STRATEGIC BLOWBACK: THE WAR ON TERROR’S ROLE IN GRIEVANCE POLITICS

A RISKSCOPE BRIEFING PAPER

Riskscope
Veritas Primo et principaliter

RISKSCOPE INTELLIGENCE

DISCLAIMER:
This report is intended for informational purposes only and reflects the independent analysis of Riskscope Intelligence. All views expressed are those of the authors and do not represent the positions of any affiliated institutions or clients. Unauthorized distribution is prohibited.

Riskscope

Executive summary

The legacy of the global war on terror (GWOT) extends beyond public distrust regarding US foreign policy – it has laid the foundations for the ideological framework which now sustains 'grievance'-based politics across the West. Initially framed as a fight against radicalism abroad, the same tools, language, and moral framing were turned inward, leading to the rise of the Grievance Industrial Complex (GIC). From mass surveillance and counterextremism laws to the weaponization of "oppression" narratives, the legacy of 9/11 now informs cultural, educational, and media institutions across the U.S. and U.K.

OUTLOOK

- Expect Middle East escalations to revive grievance-based domestic activism.
- Narrative control mechanisms originally built for counterterrorism will increasingly be used to suppress dissent and manipulate democratic discourse.

The Moral and Strategic Foundations of the GWOT

The September 11th attacks did more than legitimize Western neoconservative foreign policy – it set in motion a new ideological paradigm rooted in moral dualism. The response to the September 11th attacks from western governments was framed not as strategic containment but as a civilisational crusade: a binary struggle between good and evil. This moral absolutism enabled sweeping public compliance with war, surveillance, and narrative control and, as a result, the Global War on Terror (GWOT) became less about counterterrorism and more about how power can be moralised. This then evolved into an established political vocabulary: security, extremism and radicalisation, which were malleable, adapted, and redirected — eventually internalised within domestic contexts. On the surface, the Global War on Terror was a foreign policy doctrine, but deeper examination suggests that it was totalising narrative architecture.

The Infrastructure It Created

The global war on terror did more than enable neoconservative foreign policy abroad – it constructed an institutional architecture for perpetual control. The Patriot Act, expanded state surveillance and black-site detention systems laid the foundations for state apparatus capable of monitoring not just action, but thought. As years went by this shift became internalised. Tools originally designed to identify external terrorist threats have been subtly retooled to monitor domestic ideology, dissent and digital sentiment. Intelligence frameworks like "pre-crime profiling" and behavioural risk indicators normalized the surveillance of belief systems where agencies began tracking citizens considered ideological threats rather than operational threats. As this infrastructure evolved it enabled a seamless alignment between government, media and academia under the rhetoric of counter-extremism. This convergence established the early blueprint of the Grievance Industrial Complex: a system in which political narratives, security prerogatives, and institutional compliance fused into a self-justifying mechanism of social control.

How That Ideology Turned Inward

The long term ramifications of the Global War on Terror (GWOT) were not just geopolitical but also cultural. Foreign adversaries such as Al Qaeda, the Taliban and ISIS became less visible and politically relevant, with attention shifting inward towards narratives which emphasize injustice, trauma and grievance. Terms such as “radicalisation” and “prevention” were redirected away from externalised threats and instead applied to citizens whose views diverged from mainstream liberal orthodoxy. In this context the state found a new mission objective: managing and manipulating identity, perception, and emotional volatility which resulted in institutions rewarding victimhood as a currency, redefining legitimacy not by logic, but by the intensity of perceived ‘oppression.’ Surveillance programs, university frameworks, and corporate compliance systems were recalibrated to flag “harmful ideas” rather than dangerous individuals. The internalisation of GWOT logics created the foundations for the Grievance Industrial Complex—a sprawling ecosystem consisting of state aligned actors, Non-governmental organisations, HR departments and digital platforms that manufacture and capitalise on injustice narratives under the guise of “preventing harm” and “standing up to hate.” As a result, a new soft totalitarianism has emerged leading to the enforcement of ideological conformity, censorship and the expansion of institutional powers.

Institutional case studies

The transition of externalised threat management to domestic ideological policing can be observed through institutional case studies. In the United Kingdom the Prevent strategy which primarily focused on jihadist recruitment expanded over time in order to monitor children, individuals & political activists accused of holding “extreme views.” A four-year-old child in Luton was referred under Prevent after allegedly mispronouncing “cucumber” as “cooker bomb,” revealing how even benign speech was pathologized through the logic of radicalisation, whereas in the United States, The Department of Homeland Security’s Targeted Violence and Terrorism Prevention (TVTP) program now funds universities and community organisations to combat ideological threats framed around identity, race, and systemic bias. American University received nearly $650,000 to develop a “gender-inclusive” violence prevention model, asserting that masculine grievances are gateways to extremism. The University of Denver was awarded over $689,000 to focus on rural and white male youth as a potential radicalisation threat.

This particular ideological expansion is not limited to government security agencies. Diversity, equity and inclusion (DEI) frameworks are currently operating as grievance enforcement mechanisms. Universities that once safeguarded intellectual plurality now police language and ideology, labelling counterarguments to issues regarding race, gender identity, or decolonisation as “hate speech”. As a result we now see HR departments actively monitor speech and regulate dissent. Across these institutions Grievance becomes both the justification and the weapon - used not only to secure compliance, but to extend bureaucratic control over thought itself.

Quantitative indicators of ideological capture

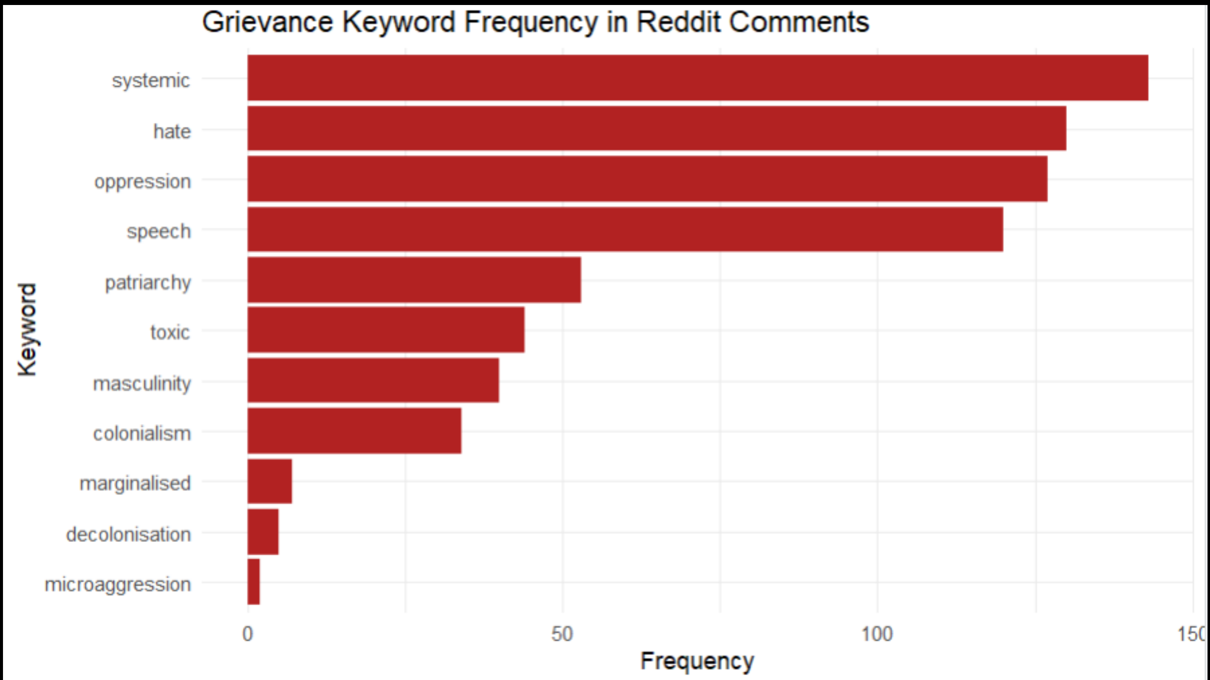

Figure 1. Grievance keyword frequency via Reddit comments

Strategic foresight:

The most prevalent grievance-related terms on Reddit overwhelmingly consist of the following: systemic, hate, oppression and speech, while traditional activist terms such as decolonisation and micro-aggression appear much less frequently.

Findings from this bar chart indicate that grievance-associated terms have shifted from fringe academic vocabulary to mainstream digital language—specifically through emotionally loaded terms such as systemic, hate and oppression. These terms established the foundations for the linguistic architecture of the Grievance Industrial Complex forming a new moral framework influencing corporate compliance, public perception and institutional policy.

Implications for clients:

- Narrative risk exposure: Grievance terms define the moral framing used to attack individuals, firms or institutions online and in person. If an organisation or individual is accused of using these terms the burden of proof is irrelevant as perception becomes reality.
- Internal ideological capture: Unaware of the ideological baggage that grievance terms carry, HR policies, DEI training, and communications teams may recklessly adopt these terms and as a consequence when left unchecked, grievance-based terms cement their way into institutional decision-making.
- Speech censorship dynamics: The rise of terms such as “hate” and “oppression” suggest a growing push to redefine dissent as “harm”. This means that individuals and organisations could face pressure to silence legitimate perspectives under the guise of safety.

- Monitoring priority: Sentiment analysis must be conducted on grievance vocabulary, staffing social media monitoring and crisis communication strategies in order to anticipate and deter reputational flashpoints before escalating.

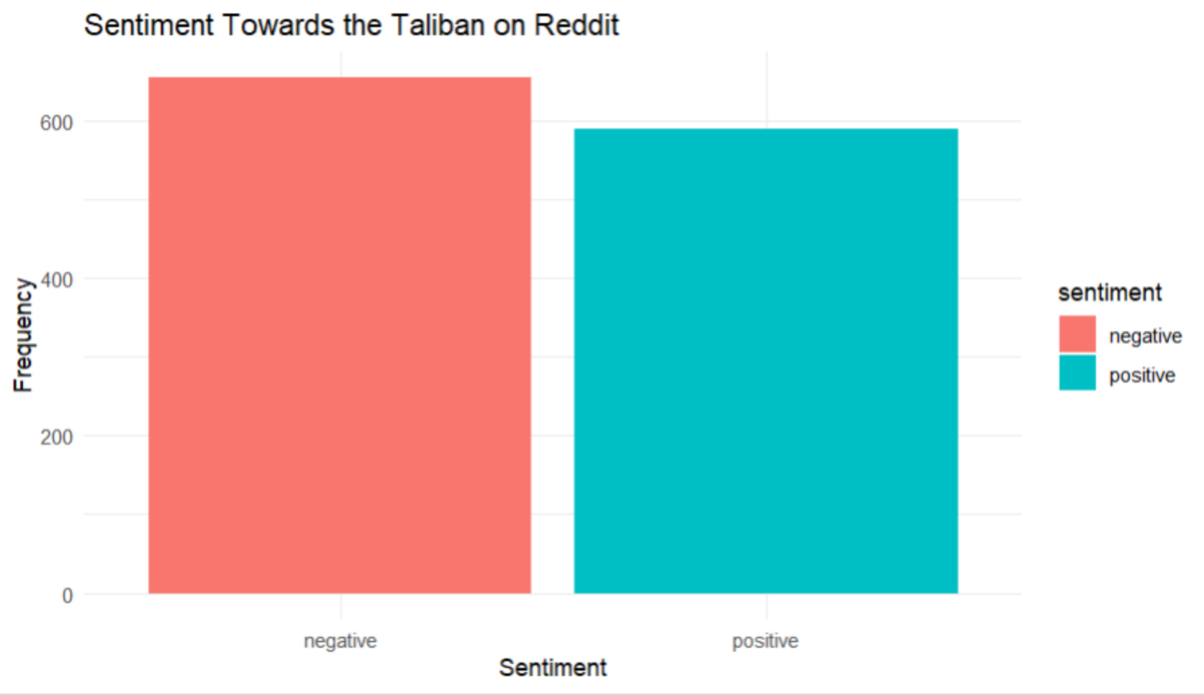

Figure 2. bar chart displaying sentiment towards the Taliban (reddit).

Strategic foresight:

The Taliban are an Islamic terrorist group with a harsh reputation for brute ideological convictions. Positive sentiment toward the Taliban is alarmingly high compared to negative sentiment. The narrowing gap between negative and positive sentiment towards the Taliban reflects a deeper narrative realignment in Western discourse. This signifies the corrosion of moral clarity in public opinion where organisations or individuals who were historically framed as threats are increasingly being perceived as victims due to ideological inversions.

Implications for clients:

- Digital brand risk: If grievance narratives dominate online platforms, public backlash may emerge when organisations condemn certain groups.
- Internal HR volatility: Employees who are significantly influenced by grievance-dominated narratives can potentially develop strong anti-western/anti-institutional views which lead to politicised workplace conflicts and compliance breakdowns (failing to adhere to company policies).
- Narrative monitoring: Tools to monitor sentiment shifts toward ideological threats must be effectively implemented to ensure brand safety and internal cohesion.

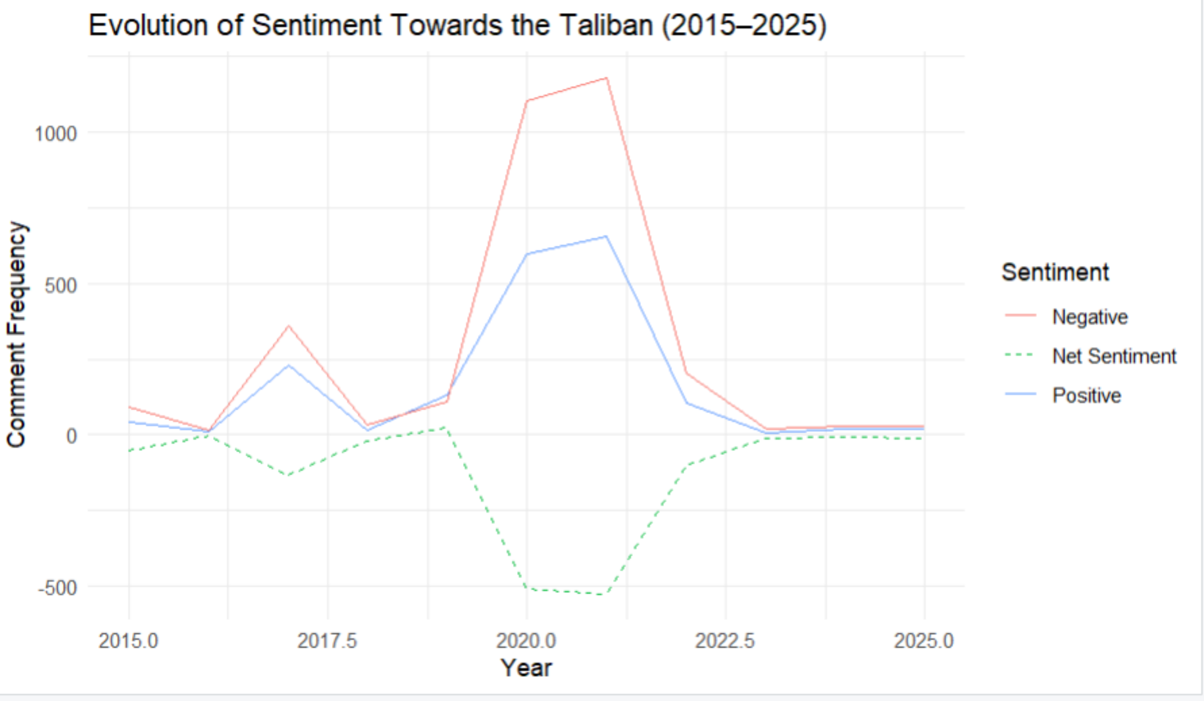

Figure 3. Time series chart displaying evolution of sentiment towards the Taliban (2015-2025).

Strategic foresight:

President Joe Biden's decision to withdraw the U.S. military from Afghanistan in 2021 caused a huge spike in Taliban-related discourse with a steep decline in both positive and negative sentiment thereafter. Net sentiment had recovered by 2023, suggesting either normalisation or apathy. This time series chart shows us how short-lived moral outrage is across digital environments and how mass exposure to ideological narratives breeds desensitisation. Groups once considered untouchable may be rehabilitated in public consciousness through digital fatigue and moral confusion.

Implications for clients

- Reputational inertia: controversial ideologies or figures may not provoke sustained backlash unless narrative architecture (like GIC framing) is challenged head-on.
- Policy risk: Governments and institutions are highly dependent terrorism-based assessments which in this context is becoming irrelevant and outdated resulting in a failure to consider the ideological risks that emerge from digital sentiment decay.
- Strategic communications: Organisations must anticipate that once-taboo positions may enter mainstream discourse so they must be prepared to take principled stances when digital morality falters.

Strategic considerations

Organisations specialising in technology, media, finance, and education must seriously consider that grievance-based narratives are deeply embedded within policy frameworks, regulatory pressures, and cultural institutions. The same ideological architecture initially designed to counter terrorism abroad has re-emerged as a vehicle for managing “hate” speech, compliance and identity politics. Businesses must account for ideological risks such as internal narrative capture, soft censorship via HR policy, ESG-induced reputational exposure, and digital platform bias. Therefore, risk frameworks should expand to include ideological influence mapping, staff exposure monitoring, and counter-narrative resilience. Failure to do so will leave institutions vulnerable not only to reputational risk, but also to internal fragmentation, and regulatory overreach driven by politicised compliance regimes.

Riskscope Disclaimer:
This briefing paper is produced by Riskscope Intelligence for strategic insight and advisory purposes. It does not constitute investment, legal, or security advice. All data, insights, and foresight included in this report are based on publicly available information, open-source intelligence (OSINT), and analytical models developed in-house. While every effort has been made to ensure accuracy, Riskscope assumes no responsibility for decisions made based on this analysis. Redistribution without written consent is strictly prohibited.