resume-writing masterclasses, and unaccredited job simulation boot camps to their audience.

The profound cynicism of this ecosystem lies in its fundamental deception. As veteran hiring managers routinely point out in anonymous "back stage" forums such as Reddit, these expensive influencer courses hold absolute zero market value.[16] Employers utilizing automated Applicant Tracking Systems (ATS) filter strictly for verifiable IT experience and recognized certifications (such as the CISSP or OSCP). Instead, the influencers manufacturing clout on LinkedIn are actively worsening the crisis by directing vulnerable candidates to invest vital time and capital into performative personal branding rather than foundational knowledge.

4 The Methodology of Influence-Hacking

The pursuit of visibility on LinkedIn is an active, adversarial engagement with a highly sophisticated machine-learning algorithm. Over the past decade, marketers and self-styled influencers have reverse-engineered the platform's distribution mechanics, creating a standardized, highly reproducible playbook for manufacturing virality.[3] Within the cybersecurity sector, these tactics are deployed to quickly establish perceived authority without the prerequisite of actual technical mastery.

4.1 The "Broetry" Epidemic

Perhaps the most pervasive and widely mocked tactical format on LinkedIn is a specific syntactic style colloquially known as "broetry" (a portmanteau of "bro" and "poetry").[3] Pioneered by growth marketers around 2017, the format was engineered specifically to exploit a core engagement metric in LinkedIn's ranking algorithm: "dwell time." Dwell time measures the precise duration, down to the millisecond, that a user spends lingering on a specific post in their feed. To artificially maximize this metric, broetry completely abandons traditional dense paragraph structures in favor of fragmented single-sentence lines separated by aggressive vertical whitespace.[3] Because LinkedIn's mobile and desktop user interfaces truncate long posts after the first few lines, this extreme vertical spacing forces the reader to stop scrolling and physically click the "See more..." button to expand the text. Historically, the algorithm interpreted this physical click, combined with the extended time required to scroll through the whitespace, as an exceptionally high-value signal of content quality,[3] rewarding it with exponential distribution.

A structural analysis of a typical cybersecurity "broem" reveals a highly predictable formula:

1. A contrarian, dramatic, or emotionally charged opening statement designed to arrest the scrolling thumb and provoke immediate curiosity (e.g. "I just threw a resume with five GIAC certifications in the trash").

2. A series of fragmented, pseudo-profound platitudes that artificially extend the physical length of the post. This delays the narrative payoff, forcing the user to commit time to the text.

3. A concluding, unassailable cliché regarding leadership, resilience, empathy, hiring practices, or some otherwise related (usually desirable) trait or topic. It usually ends with an interrogative prompt designed to farm comment engagements (e.g. "Hire for grit, not for paper. Do you agree?").

The sociological impact of broetry is the flattening of complex, nuanced technical discourse into homogenized, motivational slop.[3] In an industry dealing with intricate zero-day vulnerabilities, cryptographic standards, and advanced persistent threats (APTs), the dominance of broetry demonstrates that algorithmic compliance absolutely supersedes technical communication. The format thrives because it treats the reader as an algorithmic node to be harvested rather than an intellectual peer.

It is critical to note that LinkedIn's algorithm has evolved. By 2025 and early 2026, data analyses indicated that the algorithm shifted its treatment of dwell time from an exponential reward to a linear one, introducing the ">15 Seconds Rule." Posts that fail to retain users for more than 15 seconds are now actively de-ranked. Consequently, creators have adapted by utilizing multi-slide document carousels or writing 1,200+ character narratives, yet the underlying psychological manipulation (prioritizing retention over substance) remains identical.

4.2 Engagement Pods

To overcome the initial hurdle of algorithmic distribution, particularly given the platform's shift toward penalizing generic content, professionals frequently organize into "engagement pods." These pods act as digital cartels: private, highly coordinated groups of users who explicitly agree to systematically like, comment on, and share each other's content immediately after publication.

The primary objective of an engagement pod is to manufacture the illusion of intense, organic virality during the critical golden hour (now functionally expanded to a 90-minute window) following a post's release.[3][17] This triggers a cascading distribution effect, pushing the content out to second- and third-degree networks, effectively hijacking the feeds of thousands of unrelated users.

Engagement pods manifest in two primary architectural forms, varying by technical sophistication:

Pod Architecture	Mechanism of Action	Detection Risk by Algorithm	Sociological Impact
Manual Pods	Organized via external communication channels (Slack, Discord, Telegram, WhatsApp). Members manually drop links to their recent posts and rely on a reciprocal honor system to engage.	Moderate. Algorithms detect unusual velocity, but human-typed comments can sometimes bypass basic NLP filters if members write thoughtful replies.	Creates insular, echo-chamber communities. Fosters a transactional view of professional relationships based entirely on reciprocity rather than genuine respect.
Automated Pods	Facilitated by third-party browser extensions and software-as-a-service platforms (e.g., Lempod, Podawaa, Hyperclapper). Users grant the software access to their LinkedIn tokens.	Extreme. LinkedIn's 2025/2026 updates actively target automated scripts. API scraping and repetitive, AI-generated comments trigger immediate shadowbans or account suspension.[15]	Represents the ultimate commodification of digital identity. Users completely outsource their professional voice to an autonomous script simply to farm vanity metrics.

Table 2: Comparison of Engagement Pod Architectures

Despite their immense historical popularity, the efficacy of pods has increasingly become a critical vulnerability. LinkedIn's aggressive 2025 and 2026 algorithmic updates (internally referenced by growth analysts as the "360Brew" adjustments) were specifically engineered to detect, penalize, and eradicate artificial engagement.[15][17] The updated algorithm no longer simply counts the volume of comments, but also utilizes advanced NLP to analyze comment length, semantic variety, reply depth, and the historical relationship proximity of the interacting accounts.

Furthermore, LinkedIn executives, including VP of Product Management Gyanda Sachdeva, have explicitly stated their intent to restrict accounts relying on automated third-party commenting scripts, actively removing detected automated comments from the default "Most Relevant" feed views.[15] Consequently, while pods provide an initial, addictive injection of vanity metrics, they routinely result in severe algorithmic penalties, effectively shadowbanning the practitioner and rendering their content completely invisible to their actual target audience. The pursuit of artificial clout via this method leads directly to digital exile.

4.3 Rage-Baiting and Weaponized Incompetence

When engagement pods fail, trigger shadowbans, or simply require too much coordination, cybersecurity influencers frequently pivot to a more insidious, highly effective tactic: "rage-baiting." Rage-baiting involves the deliberate, strategic dissemination of highly polarizing, fundamentally flawed, or aggressively contrarian technical opinions for the sole purpose of provoking an immediate, emotional, corrective response from the audience.[4]

The cybersecurity community is heavily populated by engineers, threat analysts, and system architects whose core professional identities are intrinsically tied to precision, factual accuracy, and rigorous logic. As a demographic they exhibit an exceptionally high psychological susceptibility to the correction impulse; the overwhelming, almost involuntary urge to publicly correct demonstrably false or dangerous technical statements.[4] Influencers weaponize this psychological trait to farm engagement at massive scale.[4]

A prominent, anonymized example analyzed within the industry involved a Chief Information Security Officer (CISO) who published a post declaring that "Encryption is overrated".[5] The author argued that outside of defending against nation-state adversaries, encryption serves no real risk-reduction purpose, claiming that theft of physical media or packet capture across the internet is "not a concern." From a technical standpoint the post was absurd, demonstrating a shocking ignorance of basic threat modeling, man-in-the-middle attacks, and data privacy fundamentals. Yet the post generated massive algorithmic traction. Hundreds of highly qualified security professionals flooded the comments to angrily refute the premise and openly debate the CISO's competence to hold their title.[5]

To the human eye, the comment section was a unanimous, devastating condemnation of the author's professional credibility. To the LinkedIn algorithm however, sentiment is entirely irrelevant. The algorithm cannot distinguish between a chorus of unified praise and a digital mob of furious detractors; it merely registers exceptional conversational depth and massive dwell time.[4] Consequently, the algorithm rewarded the author with exponential reach, elevating their profile visibility across the entire platform. In the clout economy, being loudly, confidently, and publicly wrong is a highly viable growth strategy, proving that the platform structurally incentivizes toxic provocation over genuine education.[5]

4.4 The Heroic Struggle Narrative

While rage-baiting and broetry exploit the algorithm, the narrative of the heroic struggle exploits the deep psychological trauma inherent in the cybersecurity profession. The industry is characterized by chronic understaffing, relentless alert fatigue, constant adversarial hostility, and a high-stakes operational environment where a single configuration error can result in catastrophic corporate bankruptcy or national security breaches.[9] Empirical studies indicate that 67% of cybersecurity professionals report significant negative impacts on their personal lives due to job stress, 95% of CISOs feel chronically overworked, and the average tenure in analyst roles rarely exceeds three years.[9]

However, the unwritten rules of the LinkedIn "front stage" dictate that professionals cannot express profound exhaustion, fear, or despair authentically without violating the norms of corporate positivity. Therefore, professionals sublimate their trauma into the narrative of the heroic struggle. Routine, grueling professional survival is recast in grandiose, mythological terms. Overcoming a massive budget deficit to manually patch a crumbling legacy server is written as a David vs. Goliath battle against apathy rather

than the blatant failure of corporate resource allocation it truly is. Surviving a brutal, caffeine-fueled 72-hour incident response shift during a holiday weekend is framed as a Spartan-esque defense of the digital realm.

The heroic struggle narrative serves a vital dual psychological purpose. First, it sanitizes and justifies burnout, translating the symptoms of chronic stress and institutional abuse into a highly marketable indicator of "grit," "passion," and "resilience." Second, it dramatically elevates the status of the poster by associating their mundane, often depressing corporate labour with archetypal heroism. The practitioner is no longer merely an exhausted, underpaid employee staring at SIEM logs; they have transformed into a digital warrior holding a trench line against chaos, fighting a noble war that the uninitiated masses cannot comprehend. While psychologically comforting to the individual, this narrative is deeply cynical as it normalizes pathological overwork and shields corporate leadership from accountability regarding under-resourced security teams.

5 Evidence & Examples

To effectively illustrate the stark contrast between clout-manufacturing and genuine technical discourse, it is necessary to conduct a comparative content analysis. The following anonymized examples typify the dichotomy between the algorithmically optimized performative post and the genuinely educational technical post within the cybersecurity domain.

Example A: A Typical "Broem"

Format: High vertical spacing, single-sentence paragraphs, emotional hook.
Content:
"I threw a resume in the trash today.
It belonged to a candidate with a Master's in Cybersecurity.
He had his CISSP. He had his OSCP.
But during the interview, he couldn't answer a simple question:
'Tell me about a time you failed.'
He said he never fails. He only learns.
I stopped the interview right there.
In cyber, if you aren't failing, you aren't fighting the real adversaries.
I hired the kid with no degree who built a home lab out of broken Raspberry Pis.
He knew how to fail. He had grit.
Certifications fade. Character scales.
Do you agree?"

Analysis: This post represents the apex of performative influence-hacking. It leverages a highly controversial debate (certification vs. experience) to guarantee engagement. It utilizes the broetry format to maximize dwell time.[3] Crucially, it positions the author as a maverick, visionary gatekeeper of talent, elevating their status while providing zero actionable technical insight. This post will easily generate thousands of generic, automated comments from engagement pods ("Great insight!", "Totally agree!").

Example B: A Technical Teardown

Format: Dense paragraphs, technical jargon, external links to GitHub or documentation.
Content:
"Recent analysis of the CVE-2026-XXXX vulnerability in [Vendor Name] edge routers reveals a critical bypass in the SAML SSO configuration when combined with specific IPsec tunnels. While the vendor patch was released Tuesday, applying it without updating the underlying threat feed in the local-in policy leaves the public-facing interface exposed to credential stuffing attacks. We deployed a temporary mitigation script (link to GitHub repo below) that restricts WAN access and enforces strict trusted host protocols prior to patching. Note: Ensure your MFA implementation is fully decoupled from the vulnerable directory service before deploying, or you will lock out your own admin subnet."

Analysis: This post exemplifies authentic, back-stage technical reality. It provides immediate, critical, and highly actionable intelligence for practitioners actively defending networks.[12] However, algorithmically, this post is destined to fail. The dense formatting reduces the likelihood of "See more..." clicks. The highly specific technical jargon alienates the broader, non-technical audience. Furthermore, the inclusion of an external link (to GitHub) actively triggers a penalty from the LinkedIn algorithm, which aggressively suppresses content that directs users away from the platform. It will likely receive minimal likes, no engagement from automated pods, and zero viral traction, despite being infinitely more valuable to the industry than Example A.

6 Efficacy Audit

The central question regarding this exhaustive performance of professional identity is one of ultimate efficacy: does high engagement on algorithmically optimized fluff posts translate to actual career advancement?

The empirical evidence suggests there is a profound disconnect between the vanity metrics generated on the platform and the rigorous criteria utilized by actual technical hiring managers. Sociological and organizational studies confirm that authentic digital networking, when stripped of algorithmic manipulation, does yield measurable professional dividends. Research conducted at Harvard Business School, analyzing the LinkedIn connections of millions of employees across thousands of public companies, found a direct correlation between an organization's network centrality and its capacity for high-value innovation.[10]

Employees who build genuine, reciprocal relationships (sharing verifiable technical insights, engaging in deep peer-to-peer problem-solving, and maintaining authentic "weak ties" across industry sectors) enjoy significantly higher access to informational benefits. Users of professional networking sites like LinkedIn report higher informational benefits, including timely access to relevant resources and career opportunities.[10] This genuine engagement leads to unadvertised career opportunities and direct, high-quality recruiter outreach, bypassing the saturated ATS queues.

6.1 The Illusion of the Clout Bubble

However, the metrics generated by engagement pods, broetry, and rage-baiting do not correlate with these positive outcomes. High impression counts and vanity metrics create

an illusion of authority that rarely survives the intense scrutiny of a technical hiring process.

The efficacy of performative tactics is heavily undermined by several critical factors:

1. **Skepticism:** Technical hiring managers, Lead Architects, and senior CISOs are highly attuned to "puffing": the gross exaggeration of technical competencies through slick personal branding. In cybersecurity, hiring an individual based on their ability to write motivational poetry rather than their ability to analyze packet captures represents a severe, unacceptable operational risk. Consequently, hiring managers frequently view hyper-active influencer profiles as massive red flags, indicating a narcissist with misplaced priorities and a fundamental lack of hands-on engineering focus.

2. **Devaluation:** LinkedIn's attempts to formally gamify authority through digital badges have actively eroded trust in the platform. The "Community Top Voice" badge, for instance, was initially intended to highlight genuine subject matter experts. However, because the badge was awarded automatically based on engagement, it was immediately co-opted by clout-chasers relying on Generative AI tools to spam generic, hallucinated answers. LinkedIn ultimately had to kill the feature after it became a universally recognized marker of "AI-generated nonsense" rather than a signal of genuine human expertise.

3. **Isolation:** Algorithmic engagement hacking primarily results in severe network insularity. If a user relies on an automated pod to boost their content, the algorithm learns to display their content almost exclusively to that pod and similar clout-chasers. The content generates thousands of likes but never breaches the algorithmic perimeter to reach the screens of actual decision-makers who hold the capital to offer employment.

To clearly delineate the divide between effective digital presence and performative clout-chasing, the following comparative matrix synthesizes the varying impacts of LinkedIn behaviours on technical recruitment:

Behavioural Tactic	**Algorithmic Impact (Visibility)**	**Perception by Technical Hiring Managers**	**Actual Career ROI (Efficacy)**
"Broetry"	High. Maximizes dwell time; triggers mandatory "See more..." clicks.[3]	Low to Negative. Universally viewed as fluff, distracting from technical merit, and indicative of clout chasing.	Negligible for engineering roles. Highly effective *only* if the user is selling B2B marketing or career coaching services.
Engagement Pods	Initially High, but heavily penalized by 2025/2026 algorithm updates (360Brew) leading to immediate shadowbans.[15]	Severely Negative. Easily spotted due to generic comment quality; signals artificiality, desperation, and professional deception.	Zero. Creates a closed loop of fake engagement among peers that rarely reaches actual hiring authorities.
Rage-Baiting	Exceptionally High. Triggers massive comment velocity via the community correction impulse.[4]	Catastrophic. Permanent damage to professional reputation. The user is viewed as an operational liability or technically incompetent.	Negative. Frequently results in silent blacklisting by serious engineering teams who view the individual as a high-risk hire.
Community Badges	Moderate platform promotion.	Skeptical to Negative. Widely recognized in the industry as a byproduct of AI-generated spam and automated collabourative article farming.	Low. Devalued to the point of irrelevance; actively deprecated by LinkedIn.
In-Depth Technical Posts	Low to Moderate. Technical jargon and external links (e.g., GitHub) actively suppress algorithmic reach.	Exceptionally High. Acts as a verifiable public portfolio of competence, critical thinking, and genuine domain passion.	High. Facilitates direct peer respect and allows candidates to bypass traditional ATS filters entirely.

Table 3: Impact Matrix of Differing Behavioural Tactics on LinkedIn

7 Conclusion

The intersection of the global cybersecurity industry and the LinkedIn platform provides a profound, deeply cynical sociological case study in the corruption of professional identity by algorithmic incentives. Erving Goffman's mid-century concept of the "front stage" has been digitized, quantified, and monetized to such an extreme degree that the performance of professionalism has largely decoupled from the actual, material practice of the profession.[2] Cybersecurity is, by its very definition, an industry characterized by invisible, highly stressful, and aggressively technical labour.[9] Yet the relentless demands of the LinkedIn algorithm compel practitioners to abandon technical rigour in favour of emotional manipulation and narrative dramatization. Through the cynical deployment of broetry formatting, the cartelization of likes via engagement pods, and the weaponization of incompetence through rage-baiting, users actively hack the platform's dwell time and conversation metrics to manufacture a hollow façade of digital authority. This performative behaviour is fueled by deep psychological vulnerabilities: the innate human, evolutionary desire to win the "Status Game" in a field where real-world victories are highly classified, and the desperate need to reframe chronic occupational burnout into a highly marketable, mythological heroic struggle.

Simultaneously, the macroeconomic myth of a universal skills gap provides incredibly fertile ground for predatory influencers and clout-chasers. By leveraging these algorithmic hacks, they project false authority to thousands of anxious entry-level candidates, selling them the dangerous illusion of an easy career pivot while entirely obscuring the realities of technical hiring.[7]

Ultimately, the efficacy audit of this entire digital ecosystem reveals that while artificial engagement successfully generates a self-sustaining bubble of clout, it holds absolutely no currency among technical hiring managers, lead architects, and security executives who control legitimate career advancement. In a digital environment increasingly flooded with AI-generated slop, performative vulnerability, and coordinated sycophancy, true authority is ironically signaled by the quiet, un-optimized, and rigorous demonstration of genuine technical competence. The ultimate conclusion of the cybersecurity clout economy is that in their desperate, exhaustive attempts to hack the algorithm and project immense professional value, these performative professionals have meticulously engineered their own irrelevance.

Bibliography

1. Sprout Social: *30 LinkedIn Statistics that Marketers Must Know in 2026.* (2026). `https://sproutsocial.com/insights/linkedin-statistics/`.

2. ThoughtCo: Cole, N. L. (2025). *Goffman's Front-Stage and Back-Stage behaviour.* `https://www.thoughtco.com/goffmans-front-stage-and-back-stage-behaviour-4087971`.

3. Tom Ling: *TXSL #3: "Cool LinkedIn post, bro": why broetry sucks.* (2026). Medium. `https://medium.com/@txsling/txsl-3-cool-linkedin-post-bro-why-broetry-sucks-d548ac945aa1`.

4. Cybernews: Cook, J. (2026). *Meta and TikTok Knowingly Turned Ragebait into Revenue, Whistleblowers Claim.* `https://cybernews.com/tech/meta-tiktok-r`

agebait-revenue-whistleblowers/.

5. Reddit: Anonymous. (2026). *CISO Describes Encryption as 'Overrated' on LinkedIn.* (r/cybersecurity thread). https://www.reddit.com/r/cybersecurity/comments/130mevy/ciso_describes_encryption_as_overrated_on_linkedin/.

6. Terranova Security: *9 Examples of Social Engineering Attacks.* (2026). https://www.terranovasecurity.com/blog/examples-of-social-engineering-attacks.

7. Fortinet (press release): *2025 Cybersecurity Skills Gap Report.* (2025). https://www.fortinet.com/content/dam/fortinet/assets/reports/2025-cybersecurity-skills-gap-report.pdf.

8. J. Bird: "4.8 Million Cybersecurity Jobs Are Open. Here's Why You Still Can't Get Hired.". (2026). Medium. https://medium.com/@jbird24/4-8-million-cybersecurity-jobs-are-open-heres-why-you-still-can-t-get-hired-bd1fbce493be.

9. Interface: Cullen, A. (2024). *Building a Strong Cyber Team shouldn't Solely Rest on the CISO's Shoulders.* https://interface.media/blog/2024/12/30/building-a-strong-cyber-team-shouldnt-solely-rest-on-the-cisos-shoulders/.

10. Stanford HBS Working Knowledge: Baker Library. (2020). *The Network Effect: Why Companies Should Care About Employees' LinkedIn Connections.* https://www.library.hbs.edu/working-knowledge/the-network-effect-why-companies-should-care-about-employees-linkedin-connections.

11. Journal of Organizational Communication: Paliszkiewicz, J. & Wozniak, G. (2020). *Impression management in social media: the example of LinkedIn.* https://ijoc.org/index.php/ijoc/article/view/22850.

12. Journal of Communication: Ryan, J. (2025). *The Relationship Between Networking, LinkedIn Use, and Retrieving Informational Benefits.* https://pmc.ncbi.nlm.nih.gov/articles/PMC6444899/.

13. NIST Special Publication 800-207: Rose, S. et al. (2020). *Zero Trust Architecture.* https://csrc.nist.gov/publications/detail/sp/800-207/final.

14. EconTalk (2021). *The Status Game (with Will Storr).* https://www.econtalk.org/the-status-game-with-will-storr/.

15. Social Media Today (2026). *LinkedIn Outlines Measures To Combat Engagement Pods.* https://www.socialmediatoday.com/news/linkedin-outlines-more-measures-to-combat-engagement-pods/812290/.

16. Reddit (2026). *Why LinkedIn is sh*tty these days? (r/Entrepreneur thread).* https://www.reddit.com/r/Entrepreneur/comments/1g3b2mk/why_linkedin_is_shtty_these_days/.

17. Todorović, Ivana (2025). *LinkedIn 360Brew: What Actually Changed (And What It Means for You).* AuthoredUp. https://authoredup.com/blog/linkedin-360brew.